UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS

TRABAJO DE GRADUACIÓN PRESENTADO POR:

MUÑOZ SOSA, NORA NATHALY

RODAS LAÍNEZ, GUSTAVO MANUEL

PARA OPTAR AL GRADO DE:

MAESTRO(A) EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

SEPTIEMBRE 2024

CIUDAD UNIVERSITARIA, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

RECTOR: JUAN ROSA QUIMTANILLA, MSc.

VICERRECTORA ACADÉMICA: DRA. EVELYN BEATRIZ FARFÁN

VICERRECTOR ADMINISTRATIVO: ROGER ARMANDO ARIAS ALVARADO

SECRETARIO GENERAL: LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

AUTORIDADES DE LA FACULTAD DE CIENCIAS ECONÓMICAS

DECANA: LICDA. CELINA AMAYA DE CALDERÓN

VICEDECANO: LIC. NIXON ROGELIO HERNÁNDEZ VÁSQUEZ, MSc.

SECRETARIO: LIC. PEDRO JAVIER RIVAS MEJÍA, MSd.

ADMINISTRADOR ACADÉMICO: LIC. EDGAR ANTONIO MEDRANO MELÉNDEZ

COORDINADOR DE MAESTRÍA Y ASESOR(A) DE TRABAJO DE GRADUACIÓN:

COORDINADOR DE MAESTRÍA: LIC. LUIS ALONSO RAMÍREZ AGUILAR, MSc.

ASESOR(A): ING. MÓNICA ROMERO DE ULLOA, MSc.

TRIBUNAL EXAMINADOR DE TRABAJO DE GRADUACIÓN:

PRESIDENTE: LIC. LUIS ALONSO RAMÍREZ AGUILAR, MSc.

SECRETARIA(O): ARQ. MARIO ROBERTO ROSALES PADILLA, MSc.

VOCAL: LIC. KATIA NAVARRETE DE SOSA, MSc.

SEPTIEMBRE 2024

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD (MASIG)

DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS

PRESENTA:

ING. NORA NATHALY MUÑOZ SOSA

ING. GUSTAVO MANUEL RODAS LAÍNEZ

Trabajo de Graduación de Maestría, como requisito para optar al título de:

MAESTRO(A) EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

COORDINADOR DE MAESTRÍA:

LIC. LUIS ALONSO RAMÍREZ AGUILAR, MSc.

ASESOR(A):

ING. MÓNICA ROMERO DE ULLOA, MSc.

SEPTIEMBRE 2024

CIUDAD UNIVERSITARIA, EL SALVADOR, CENTROAMÉRICA

DECLARACIÓN DE AUTORÍA

ING. NORA NATHALY MUÑOZ SOSA

ING. GUSTAVO MANUEL RODAS LAÍNEZ

DECLARAN QUE:

El presente Trabajo de Graduación denominado: "**DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS"** ha sido desarrollado sobre el fundamento de una investigación aplicada, respetando derechos intelectuales; conforme a citas y referencias bibliográficas correspondientes, según normas APA en su versión vigente. Consecuentemente este trabajo de graduación es de la autoría de los maestrantes autores y de propiedad intelectual de la Maestría en Sistemas Integrados de Gestión de Calidad (MASIG) de la Facultad de Ciencias Económicas de la Universidad de El Salvador.

En virtud de esta declaración, los autores graduandos son responsables del contenido de los diferentes marcos de referencia, marco teórico, métodos, técnicas y herramientas utilizadas, resultados de la investigación y la propuesta de diseño del sistema integrado de gestión, como su veracidad y alcance metodológico académico e investigativo aplicado a los Sistemas Integrados de Gestión de Calidad y otros ámbitos relacionados.

Ciudad Universitaria, San Salvador, septiembre de 2024.

Ing. Nora Nathaly Muñoz Sosa **Ing. Gustavo Manuel Rodas Laínez**

APROBACIÓN DE TRABAJO DE GRADUACIÓN

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

FACULTAD DE CIENCIAS ECONÓMICAS

UNIVERSIDAD DE EL SALVADOR

El Tribunal Examinador de la Maestría en Sistemas Integrados de Gestión de Calidad (MASIG), conformado por los distinguidos maestros abajo detallados; ***aprueban*** el presente Trabajo de Graduación denominado:

DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS

Presentado por:

ING. NORA NATHALY MUÑOZ SOSA

ING. GUSTAVO MANUEL RODAS LAÍNEZ

Asesor(a):

ING. MÓNICA ROMERO DE ULLOA, MSc.

Aprobado por Tribunal Examinador MASIG:

LIC. LUIS ALONSO RAMÍREZ AGUILAR, MSc.

Coordinador MASIG – Presidente

ARQ. MARIO ROBERTO ROSALES PADILLA, MSc. Secretaria(o)

LIC. KATIA NAVARRETE DE SOSA, MSc Vocal

Ciudad Universitaria, Septiembre de 2024

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

FACULTAD DE CIENCIAS ECONÓMICAS

UNIVERSIDAD DE EL SALVADOR

CERTIFICACIÓN

En calidad de miembros del Tribunal Examinador **CERTIFICAMOS QUE:** El presente Trabajo de Graduación denominado: **DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS.** Previo a la obtención del grado de

MAESTRA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD; ha sido elaborado por los maestrantes **Ing. Nora Nathaly Muñoz Sosa e Ing. Gustavo Manuel Rodas Laínez,** documento que contiene un proceso riguroso de revisión metodológica, académica y profesional, por tanto, se encuentra apto para su presentación y publicación.

Ciudad Universitaria, San Salvador. Septiembre de 2024.

LIC. LUIS ALONSO RAMÍREZ AGUILAR, MSc.
Coordinador MASIG – Presidente

ARQ. MARIO ROBERTO ROSALES PADILLA, MSc.
Secretaria(o)

LIC. KATIA NAVARRETE DE SOSA, MSc
Vocal

ACUERDO DE RATIFICACIÓN

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS

LUGAR Y FECHA : San Salvador, 07 de octubre de 2024
RAMO : Ministerio de Educación
DEPENDENCIA : Universidad de El Salvador, Facultad de Ciencias Económicas
TIPO DE ACUERDO : RATIFICACIÓN DE ACTA
NUMERO DE ACUERDO: **SEISCIENTOS OCHENTA Y CINCO BIS DE JUNTA DIRECTIVA**

Para su conocimiento y efectos legales consiguientes transcribo acuerdo tomado en Sesión Ordinaria No.35-2024, período 2023/2025, de Junta Directiva de la Facultad de Ciencias Económicas, celebrada el día viernes cuatro de octubre del año dos mil veinticuatro.

PUNTO VI – 6.2 RATIFICACIÓN DE RESULTADOS DEL TRABAJO DE GRADUACIÓN DEL ACTA DE EVALUACIÓN N°7/2024, EGRESADOS MASIG.

Conocida la solicitud de ratificación de resultados del Trabajo de Graduación del Acta de Evaluación N°7/2024 Egresados MASIG, correspondiente al año 2024, presentado por el M.Sc. Luis Alonso Ramírez Aguilar, Coordinador de la Maestría en Sistemas Integrados de Gestión de Calidad (MASIG).

Luego de verificar que el acta contiene los datos pertinentes y con base en los Artículos 35 y 36 literal "e" del Reglamento General de la Ley Orgánica de la UES y Art.48 inciso tres Reglamento General del Sistema de Estudios de Posgrado de la UES.
Junta Directiva por SEIS (6) votos a favor, CERO (0) abstenciones y CERO (0) en contra de los miembros propietarios presentes, ACUERDAN:

Ratificar los resultados del Trabajo de Graduación del Acta de Evaluación N°7/2024, correspondiente al año 2024, de la Maestría en Sistemas Integrados de Gestión de Calidad, según detalle:

ACTA N° 7/2024

FECHA DE EXAMEN	NOMBRES DE LOS GRADUANDOS	CARNE	TEMA DE TRABAJO DE GRADUACION	NOTA GENERAL	TRIBUNAL EXAMINADOR
25/09/2024	NORA NATHALY MUÑOZ SOSA GUSTAVO MANUEL RODAS LAÍNEZ	MS21032 RL21027	"DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS"	7.60 7.66	**PRESIDENTE** LIC. LUIS ALONSO RAMÍREZ AGUILAR, M.Sc. **SECRETARIO** ARQ. MARIO ROBERTO ROSALES PADILLA, M.Sc. **VOCAL** LICDA. KATIA NAVARRETE DE SOSA, M.Sc.

Lo que comunico a usted para su conocimiento y efectos legales consiguientes.
Atentamente,
"HACIA LA LIBERTAD POR LA CULTURA"

FACULTAD DE CIENCIAS ECONÓMICAS
SECRETARÍA
SAN SALVADOR - EL SALVADOR, C.A. -

MsD. PEDRO JAVIER RIVAS MEJÍA
SECRETARIO FCE-UES
CC: DECANATO, VICEDECANATO, ADMINISTRACIÓN ACADÉMICA DE LA FACULTAD DE CC.EE., COORDINADOR MASIG, ARCHIVO.

DEDICATORIA / RECONOCIMIENTO

Quiero comenzar expresando mi profundo agradecimiento a Dios, pues sin su guía y fortaleza, alcanzar este importante logro no habría sido posible. También deseo agradecer de todo corazón a mi familia por su inquebrantable apoyo y su infinita paciencia a lo largo de este camino.

No puedo dejar de reconocer el invaluable aporte de mis maestros, quienes generosamente compartieron su sabiduría y nos impulsaron a superarnos constantemente en este viaje que hoy llega a su conclusión con este trabajo de graduación. También a mi compañero de tesis, por su colaboración, paciencia y comprensión.

Nathaly Muñoz

Quiero expresar mi profundo agradecimiento a Dios por haberme guiado y fortalecido durante este arduo camino hacia la culminación de mi tesis de maestría. También doy gracias a la vida por las oportunidades y lecciones que me ha brindado a lo largo de este viaje académico. Agradezco infinitamente a mi madre por su inquebrantable apoyo, amor incondicional y sacrificio, que han sido el pilar fundamental en mi vida y en la consecución de este logro. Asimismo, a mi compañera de tesis, agradezco su colaboración, comprensión y amistad.

Sin el respaldo de Dios, este éxito no habría sido posible.

Gustavo Rodas

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE APÉNDICES CAPÍTULARES

ÍNDICE DE ANEXOS CAPÍTULARES

CAPÍTULO I. MARCO REFERENCIAL

SIGLAS Y ACRONIMOS

Sigla o Acrónimo	Significado o equivalencia
APA	American Phycological Association
BCP	Plan de continuidad del negocio
DLP	Prevención de Fuga de Datos
IEC	Comisión Electrotécnica Internacional (International Electrotechnical Commission)
ISO	Organismo Internacional de Normalización (International Organization for Standardization)
NDA	Acuerdo de confidencialidad o no divulgación
MASIG	Maestría en Sistemas Integrados de Gestión de Calidad
PI	Propiedad intelectual
PPI	Privacidad y protección identificable de una persona
PUA	Política de uso aceptable
SIG	Sistema Integrado de Gestión
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información
TI	Tecnología de la información
TIC	Tecnologías de la Información y las Comunicaciones
VPN	Red Privada Virtual
UNE	Una Norma Española
URL	Localizador uniforme de recursos

RESUMEN EJECUTIVO

El mercado de seguros fluctúa constantemente y se vuelve cada vez más complejo, la necesidad de los consumidores para adquirir seguros aumenta; además, las herramientas tecnológicas se perfeccionan y se facilita el ingreso a nuevos mercados por medio de canales de comercialización digitales. Los requisitos y las tendencias de los consumidores cambian constantemente debido a la globalización y el auge del desarrollo de las tecnologías de la información y las comunicaciones, por lo cual las organizaciones se ven obligadas a adaptarse a estrategias que fortalezcan la calidad de sus servicios y las garantías de seguridad de la información de los millones de datos de clientes y otras partes interesadas.

Aseguradora ABANK, una institución financiera salvadoreña especializada en seguros de vida y gastos médicos, fue constituida legalmente en 2020. Como una organización de reciente creación, con un nuevo capital de inversión y una renovada filosofía de negocio, ABANK enfrenta el desafío de superar un legado comercial desfavorable heredado de su predecesora, Aseguradora Vivir. Hasta la fecha, la empresa no ha logrado implementar estrategias efectivas que garanticen a sus asegurados y demás partes interesadas servicios de calidad que satisfagan sus necesidades y expectativas, así como mecanismos robustos de seguridad para protegerse contra ciberataques y otros riesgos asociados con las tecnologías de la información.

Por consiguiente, el presente trabajo de graduación se plantea desde el enfoque del Diseño de un Sistema Integrado de Gestión (SIG), basado en normativas ISO 9001:2015, Sistemas de Gestión de Calidad (SGC) e ISO/IEC 27001:2022, Sistema de Gestión de la Seguridad de la Información (SGSI); por lo tanto, será la herramienta para determinar las acciones necesarias que la organización podría optar para darle solución a la problemática.

A partir del análisis de la situación actual de la organización en cuanto a calidad y seguridad de la información, junto con la identificación de las necesidades de los clientes y partes interesadas, se plantearon conclusiones sobre el estudio. Basándose en la norma de referencia, se establecieron los controles necesarios para la seguridad de la información, considerando su contexto y necesidades específicas. Finalmente, se llevó a cabo la identificación y diseño de la información documentada relacionada con los requisitos de ambas normativas.

INTRODUCCIÓN

El diseño de un Sistema Integrado de Gestión que se presenta a continuación subraya la importancia de la calidad y seguridad de la información en Aseguradora ABANK, desarrollado en su única sede en Urbanización Madre Selva 3, Antiguo Cuscatlán. Esta investigación es crucial, ya que establece las bases para garantizar que la organización cumpla con los estándares más exigentes. Por ello, se ha considerado esencial, dentro del proceso investigativo, formular una propuesta basada en la norma ISO/IEC 27001:2022 para la seguridad de la información y en la ISO 9001:2015 para el Sistema de Gestión de Calidad.

Capítulo I: Marco Referencial, este capítulo se inicia con un diagnóstico inicial que define la problemática que enfrenta Aseguradora ABANK. Se presenta el planteamiento del problema, se exponen los objetivos del sistema de gestión, se establece el alcance de la investigación y se justifica la imperiosa necesidad de la implementación de un sistema de gestión integrado.

En el siguiente **Capítulo II:** Marco Teórico En esta sección, se recopila y analiza información de fuentes académicas relacionadas con los sistemas de gestión, en particular, con la calidad y seguridad de la información. Se definen los fundamentos teóricos necesarios para llevar a cabo la investigación. Se describen los requisitos de la norma ISO 9001:2015 para la gestión de la calidad y los requisitos de la norma ISO/IEC 27001:2022, seguridad de la información.

El **Capítulo III**: Marco Metodológico y Resultados, detalla el diseño metodológico empleado para responder a las preguntas e hipótesis de la investigación, asegurando su relevancia para solucionar el problema identificado. Se describe la población y muestra representativa, junto con los métodos, técnicas e instrumentos adecuados para la recopilación de datos. Los resultados se presentan en diagramas proporcionando respuestas claras a las variables estudiadas.

La propuesta del trabajo de investigación se presenta en el **Capítulo IV**: Diseño de un Sistema Integrado de Gestión, como un proyecto factible y se apoya de documentos para el desarrollo del Sistema Integrado de Gestión (SIG), tales como un Manual del SIG, manual de procedimientos, manual de interpretación e implementación de controles de seguridad de la información; estos documentos resultan de beneficio para el entendimiento y estructuración adecuada de un modelo de operación acorde a principios de calidad y en fortalecimiento de la seguridad de la información de la organización.

Por último, el **Capítulo V:** Conclusiones y Recomendaciones, presentan las conclusiones obtenidas a partir del estudio realizado, destacando los argumentos fundamentales relacionados con la problemática. Asimismo, se ofrecen recomendaciones que reflejan la esencia de la propuesta, aportando estrategias y proyecciones que tienen como objetivo reforzar la calidad y seguridad de la información de Aseguradora ABANK.

CAPÍTULO I. MARCO REFERENCIAL

En este marco referencial, se abordaron aspectos vitales que guiaron el desarrollo de la investigación. En primer lugar, se describió al sujeto de estudio y su contexto, también se detalló la situación problemática de la organización, destacando los desafíos y oportunidades. Posteriormente, se realizó la formulación y sistematización del problema. Asimismo, se abordaron los límites y alcances que permiten enfocar el estudio de manera efectiva. Además, se plasmaron los objetivos que se persiguen, delineando las metas que se pretenden alcanzar y los resultados que se esperan obtener; por último, se consideró la justificación de la labor investigativa, las hipótesis y los fundamentos éticos que componen la investigación.

1.1 Descripción de sujeto de estudio

Aseguradora ABANK, S.A. Seguros de Personas, es el título legal con el cual se oficializó la compañía en el año 2020, con la autorización de la Superintendencia del Sistema Financiero[1] para su operación en el rubro de los seguros de vida y gastos médicos. Es así como la sociedad Perinversiones, S.A. de C.V. adquirió la totalidad de las acciones de la empresa, antes Aseguradora Vivir[2] (empresa de origen dominicano), a partir del año 2020 pasó a ser constituida por capital 100% salvadoreño (Aseguradora ABANK, 2020, pág. 3).

Aseguradora ABANK, S.A. Seguros de Personas, de ahora en adelante Aseguradora ABANK, es una empresa innovadora y con amplia experiencia en el aseguramiento de salud y vida, ofreciendo ventajas y valores agregados a los asegurados. Su filosofía es adoptar constantemente mejoras tecnológicas para brindar un servicio más eficiente con productos hechos a la medida de sus clientes. La aseguradora establece su visión y misión:

Visión:

"*Ser la primera Insurtech*[3] *de última generación en El Salvador".*

---

[1] La Superintendencia tiene la responsabilidad de supervisar la actividad individual y consolidada de las instituciones integrantes del sistema financiero en El Salvador: bancos, aseguradoras, entre otros.

[2] Aseguradora Vivir existió en el mercado de seguros da inicio en el año 2011, manteniéndose a lo largo de 9 años.

3 "La palabra Insurtech proviene de la combinación de dos palabras en inglés: insurance y technology, tecnología. Se trata de la combinación de las más nuevas tecnologías en el sector de los seguros." (Estruga, 2021)

Misión:

"Elevar la calidad de vida de nuestros asegurados, brindando coberturas con productos innovadores y a la medida, a través de una red de atención médica de alta calidad y de tecnología para brindar un servicio ágil y confiable".

El conglomerado ABANK, compuesto por Banco ABANK, Aseguradora ABANK y la Sociedad de Ahorro y Crédito Constelación, comparte una filosofía organizacional común basada en los valores de "Experiencia", que se despliegan en los pilares de Liderazgo, Aprendizaje y Comunicación. Sin embargo, aunque comparten esta visión estratégica, cada entidad opera de manera independiente en términos administrativos y financieros. Esto significa que cada empresa dentro del conglomerado tiene su propia estructura de gestión, toma de decisiones y políticas financieras, para mayor referencia ver *Figura 1*

Figura 1. Valores de Aseguradora ABANK

Fuente: (Aseguradora ABANK, 2022)

El volumen de operaciones varía según el sector, con el Banco ABANK concentrando la mayor parte del negocio financiero, mientras que la Aseguradora ABANK se especializa en productos de seguros, y la Sociedad de Ahorro y Crédito Constelación atiende a un nicho específico de clientes enfocados en ahorro y crédito.

La distribución de los empleados también refleja esta independencia, ya que cada empresa maneja su propia nómina y estructura de recursos humanos, aunque existen iniciativas conjuntas para el desarrollo de talento y formación continua. En cuanto a la clientela, aunque existen sinergias y productos integrados entre las entidades, cada empresa mantiene su base de clientes de forma autónoma, alineando sus estrategias comerciales con las necesidades específicas de su mercado.

La aseguradora, como parte del conglomerado financiero, opera bajo un estricto cumplimiento de las Normas de la Superintendencia del Sistema Financiero (SSF) y demás regulaciones aplicables al sector. A la fecha la organización se encuentra en el desarrollo de políticas y documentaciones que respalden la operatividad a través de mecanismos de cumplimiento normativo, tanto para temáticas, técnicas, operacionales, financieras, como hasta de seguridad de la información en la institución de seguros.

Aseguradora ABANK comercializa seguros de gastos médicos tanto para grupos como para individuos. Estos seguros cubren aspectos de salud para quienes los contratan, ya sean empresas u organizaciones (personas jurídicas) o consumidores individuales (personas naturales). Los asegurados pueden utilizar estos seguros al visitar clínicas u hospitales privados, al comprar productos médicos en farmacias o en casos de emergencia debido a accidentes u otros eventos que afecten la salud y estén dentro de la cobertura del seguro.

De igual manera, la aseguradora ofrece seguros de vida para empresas. Estos seguros se destacan por proporcionar a los familiares del asegurado fallecido una suma de dinero acordada en contrato, además de cubrir los gastos funerarios relacionados con el proceso. Los diferentes tipos de seguros ofrecidos por la aseguradora se detallan en *Tabla 1:*

Tabla 1. Seguros comercializados por Aseguradora ABANK

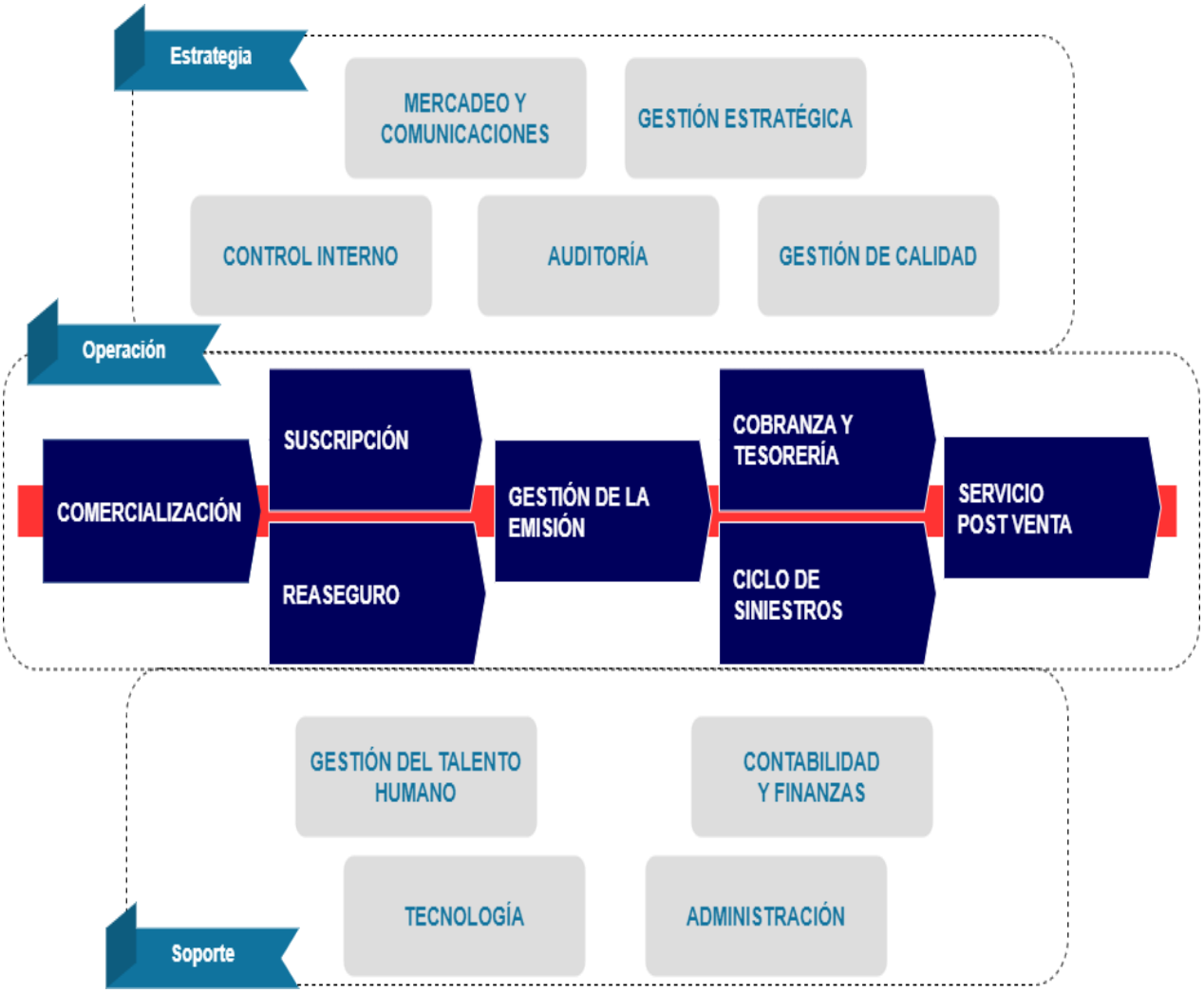
Oferta de seguros – Aseguradora ABANK			
Seguros de gastos médicos (salud)			
Planes	Nombre de producto	Mercado al que está orientado	Límites de cobertura
Seguros de gastos médicos	Plan Superior	Personas naturales/ Personas jurídicas	Hasta $5,000
	Plan Royal	Personas naturales/ Personas jurídicas	Hasta $10,000
	Plan Max	Personas naturales/ Personas jurídicas	Hasta $20,000
Salud internacional	Programa buen viaje	Personas naturales	Hasta $2,000,000
Seguros de vida			
Planes	Nombre de producto	Mercado al que está orientado	Características
Seguros de personas	Vida colectiva	Personas jurídicas	Cobertura que pagará a los beneficiarios de la persona asegurada la suma contratada, por fallecimiento.
	Accidentes personales	Personas jurídicas	Cobertura ante cualquier accidente a los empleados o personas aseguradas.
	Vida crédito e hipotecario	Personas jurídicas	Asegura la vida de los deudores de una entidad empresa, garantizando el pago de la deuda pendiente, por fallecimiento, a consecuencia de enfermedad o accidente.

Fuente: (Aseguradora ABANK, 2022)

En cuanto al tamaño de la organización, según MIPYMES[4] se clasifica como "Mediana Empresa", ya que la cantidad total de trabajadores de la compañía es equivalente a 71 personas hasta el año 2023 en que se desarrolla la investigación.

En la actualidad se poseen 16 procesos en la organización, identificados por medio de un mapeo que refleja tanto los procesos vinculados a las estrategias del negocio, procesos de operación y procesos de soporte, a continuación, se muestra en Figura *2*.

Figura 2. Mapa de procesos de Aseguradora ABANK



Fuente: Adaptado de Intranet de Aseguradora ABANK

[4] La Micro, Pequeña y Mediana Empresa (MIPYMES) es la clasificación que reciben las empresas por parte del gobierno salvadoreño (Ministerio de Economía) a partir de un análisis de la cantidad de trabajadores de una empresa y los ingresos brutos anuales.

Se establece una relación entre las diferentes áreas de la organización y los procesos que fueron considerados en la investigación, a continuación, en Tabla 2.

Tabla 2. Áreas funcionales y procesos en la investigación

Áreas funcionales de la compañía y sus procesos		
Dirección/ Gerencia	Descripción del área	Procesos que aplican para la investigación
Dirección comercial	**Iniciales:** ejecución de las ventas de seguros de la compañía, orientado a nuevos Clientes. **Renovaciones:** gestión de renovaciones de contratos (pólizas) de Clientes ya vinculados al negocio. **Bancaseguros:** actividades relacionadas a los procesos que vinculan la comercialización de seguros de la compañía por medio de instituciones bancarias. **Mercadeo y comunicaciones**: realizar la administración de las redes sociales de la organización, así como la planificación y ejecución de actividades publicitarias y manejo de la marca a nivel comercial.	Comercialización. Mercadeo y comunicaciones.
Dirección técnica	**Reclamos:** análisis y liquidación de siniestros[5]. **Suscripción:** Análisis de las condiciones contractuales de las pólizas de seguros en contraste a la situación médica de los clientes. **Auditoría médica:** garantizar la calidad, la eficiencia y el cumplimiento normativo en los servicios de atención médica. A través del control de calidad, la eficiencia en el uso de recursos, el cumplimiento normativo, la detección y prevención de fraudes. **Reaseguro:** gestionar y transferir parte del riesgo asumido por la compañía a otras entidades especializadas en reaseguro[6]. **Portafolio de productos:** administración de los productos (seguros) que ofrece la aseguradora, de igual forma aplica el diseño y desarrollo de estos.	Suscripción. Ciclo de siniestros. Reaseguro. Gestión estratégica.
Dirección financiera administrativa	**Operaciones:** Creación y registro de la póliza de seguro en el sistema informático de la organización. **Archivo:** Gestión para el resguardo de todos los expedientes de asegurados y demás registros de la operación diaria del negocio. **Administración:** Gestión de la papelería, mensajería, infraestructura física. **Contabilidad:** registro y control de transacciones, la elaboración de estados financieros, el cumplimiento normativo, el establecimiento	Gestión de la emisión. Administración. Contabilidad y finanzas. Cobranza y tesorería.

Continúa Tabla 2 en la siguiente página →

[5] En la lenguaje de los seguros, un reclamo es una solicitud que hace un asegurado a la compañía de seguros para recibir una compensación por un siniestro o pérdida cubierta por su póliza de seguros; desde el punto de vista de las normativas ISO 9001:2015 e ISO/IEC 27001:2022, un reclamo se entiende como una inconformidad por parte del cliente, pero en la presente propuesta investigativa las inconformidades se contemplarán no desde la perspectiva de los reclamos, sino que de las "quejas", las cuales se atienden en la aseguradora en el área de Atención al Cliente, parte del proceso de Servicio posventa.

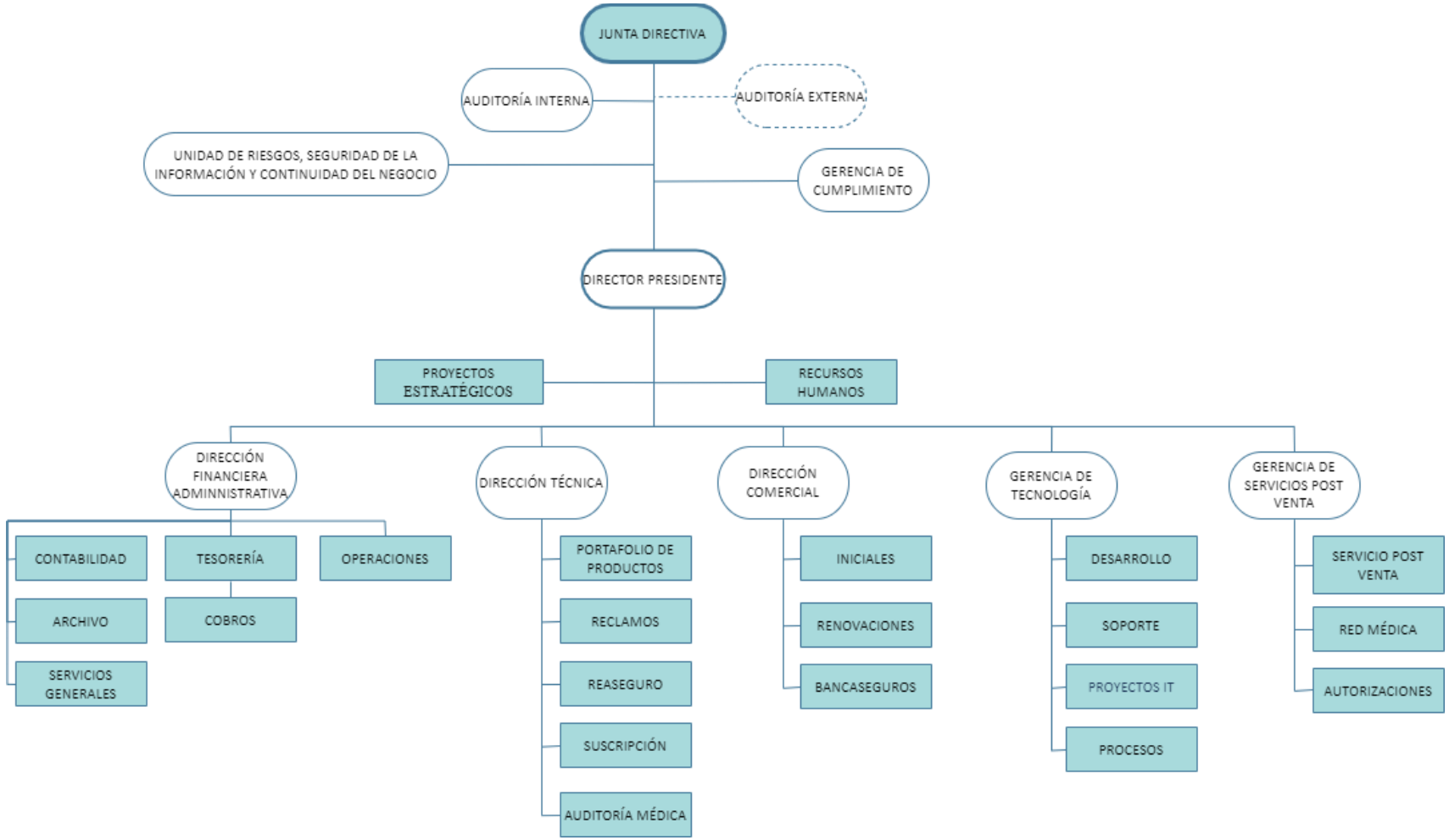
[6] El reaseguro es un mecanismo mediante el cual una aseguradora cede una parte de sus riesgos a otra entidad aseguradora, conocida como reaseguradora, a cambio de una prima.

Áreas funcionales de la compañía y sus procesos		
Dirección/ Gerencia	Descripción del área	Procesos que aplican para la investigación
	de controles internos, y la provisión de información relevante para la toma de decisiones financieras y estratégicas. **Cobros:** realizar una adecuada gestión de la cobranza de primas de seguros. **Tesorería:** administración y aplicación de pagos a proveedores administrativos y médicos, así como también el pago de reclamos presentados por los asegurados.	
Gerencia de Servicio Post venta	**Atención al cliente:** seguimiento y atención a los asegurados vinculados a la organización **Red médica:** Atención a proveedores médicos (hospitales, farmacias, laboratorios). **Autorizaciones:** aprobaciones de acciones de los asegurados en cuanto al uso de su póliza de seguro de gastos médicos (medicamentos, estudios especiales, ingresos hospitalarios, etc.).	Servicio posventa.
Auditoría interna	**Auditoría interna:** realización de auditorías internas conforme a los requisitos que los organismos reguladores y leyes vigentes apliquen al negocio.	Auditoría
Unidad de riesgos, seguridad de la información y continuidad del negocio	**Riesgos:** Administración de los riesgos organizacionales (financieros y operativos) a partir de los requerimientos de los entes reguladores y la normativa legal vigente. **Coordinación de la Seguridad de la información y continuidad del negocio:** planeación y aplicación de acciones relacionadas a la protección de la organización y sus asegurados en cuanto a temas relacionados con seguridad de la información y continuidad del negocio de acuerdo con las normativas legales vigentes.	Control interno
Gerencia de cumplimiento	Garantizar la organización cumpla con las leyes y regulaciones aplicables en el rubro.	Control interno
Gerencia de tecnología	**Desarrollo:** Gestión del desarrollo de software especializado para apoyo a las actividades de la organización. **Soporte:** Atención al cliente interno en temas relacionados a las tecnologías de la información y las comunicaciones. **Proyectos IT:** Planificación y seguimiento de proyectos relacionados a las tecnologías de la aseguradora. **Procesos:** Administración del inventario de procesos de la organización y aplicación de la gestión por procesos.	Tecnología. Gestión de Calidad.
Recursos humanos	Gestión del talento humano, a partir de la atención a solicitudes de colaboradores de la compañía, pago de planillas, reclutamiento y selección de personal.	Gestión del talento humano.
Proyectos estratégicos	Planificación de estrategias de negocio para la organización.	Gestión estratégica.
Dirección Presidencia	Supervisar la gestión general de la empresa y garantizar que se alcancen los objetivos estratégicos de la organización.	Gestión estratégica.

Fuente: Elaboración propia

A nivel de estructura organizacional el personal de la aseguradora se encuentra distribuido de la siguiente manera, según organigrama (*Figura 3):*

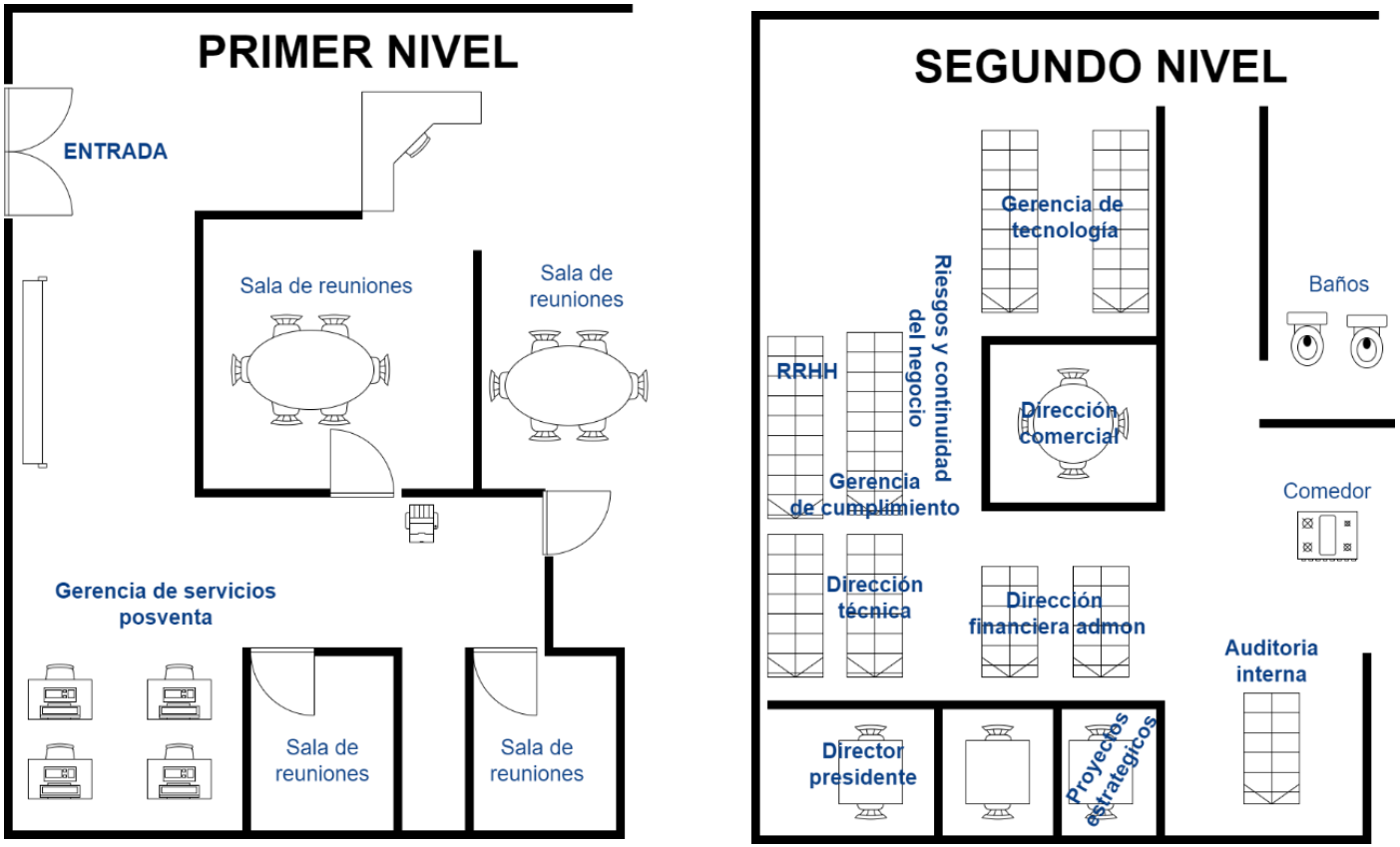
Figura 3. Organigrama Aseguradora ABANK



Fuente: Adaptado de Intranet de Aseguradora ABANK (La cantidad de empleados por área se detalla en la *Tabla 9*)

En las instalaciones de la sede central y única ubicación de Aseguradora ABANK, localizada en Antiguo Cuscatlán, departamento de La Libertad, las áreas funcionales representadas en el organigrama anterior se distribuyen a nivel de croquis de la siguiente forma (Ver Figura *4*):

Figura 4. Distribución de oficinas de Aseguradora ABANK



Fuente: Elaboración propia

En las instalaciones de la aseguradora, actualmente no se poseen servicios subcontratados directamente. Sin embargo, en el área de desarrollo de software, sí se requiere subcontratación, la cual se gestiona de forma virtual bajo la supervisión de la Gerencia de Tecnología. Es importante destacar que la empresa utiliza una combinación de sistemas automatizados y manuales para la gestión de sus procesos de negocio, tal es el caso del sistema core de aseguradora donde se registra y gestionan las pólizas de seguros, como sistemas periféricos vinculados a los análisis de reclamos.

Aunque algunos procesos clave han sido automatizados, como la gestión de reclamos y la administración de pólizas, aún existen áreas donde la automatización no se ha implementado por completo. Los proyectos de desarrollo y mantenimiento de software, esenciales para la operación diaria, son liderados por la Gerencia de Tecnología y en ocasiones requieren la participación de proveedores externos para asegurar la calidad y continuidad del servicio.

1.2 Planteamiento del problema

"El planteamiento del problema es el centro, el corazón de la investigación" (Sampieri, 2018, pág. 38). Plantear el problema es importante para la exploración inicial del sujeto de estudio, establecer el objetivo de la investigación, así como la declaración de los supuestos que fueron el punto de partida, de forma planificada, para la labor investigativa.

Para enfocar la investigación de manera efectiva, se han formulado preguntas orientativas que abordan los problemas principales detectados. Estas preguntas guían el análisis y la búsqueda de soluciones. A continuación, se presentan dichas preguntas:

- ¿Cómo mejorar la gestión de procesos organizacionales para implementar eficientemente las iniciativas estratégicas?
- ¿Qué procedimientos son necesarios para el control de la información documentada y cómo implementarlos?
- ¿Cómo entender mejor las necesidades de los clientes y partes interesadas?
- ¿Qué estrategias fortalecerán la comunicación y el trabajo en equipo?
- ¿Cómo puede la alta dirección mejorar su compromiso y liderazgo en las iniciativas estratégicas?

- ¿Qué cambios son necesarios para corregir errores en operaciones y servicios al cliente?
- ¿Qué medidas se deben tomar para abordar las vulnerabilidades en la seguridad de la información?

1.2.1 Antecedentes y contexto de situación problemática

La organización se encuentra en una etapa crítica de transición en su filosofía de negocio, impulsada por la visión de los nuevos accionistas, quienes buscan redefinir el enfoque de la empresa hacia la satisfacción plena de las necesidades y expectativas de sus clientes. En este contexto, se pretende ofrecer productos de seguros que no solo cumplan con los más altos estándares de calidad, sino que también garanticen la seguridad de la información, un aspecto cada vez más crucial en el entorno actual. Este cambio de rumbo estratégico no solo apunta a mejorar la calidad de los productos, sino también a fortalecer la confianza de los clientes a través de la transparencia y la protección de sus datos sensibles.

Durante esta transición, la organización ha identificado la necesidad de implementar una serie de iniciativas clave relacionadas con la gestión por procesos y la adopción de herramientas tecnológicas avanzadas para mejorar la atención al cliente. Esto incluye actualizaciones significativas a sus sistemas informáticos, con el fin de cumplir con los requerimientos legales sobre seguridad de la información, así como la integración de proyectos de digitalización que permitan optimizar las operaciones y mejorar la eficiencia general. Sin embargo, estos esfuerzos han enfrentado dificultades considerables, principalmente debido a la falta de una metodología adecuada para el desarrollo de iniciativas estratégicas.

La ausencia de un liderazgo claro y comprometido por parte de la alta dirección, junto con la falta de una comprensión integral de la importancia de estos cambios por parte del personal, ha obstaculizado la implementación efectiva de estas mejoras.

Entre los problemas específicos que se han detectado, destaca una inadecuada gestión de los procesos organizacionales, lo que ha llevado a una falta de procedimientos efectivos para el control de la información documentada. Esta situación ha generado un impacto negativo en la satisfacción de los clientes, ya que no se han comprendido ni integrado adecuadamente sus necesidades y expectativas dentro de las estrategias corporativas.

La desconexión entre la visión estratégica de la empresa y la realidad operativa ha exacerbado la insatisfacción de los clientes, poniendo en riesgo la lealtad y la reputación de la organización.

Existen también debilidades en la comunicación y el trabajo en equipo dentro de la aseguradora, y falta de compromiso y liderazgo de un importante número de gerentes y directores respecto al desarrollo de iniciativas estratégicas y mejores prácticas operacionales. En cuanto a las operaciones y servicios al cliente, se han identificado problemas como contratos de seguros entregados con errores, solicitudes de información documentada burocrática, tiempos de respuesta para la emisión de seguros tardíos, pagos a proveedores fuera de tiempo, respuestas a autorizaciones médicas inadecuadas, análisis de suscripción de pólizas de seguros incorrectas, pérdidas de negocios en licitaciones y falta de seguimiento a los proyectos estratégicos debido a la ausencia de liderazgo por parte de la alta dirección.

En relación a la seguridad de la información, la aseguradora trabaja con alrededor de 40,000 asegurados que incluyen miles de datos confidenciales, además de datos de partes interesadas (proveedores, intermediarios, entes reguladores, entre otros) y de la misma organización. Esta información es administrada a través de servicios tecnológicos alojados en bases de datos físicas y en la nube, y la organización se encuentra en el desarrollo de canales digitales de venta de seguros, a pesar de no haber sufrido de momento un flagelo de este tipo, el desarrollar e involucrar cada vez más tecnologías tiene como consecuencia el aumenta los riesgos relacionados a las vulnerabilidades de la seguridad de la información.

Los problemas específicos de seguridad de la información incluyen la ausencia de controles para la transferencia de información de un dispositivo a otro, la falta de políticas para la seguridad de la propiedad intelectual, la insuficiencia de controles para la seguridad de la información en cuanto al trabajo remoto y la falta de control eficaz para el acceso a las instalaciones con información crítica. Estos problemas afectan significativamente el desarrollo del negocio y la percepción de la aseguradora tanto por parte de los clientes internos como externos.

1.2.2 Definición (formulación) del problema

De acuerdo con la problemática planteada y considerando los antecedentes descritos en el apartado anterior se estableció la siguiente interrogante:

¿De qué manera se puede llevar a cabo la sistematización de los procesos para mejorar aspectos de calidad y seguridad de la información en Aseguradora ABANK?

Una vez se realizó la definición del problema en cuestión, fue necesario profundizar en el análisis de las causas subyacentes y los efectos resultantes. Para lograr esto, se lleva a cabo una sesión de lluvia de ideas en la que se exploran diferentes perspectivas. Estas ideas se plasmaron en un árbol de problemas, una herramienta visual que permite desarrollar un modelo estructurado que explica los efectos y las causas de la problemática principal.

El árbol de problemas es una esquematización gráfica que se puede definir como: "es una herramienta que consiste en desarrollar ideas creativas para identificar las posibles causas del conflicto, generando de forma organizada un modelo que explique las razones y consecuencias del problema" (Hernández-Hernández & Garnica-González, 2015, pág. 40).

1.2.3 Sistematización (problematización) del problema

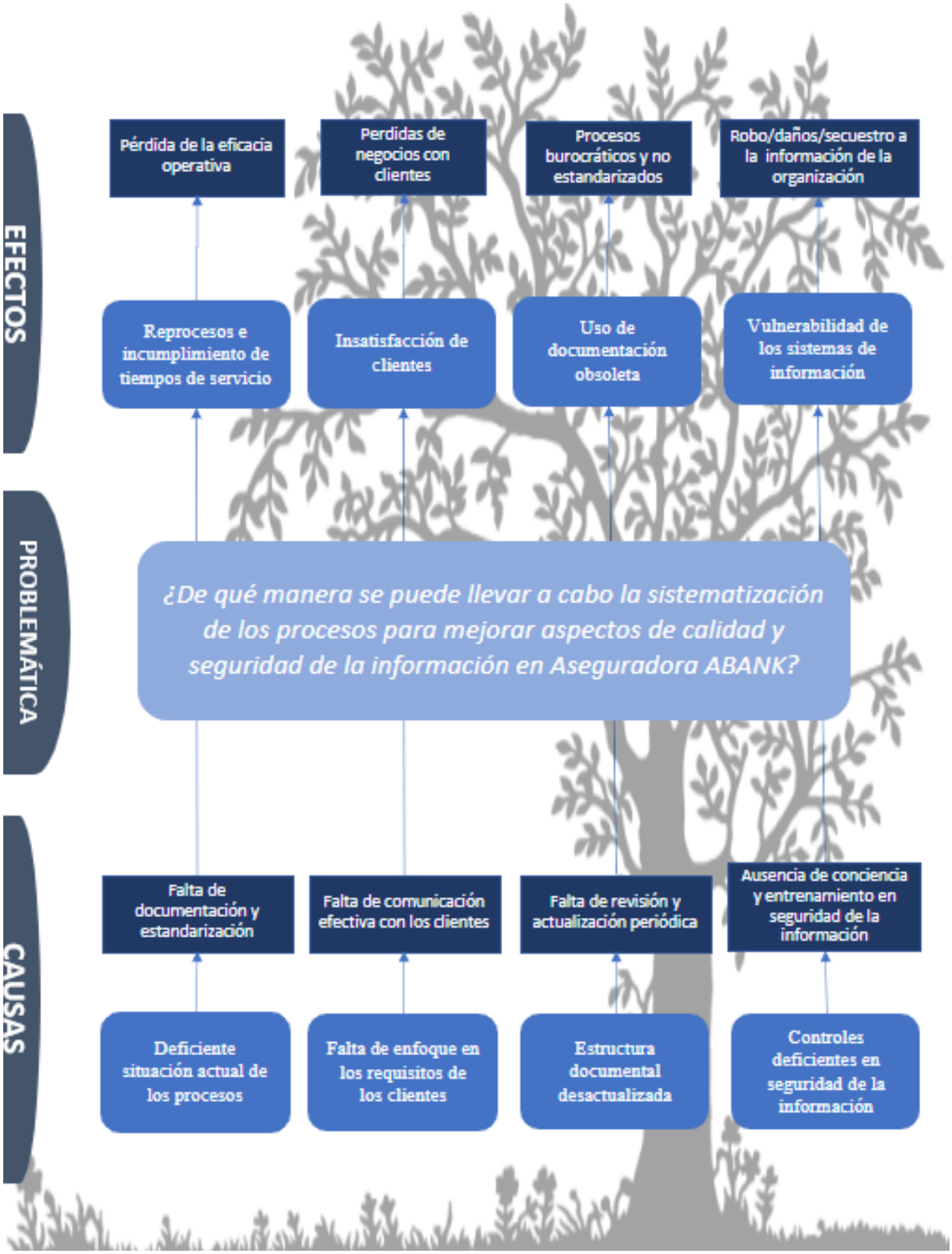
La sistematización del problema en la investigación es de vital importancia, ya que proporciona un enfoque claro para abordar cualquier estudio.

A partir del establecimiento de la declaración general de la situación problemática, se desglosan cuatro preguntas particulares:

1. ¿En qué estado se encuentran los procesos de Aseguradora ABANK en relación con la calidad de sus servicios?
2. ¿De qué manera se identifican las necesidades y expectativas de los clientes de la organización?
3. ¿Cuál es la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización?
4. ¿Cuáles son las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información?

Con el objetivo de brindar una visión clara y estructurada de la problemática, se utilizó una herramienta visual conocida como "diagrama de árbol de problemas", (Ver Figura 5).

Figura 5. Árbol de problemas de la investigación



Fuente: Elaboración propia

1.2.4 Matriz diagnóstica de planteamiento del problema

La matriz diagnóstica es una herramienta metodológica donde se describe de manera preliminar la problemática del sujeto de estudio, los síntomas y causas (por qué está ocurriendo), los efectos, el pronóstico (qué sucedería de mantenerse la problemática), el control del pronóstico (alternativas para superar la problemática) formulación y sistematización del problema.

El objetivo de la matriz diagnóstica del planteamiento del problema es obtener una visión más clara y estructurada de los diferentes elementos que intervienen en el problema. Esto facilitó la identificación de las causas fundamentales y ayudó a orientar los esfuerzos para encontrar soluciones efectivas. En el *Apéndice 2 se* presenta la matriz de diagnóstico.

1.3 Delimitación de la investigación

La delimitación establece los límites precisos y definidos de la investigación. Es decir, se define claramente los aspectos que se van a investigar y los que no. El definir claramente las limitaciones investigativas facilitan la recopilación y análisis de datos.

También, sirve para evitar la incorporación de detalles irrelevantes o no relacionados a la investigación. Por lo tanto, en este trabajo se definió una delimitación geográfica y temporal.

1.3.1 Delimitación espacial o geográfica

El alcance geográfico de la investigación se limita a la sede central de la compañía Aseguradora ABANK[7], ubicada en Boulevard Merliot, Urbanización Jardines de la Hacienda, Zona Comercial 5, departamento de La Libertad, municipio de Antiguo Cuscatlán, El Salvador.

Ésta es la única sede de la aseguradora, es aquí donde se encuentra la totalidad de los colaboradores que generan toda la operación diaria de la organización y que aportaron los insumos de información que la presente investigación requería. (Ver *Figura 6*).

[7] A finales del año 2023 pasaría a mudarse al edificio Avante, ubicado en urbanización Madre Selva 3, Calle Llama del Bosque Poniente, pasaje S, Lotes 15 y 17, Antiguo Cuscatlán, El Salvador.

Figura 6. Sede de Aseguradora ABANK

Fuente: Fotografía tomada en octubre 2022 en las instalaciones de Aseguradora ABANK

1.3.2 Delimitación temporal

La delimitación temporal hace referencia al establecimiento de los límites temporales o periodos específicos que se consideraron en la investigación. Para la presente investigación se realizaron actividades de recolección de información y contacto con el sujeto de estudio a partir de septiembre 2022 hasta octubre 2023, periodo en el cual se distribuyó las etapas de concientización, recolección y análisis de datos, uso de la información para la estructuración del diseño del Sistema Integrado de Gestión.

1.4 Justificación

La justificación es una parte fundamental de una investigación, ya que es la sección donde se explica detalladamente el propósito y la relevancia del estudio realizado, esto es importante debido a que a partir de ello se demuestra la importancia y el valor potencial de los resultados investigativos en el mundo real y de acuerdo con el contexto de Aseguradora ABANK.

1.4.1 Justificación práctica

La justificación práctica hace referencia a la fundamentación de una investigación basada en su utilidad y aplicabilidad real en un contexto práctico o profesional. Méndez Álvarez (2020, Pág.104) establece sobre este tipo de investigación que "Las motivaciones prácticas se manifiestan en el interés del investigador por acrecentar sus conocimientos, obtener un título académico o, si es el caso, por contribuir a la solución de problemas concretos que afectan a organizaciones empresariales, públicas o privadas".

El diseño de un Sistema Integrado de Gestión de calidad y seguridad de la información ISO 9001:2015 e ISO/IEC 27001:2022 permitió a la aseguradora identificar acciones específicas para la atención de las problemáticas organizacionales, a partir de 3 ejes:

Mejora de la calidad: La normativa ISO 9001:2015 tiene como objetivo mejorar la calidad de los procesos y servicios de una empresa. Al considerar este aspecto, la empresa puede establecer procedimientos claros, eficientes, eficaces y estandarizados, lo que garantiza un mayor rendimiento en la prestación de servicios de cara a los asegurados y demás partes interesadas.

Aumento de la satisfacción del cliente: La normativa ISO 9001:2015 también se enfoca en la satisfacción del cliente. Considerar esta normativa es de apoyo a las empresas del rubro de seguros para identificar las necesidades y expectativas de los clientes, lo que permitirá brindar un mejor servicio y aumentar su satisfacción.

Protección de datos: La normativa ISO 27001:2022 se enfoca en la gestión de la seguridad de la información. Una empresa de seguros maneja una gran cantidad de datos personales de los clientes, como información financiera y de salud.

El diseño sistematizado de esta normativa garantiza que se establezcan medidas adecuadas para la protección de los datos de los clientes y de la misma aseguradora, reduciendo el riesgo de fraude y pérdida de información confidencial.

1.5 Objetivos

Los objetivos son primordiales para establecer el destino a alcanzar por medio de la investigación, ya que proporcionan una dirección clara y definida, permitiendo enfocar los esfuerzos y recursos de manera eficiente.

Existe una estrecha relación entre la formulación de la problemática y los objetivos ya que definen las propuestas específicas para la resolución del problema del sujeto de estudio. Sampieri (2018, pág. 38) establece “Los objetivos de investigación señalan a lo que se aspira en la investigación y deben expresarse con claridad, son la guía del estudio”.

1.5.1 Objetivo general

El objetivo general en una investigación es la meta principal que se busca alcanzar a través del estudio y análisis del sujeto de estudio, y debe estar enmarcado en el contexto teórico y conceptual de la investigación.

Los objetivos deben establecerse de forma clara, específica, medible y realista al contexto de la organización, por lo que, para la investigación se definió como objetivo general: *Diseñar un Sistema Integrado de Gestión de la calidad ISO 9001:2015, y seguridad de la información ISO/IEC 27001:2022; aplicable en Aseguradora ABANK, S. A. Seguros de personas.*

1.5.2 Objetivos específicos

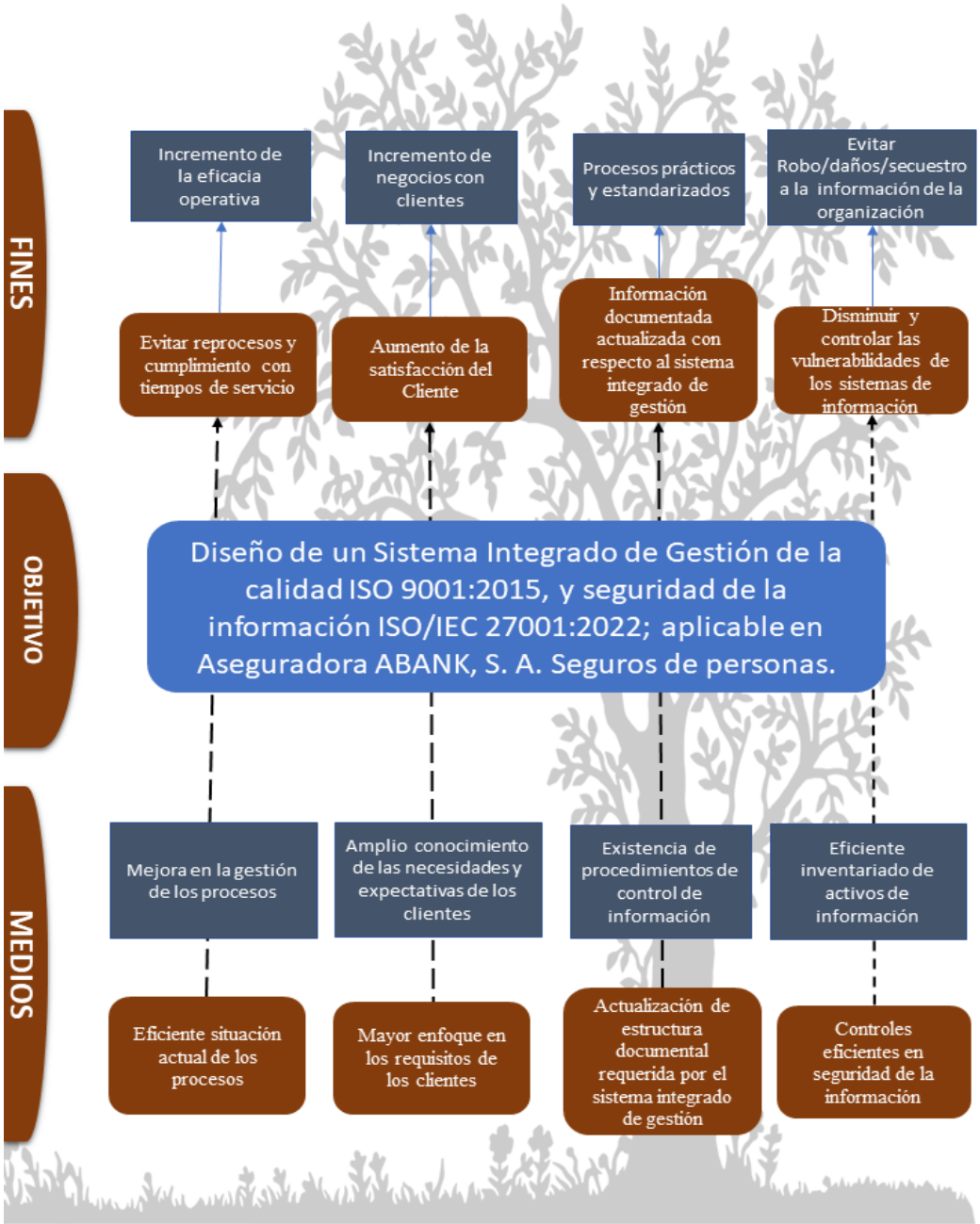
Los objetivos específicos son metas detalladas y concretas que se establecen para alcanzar un objetivo general más amplio. Mientras que los objetivos generales proporcionan una visión general de lo que se quiere lograr, los objetivos específicos se centran acciones específicas.

A continuación, se exponen los objetivos del trabajo de graduación:

1. Analizar la situación actual en gestión de calidad en Aseguradora ABANK, según ISO 9001:2015.
2. Identificar las necesidades y expectativas de los clientes de la organización conforme a ISO 9001:2015 e ISO IEC 27001:2022.
3. Identificar la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización.
4. Identificar la situación actual de Aseguradora ABANK en relación con aspectos de seguridad de la información, según ISO/IEC 27001:2022.

En la Figura *7* se muestra el árbol de objetivos para Aseguradora ABANK, el cual cumple la función de mostrar esquemáticamente la relación existente entre los medios (objetivos específicos), el objetivo general y por último los fines que se alcanzaron con el cumplimiento de cada uno de ellos en la investigación.

Figura 7. Árbol de objetivos de la investigación



Fuente: Elaboración propia

1.6 Formulación de hipótesis o supuestos

Las hipótesis expresan las posibles suposiciones sobre la problemática abordada, por lo tanto, su definición es crucial para establecer un enfoque hacia los fenómenos relacionados con el objeto de estudio. Estas son esenciales para guiar la investigación hacia la resolución de dicho problema, según lo menciona Rojas Soriano "Las hipótesis tienen que estructurarse de acuerdo con la forma en que se ha orientado el planteamiento del problema, considerando también las exigencias expresadas en los objetivos de la investigación" (Rojas, 2013, pág. 136).

1.6.1 Hipótesis general

La hipótesis general es una herramienta esencial en una investigación, debido que es el punto de partida de cualquier investigación, además de guiar la investigación y orientar la discusión y comunicación de los resultados. Su importancia radica en que proporciona un marco contextual sólido, guía el diseño y desarrollo de la investigación.

Por lo tanto, se declaró la siguiente hipótesis general:

El diseño e implementación de un Sistema Integrado de Gestión de la Calidad y Seguridad de la Información, basado en las normas ISO 9001:2015 e ISO/IEC 27001:2022, permitirá a Aseguradora ABANK mejorar la comunicación y el trabajo en equipo, aumentar el compromiso y liderazgo de gerentes y directores, optimizar las operaciones y servicios al cliente, y fortalecer la seguridad de la información, resultando en una mayor eficiencia operativa y mitigación de riesgos relacionados con la gestión de datos confidenciales.

1.6.2 Hipótesis específicas

Las hipótesis específicas se derivan de la hipótesis general, son importantes porque guían el proceso de investigación, establecen objetivos específicos y ayudan a determinar qué datos deben ser recopilados para probar o rechazar la hipótesis general, para el presente trabajo de investigación se propuso[8]:

[8] Se aprecia de forma general que la mayor parte de hipótesis específicas se encuentran estructuradas desde un enfoque cuantitativo, sin embargo, al definir cada una de las variables que sustentan a cada una de ellas se desglosan indicadores de orden cualitativo.

1. Las condiciones actuales de Aseguradora ABANK en aspectos de calidad, según ISO 9001:2015, están por debajo del 50% debido a problemas en la gestión de procesos, control de la información documentada, errores operacionales y deficiencias en liderazgo y compromiso.
2. Las necesidades y expectativas de los clientes de Aseguradora ABANK no se identifican y no se consideran en las estrategias de la organización, por lo cual se genera insatisfacción de estos.
3. El nivel de cumplimiento de información documentada de la organización, con relación a los requisitos ISO 9001:2015 e ISO/IEC 27001:2022 es inferior a 40%.
4. Las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información, según ISO/IEC 27001:2022 es inferior a 40%.

1.7 Variables e indicadores de investigación

Roberto Sampieri (2018) define las variables como "una propiedad o concepto que puede variar y cuya fluctuación es susceptible de medirse u observarse". En la investigación las variables surgieron a partir del objetivo de la investigación y la sistematización de la problemática.

Ahora bien, los indicadores son herramientas que se emplean para medir las variables, permitiendo así expresarlas en términos observables y cuantificables. Por ejemplo, en el caso de la variable de estudio sobre la satisfacción del cliente, los indicadores podrían incluir tanto la satisfacción del cliente interno como la del cliente externo. Por otro lado, si la variable se refiere a la información documental disponible, un indicador relevante podría ser la identificación de la documentación existente dentro de la organización.

A continuación, se presenta la matriz de conceptualización y operación de las variables de la investigación, la cual expone los elementos que se plantearon medir en la investigación a través de indicadores específicos que sustentaron los objetivos de la investigación y representativos de la problemática del sujeto de estudio. La matriz jugó un papel fundamental en el proceso de investigación al proporcionar una visión general y sistemática de los elementos estudiados y garantizó la rigurosidad en el análisis y la interpretación de datos (Ver Tabla *3*).

Tabla 3. Matriz de conceptualización y operación de las variables

MATRIZ DE CONCEPTUALIZACIÓN Y OPERACIÓN DE LAS VARIABLES				
VARIABLE	**DEFINICIÓN CONCEPTUAL**	**DIMENSIONES**	**INDICADORES**	**ESCALA (MEDICIÓN)**
1.Grado de conformidad con respecto a requisitos de Calidad	Requisito: necesidad o expectativa establecida, generalmente implícita u obligatoria (ISO 9000:2015, 3.1.2, 2015, pág. 8).	-Requisitos de gestión de calidad - Riesgos organizacionales	Identificación del cumplimiento de la organización ante los requisitos de normativa ISO 9001:2015	Cualitativo
			(Requisitos cumplidos ante ISO 9001:2015/ Total de requisitos requeridos por ISO 9001:2015) *100	Cuantitativo
2.Satisfacción de las necesidades y expectativas de los clientes	Satisfacción del cliente: percepción del cliente sobre el grado en que se han cumplido sus requisitos (ISO 9000:2015, 3.1.4, 2015, pág. 8) Cliente: persona u organización que podría recibir o que recibe un producto o un servicio destinado a esa persona u organización o requerido por ella (ISO 9000:2015, 3.2.4, 2015, pág. 13)	-Clientes	Identificación de necesidades y expectativas de Clientes	Cualitativo
			(Número de clientes (asegurados) Muy satisfechos y satisfechos/Total de encuestados) *100	Cuantitativo
3.Información documental existente	Información: datos que poseen significado (ISO 9000:2015, 3.7.1, 2015, pág. 12)	-Documentos -Registros -Procedimientos -Procesos	Identificación de información documentada de la organización	Cualitativo
			(Información documentada de la organización/ información documentada requerida por ISO 9001:2015 e ISO/IEC 27001:2022) * 100	Cuantitativo
4.Grado de conformidad con respecto a requisitos de Seguridad de la información	Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000:2018, 3.77, pág. 11)	-Requisitos de Seguridad de la información - Activos de información -Controles organizacionales -Controles de personas -Controles físicos -Controles tecnológicos	Identificación del cumplimiento de la organización ante los requisitos de normativa ISO/IEC 27001:2022	Mixto
			Identificación de los activos de información	Cualitativo
			Identificación de controles de seguridad de la información	Cualitativo
			(Controles de seguridad de seguridad de la información cumplidos/ Total de controles de seguridad de la información según ISO/IEC 27001:2022) *100	Cuantitativo

Fuente: elaboración propia

1.8 Matriz de consistencia de marco referencial

La matriz de consistencia con respecto al marco referencial establece la relación entre el diagnóstico preliminar (formulación del problema), su sistematización y los objetivos que dan solución a las hipótesis definidas para el sujeto de estudio (Ver *Apéndice 3*).

1.9 Fundamentos éticos

Los fundamentos éticos definen el compromiso en la investigación con respecto a la propiedad intelectual de las fuentes de información, originalidad del estudio y el consentimiento informado del sujeto de estudio, esto debido que es necesario garantizar que la investigación se desarrolle basada en principios éticos y de respeto a todos los involucrados.

1.9.1 Originalidad del estudio y exigencia crítica

Al haber realizado una exhaustiva revisión documental relacionada al sector de seguros, a través de repositorios académicos, artículos, publicaciones a nivel nacional e internacional se concluye que la investigación declara una investigación novedosa, debido a que plantea estrategias para identificar soluciones a la problemática que afecta a la organización a partir del diseño de un sistema integrado de gestión basado en normativa ISO 9001:2015 e ISO/IEC 27001:2022.

La investigación es considerada vanguardista en el rubro de los seguros a nivel nacional[9], debido que no existen registros documentales que demuestren evidencias del diseño ni mucho menos implementación de ambos sistemas de gestión; a pesar que pudiesen existir diferentes tipos de metodologías, principios o buenas prácticas en el mercado, la actual investigativa establece un marco de trabajo en el que se vinculan principios de calidad y fundamentos de la seguridad de la información desde una perspectiva integral y con el respaldo de más de medio siglo del Organismo Internacional de Normalización y la Comisión Electrotécnica Internacional (de su acrónimo en inglés ISO e IEC, respectivamente).

[9] A la fecha, solamente existen 2 de 24 aseguradoras oficialmente registradas en El Salvador, las cuales se encuentran trabajando bajo principios basados en normativas ISO, en específico 9001:2015. De igual forma, ambas aseguradoras (Seguros Futuro y Seguros Comédica) se encuentran certificadas en dicha normativa.

1.9.2 Propiedad intelectual

Los maestrantes egresados nos comprometemos a garantizar el respeto a los derechos de autor de las diferentes fuentes bibliográficas que se utilizan para el enriquecimiento y soporte documental, es por ello que, al utilizar información de fuentes no propias de los autores de esta investigación, se hizo referencia utilizando los lineamientos de la Asociación Americana de psicología (de sus siglas en inglés APA) en su versión 7.

1.9.3 Consentimiento informado de resultados investigativos

Se comunicó al sujeto de estudio, por parte de la Dirección de la Maestría en Sistemas Integrados de Gestión de Calidad (MASIG), la petición de atención para la realización del trabajo de graduación en dicha organización, bajo las condiciones expuestas en el alcance de la investigación que se encuentra en el *Anexo 1.* La petición fue recibida, sellada y firmada por director y presidente de Aseguradora ABANK en muestra de conformidad con la solicitud.

1.10 Viabilidad del trabajo de graduación

La viabilidad del trabajo de graduación establece la factibilidad del desarrollo de una investigación académica para el sujeto de estudio, por lo que se define tanto las competencias necesarias por parte de los investigadores, como de la aceptación y acompañamiento del sujeto de estudio, es así como se definen las cartas de viabilidad técnica, viabilidad de consentimiento informado del sujeto de estudio y la viabilidad metodológica, como respaldos de la viabilidad.

1.10.1 Viabilidad técnica

La Viabilidad Técnica (Ver *Apéndice 3*) expuso que los maestrantes cuentan con las competencias necesarias para llevar a cabo el trabajo de graduación, y son responsables de la ejecución de investigación académica, según los requerimientos en la Maestría en Sistemas Integrado de Gestión de Calidad y Aseguradora ABANK.

1.10.2 Viabilidad del consentimiento informado del sujeto de estudio

El consentimiento informado es un proceso ético y legalmente necesario para asegurarse de que el sujeto de estudio aprueba el desarrollo de la investigación, por lo que se expresa el consentimiento que están de acuerdo en participar de manera voluntaria y consciente.

Por consiguiente, Aseguradora ABANK emitió el consentimiento informado para la realización del trabajo de graduación, por medio de una carta firmada por el director y presidente de la organización, en la que se aprueba la realización de la investigación según los parámetros definidos en la Carta de consentimiento informado de resultados investigativos, la cual fue previamente recibida por la organización (V*er Anexo 2).*

1.10.3 Viabilidad metodológica

La viabilidad metodológica de este trabajo de graduación ha sido confirmada a través de la carta de aprobación del Anteproyecto de Trabajo de Graduación emitida por la Maestría de Sistemas Integrados de Gestión de Calidad (V*er Anexo 3)*. Este dictamen certifica que el escrito presenta una coherencia adecuada entre la metodología propuesta, los objetivos del estudio y el problema planteado, lo cual refleja nuestra capacidad para llevar a cabo la investigación de manera efectiva y ética. Además, se garantiza el uso de métodos y técnicas apropiadas para el tipo de datos recolectados durante el proyecto de investigación.

1.11 Dificultades y limitaciones

Las dificultades y limitaciones se deben identificar para garantizar el desarrollo de la investigación, por medio de idear métodos adecuados para contrarrestar el riesgo que representan; en toda organización existen limitaciones a la hora de desarrollar actividades teóricas como la presente investigación, por lo que el identificarlas y plantear una metodología de recolección de información y acercamiento al sujeto de estudio adecuada, puede significar el superar dichos obstáculos, disminuyendo el riesgo que representan.

En Aseguradora ABANK y en consideración a los requisitos del método de la investigación, se identificaron las siguientes dificultades:

- Adaptación de los tiempos para la recolección de los datos necesarios para la investigación, con respecto a los tiempos de disponibilidad del personal seleccionado para brindar información al desarrollo de la misma.
- Adecuación de las técnicas y métodos en la recolección de información para el desarrollo de la investigación, con respecto a los principios de confidencialidad de la organización.

Algunas limitaciones de la investigación fueron las siguientes:

- La norma ISO/IEC 27001 se actualizó recientemente de versión 2013 a versión 2022, por lo que las investigaciones, publicaciones, noticias de referencia y demás canales de información que aportan conocimientos para el desarrollo de la presente investigación es poca, en comparación de la versión anterior a la normativa.
- Información bibliográfica escasa relacionada a la integración de sistemas de gestión en Aseguradoras con base a normativas ISO/IEC 27001 e ISO 9001.

Al finalizar el capítulo del marco referencial, se puede resumir que es una sección muy importante en la elaboración del trabajo de graduación, ya que estableció el punto de partida para la labor investigativa, permitió establecer el contexto y los antecedentes de la problemática que fueron necesarios para analizar la situación del sujeto de estudio. A través de la sección que finaliza, se estableció un panorama más detallado de la problemática, sus causas y efectos, de igual forma se declaran las delimitaciones de la investigación y se diseñan los objetivos del desarrollo de ésta, así como la justificación y las variables e indicadores de las hipótesis declaradas en la presente investigación.

Posteriormente se tomó en consideración aspectos relacionados a la propiedad intelectual de la investigación, carta de consentimiento informado, viabilidad técnica y metodológica que sustentaron la aprobación tanto del sujeto de estudio, como de la Dirección de la Maestría en Sistemas Integrados de Gestión de Calidad, para la realización de esta.

Finalmente, se redactaron las dificultades y limitaciones que se ven inmersas en la labor investigativa y que fueron consideradas para anticiparse a los riesgos que representaron.

Es así como se dio paso al siguiente capítulo denominado marco teórico, en el que se sustentó la base de información a nivel de bibliografía y de referencias documentales, antecedentes, conceptos y sus definiciones, así como también el desarrollo de teorías fundamentales.

CAPÍTULO II. MARCO TEÓRICO

El marco teórico se refiere a la sección donde se llevó a cabo un acercamiento inicial a través de una revisión bibliográfica de teorías previamente elaboradas por otros investigadores que están relacionadas con el tema de investigación. Asimismo, en este apartado se incorporaron los conceptos y la teoría fundamental que respalda el trabajo investigativo y permiten una mejor comprensión de este. Finalmente se incluyó un marco legal y reglamentario.

Rojas Soriano (2013, Pág. 96) establece que existen tres niveles, no consecutivos que una investigación debe considerar para construir el marco teórico y conceptual, estos niveles aplicados a la presente investigación hicieron referencia al primer nivel cuando se habló sobre fundamentos teóricos relacionados a las normativas ISO 9001:2015 e ISO/IEC 27001:2022; el segundo nivel, hizo referencia a estudios, tesis, informes y páginas web institucionales que estaban relacionados a la temática investigativa; en el tercer nivel, se consideró el uso de información obtenida por medio de entrevistas y observación al sujeto de estudio.

2.1 Marco de antecedentes

El marco de antecedentes incluye información referente a estudios previos, investigaciones y teorías pertinentes al área de investigación. Se procedió a realizar una revisión bibliográfica en dos vías específicas: marco de antecedentes nacional y marco de antecedentes internacional.

2.1.1 Marco de antecedentes nacional

A través de una revisión bibliográfica en los repositorios documentales de universidades y otras fuentes investigativas a nivel nacional, se identificaron únicamente dos instituciones que presentaron antecedentes pertinentes: la Universidad de El Salvador y la Universidad Don Bosco. Lo anterior deja en evidencia una escasez de investigaciones en este ámbito. A continuación, se presenta el detalle de lo encontrado:

- Investigación denominada “Sistema de gestión de calidad basado en riesgos para las pequeñas y medianas empresas corredoras de seguros del área Metropolitana de San Salvador” de la Universidad de El Salvador en el cual se expone la importancia de la elaboración del diseño de un Sistema de Gestión de la Calidad para las corredurías de seguros, en base a ISO 9001:2015.

La investigación busca motivar la calidad en las corredurías de seguros para tratar riesgos y oportunidades relacionadas al contexto de la empresa, cumplir con objetivos de calidad y mejorar de procesos (Alvarado de Duran, Parras Velasco, & Zamora Zabaleta, 2017).

- Asimismo, otra bibliografía consultada fue el proyecto denominado "Metodología para implantar Seguridad de la Información en una empresa financiera en El Salvador" de la Universidad Don Bosco en la cual se presenta una revisión teórica sobre los conceptos y estándares de seguridad de la información, como ISO 27001.

  En la investigación se concluye que la implementación de una de las metodologías propuestas permitirá a las empresas financieras en El Salvador proteger información y garantizar la confidencialidad, integridad y disponibilidad de los datos, reduciendo los riesgos y aumentando la confianza de los clientes. (Najarro Alfaro, Urrutia López, & Ibarra de Martínez, 2015).

  Estas investigaciones proporcionaron una base sólida de conocimientos teóricos relacionados con la gestión de calidad y la seguridad de la información en el contexto específico de las pequeñas y medianas empresas corredoras de seguros y las empresas financieras en El Salvador. De la misma manera al ser investigaciones realizadas a nivel nacional aportan conocimiento importante sobre el contexto del país lo cual ayuda a comprender los desafíos y oportunidades a tomar en cuenta en la presente investigación.

2.1.2 Marco de antecedentes internacional

Se llevó a cabo una revisión de estudios realizados a nivel internacional. A partir de esta investigación, se identificaron los siguientes documentos académicos relevantes:

- La Fundación Universidad de América de Bogotá llevó a cabo un estudio titulado "Propuesta de implementación de la norma NTC ISO 9001:2015 en la Organización Integral de Seguros LTDA", donde se expone la factibilidad de implementación de una normativa ISO 9001 a una organización de seguros.

  La investigación se enfoca en la identificación de los procesos clave de la organización, la definición de los indicadores de desempeño y la implementación de un sistema de gestión de calidad que cumpla con los requisitos de la norma (Pineda Capador, 2021).

El trabajo incluye la definición de procedimientos documentados, la capacitación del personal y la realización de auditorías para verificar la efectividad del sistema de gestión de calidad.

- Otro trabajo de investigación desarrollado en Quito, Ecuador por la Universidad Tecnológica Equinoccial fue la investigación denominada: “Diseño de un Sistema de Gestión de Calidad para el proceso de indemnizaciones de vehículos, en Aseguradora del Sur” donde se diseñó un sistema de gestión de calidad basado en la norma ISO 9001:2015, adaptado a particularidades de la organización. Se establecieron indicadores de desempeño, se definieron procesos y procedimientos para asegurar la calidad del servicio prestado, con la finalidad de mejorar la eficiencia, eficacia y satisfacción del cliente de la organización (Viteri Zambrano, 2016).
- Asimismo, se encontró otro trabajo de investigación denominado: “Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A”. En la investigación se consideran las fases:
    - Fase 1: Diagnóstico de la situación actual en materia de seguridad informática.
    - Fase 2: Identificar los activos informáticos, definir y aplicar metodología de análisis y gestión del riesgo.
    - Fase 3: Determinar y evaluar la aplicabilidad de los controles de seguridad de la información bajo la norma ISO/IEC 27002:2013.
    - Fase 4: Definición de alcance, objetivos y política del Sistema de Gestión de Seguridad de la Información.

En la investigación se concluyó que un SGSI implementado permite mejorar la seguridad de la información y proteger los activos críticos de la compañía, lo que aumenta la confianza de los clientes y reduce los riesgos de posibles incidentes de seguridad (Ardila Navarrete, 2016).

No se encontraron estudios o investigaciones realizadas sobre sistemas de gestión que integren Calidad y Seguridad de la Información en organizaciones similares a Aseguradora ABANK, especializadas en la comercialización de seguros médicos y de vida.

No obstante, se encontró una investigación que abordaba la integración de las normativas en una organización dedicada a la emisión de documentos de identificación militar:

- “Diseño de un Sistema Integrado de Gestión basado en las normativas ISO 9001:2015 e ISO 27001:2013, para la emisión de documentos de identificación militar en la matriz de la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas” es un proyecto publicado por la Universidad Andina Simón Bolívar de Quito, Ecuador.

El proyecto consta de varias fases, comenzando con una evaluación inicial de la situación actual de la matriz de la Dirección de Movilización. Luego se procede a la identificación de los procesos críticos y se establecen los procedimientos necesarios para garantizar la calidad y la seguridad de los documentos emitidos. En resumen, la investigación busca establecer un sistema integrado de gestión que garantice la calidad y seguridad de los documentos de identificación militar cumpliendo con las normas ISO 9001:2015 e ISO 27001:2013 (García Remache, 2020).

Estas investigaciones internacionales ejemplifican el exitoso uso de las normas ISO 9001:2015 e ISO/IEC 27001:2022 en empresas de seguros, mostrando una relación sólida entre ambos estándares a nivel global, en contraste con el contexto nacional.

Estos estudios resaltan la eficacia de implementar dichas normativas en el ámbito internacional, demostrando su relevancia y beneficios en la gestión y seguridad de las organizaciones aseguradoras. En las investigaciones identificadas se obtienen importantes aportes, tales como metodología de implementación de ISO 9001 e ISO/IEC 27001 en aseguradoras, fases para la adecuación de un Sistemas de Seguridad de la Información en el rubro de seguros, importancia del establecimiento de procesos, entre otros.

2.2 Marco conceptual

El marco conceptual son términos y definiciones relevantes y relacionadas a las variables definidas en la investigación. La claridad en la definición de dichos conceptos es fundamental para comprender mejor el estudio y para garantizar una interpretación correcta del lector. A continuación, se presenta un desglose de los conceptos claves identificados:

a) Activo de información: componente que sustenta uno o más procesos de negocio y genera valor a la entidad. Pueden ser de diversos tipos, entre ellos: datos o información, servicios, programas informáticos, dispositivos físicos, redes de comunicación, soportes de información, equipamiento auxiliar e instalaciones físicas, e intangibles (NPR-23. Norma Técnica para la Gestión de la Seguridad de la Información, 2020, pág. 3).

Los activos de información son piezas importantes de datos, archivos o recursos que una organización posee. Por tanto, se necesitan proteger y evitar accesos no autorizados ya que su pérdida o alteración puede llegar a ocasionar problemáticas tanto financieras, como de reputación entre otras.

b) **Calidad:** grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos (ISO 9000:2015, 3.6.2, 2015, pág. 19). Calidad es el nivel de cumplimiento de estándares y expectativas en un producto o servicio. Una alta calidad significa que algo está bien hecho, es confiable y cumple con lo que se espera de ello.

c) **Control de acceso:** medios para garantizar que el acceso a los activos esté autorizado y restringido en función del negocio y la seguridad requisitos (ISO 27000:2018, 3.1, 2022, pág. 1). Los controles de acceso toman relevancia al establecer parámetros de seguridad para ingreso de usuarios a los sistemas informáticos de una organización, por ejemplo, control de acceso por escaneo de huellas o retina, doble factor de autenticación, entre otros mecanismos para asegurar que individuos no deseados alteren o roben información de la organización y de sus clientes.

d) **Información documentada:** información que una organización tiene que controlar y mantener y el medio que la contiene (ISO 9000:2015, 3.8.6, 2015, pág. 24). La información documentada es toda aquella que ha sido registrada o plasmada por escrito o en formato digital y que está lista para ser consultada cuando se necesite.

e) **Parte interesada:** persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad (ISO 9000:2015, 3.2.3, 2015, pág. 12). Las partes interesadas pueden ser internas como externas, cada cual posee características que deben ser estudiadas y consideradas por las organizaciones.

f) **Seguridad de la información:** preservación de confidencialidad, integridad y disponibilidad de información. (ISO 27000:2018, 3.28, 2018, pág. 4). La seguridad de la información evita que la información se pierda, se dañe o caiga en manos equivocadas, manteniéndola protegida y disponible solo para quienes realmente la necesitan.

2.3 Marco de teoría fundamental

El marco de teoría fundamental son planteamientos relacionados con la problemática a investigar; es esencial para ampliar los conocimientos relacionados con las variables establecidas en la investigación. Es así como, se inició con la teoría de los Sistemas de Gestión de Calidad ISO 9001:2015, Asimismo, se profundizó en la teoría de los Sistemas de Seguridad de la Información ISO/IEC 27001:2022 y finalmente la integración de los mismos.

2.3.1 Sistemas de Gestión de la Calidad ISO 9001:2015

Un sistema de gestión de calidad según la norma ISO 9001:2015 es un conjunto de procesos, políticas y procedimientos que una organización establece para asegurar que sus productos o servicios cumplen con los requisitos y expectativas de sus clientes de manera consistente.

Algunas características clave de un sistema de gestión de calidad ISO 9001:2015:

- Enfoque en el cliente: La organización debe comprender y cumplir con las necesidades y expectativas de sus clientes, buscando su satisfacción a través de productos y servicios que cumplan con sus requisitos.
- Enfoque basado en procesos: Se deben identificar, gestionar y mejorar los procesos clave que contribuyen a la eficiencia y eficiencia de la organización en la entrega de productos o servicios.

  En lugar de considerar a la organización como una serie de funciones separadas, la norma promueve la comprensión de cómo los procesos interactúan entre sí y cómo contribuyen al logro de los objetivos organizacionales.

La norma ISO 9001 establece los criterios para implementar un sistema de gestión de calidad (SGC) a nivel internacional. Su propósito es ayudar a las organizaciones a cumplir con las expectativas de sus clientes y demás partes interesadas mediante la aplicación efectiva del sistema, que incluye la mejora continua y el cumplimiento de los requisitos legales y de los clientes.

Esta norma es aplicable en una amplia gama de sectores, desde la manufactura hasta los servicios y la tecnología, está compuesta por 10 capítulos que están diseñados para facilitar la integración con otras normas. Esta estructura uniforme se conoce como Estructura de Alto Nivel y ha sido establecida por ISO en el Anexo SL. A continuación, se presenta dicha estructura:

1. Objeto y campo de aplicación

- Define la finalidad de implmentación de la norma por parte de cualquier organización, independientemente del tamaño o actividad económica.

2. Referencias normativas

- Proporciona detalles sobre las normas de referencia o publicaciones relevantes en relación a la norma concreta.

3. Términos y definiciones

- Resalta que los términos y definiciones aparecen a lo largo de la norma deben ser consultados en la norma ISO 9000 versión 2015.

4. Contexto de la organización

- La organización debe identificar todos aquellos factores internos como externos que puedan afectar al Sistema de Gestión de Calidad. También se deben identificar partes interesas y sus necesidades. Finalemente se hace referencia a que se debe definir el alcance del SGC, es decir sus límites y requisitos de la norma no aplicables, debidamente justificados.

5. Liderazgo

- En este capítulo, se enfatiza en el compromiso y protagonismo que tiene que tener la alta dirección en el diseño, implementación y mejora del SGC. Entre las responsabilidades de la alta dirección aparecen la concientización a la organización acerca de la importancia del SGC, aportar los recursos necesarios, fomentar la participación del personal, el seguimiento y medición, entre otros.

6. Planificación

- Proporciona directrices de cómo, una vez identificados los riesgos y oportunidades de la organización (derivados de la descripción y análisis del contexto de la organización), esta tiene que establecer cómo estos van a ser tratados mediante la planificación. En este capítulo también se pone de manifiesto la necesidad de establecer objetivos que debe alcanzar el SGC, los cuales deben ser coherentes con la política del SGC, comunicados a toda la organización, medibles y monitoreados periódicamente.

7. Apoyo

- Una vez la organización ha analizado su contexto y ha realizado la planificación respectiva, debe asegurarse de que dispondrá de los recursos necesarios para cumplir con sus metas y objetivos; esto incluye los recursos, comunicaciones internas y externas, así como la información documentada necesaria (documentos y registros).

8. Operación

- Representa el capítulo que tiene la mayor cantidad de requisitos. En síntesis, este capítulo establece las condiciones en que se deben gestionar las actividades relacionadas con la producción del bien o la prestación del servicio, así como las actividades propias del SGC.

9. Evaluación de desempeño

- Este capítulo señala que la organización debe determinar qué, cómo y cuándo ha de supervisar, medir, analizar y evaluar el SGC. Dentro de la evaluación del desempeño está la auditoría del sistema, que es un proceso sistemático, independiente y documentado para obtener evidencia que permita determinar si es eficaz el SGC, es decir, si está cumpliendo con los requisitos de la organización y los de la norma. Aquí también se contempla la revisión del sistema por parte de la alta dirección, de tal forma que esta pueda determinar si el sistema es adecuado o no y dependiendo de ellos, seguir las acciones necesarias.

10. Mejora

- En este capítulo la norma pide establecer las formas en que la organización afrontará las no conformidades y las acciones correctivas, así como las estrategias de mejora continua. En esta versión de la ISO 9001 se hace énfasis en que se implementen herramientas que permitan gestionar de forma organizada las acciones a desarrollar en función de la mejora continua.

Los capítulos de la norma se organizan de acuerdo con el modelo de mejora continua PHVA (planear, hacer, verificar y actuar), propuesto por Edwards Deming (Ver *Tabla 4).*

Tabla 4. Descripción de las etapas del ciclo PHVA

Descripción de las etapas PHVA	
Concepto	Descripción
Planificar	Establecer los objetivos del sistema y sus procesos, y los recursos necesarios para generar y proporcionar resultados de acuerdo con los requisitos del cliente y las políticas de la organización, e identificar y abordar los riesgos y las oportunidades.
Hacer	Implementar lo planificado.
Verificar	Realizar el seguimiento y (cuando sea aplicable) la medición de los procesos y los productos y servicios resultantes respecto a las políticas, los objetivos, requisitos y las actividades planificadas, e informar resultados.
Actuar	Tomar acciones para mejorar el desempeño, cuando sea necesario.

Fuente: Adaptado de ISO 9001:2015

En la *Figura 8* se ilustra la interrelación del ciclo PHVA con los requerimientos establecidos en la norma ISO 9001:2015. Es importante destacar que los requisitos del 1 al 3 de la norma no se incluyen en la imagen, ya que estos apartados ofrecen información general, como la introducción, el alcance y las referencias de la norma, que no contienen requerimientos específicos que puedan ser planificados, implementados, verificados y mejorados.

La planificación se relaciona con el requerimiento 6 de la norma, el cual lleva el mismo título; hacer, se vincula con el apartado 8 de Operaciones; la verificación, está relacionada con el requerimiento 9 de Evaluación de desempeño; actuar, se asocia con el requerimiento 10 de Mejora. Es importante señalar que los requerimientos 4 de Contexto de la organización, 5 de Liderazgo y 7 de Soporte no se vinculan directamente a un elemento del ciclo PHVA, sin embargo, son parte fundamental para estructuración de un Sistema de Gestión.

Figura 8. Relación de requisitos de ISO 9001:2015 con el ciclo PHVA

Fuente: Adaptado de ISO 9001:2015

2.3.2 Sistemas de Gestión de Seguridad de la información ISO 27001:2022

La norma ISO 27001:2022 es una norma internacional de sistemas de gestión de seguridad de la información (SGSI), proporciona un marco sistemático y estructurado para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI en una organización. Se enfoca en la protección de los activos de información, y también busca preservar la confidencialidad, la integridad y la disponibilidad de dicha información. En un mundo donde la información es un activo invaluable y su seguridad es de suma importancia, la adopción de la norma ISO 27001:2022 se convierte en una estrategia esencial para salvaguardar los intereses de la organización y mantener la confianza de sus partes interesadas.

Para garantizar la seguridad de los activos de información, resulta crucial llevar a cabo un inventario de estos. En la Figura *9* se detalla una clasificación de estos recursos.

Figura 9. Clasificación de los activos de información

Fuente: Adaptado de (Wrobel, 2023)

Para proteger los activos de información descritos en la Figura *9* la norma ISO/IEC 27001:2022 cuenta con un Anexo A que es de carácter normativo, que proporciona un listado de controles de seguridad de la información para ayudar a las organizaciones a establecer, implementar, mantener y mejorar un SGSI. Este anexo facilita una estructura sólida y orientativa que abarca diversos aspectos de la seguridad de la información, desde la gestión de accesos hasta la gestión de incidentes, brindando así un marco integral para enfrentar los desafíos de seguridad.

Estos controles son de carácter obligatorios, sin embargo, son flexibles y pueden adaptarse a las necesidades y contextos particulares de cada organización, permitiendo un enfoque personalizado en la implementación de la seguridad de la información.

Son 93 controles en la norma ISO/IEC 27001:2022 clasificados de la siguiente manera:

1**. Controles organizacionales (37 controles):** Los controles organizacionales según ISO/IEC 27001:2022 abarcan políticas de seguridad, organización de la seguridad, gestión de recursos humanos, gestión de activos, control de accesos y seguridad física y ambiental. Se establecen políticas y roles claros, se aseguran procedimientos adecuados para la selección y formación de personal, se mantiene un inventario actualizado de activos, se gestionan adecuadamente los accesos y se protegen físicamente los activos de información. Estos controles buscan garantizar una gestión integral y segura de la información dentro de la organización, promoviendo la eficiencia operativa y la reducción de riesgos.

2. **Control de personas (8 controles):** Los controles de personas según ISO/IEC 27001:2022 incluyen la selección de personal con verificación de antecedentes, la definición de términos y condiciones del empleo que aseguren responsabilidades de seguridad, programas de concienciación y formación continua, procesos disciplinarios para incumplimientos, gestión adecuada de la finalización y cambio de empleo, y la asignación clara de roles y responsabilidades de seguridad en la gestión de proyectos, todo con el objetivo de proteger la seguridad de la información dentro de la organización.

3. **Controles físicos (14 controles):** Los controles físicos según ISO/IEC 27001:2022 incluyen medidas para proteger los activos de información mediante la implementación de áreas seguras, el control de acceso físico, la protección de equipos contra amenazas ambientales y desastres naturales, la gestión segura de medios removibles y equipos desechados, la protección contra interrupciones y fallos de suministro, y el mantenimiento de instalaciones adecuadas para la seguridad de la información, todo con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de los activos de información.

4. **Controles tecnológicos (34 controles):** Los controles tecnológicos según ISO/IEC 27001:2022 abarcan la gestión de accesos, protección contra malware, actualización de software, criptografía, seguridad de comunicaciones y redes, gestión de configuraciones y cambios, monitoreo y auditoría de sistemas, manejo de incidentes de seguridad, y medidas para continuidad del negocio y recuperación ante desastres. Estos controles aseguran la protección integral de los sistemas de información y tecnología contra amenazas y vulnerabilidades.

Para mayor detalle sobre los controles, ver *Apéndice 4*

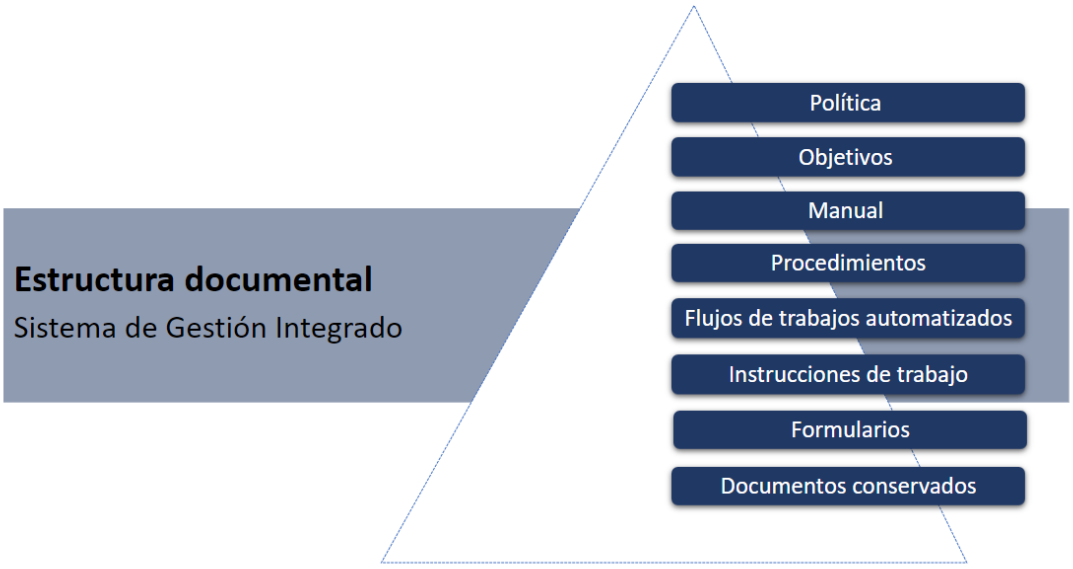
Para el caso de Aseguradora ABANK los 93 controles descritos anteriormente son aplicables, por tanto, para el desarrollo de la investigación se tomaron en cuenta el total de ellos.

2.3.3 Documentación de Sistemas de Gestión

La gestión documental es un componente crítico en el diseño de un Sistema Integrado de Gestión, ya que este tipo de sistemas se apoyan en gran medida de una serie de documentos fundamentales, como la política, procedimientos, registros que describen los diferentes procesos incluidos en el sistema de gestión.

La información documental de un sistema integrado se estructura de la siguiente forma:

Figura 10. Pirámide documental



Fuente: Adaptado de ISO 10013:2021

La forma de la pirámide no es casual. La base representa los documentos que más frecuentemente se encuentran en el sistema documental del sistema de gestión y en la cúspide se encuentra un documento que suele ser el que marca las líneas maestras o directrices generales de sistemas de gestión. De igual forma, a medida que ascendemos en la pirámide, la relevancia del documento aumenta, y al descender, aumenta el detalle del documento (López Lemos, 2015, pág. 28).

Cada organización debe estructurar información documentada, según sus necesidades y otros factores como el liderazgo, los resultados esperados del sistema de gestión, el contexto (incluyendo requisitos legales y reglamentarios) y las partes interesadas de la organización.

2.3.4 Sistemas Integrados de Gestión (SIG)

Un Sistema Integrado de Gestión tiene por objeto el unificar dos o más sistemas de gestión, de forma coherente y holística, en diferente índole, sean estos de calidad, seguridad y salud en el trabajo, ambiental, seguridad de la información, entre otros.

Hay numerosas ventajas estratégicas y operativas para una organización al combinar los requisitos de calidad y seguridad de la información en un solo sistema. Esto promueve la eficiencia operativa y la optimización de los procesos, lo que a su vez resulta en una reducción de los costos operativos y administrativos. Se busca la mejora continua al adoptar un enfoque basado en procesos y liderazgo, lo que conduce a una mayor calidad de los servicios y a la satisfacción del cliente.

Al mismo tiempo, se fortalece la seguridad de la información al gestionar los riesgos de manera integrada y establecer controles efectivos en la organización y su contexto. Esto se traduce en una mejora de la confidencialidad, integridad y disponibilidad de la información, generando una mayor confianza entre los socios comerciales, asegurados, empleados y otras partes interesadas.

Este aumento de la confianza puede abrir nuevas oportunidades de negocio y demuestra el compromiso de la organización con las mejores prácticas y el cumplimiento de los estándares legales y regulatorios aplicables, entre otros beneficios que se obtienen en las organizaciones que consideran un Sistema Integrado de Gestión.

Para la integración de sistemas de gestión, existen diversas normativas y guías que proporcionan directrices y marcos de trabajo. En el desarrollo de esta investigación, se optó por utilizar la norma de integración PAS 99 como base para el proceso.

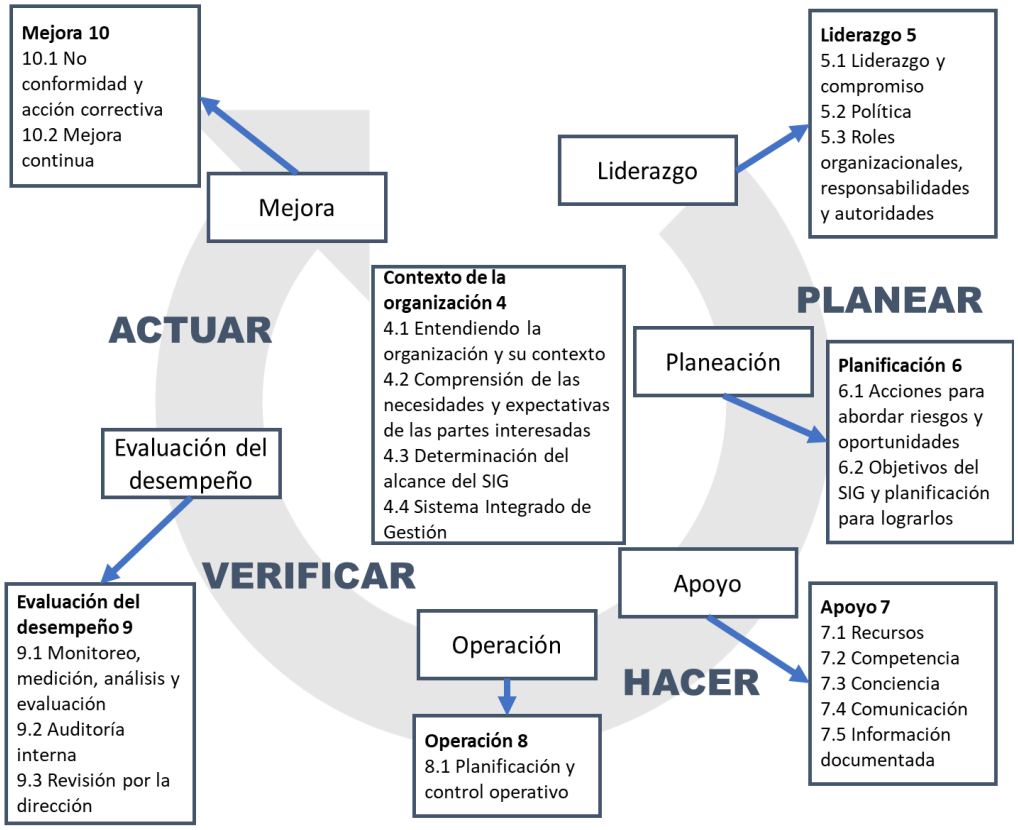
La decisión para seleccionar una opción de integración la normativa anteriormente mencionada se basó en la relación existente entre las características del método de integración con respecto al contenido de las normativas que son parte del alcance de la investigación.

En base a lo anterior se seleccionó la normativa PAS 99 en su versión 2012, la cual es la versión vigente en el mercado por parte del Instituto Británico de Normalización (BSI, de sus siglas en inglés), esto debido que comparte con los sistemas de gestión basados en normativas ISO, similitudes relacionadas con la estructura de alto nivel o anexo SL y el ciclo de Deming (PHVA).

La inclusión del Anexo SL en PAS 99:2012 se asegura que esta sea coherente con otras normas de sistemas de gestión y se reduce la necesidad de duplicación de esfuerzos en la documentación y la implementación de diferentes sistemas.

De igual forma, la norma PAS 99:2012 hace uso del ciclo PHVA porque es un enfoque sistemático y estructurado para la mejora continua, por lo que, al utilizarlo, se asegura que la integración sea efectiva, eficiente y sostenible a largo plazo. En la *Figura 11* se presenta la relación entre el Anexo SL y el ciclo de Deming presente en la estructura de PAS 99:2012.

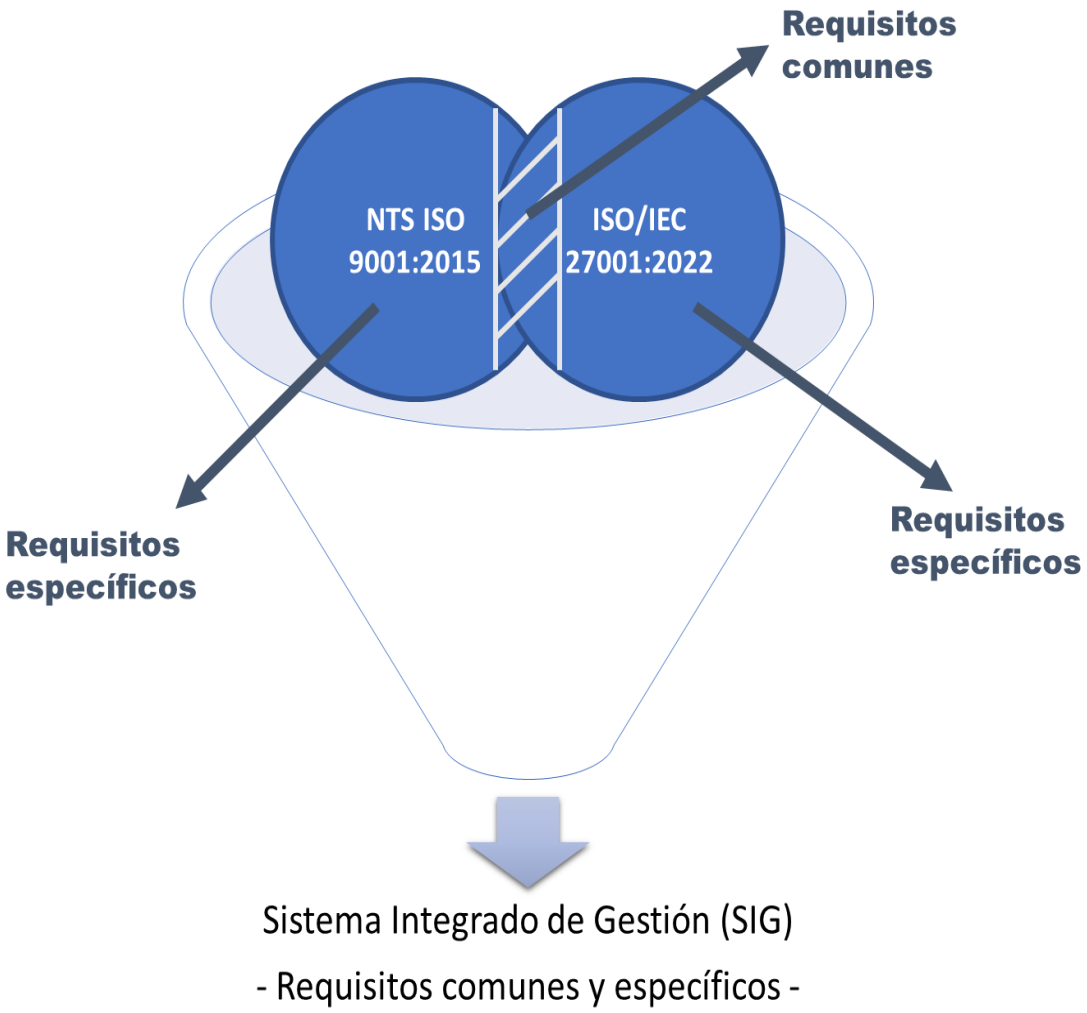
Figura 11. Estructura de Anexo SL y Ciclo PHVA en PAS 99:2012



Fuente: Adaptado de PAS 99:2012, Pág. 5

PAS 99:2012 busca el integrar sistemas de gestión a partir de los 7 requisitos comunes, que según Anexo SL comprenden: Contexto de la organización, Liderazgo, Planificación, Soporte, Operación, Evaluación del desempeño y Mejora. Para lograr dicha integración, basándose en el marco de trabajo de la normativa de integración se consideraron tres etapas principales: etapa 1, Identificación de requisitos comunes; etapa 2, Integrar requisitos comunes; etapa 3, Desarrollar requisitos únicos. En el caso de los requisitos únicos, se desarrollaron de forma independiente según la singularidad de cada enfoque de cada normativa (Ver *Figura 12*).

Figura 12. Integración de requisitos para SIG según PAS 99:2012



Fuente: Elaboración propia

Por consiguiente, PAS 99, declara que:

> Muchos de los requisitos de las normas son comunes y pueden acomodarse prácticamente en un Sistema de Gestión genérico. De ello se deduce que la reducción de la duplicación mediante la combinación de dos o más sistemas de esta manera tiene el potencial de reducir significativamente el tamaño total del Sistema de Gestión y mejorar su eficiencia y eficacia (British Standards Institution [BSI], 2012, Pág. 4).

A continuación, se presenta la relación entre ambas normativas, el exponer la relación entre ISO 9001:2015 e ISO/IEC 27001:2022 en el marco teórico es crucial para entender cómo estas normas, que abordan la gestión de calidad y la seguridad de la información, respectivamente, pueden integrarse para mejorar la eficiencia organizacional. Analizar su interrelación permite ilustrar cómo la combinación de sus principios y prácticas puede promover una mejora continua en ambos ámbitos, optimizar la gestión de riesgos y asegurar un cumplimiento más robusto, reflejando así una estrategia organizacional integral que potencia tanto la calidad del producto/servicio como la protección de la información.

La relación entre ambas normativas se clasifica por medio variables de relación, las cuales se describen en la *Tabla 5*. En la *Tabla 6* se visualiza los apartados comunes y específicos entre los sistemas de gestión involucrados en el alcance de la investigación:

Tabla 5. Variables de relación entre requisitos de ISO 9001:2015 e ISO/IEC 27001:2022

Variable de relación	Color identificador	Significado
Relación alta		Existe una similitud notable en el contenido de ambos apartados.
Relación media		Existe una relación importante entre los apartados de ambas normativas, pero el contenido de estas no se ve directamente relacionado.

Continúa Tabla 5 en la siguiente página →

Relación baja		Relación entre los apartados es leve debido a que a pesar de que el título de la cláusula pudiese ser igual, su contenido no en casi en su totalidad.
Sin relación		Significa que no existe relación directa o indirecta entre los apartados, ni en título o contenido.

Fuente: Elaboración propia

Además, se realizó la relación de ISO 9001:2015 con un apartado único referente la normativa de seguridad de la información ISO/IEC 27001:2022, el cual es conocido como los controles de seguridad de la información, titulado "Anexo A - Controles de seguridad de la información", el cual es de carácter obligatorio.

Tabla 6. Relación de requisitos entre ISO 9001:2015 e ISO/IEC 27001:2022

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
4. Contexto de la organización			
4.1 Comprensión de la organización y su contexto	4.1 Comprensión de la organización y su contexto	Relación alta	
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Relación alta	A.5.6 Contacto con grupos de interés
4.3 Determinación del alcance del sistema de gestión de la calidad	4.3 Determinación del alcance del sistema de gestión de la seguridad de la información	Relación alta	
4.4 Sistema de gestión de la calidad y sus procesos	4.4 Sistema de gestión de seguridad de la información	Relación media	

Continúa Tabla 6 en la siguiente página →

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
4.4.1 Sin título (Determinación de entradas, salidas, secuencia e interacción de procesos, criterios y métodos para asegurar la operación y control de procesos, recursos para procesos, responsabilidades y autoridades para los procesos, riesgos y oportunidades, evaluación de procesos, mejora de procesos y sistema de gestión de calidad)	No posee un título equivalente	Relación baja	A.5.37 Procedimientos operativos documentados
4.4.2 Sin título (mantener información documentada para la operación de los procesos, conservar información documentada para garantizar la confianza en que los procesos se realizan según lo planificado)	No posee un título equivalente	No relación	
5. Liderazgo			
5.1 Liderazgo y compromiso	5.1 Liderazgo y compromiso	**Relación media**	
5.1.1 Generalidades	No posee un título equivalente	Relación baja	A.5.4 Responsabilidades de la gestión
5.1.2 Enfoque al cliente	No posee un título equivalente	No relación	
5.2 Política	5.2 Política	Relación media	
5.2.1 Establecimiento de la política de la calidad	No posee un título equivalente	Relación media	A.5.1 Política de seguridad de la información
5.2.2 Comunicación de la política de la calidad	No posee un título equivalente	Relación media	
5.3 Roles, responsabilidades y autoridades en la organización	5.3 Roles, responsabilidades y autoridades en la organización	Relación alta	A.5.2 Roles y responsabilidades de la seguridad de la información
6. Planificación			
6.1 Acciones para abordar riesgos y oportunidades	6.1 Acciones para abordar riesgos y oportunidades	Relación media	
6.1.1 Sin título (la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el 4.2 y determinar los riesgos y oportunidades)	6.1.1 Generalidades	Relación alta	

Continúa Tabla 6 en la siguiente página →

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
6.1.2 Sin título (la organización debe planificar acciones para abordar riesgos y oportunidades, integrar e implementar acciones en sus procesos, evaluar la eficacia de las acciones)	6.1.2 Evaluación de riesgos de seguridad de la información	Relación media	
No posee un título equivalente	6.1.3 Tratamiento de riesgos de seguridad de la información	Relación baja	
6.2 Objetivos de la calidad y planificación para alcanzarlos	6.2 Objetivos de la seguridad de la información y planificación para alcanzarlos	Relación alta	
6.2.1 Sin título (la organización debe establecer objetivos de la calidad y ser coherentes con la política de la calidad, ser medibles…)	No posee un título equivalente	Relación alta	
6.2.2 Sin título (al planificar cómo lograr los objetivos la organización debe considerar lo que se va a hacer, los recursos que se requerirán, quién será responsable, cuándo se finalizará…)	No posee un título equivalente	Relación alta	
6.3 Planificación de los cambios	6.3 Planificación de los cambios	Relación media	A.8.32 Gestión del cambio
7. Apoyo			
7.1 Recursos	7.1 Recursos	Relación baja	
7.1.1 Generalidades	No posee un título equivalente	Relación media	
7.1.2 Personas	No posee un título equivalente	No relación	
7.1.3 Infraestructura	No posee un título equivalente	No relación	A.7.3 Aseguramiento de oficinas, salas e instalaciones A.7.9 Seguridad de los activos fuera de las instalaciones
7.1.4 Ambiente para la operación de los procesos	No posee un título equivalente	No relación	A.7.5 Protección contra amenazas físicas y ambientales A.7.6 Trabajar en áreas seguras
7.1.5 Recursos de seguimiento y medición	No posee un título equivalente	No relación	
7.1.5.1 Generalidades	No posee un título equivalente	No relación	
7.1.5.2 Trazabilidad de las mediciones	No posee un título equivalente	No relación	

Continúa Tabla 6 en la siguiente página →

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
7.1.6 Conocimientos de la organización	No posee un título equivalente	No relación	
7.2 Competencia	7.2 Competencia	Relación alta	
7.3 Toma de conciencia	7.3 Toma de conciencia	Relación alta	A.6.3 Concientización, educación y capacitación en seguridad de la información A.6.4 Proceso disciplinario
7.4 Comunicación	7.4 Comunicación	Relación alta	
7.5 Información documentada	7.5 Información documentada	Relación alta	
7.5.1 Generalidades	7.5.1 Generalidades	Relación alta	A.5.12 Clasificación de la información
7.5.2 Creación y actualización	7.5.2 Creación y actualización	Relación alta	
7.5.3 Control de la información documentada	7.5.3 Control de la información documentada	Relación alta	A.5.13 Etiquetado de la información
7.5.3.1 Sin título (la información documentada debe estar disponible y ser idónea para su uso, debe estar protegida adecuadamente)	No posee un título equivalente	Relación alta	
7.5.3.2 Sin título (para el control de la información documentada se debe considerar la distribución acceso, recuperación y uso, almacenamiento y preservación, control de cambios…)	No posee un título equivalente	Relación alta	
8. Operación			
8.1 Planificación y control operacional	8.1 Planificación y control operacional	Relación media	
8.2 Requisitos para los productos y servicios	8.2 Evaluación de riesgos de seguridad de la información	No relación	
8.2.1 Comunicación con el cliente	No posee un título equivalente	No relación	
8.2.2 Determinación de los requisitos para los productos y servicios	No posee un título equivalente	No relación	
8.2.3 Revisión de los requisitos para los productos y servicios	No posee un título equivalente	No relación	
8.2.3.1 Sin título (la organización debe asegurarse que tiene la capacidad de cumplir los requisitos para los productos y servicios que se van a ofrecer a los clientes)	No posee un título equivalente	No relación	

Continúa Tabla 6 en la siguiente página →

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
8.2.3.2 Sin título (conservar información documentada sobre los resultados de la revisión y cualquier requisito nuevo para los productos y servicios)	No posee un título equivalente	No relación	
8.2.4 Cambios en los requisitos para los productos y servicios	No posee un título equivalente	No relación	
8.3 Diseño y desarrollo de los productos y servicios	8.3 Tratamiento de riesgos de seguridad de la información	No relación	
8.3.1 Generalidades	No posee un título equivalente	No relación	
8.3.2 Planificación del diseño y desarrollo	No posee un título equivalente	No relación	
8.3.3 Entradas para el diseño y desarrollo	No posee un título equivalente	No relación	
8.3.4 Controles del diseño y desarrollo	No posee un título equivalente	No relación	
8.3.5 Salidas del diseño y desarrollo	No posee un título equivalente	No relación	
8.3.6 Cambios del diseño y desarrollo	No posee un título equivalente	No relación	
8.4 Control de los procesos, productos y servicios suministrados externamente	No posee un título equivalente	No relación	
8.4.1 Generalidades	No posee un título equivalente	No relación	A.5.19 Seguridad de la información en las relaciones con los proveedores A.5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores
8.4.2 Tipo y alcance del control	No posee un título equivalente	No relación	A.5.20 Abordar la seguridad de la información en los acuerdos con los proveedores A.8.30 Desarrollo subcontratado
8.4.3 Información para los proveedores internos	No posee un título equivalente	No relación	
8.5 Producción y provisión del servicio	No posee un título equivalente	No relación	
8.5.1 Control de la producción y de la provisión del servicio	No posee un título equivalente	No relación	
8.5.2 Identificación y trazabilidad	No posee un título equivalente	No relación	

Continúa Tabla 6 en la siguiente página →

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
8.5.3 Propiedad perteneciente a los clientes o proveedores externos	No posee un título equivalente	No relación	
8.5.4 Preservación	No posee un título equivalente	No relación	
8.5.5 Actividades posteriores a la entrega	No posee un título equivalente	No relación	
8.5.6 Control de cambios	No posee un título equivalente	No relación	
8.6 Liberación de los productos y servicios	No posee un título equivalente	No relación	
8.7 Control de salidas no conformes	No posee un título equivalente	No relación	
8.7.1 Sin título (la organización debe asegurarse de que las salidas que no sean conformes con sus requisitos se identifican y se controlan para prevenir su uso o entrega no intencionada.)	No posee un título equivalente	No relación	
8.7.2 Sin título (conservar información documentada sobre salidas no conformes)	No posee un título equivalente	No relación	
9. Evaluación del desempeño			
9.1 Seguimiento, medición, análisis y evaluación	9.1 Seguimiento, medición, análisis y evaluación	Relación media	
9.1.1 Generalidades	No posee un título equivalente	Relación alta	
9.1.2 Satisfacción del cliente	No posee un título equivalente	No relación	
9.1.3 Análisis y evaluación	No posee un título equivalente	Relación baja	
9.2 Auditoría interna	9.2 Auditoría interna	Relación alta	
9.2.1 Sin título (se deben realizan auditorías a intervalos planificados)	9.2.1 Generalidades	Relación alta	A.5.35 Revisión independiente de la seguridad de la información A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información A.8.34 Protección de los sistemas de información durante las pruebas de auditoría
9.2.2 Sin título (la organización debe mantener programas de auditoría, criterios de auditoría, selección de auditores…)	9.2.2 Programa de auditoría interna	Relación alta	
9.3 Revisión por la dirección	9.3 Revisión por la dirección	Relación alta	
9.3.1 Generalidades	9.3.1 Generalidades	Relación alta	
9.3.2 Entradas de la revisión por la dirección	9.3.2 Entradas de la revisión por la dirección	Relación alta	

Continúa Tabla 6 en la siguiente página →

ISO 9001:2015	ISO/IEC 27001:2022	Relación de requisitos de ambos Sistemas de Gestión	Controles ISO/IEC 27001:2022 – Anexo A relacionados a ISO 9001:2015
9.3.3 Salidas de la revisión por la dirección	9.3.3 Salidas de la revisión por la dirección	Relación alta	
10. Mejora			
10.1 Generalidades	10.1 Mejora continua	Relación media	
10.2 No conformidad y acción correctiva	10.2 No conformidad y acción correctiva	Relación alta	
10.2.1 Sin título (cuando ocurra una No conformidad se debe: reaccionar ante la no conformidad, evaluar la necesidad de acciones, implementar cualquier acción necesaria, revisar la eficacia de las acciones…)	No posee un título equivalente	Relación alta	
10.2.2 Sin título (se debe conservar información documentada sobre no conformidades)	No posee un título equivalente	Relación alta	
10.3 Mejora continua	No posee un título equivalente	Relación alta	

Fuente: Elaboración propia a partir de datos de ISO 9001:2015 e ISO/IEC 27001:2022

A partir de la tabla anterior y considerando como normativa base la ISO 9001:2015, se tomaron los puntos desde 4.1 al 10.3 y se verifica el resultado de las relaciones sobre un total de 70 requisitos, es así como se obtiene que 25/70 requisitos se clasifican como relación alta, es decir 37.5%; relación media 7/70, lo que es igual a un 10%; relación baja, 4/70, lo cual es equivalente a 5.7%; sin relación, 34/70, representado como un 48.6%.

Con respecto a los 93 controles del Anexo A de ISO/IEC 27001:2022, se realizó una relación entre cada control y requisitos de ISO 9001:2015 y se identificó afinidad de 22.6% (21/93).

2.4 Marco legal y reglamentario

En un trabajo de investigación es importante considerar el marco legal nacional. Esto implica identificar y describir las leyes y regulaciones relevantes relacionadas a los sistemas integrados de gestión de calidad y seguridad de la información.

2.4.1 Requisitos legales para el Sistema de Gestión de Calidad

Los requisitos legales relacionados al contexto nacional de El Salvador y pertinentes para Aseguradora ABANK con respecto a un Sistema de Gestión de Calidad son los siguientes:

a) Ley de protección al consumidor

La Ley de Protección al Consumidor es la legislación principal que establece los derechos y protecciones generales para los consumidores en El Salvador. Esta legislación aborda una amplia gama de temas vitales para la defensa de los intereses de los consumidores. Entre ellos, se destacan las disposiciones sobre garantías de productos y servicios, garantizando que los consumidores reciban servicios de calidad y que estén protegidos en caso de faltas por parte de los proveedores.

En el Capítulo III se encuentra el apartado "Derecho a la seguridad y a la calidad", donde se establece en el artículo 6 “los productos y servicios puestos en el mercado a disposición de los consumidores no deben implicar riesgos para su vida, salud o seguridad, ni para el medio ambiente, salvo los legalmente admitidos en condiciones normales y previsibles de utilización. Los riesgos que provengan de una utilización previsible de los bienes y servicios, en atención a su naturaleza y de las personas a las que van destinados, deben ser informados previamente a los consumidores por medios apropiados.” (Ley de Protección al Consumidor, 2021).

El propósito de esta ley es garantizar los derechos de los consumidores, buscando establecer un equilibrio justo y garantizar la seguridad jurídica en sus interacciones con los proveedores.

b) Reglamento de protección al consumidor

El Reglamento de Protección del Consumidor, es una normativa secundaria que se emite para complementar y detallar las disposiciones establecidas en la Ley de Protección al Consumidor.

Dentro de los aspectos que se abordan dentro del reglamento están:

- Derechos básicos del consumidor: El reglamento establece los derechos básicos de los consumidores, como el derecho a la protección de la salud y seguridad, el derecho a la información veraz y completa, el derecho a la elección, el derecho a la protección contra la publicidad engañosa, el derecho a la indemnización por daños y perjuicios, etc.
- Información en productos y servicios: El reglamento regula la información que debe proporcionarse a los consumidores sobre los productos y servicios, como las características, el precio, la forma de uso, las instrucciones de seguridad y cualquier otra información relevante para una elección informada.

- Prácticas comerciales desleales: Se prohíben las prácticas comerciales engañosas, abusivas o desleales que puedan perjudicar a los consumidores. Esto incluye la publicidad falsa o engañosa, la manipulación de precios, las cláusulas abusivas en los contratos y otras prácticas injustas.
- Garantías y devoluciones: establece las condiciones para las garantías ofrecidas por los proveedores y los procedimientos para las devoluciones y reclamaciones de los consumidores en caso de productos defectuosos o servicios insatisfactorios.

La ley de protección al consumidor es el marco legal principal que establece los derechos y obligaciones generales de los consumidores y proveedores, mientras que el reglamento de protección al consumidor proporciona pautas y detalles más específicos sobre cómo se aplicará la ley en la práctica. Ambos son importantes para garantizar la protección de los consumidores y asegurar un entorno comercial justo (Reglamento de Protección al Consumidor, 2021).

c) Código de comercio

El código de comercio tiene como función regir cualquier actividad relacionada con los actos de comercio y otras actividades mercantiles. El título X regula los contratos de seguros; el artículo 1,344 del Código de comercio establece “Por el contrato de seguro, la empresa aseguradora se obliga, mediante una prima, a resarcir un daño o a pagar una suma de dinero al verificarse la eventualidad prevista en el contrato”. De igual manera se establece en el título II, capítulo XIV, artículo 362 que la vigilancia y supervisión de empresas de seguro estará a cargo del Estado, de la Superintendencia del Sistema Financiero (Código de comercio, 2021).

d) Normas técnicas para la transparencia y divulgación de la información de las sociedades de seguros (NCM-03)

Estas normas están diseñadas para fortalecer y optimizar las relaciones entre las sociedades de seguros y sus usuarios, asegurados, beneficiarios y contratantes. Su principal objetivo es generar un ambiente de confianza y credibilidad mutua, facilitando una comunicación clara y efectiva sobre los servicios ofrecidos por las entidades aseguradoras. Para lograr este objetivo, las normas establecen directrices específicas sobre la transparencia y la divulgación de información clave relacionada con los productos y servicios de seguros.

En el artículo 8 se establece que las sociedades de seguros deberán informar sobre el servicio formal de atención, para atender por cualquier medio las denuncias o inconformidades de los contratantes, asegurados o beneficiarios, especificando el horario para la atención al público y los medios de comunicación, tales como: teléfono de atención o cabina de servicio, correo electrónico, dirección física de la oficina de atención, entre otros (NCM-03 Normas técnicas para la transparencia y divulgación de la información de las sociedades de seguros, 2019).

2.4.2 Requisitos legales para el Sistema de Gestión de Seguridad de la Información

Entre los elementos legales que Aseguradora ABANK debe cumplir de manera obligatoria en relación con la seguridad de la información, se identificaron varios aspectos clave que constituyen el marco regulatorio y normativo en el cual debe operar. Estos requisitos incluyen:

a) Normas técnicas para la Gestión de la Seguridad de la Información (NRP -23)

Estas normas tienen como objetivo establecer los criterios mínimos necesarios para la gestión integral de la seguridad de la información y la ciberseguridad en las entidades. Basadas en prácticas internacionales reconocidas, estas normas se adaptan a la naturaleza y perfil de riesgo específico de cada entidad, así como al volumen y complejidad de sus operaciones. Además, promueven un enfoque sistemático para identificar, evaluar y mitigar riesgos asociados con la información, garantizando la protección adecuada frente a amenazas emergentes y vulnerabilidades.

En el artículo 4 se establece que las organizaciones “deberán contar con una estructura organizacional acorde a sus productos, servicios, operaciones, tamaño, perfil de riesgos y modelo de negocio, de tal forma que delimite claramente las funciones, roles, responsabilidades y facultades asociadas a la seguridad de la información y la ciberseguridad, así como los niveles de dependencia e interrelación que corresponde con cada una de las demás áreas de la entidad.

Asimismo, las entidades deberán asegurarse de que todo su personal reconozca a la seguridad de la información y ciberseguridad como una de sus responsabilidades, aplicando las medidas de confidencialidad que fueran necesarias.

La información cuya seguridad deberá preservarse, será la que de acuerdo con la clasificación de los activos de información que realice la entidad, requiera tratamiento de aseguramiento o protección.” (NRP-23 Normas técnicas para la Gestión de la Seguridad de la Información, 2020).

b) Ley Especial Contra Actos de Terrorismo

Esta ley tiene como objeto prevenir, investigar, sancionar y erradicar los delitos que se describen en ésta, así como todas sus manifestaciones, incluido su financiamiento y actividades conexas, y que, por la forma de ejecución, medios y métodos empleados, evidencien la intención de provocar estados de alarma, temor o terror en la población, al poner en peligro inminente o afectar la vida o la integridad física o mental de las personas, bienes materiales.

En el artículo 12 literal a) se establece que cualquiera que utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia de seguridad nacional, de entidades nacionales, internacionales o de otro país, será sancionado con pena de prisión de diez a quince años (Ley Especial Contra Actos de Terrorismo, 2006) .

c) Normas Técnicas para la Gestión de la Continuidad del Negocio (NRP-24)

Estas normas tienen como objeto establecer las disposiciones mínimas que deben considerar las entidades para la Gestión de la Continuidad del Negocio y criterios para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías para su respectiva gestión, acordes a prácticas internacionales, el tamaño, naturaleza de sus operaciones, segmentación de negocios y la complejidad organizacional de cada entidad y, de esta forma, fortalecer su gestión de riesgos.

En el artículo 14 de la norma se destaca la importancia de realizar análisis de ciberamenazas y evaluación de riesgos considerando diversas fuentes como geográfico, sociopolítico, pandémico, físico, ambiental y tecnológico.

Además, debe evaluar el impacto, por lo menos, en los siguientes ámbitos: finanzas, clientes, personal, cumplimiento regulatorio y opinión pública. El impacto total de una actividad, proceso, producto o servicio podrá ser cuantificado según el impacto del ámbito en cuestión.

El resultado del análisis de las ciberamenazas puede provocar una alteración de las actividades críticas de las organizaciones, por lo que se elaboran escenarios de interrupción para los que se diseñan estrategias concretas que permitan manejar un incidente de interrupción (NRP-24 Normas Técnicas para la Gestión de la Continuidad del Negocio, 2020).

2.4.3 Requisitos legales para el Sistema de Gestión de Calidad y para el Sistema de Gestión de Seguridad de la Información

a) Normas técnicas para la Gestión Integral de Riesgos de las Entidades Financieras (NRP-20)

Estas normas establecen que las organizaciones deberán contar con un sistema de gestión integral de riesgos, que deberá entenderse como un proceso estratégico realizado por toda la entidad, mediante el cual identifican, miden, controlan, mitigan, monitorean y comunican los distintos tipos de riesgos a los que se encuentran expuestas y las interrelaciones.

El proceso integral para la gestión de riesgos deberá estar debidamente documentado y revisado periódicamente en función de los cambios en el perfil de riesgo de la entidad. (NRP-20 Normas técnicas para la Gestión Integral de Riesgos de las Entidades Financieras, 2020).

En la Tabla 7 se encuentra un resumen del marco legal regulatorio.

Tabla 7. Marco legal del Sistema de Gestión de Calidad y Seguridad de la Información

Año de actualización	Título	Resumen	Emisor	Artículos aplicables
SISTEMA DE GESTIÓN DE CALIDAD				
2023	Ley de protección al consumidor	Establece los derechos y protecciones generales para los consumidores en El Salvador.	Defensoría del consumidor	1, 2, 3, 4, 5, 6, 7, 13B, 18, 19, 20, 27, 40, 41, 42, 43, 44, 45, 46, 47, 48
2021	Reglamento de protección al consumidor	Es una normativa secundaria que se emite para complementar y detallar las disposiciones establecidas en la Ley de Protección al Consumidor.		1, 3, 12, 25, 26, 30, 35

Continúa Tabla 7 en la siguiente página →

Año de actualización	Título	Resumen	Emisor	Artículos aplicables
2021	Código de comercio	Regir cualquier actividad relacionada con los actos de comercio y otras actividades mercantiles.	Ministerio de Justicia	362, 1344-1351
2019	Normas técnicas para la transparencia y divulgación de la información de las sociedades de seguros (NCM-03)	Refuerza las relaciones entre las entidades y los usuarios, asegurados, beneficiarios o contratantes, a efectos de generar confianza entre los mismos, a través de la divulgación de información sobre los servicios que brinden las entidades.	Superintendencia del Sistema Financiero	8
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN				
2020	Normas técnicas para la Gestión de la Seguridad de la Información (NRP - 23)	Establece los criterios mínimos para la gestión para la seguridad de la información y la ciberseguridad de ésta.	Superintendencia del Sistema Financiero	10-31
2006	Ley Especial Contra Actos de Terrorismo	Tiene como objeto prevenir, investigar, sancionar y erradicar los delitos que se describen en ésta.		12
2020	Normas Técnicas para la Gestión de la Continuidad del Negocio (NRP-24)	Establece las disposiciones mínimas que deben considerar las entidades para la Gestión de la Continuidad del Negocio y criterios para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías para su respectiva gestión	Banco Central de Reserva	2, 14
SISTEMA DE GESTIÓN DE CALIDAD Y DE SEGURIDAD DE LA INFORMACIÓN				

Continúa Tabla 7 en la siguiente página →

Año de actualización	Título	Resumen	Emisor	Artículos aplicables
2020	Normas técnicas para la Gestión Integral de Riesgos de las Entidades Financieras (NRP-20)	Establecer las disposiciones mínimas que deben observar las entidades para la gestión integral de riesgos de conformidad con las leyes aplicables y estándares internacionales.	Banco Central de Reserva	2, 4, 5, 6

Fuente: elaboración propia

En síntesis, el capítulo del marco teórico sirvió como base teórica y conceptual para respaldar y contextualizar la investigación, proporcionando un marco de referencia sobre el cual se construyó el estudio. También proporcionó una visión general de los estudios previos realizados en el campo y resalta las brechas en el conocimiento existente.

A continuación, se presenta el marco metodológico donde se describe el tipo de investigación que se realizó. También se explica la población y muestra seleccionada para el estudio, así como los criterios utilizados para su selección. Además, se detallan los métodos y técnicas que se emplearon para recopilar los datos correspondientes a la investigación.

CAPÍTULO III. MARCO METODOLÓGICO

El marco metodológico proporcionó una guía integral para la investigación, definiendo enfoques, técnicas y recursos necesarios para abordar la problemática identificada de manera consistente y responder adecuadamente a las preguntas planteadas en el trabajo de graduación. Baena Paz (2014, pág. 43) declara que "la metodología ejerce el papel de ordenar, se apoya en los métodos, como sus caminos y éstos en las técnicas como los pasos para transitar por esos caminos del pensamiento del pensamiento a la realidad y viceversa".

3.1 Tipo de investigación

El trabajo de graduación se enmarcó en la categoría de investigación aplicada, caracterizada por su enfoque en la resolución de problemas prácticos mediante la aplicación de conocimientos teóricos. En este caso, se buscó ofrecer una propuesta concreta de solución a una problemática identificada, basándose en un modelo teórico sólido. Este modelo se centró en el diseño de un Sistema Integrado de Gestión que combina los estándares de calidad ISO 9001:2015 y de seguridad de la información ISO/IEC 27001:2022.

Según Ñaupas H. et al. (2014) la investigación aplicada es:

> Aquella que basándose en los resultados de la investigación básica, pura o fundamental[10] está orientada a resolver problemas sociales de una comunidad, región o país, como problemas de salud, contaminación, legislación laboral, crisis financieras y otros…

Las problemáticas presentadas por Ñaupas. H son ejemplos de problemáticas sociales reales, por lo que se requiere de soluciones apegadas al contexto y pragmáticas para beneficio de la población, o como en el presente caso, del sujeto de estudio.

Este enfoque de investigación aplicada permitió no solo analizar la teoría y los conceptos relacionados con los sistemas de gestión de calidad y seguridad de la información, sino también poner en práctica estos conocimientos para abordar un desafío real en un contexto específico.

[10] Los tipos de investigación se clasifican, según Ñaupas. H. (2014), como: investigación básica, pura o fundamental y la investigación aplicada o tecnológica; esta primera clasificación desglosa niveles de investigación específicos como investigación exploratoria, descriptiva, explicativa y predictiva.

La investigación se enfocó en proporcionar propuestas de solución a una problemática específica y delimitada, a través de la información que se recopiló como insumo.

3.2 Enfoque o ruta de la investigación

La ruta de investigación para el trabajo de graduación tuvo un enfoque mixto, es decir, fue una combinación entre un enfoque cualitativo y cuantitativo. Se realizó análisis de información desde la perspectiva cualitativa, utilizando metodologías como entrevistas, revisión documental, entre otros; De igual forma a través del enfoque cuantitativo, se analizaron datos por medio de muestreos, cálculos estadísticos, entre otros. De esta manera se obtuvieron los insumos necesarios para establecer una propuesta de solución a la problemática.

Sampieri (2018, Pág. 10) define que los métodos mixtos representan para la investigación:

> Un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos tanto cuantitativos como cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio.

3.3 Alcance o tipo de estudio

Existen diferentes tipos de alcances en el trabajo de graduación, Méndez Álvarez (2020) describe tres categorías según el nivel de conocimiento al que el investigador espera llegar, estos tipos son: “descriptivo, exploratorio y de tipo observación”. Para el presente trabajo se contempló hacer uso de los estudios exploratorios y descriptivos, debido que los primeros permiten familiarizarse con la problemática, descubrir nuevos conocimientos y generar nuevas hipótesis, mientras que los segundos proporcionan una descripción más detallada de un fenómeno o problemática en cuestión.

Sampieri (2018, Pág. 106) describe que el estudio exploratorio “Se lleva a cabo cuando el propósito es estudiar fenómenos y problemas nuevos, desconocidos o poco estudiados”, además, describe que los estudios descriptivos “Tienen como finalidad especificar propiedades y características de conceptos, fenómenos, variables o hechos en un contexto determinado”.

Ambos enfoques son necesarios y complementarios para la investigación debido a su repercusión en la obtención de información del sujeto de estudio.

3.4 Métodos de investigación

En la sección anterior, se proporcionaron detalles sobre el tipo de estudio seleccionado. En este nuevo apartado, se abordó otro concepto crucial para la investigación: los métodos de investigación. Estos constituyen la estrategia a seguir para obtener respuestas lo más precisas posibles, estrechamente vinculadas al contexto real de la organización.

Para el desarrollo del trabajo de graduación se utilizaron los siguientes métodos de investigación, definidos por Méndez Álvarez (2020, pág. 126-128):

- **Método de observación**, proceso de conocimiento por el cual se perciben deliberadamente ciertos rasgos existentes en el objeto de conocimiento.
- **Método deductivo**, Se observan fenómenos generales para identificar particularidades, lo que fue útil en el trabajo de graduación para interpretar resultados cualitativos y cuantitativos obtenidos de varios instrumentos investigativos.
- **Método de análisis**, se da la identificación de cada parte que caracteriza la realidad del sujeto de estudio y la problemática en cuestión, para poder establecer la relación causa-efecto de los elementos de la investigación.
- **Método de síntesis**, cada insumo de información se estudia a partir de este método se dan las conclusiones específicas que dan respuesta al objetivo y las hipótesis planteadas.

3.5 Diseño metodológico

El diseño metodológico, según Sampieri (2018), abarca el plan concebido para adquirir la información necesaria con el propósito de abordar el planteamiento del problema (pág. 150). En el desarrollo de la investigación, se optó por un enfoque no experimental, ya que no se tiene la intención de manipular las variables o fenómenos que causan la problemática.

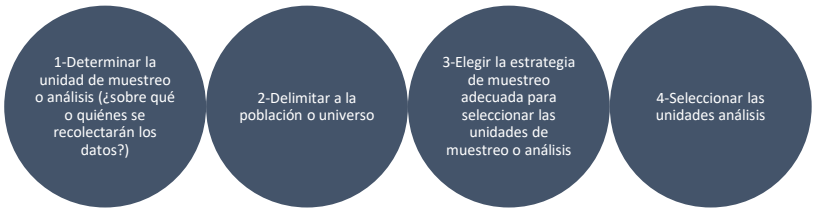
3.6 Determinación de población y muestra

En una investigación, la población se refiere al conjunto completo de elementos o individuos que comparten una característica específica y son objeto de estudio. La muestra, por otro lado, es un subconjunto representativo de la población que se selecciona para ser investigado.

Sampieri comenta: “La población y la unidad de muestreo debe ser consistente con los objetivos y preguntas de investigación” (Sampieri, 2018, Pág. 197).

Para la identificación de la población y la muestra, se utilizaron las etapas del proceso de selección propuesto por Sampieri (2018, pág. 196), representado en la *Figura 13*:

Figura 13. Proceso de selección de población y muestra



Fuente: Adaptado de (Sampieri, 2018).

A partir de la visualización del esquema anterior se estructuró la *Tabla 8*, en la que se representa la acción tomada por cada una de las etapas del proceso de selección de población y muestra, pero ya considerando el presente contexto investigativo:

Tabla 8. Aplicación del proceso de selección de la población y muestra

Nro.	Etapa de proceso	Descripción
1	Determinar la unidad de análisis	Implica identificar y definir claramente la entidad o elemento básico que será sujeto de estudio y análisis dentro de la problemática investigada. Es el proceso de seleccionar la unidad de análisis que será examinada y sobre la cual se recopilarán y analizarán los datos relevantes. En la presente investigación, existen dos unidades de análisis: 1.Personal interno de Aseguradora ABANK. 2. Clientes o asegurados de la organización.
2	Delimitar a la población o universo	Se selecciona la población o universo total por cada unidad de análisis identificada para la investigación.
3	Elegir estrategia o criterio de muestreo adecuado	En la primera fase del proceso de selección de población y muestra, se identifican dos unidades de análisis que participarán en la investigación. Ambas unidades poseen atributos distintivos y particulares que son relevantes para los objetivos del estudio, por lo cual se han definido dos criterios para la selección de una muestra apropiada para cada una de ellas: **Unidad de análisis 1: Personal interno de Aseguradora ABANK.** **Muestreo no probabilístico o dirigido**, Sampieri (2018, pág.200) expone que este tipo de muestreo: > no es mecánico o electrónico, ni con base en fórmulas de probabilidad, sino que depende del proceso de toma de decisiones de un investigador o de un grupo de investigadores y, desde luego, las muestras seleccionadas obedecen a otros criterios. En este estudio, la elección de la muestra se realiza mediante el criterio de juicio o

Continúa Tabla 8 en la siguiente página →

Nro.	Etapa de proceso	Descripción
		conveniencia. Es decir, las muestras son seleccionadas a partir de la evaluación del investigador, quien estima que son representativos y cumplen con los requisitos de información necesarios para llevar a cabo la investigación. **Unidad de análisis 2: Clientes o asegurados de la organización.** **Muestreo probabilístico,** Sampieri (2018, pág.200) define que: > todas las unidades, casos o elementos de la población tienen al inicio la misma posibilidad de ser escogidos para conformar la muestra y se obtienen definiendo las características de la población y el tamaño adecuado de la muestra, y por medio de una selección aleatoria de las unidades de muestreo. Por lo tanto, la fórmula a utilizar se define a partir de un **muestreo probabilístico aleatorio simple**, del cual Méndez Álvarez (2020, Pág.151) define que este método se usa "Cuando una muestra de tamaño n se selecciona de una población de tamaño N, de tal manera que cada muestra posible de tamaño n tiene la misma probabilidad de ser seleccionada", por lo que se utilizará la siguiente fórmula: $$\frac{\frac{Z^2 * p(1-p)}{e^2}}{1 + (\frac{Z^2 * p(1-p)}{e^2 N})}$$ Donde: N= tamaño de la población o el universo Z = nivel de confianza (normalmente entre 95% a 99%[11]). p= probabilidad del éxito (normalmente es 50%) e= margen de error (por lo regular es de 5% o menos)
4	Seleccionar las unidades de muestreo o análisis	Se selecciona muestra a partir del criterio seleccionado.

Fuente: elaboración propia

3.6.1 Unidad de análisis y población

La unidad de análisis se refiere a la entidad, individuo o grupos de personas que se seleccionan y estudian en un proceso de investigación. Debido a las variables de investigación identificadas, se consideraron dos unidades de muestra de la población total; una de las unidades estuvo orientada al personal de la aseguradora y la otra vinculada a los asegurados de la compañía.

[11] El valor del nivel de confianza Z, se define a partir de una puntuación específica, debido que es la cantidad de desviaciones estándar que una proporción determinada se aleja de la media. Para encontrar la puntuación z adecuada se debe hacer uso de tablas específicas, por ejemplo, para un nivel de confianza de 80%, la puntuación en tablas sería de 1.28; para nivel de confianza de 85%, entonces su puntuación es 1.44; 90%, su valor es 1.65; para un valor de confianza de 95%, Z=1.96.

La población total de Aseguradora ABANK es de 71 personas, de la cuales se consideró una unidad de análisis formada por 39 personas; la segunda unidad de muestra consideró a 381 asegurados de la compañía, de un total de 40,000 clientes.

3.6.2 Diseño de la muestra

La muestra es un subgrupo de la población, sobre el cual se recolectaron los datos pertinentes para dar solución al planteamiento del problema (Sampieri, 2018, pág. 196). Del total de 71 empleados de la compañía, se seleccionaron 39 personas; por parte del total de 40,000 asegurados, se seleccionó 381 clientes para conformar la muestra específica de la que se obtuvo información relevante para el desarrollo de la investigación. El detalle la muestra se presenta en la *Tabla 9.*

Tabla 9. Muestra para investigación

Identificación de muestra objetivo para la investigación					
Unidad de análisis 1 - Empleados					
Gerencia/ Dirección	Macroproceso relacionado	Área	Población total de las áreas implicadas en investigación	**Muestra a considerar**	Descripción de cada muestra
Dirección comercial	Comercialización	Dirección	1	**1**	1 Director comercial
		Iniciales	5	**2**	1 Gerente comercial 1 Asistente comercial
		Renovaciones	2	**1**	1 Gerente de renovaciones
		Bancaseguros	2	**1**	1 Asistente comercial
	Mercadeo y comunicaciones	Mercadeo y comunicaciones	1	**1**	1 Encargado de mercadeo y comunicaciones
Dirección técnica		Dirección	1	**1**	1 Director técnico
	Suscripción	Suscripción	3	**1**	1 Analista de suscripción
	Ciclo de siniestros	Reclamos	4	**1**	1 Supervisor de reclamos
		Auditoría médica	2	**1**	1 Auditor médico
	Reaseguro	Reaseguro	1	**1**	1 Analista de reaseguro
	Gestión estratégica	Portafolio de productos	1	**1**	1 Gerente de portafolio de productos
Dirección financiera administrativa		Dirección	1	**1**	1 Director financiero administrativo
	Gestión de la emisión	Operaciones	5	**2**	1 Supervisor de operaciones 1 Técnico de operaciones
	Administración	Archivo	2	**1**	1 Encargado de archivo
		Administración	1	**1**	1 Asistente administrativo
	Contabilidad	Contabilidad	4	**2**	1 Contador general 1 Auxiliar contable
	Cobranzas y tesorería	Cobros	3	**1**	1 Supervisor de cobros
		Tesorería	1	**1**	1 Asistente de tesorería
Gerencia de servicios postventa	Servicios post venta	Gerencia	1	**1**	1 Gerente de servicios post venta
		Atención al cliente	8	**2**	1 Encargado de atención al cliente 1 Oficiales de atención al cliente
		Red médica	2	**1**	1 Analista de red médica

Continúa Tabla 9 en la siguiente página →

Identificación de muestra objetivo para la investigación					
Unidad de análisis 1 - Empleados					
Gerencia/ Dirección	Macroproceso relacionado	Área	Población total de las áreas implicadas en investigación	**Muestra a considerar**	Descripción de cada muestra
		Autorizaciones	5	**2**	1 Supervisor de autorizaciones 1 Oficial de autorizaciones
Auditoría	Control interno	Auditoría	1	**1**	1 Auditor interno
Unidad de riesgos/ Unidad de seguridad de la información y continuidad del negocio		Riesgos	1	**1**	1 Gerente de riesgos
		Seguridad de la información y continuidad del negocio	1	**1**	1 Encargado de seguridad de la información y continuidad del negocio
Gerencia de cumplimiento		Cumplimiento	1	**1**	1 Gerente de cumplimiento
Gerencia de tecnología	Tecnología	Gerencia	1	**1**	1 Gerente de tecnología
		Desarrollo	3	**1**	1 Desarrollador Senior.
		Soporte	1	**1**	1 Auxiliar de tecnología
		Proyectos IT	1	**1**	1 Administrador de proyectos de IT
	Gestión de calidad	Procesos	2	**1**	1 Analista de proceso Senior.
Recursos humanos	Gestión del talento humano	Recursos humanos	1	**1**	1 Encargado de recursos humanos
Gerencia de proyectos estratégicos	Gestión estratégica	Proyectos estratégicos	1	**1**	1 Gerente de proyectos estratégicos
Presidencia		Presidencia	1	**1**	1 Director presidente
		TOTAL	**71**	**39**	
Unidad de análisis 2 – Asegurados					
Asegurados			**40,000**	**381**	$\frac{\frac{Z^2 * p(1-p)}{e^2}}{1 + (\frac{Z^2 * p(1-p)}{e^2 N})}$ Donde: $\frac{\frac{1.96^2 * 0.5(1-0.5)}{0.05^2}}{1 + (\frac{1.96^2 * 0.5(1-0.5)}{0.05^2 * 40{,}000})}$

Fuente: elaboración propia

3.7 Fuentes, técnicas e instrumentos de recolección de datos

Méndez Álvarez (2020, Pág.131) expone las fuentes de información como “hechos o información contenida en documentos, en libros y/o sitios de internet a los que acude el investigador con el propósito de obtener información.

En este propósito se utilizan técnicas para recolectar información". Es decir que las fuentes se refieren a los lugares de donde se obtiene la información (sean estas fuentes primarias o secundarias), las técnicas son los métodos utilizados para recopilar datos (por ejemplo: la observación, entrevistas, entre otros) y los instrumentos son las herramientas específicas utilizadas dentro de esas técnicas (por ejemplo, para la técnica de entrevista se utilizaría de instrumento una guía de preguntas o un cuestionario).

Al combinar estas tres dimensiones, se logró obtener información relevante y precisa para alcanzar el objetivo de la investigación. A continuación, se comparte el detalle de la aplicación en la investigación de las tres dimensiones expuestas en el párrafo anterior:

3.7.1 Fuentes de información

Las fuentes de información son los lugares, medios o recursos de los cuales se obtiene la información necesaria para una investigación. Pueden ser primarias (información original y directamente extraída del sujeto de estudio) o secundarias (información ya publicada o documentada por otros). Para la investigación actual se consideraron en cada una de las fuentes de información los siguientes criterios:

Fuentes primarias: son los datos obtenidos directamente del sujeto de estudio a partir de la recolección de información a través de técnicas y sus instrumentos definidos, tales como entrevistas, revisiones documentales, entre otros. Para el desarrollo de la investigación como fuentes primarias se utilizaron entrevistas, encuestas, revisión documental y observación.

Fuentes secundarias: en la investigación aplica para la información bibliográfica recolectada a través de diferentes fuentes de información, tales como libros, tesis, leyes, normativa, entre otros documentos que agreguen insumos para integrar en la labor investigativa. Se obtendrá información existente relacionada al sujeto de estudio, resumiendo fuentes documentales y trabajo preliminar de campo, con la finalidad de ordenar y clasificar el material recopilado.

3.7.2 Técnicas e instrumento de recolección de datos

La recolección de datos relacionados al trabajo de graduación se realizó por medio de diferentes técnicas e instrumentos.

Rojas Soriano (Rojas, 2013, pág. 92) define "*Los métodos y técnicas son las herramientas metodológicas de la investigación, ya que permiten instrumentar los distintos procesos específicos de ésta.";* de igual forma, Sampieri (2018, pág. 228) establece que los instrumentos de medición son *"recursos que utiliza el investigador para registrar información o datos sobre las variables que se tienen en mente".*

En la *Tabla 10* se detallan las técnicas de recolección de datos que se utilizó durante el desarrollo de la investigación, a partir de las fuentes de información primaria y secundaria.

Tabla 10. Técnicas e instrumentos de recolección de datos

Técnicas e instrumentos de recolección de datos			
Fuente de información	**Técnica**	**Enfoque**	**Instrumento**
Primaria	**Observación**: estrategia de recolección de datos sobre algún aspecto durante la visita de campo al sujeto de estudio.	Cualitativo	**Guía de entrevista:** Se diseñó con preguntas cerradas, los datos se recopilaron en registros de visitas de campo para facilitar su análisis. **Lista de verificación:** Se registró a través de una lista de chequeo los requisitos y controles con los que cumple la organización.
	Entrevistas estructuradas: entrevistas personales como grupales, con una serie de cuestionamientos definidos en una amplia diversidad de instrumentos los cuales se completan a partir de la participación activa de los actores claves del sujeto de estudio.	Cualitativo/ Cuantitativo	
	Revisión documental: revisión documental de la información de la organización con el fin de recopilar insumos para la investigación.		
	Encuesta: recopilación de información por medio de opiniones y valoraciones de una unidad de análisis relacionada al sujeto de estudio.	Cuantitativo	**Cuestionario:** recopilar información a través de un medio de una lista de preguntas orientadas a un público específico, por medio de un medio virtual (Google forms).

Continúa Tabla 10 en la siguiente página →

Técnicas e instrumentos de recolección de datos			
Fuente de información	**Técnica**	**Enfoque**	**Instrumento**
Secundario	**Sistematización bibliográfica:** Se obtendrá información existente relacionada al sujeto de estudio, resumiendo fuentes documentales y trabajo preliminar de campo, con la finalidad de ordenar y clasificar el material recopilado.	Cualitativo	**Ficha de referencia bibliográfica:** proporcionan los datos para escribir la referencia bibliográfica en formato APA, e incluye todas las fuentes documentales consultadas

Fuente: Elaboración propia, a partir de Rojas Soriano, R. (2013, pág. 202-203)

Ir al Apéndice 14 para visualizar las plantillas de los instrumentos de investigación mencionados en la tabla anterior.

3.7.3 Prueba piloto de los instrumentos de recolección de datos

Se realizó una prueba piloto con los líderes de procesos de Aseguradora ABANK con el objetivo de identificar posibles problemas, ajustar los instrumentos según sea necesario y asegurarse de que la recopilación de datos se realice de manera eficiente y efectiva durante la investigación.

En esta reunión la estructuración de cada uno de los instrumentos fue sometida a una rigurosa validación en la que se consideraron los siguientes criterios: estructura de contenido, se verificó que exista el orden y ubicación adecuada de todos los parámetros de información a ser recolectados según el objetivo del instrumento y de la investigación; validez del contenido, es decir que la información que se previó recolectar debió ser coherente con la investigación y su propósito, esta información debió generar valor para la actividad investigativa.

3.7.4 Matriz metodológica de variables, técnicas e instrumentos

En el *Apéndice 5* se visualiza de forma integral la forma en la que se recopilaron los datos necesarios para la investigación, considerando tanto las unidades de análisis y su muestra, como también las variables que se han considerado pertinentes para dar respuesta a la problemática, esto sumado a los métodos técnicas y sus instrumentos que facilitaron la recopilación de información significativa para la investigación.

3.8 Tabulación de datos y análisis de la información

La tabulación de datos y el análisis de la información se llevaron a cabo mediante la representación gráfica de los resultados. Se utilizaron diversos tipos de gráficos, como gráficos de barras, de línea, de radar y de pastel, con el objetivo de ofrecer una visualización clara y comprensible de los datos recopilados y contribuir así a una interpretación efectiva de estos.

Para este propósito, se emplearon herramientas informáticas como Microsoft Word y Excel, que proporcionaron una plataforma eficiente y versátil para la creación de gráficos precisos y detallados. Estas herramientas no solo facilitaron el proceso de tabulación y análisis, sino que también permitieron una síntesis efectiva de los datos obtenidos a través de los métodos e instrumentos de investigación descritos previamente. De esta manera, se logró una presentación visualmente atractiva y fácil de interpretar de los hallazgos del estudio, lo que contribuyó significativamente a la comprensión y comunicación de los resultados obtenidos.

La metodología para la tabulación y análisis de la información se basó en las etapas reflejadas en la *Tabla 11* a continuación:

Tabla 11. Metodología para la tabulación y análisis de la información

Etapa	Fase	Descripción
Tabulación, ordenamiento y procesamiento de la información	Tabulación	La tabulación de información se refiere al proceso de organizar y presentar datos de manera sistemática en forma de una tabla o matriz.
	Ordenamiento	Proceso de organizar los datos de manera sistemática y estructurada según un criterio específico. Es una técnica que permite clasificar y reorganizar los datos de forma coherente, lo que facilita su análisis, búsqueda y comprensión.
	Procesamiento	Los datos se someten a operaciones específicas para transformarlos y obtener información valiosa. Esto puede incluir cálculos cuantitativos, como análisis estadístico o valoraciones cualitativas sobre los datos, como por ejemplo la interpretación.

Continúa Tabla 11 en la siguiente página →

Etapa	Fase	Descripción
	Presentación de resultados	Uso de gráficos de barras, de línea, gráfico de radar y de pastel para presentar datos en la investigación.
Análisis de resultados	Identificación de las variables	Se identifica a qué variables de la problemática corresponde la información obtenida.
	Verificación de preguntas de investigación	Se verificará la información obtenida y procesada con respecto a las preguntas de investigación planteadas.
	Verificación de objetivos	Conforme a la información obtenida por medio del análisis realizado, se contrastan los resultados con los objetivos, se verificará si se cumplieron, y si se alcanzan de manera satisfactoria.
	Verificación de hipótesis	Se realiza con el propósito de conocer si el hecho, evento o situación propuesta se presenta en la realidad del sujeto de estudio y la problemática. Este análisis se realizará de la misma forma que con los objetivos y las preguntas de investigación.
	Establecimiento de conclusiones	Se concluye a partir de los análisis de información previamente realizados.

Fuente: adaptado de Méndez Álvarez C. (2020). Pág. 142

3.9 Matriz metodológica de consistencia de la investigación

La matriz metodológica de consistencia de la investigación estableció la relación entre el diseño metodológico y la formulación del problema tomando en cuenta los objetivos y la hipótesis definida para el sujeto de estudio. La matriz es una herramienta importante para verificar si los elementos clave de su estudio se corresponden entre sí y se ajustan a la lógica del diseño general de la investigación (*Ver Apéndice 6*).

3.10 Respuestas o refutaciones a las hipótesis formuladas

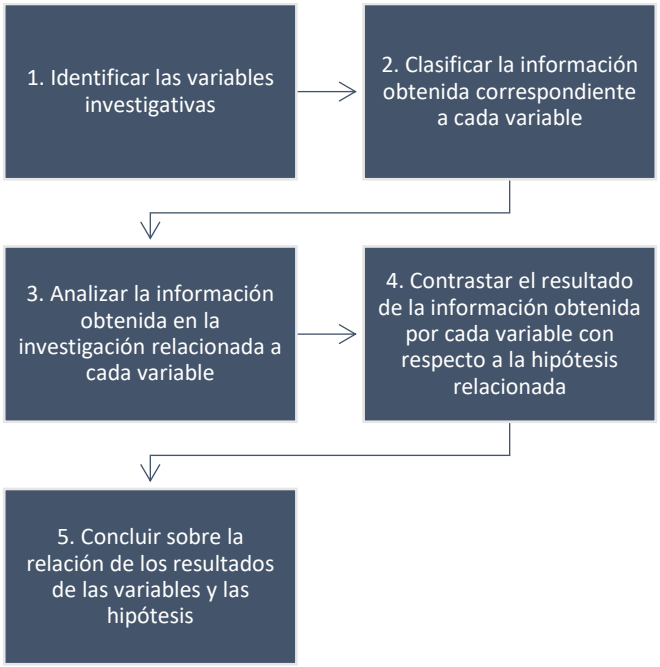
La investigación se propuso abordar de manera exhaustiva las hipótesis planteadas, asegurándose de expresarlas con claridad y coherencia, y vincularlas de manera lógica con la información recopilada a lo largo del estudio.

Este proceso implicó la implementación de diversas actividades de recolección de datos, que incluyeron entrevistas, observaciones y revisión documental, tal como se detalla en el apartado 3.7.2 del documento bajo el título "Técnicas e instrumentos de recolección de datos".

Las hipótesis formuladas fueron evaluadas minuciosamente en relación con cada uno de los resultados obtenidos de los indicadores estipulados para la investigación. En palabras de Méndez Álvarez (2020, Pág.175), "La verificación de hipótesis se realiza con el propósito de conocer si el hecho, evento o situación propuesta se presenta en realidad en este objeto de conocimiento". Este proceso de evaluación y contrastación permitió validar o refutar las hipótesis planteadas, contribuyendo así a la solidez y robustez de los hallazgos obtenidos en el estudio.

Dado el enfoque aplicado de la investigación, con un alcance exploratorio y descriptivo, y considerando que el contexto y los objetivos del estudio no están directamente relacionados con un ámbito científico específico, no se optó por llevar a cabo una prueba de hipótesis con el mismo nivel de rigurosidad estadística que otros estudios centrados en temas científicos. Sin embargo, se siguió una metodología que aseguró el análisis de los resultados de acuerdo con las hipótesis planteadas, permitiendo así determinar su validez en el contexto del estudio. La metodología se refleja en la Figura *14*:

Figura 14. Proceso para la verificación de las hipótesis



Fuente: Adaptado de Méndez Álvarez, C. (2020, pág. 176).

3.11 Redacción y presentación de los resultados

La presentación de resultados tiene como objetivo comunicar de manera clara los datos recolectados en la investigación. Se redactó la información para garantizar coherencia y fluidez, destacando los aspectos relevantes. Se utilizaron tablas, gráficos y figuras según APA para facilitar la comprensión visual. La organización de los resultados sigue un enfoque lógico y ordenado, esencial para una presentación accesible. Este apartado fue crucial, transmitiendo efectivamente las conclusiones y contribuciones en el mercado asegurador, sirviendo como base para investigaciones relacionadas a la misma temática.

Méndez Álvarez (2020, Pág.175) afirma que: "La presentación de los resultados en un informe debe ser concisa, y además tener un gran soporte en la información procesada y analizada.

3.12 Resultados

3.12.1 Aplicación de instrumentos seleccionados y descripción de resultados

En las próximas páginas se detallan los diversos instrumentos empleados durante la realización de la investigación aplicada, en conjunto a los resultados adquiridos en el proceso para dar respuesta a las 4 variables y sus indicadores establecidos.

Las calificaciones que fueron utilizadas para realizar las valoraciones ante la lista de verificación se basaron en los siguientes intervalos:

- Se cumple en su totalidad = hasta 100%.
- Cumple medianamente bien = hasta 50%.
- Se tiene una noción vaga del cumplimiento a requisito = hasta 30%.
- No se cumple en su totalidad = 0%.

i. Resultados de variable: Grado de conformidad con respecto a requisitos de Calidad según ISO 9001:2015 (Variable Nro.1)

Instrumento: lista de verificación.

La lista de verificación se utilizó para verificar el grado de conformidad del contexto actual de Aseguradora ABANK en contraste a los requisitos de la normativa ISO 9001:2015.

La plantilla utilizada se estructuró de tal forma que abarque cada uno de los 7 capítulos del documento normativo partiendo del capítulo 4 “Contexto de la organización” hasta el capítulo 10 “Mejora continua”. El llenado de éste se realizó al hacer contacto con la unidad de procesos y la gerencia de tecnología de la aseguradora y realizando las preguntas correspondientes. (Ver Apéndice 13 para visualizar la plantilla de la lista de verificación y el detalle de las respuestas).

La lista de verificación se realizó a: Analista de procesos Senior. y Gerente de Tecnología.

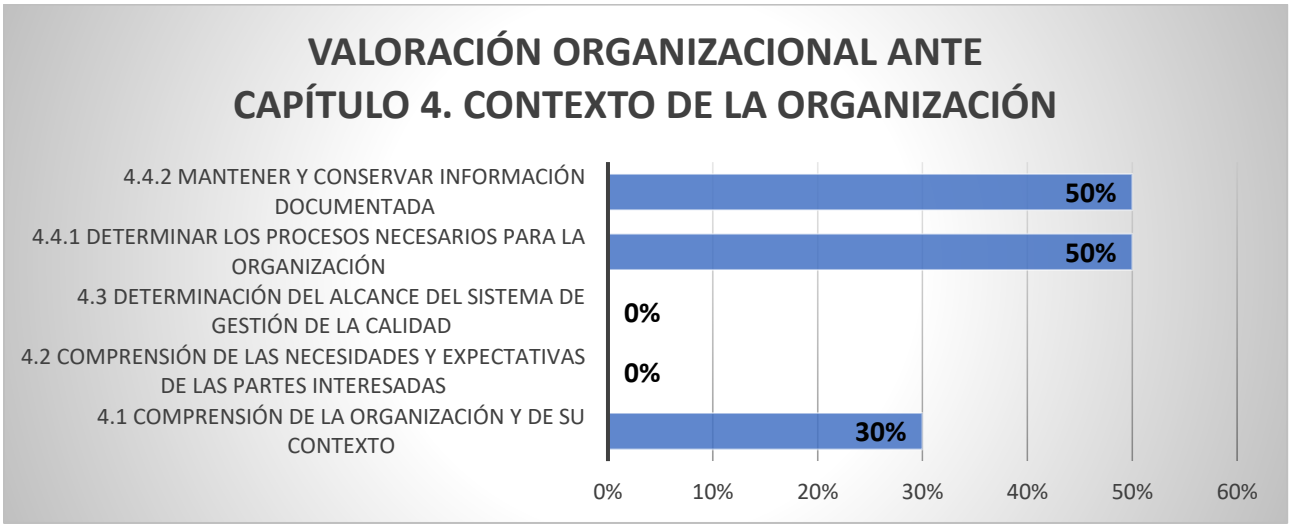
- Capítulo 4. Contexto de la organización

Tabla 12. Lista de verificación-Capítulo 4. Contexto de la organización

Capítulo de norma	Punto de norma	Valoración
4. Contexto de la Organización	4.1 Comprensión de la organización y de su contexto	30%
4. Contexto de la Organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	0%
4. Contexto de la Organización	4.3 Determinación del alcance del sistema de gestión de la calidad	0%
4. Contexto de la Organización	**4.4 Sistema de gestión de la calidad y sus procesos**	
4. Contexto de la Organización	4.4.1 Determinar los procesos necesarios para la organización	50%
4. Contexto de la Organización	4.4.2 Mantener y conservar información documentada	50%

Fuente: elaboración propia

Figura 15. Capítulo 4. Contexto de la organización – resultados



Fuente: elaboración propia

Análisis: El resultado promedio fue del 26% en el capítulo 4 “contexto de la organización” de la normativa ISO 9001:2015. El análisis reveló una disparidad en los resultados. Mientras que se ha logrado un avance del 30% en la comprensión de la organización y su contexto, los aspectos cruciales de la comprensión de las necesidades y expectativas de las partes interesadas, así como la determinación del alcance del sistema de gestión de calidad, muestran un bajo 0%. No obstante, se ha alcanzado un nivel medio del 50% en la determinación de procesos necesarios y el mantenimiento de información.

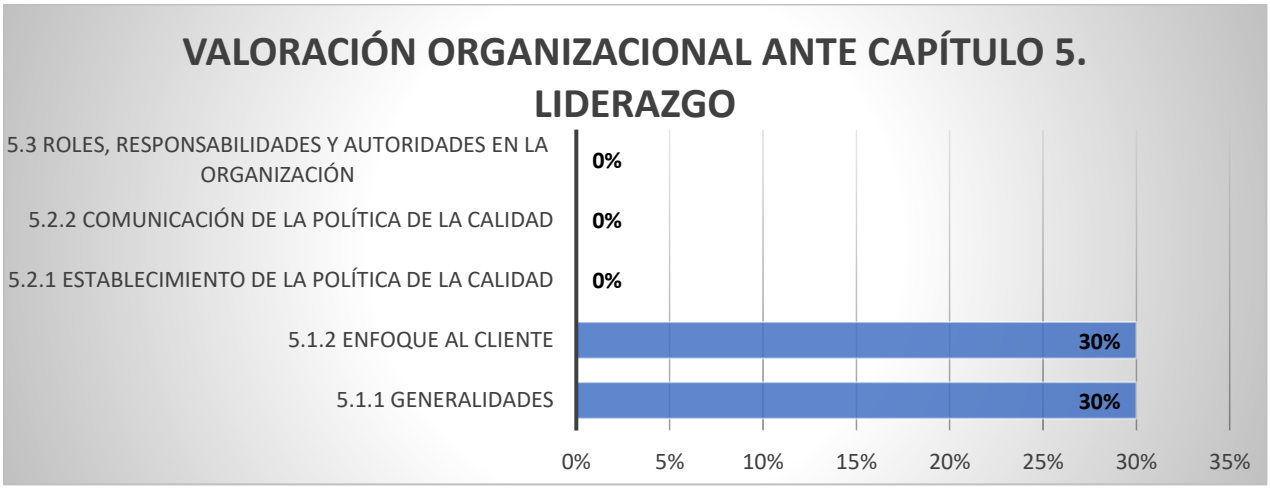
- Capitulo 5. Liderazgo

Tabla 13. Lista de verificación - Capítulo 5. Liderazgo

Capítulo de norma	Punto de norma	Valoración
5. Liderazgo	**5.1 Liderazgo y compromiso**	
5. Liderazgo	5.1.1 Generalidades	30%
5. Liderazgo	5.1.2 Enfoque al cliente	30%
5. Liderazgo	**5.2 Política**	
5. Liderazgo	5.2.1 Establecimiento de la política de la calidad	0%
5. Liderazgo	5.2.2 Comunicación de la política de la calidad	0%
5. Liderazgo	5.3 Roles, responsabilidades y autoridades en la organización	0%

Fuente: elaboración propia

Figura 16. Capítulo 5. Liderazgo – resultados



Fuente: elaboración propia

Análisis: El resultado promedio fue del 12% en el capítulo 5 “liderazgo” de la normativa ISO 9001:2015. Los resultados manifestaron un progreso desigual en diferentes áreas clave. Tanto las generalidades como el enfoque al cliente reflejan un avance del 30%, indicando cierta conciencia sobre estos aspectos fundamentales. Sin embargo, el establecimiento y la comunicación de la política de calidad, junto con la definición de roles, responsabilidades y autoridades en la organización, exhiben un nivel bajo del 0%.

- Capítulo 6. Planificación

Tabla 14. Lista de verificación - Capítulo 6. Planificación

Capítulo de norma	Punto de norma	Valoración
6. Planificación	**6.1 Acciones para abordar riesgos y oportunidades**	
6. Planificación	6.1.1 Al planificar el SGC la organización debe considerar que se puedan lograr los resultados previstos, aumentar defectos deseables, mejora.	30%
6. Planificación	6.1.2 Planificar las acciones para abordar riesgos y oportunidades	0%
6. Planificación	**6.2 Objetivos de la calidad y planificación para lograrlos**	
6. Planificación	6.2.1 Establecer objetivos de calidad	0%
6. Planificación	6.2.2 Al determinar los objetivos se debe planificar: qué se hará, recursos, responsables, cuándo se finalizará, evaluación de resultados	0%
6. Planificación	6.3 Planificación de los cambios	0%

Fuente: elaboración propia

Figura 17. Capítulo 6. Planificación – resultados

Fuente: elaboración propia

Análisis: El resultado promedio fue del 6% en el capítulo 6 "planificación" de la normativa ISO 9001:2015 resalta un desempeño diverso en sus distintos apartados. Si bien el proceso de acciones para abordar riesgos y oportunidades muestra un avance del 30%, indicando cierto nivel de consciencia en esta área, los aspectos de planificación de cambios, gestión de riesgos y oportunidades, junto con la consideración de objetivos de calidad, gestión del cambio, exhiben un progreso de 0%.

- Capitulo 7. Apoyo

Tabla 15. Lista de verificación - Capítulo 7. Apoyo

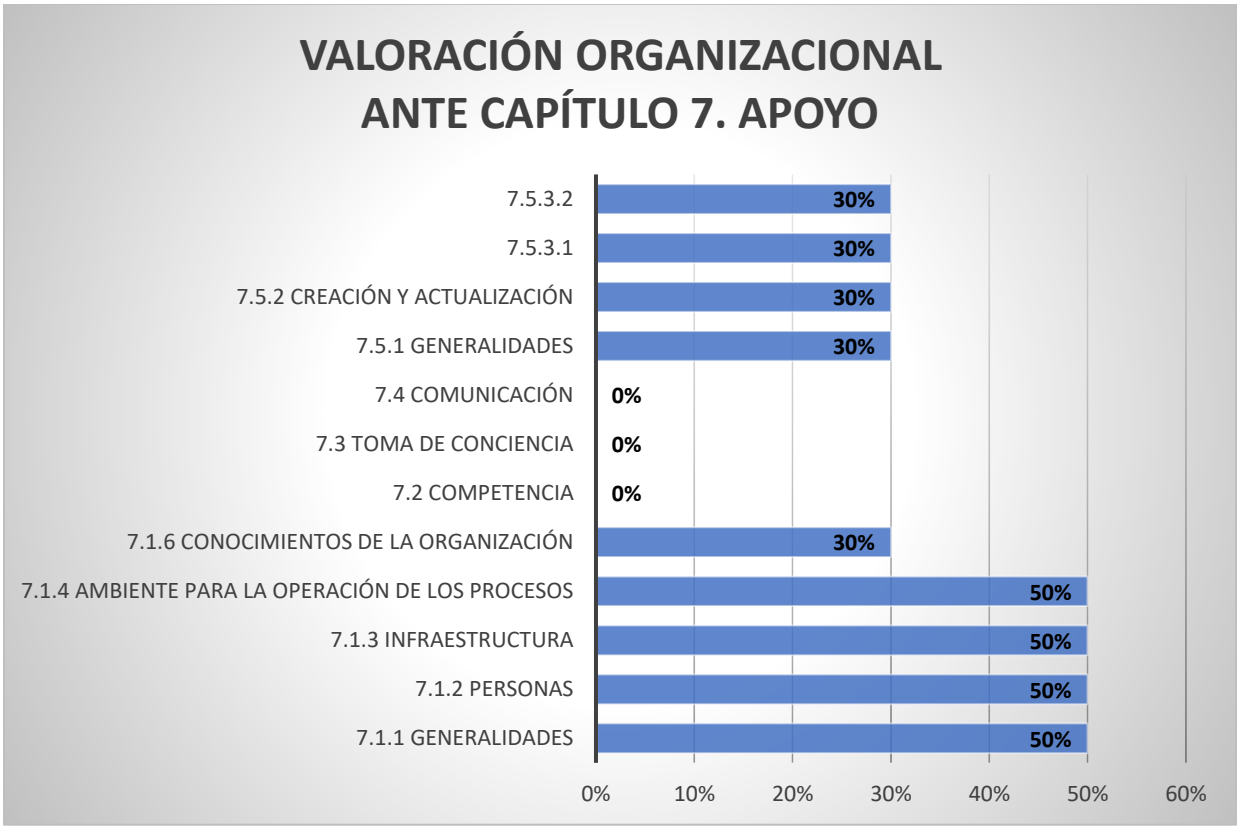
Capítulo de norma	Punto de norma	Valoración
7. Apoyo	**7.1 Recursos**	
7. Apoyo	7.1.1 Generalidades	50%
7. Apoyo	7.1.2 Personas	50%
7. Apoyo	7.1.3 Infraestructura	50%
7. Apoyo	7.1.4 Ambiente para la operación de los procesos	50%
7. Apoyo	**7.1.5 Recursos de seguimiento y medición**	

Continúa Tabla 15 en la siguiente página →

Capítulo de norma	Punto de norma	Valoración
7. Apoyo	7.1.6 Conocimientos de la organización	30%
7. Apoyo	7.2 Competencia	0%
7. Apoyo	7.3 Toma de conciencia	0%
7. Apoyo	7.4 Comunicación	0%
7. Apoyo	7.5.1 Generalidades	30%
7. Apoyo	7.5.2 Creación y actualización	30%
7. Apoyo	**7.5.3 Control de la información documentada**	
7. Apoyo	7.5.3.1 Esté disponible y sea idónea para su uso, está protegida adecuadamente.	30%
7. Apoyo	7.5.3.2 Distribución, acceso, recuperación y uso, almacenamiento y preservación, control de cambios, conservación y disposición.	30%

Fuente: elaboración propia

Figura 18. Capítulo 7. Apoyo – resultados



Fuente: elaboración propia

Análisis: El resultado promedio fue del 29% en el capítulo 7 “apoyo” de la normativa ISO 9001:2015, lo cual refleja un conjunto de resultados variados en diferentes aspectos. La identificación de los procesos y sus interacciones, los criterios de control, la asignación de recursos y la competencia del personal alcanzan un nivel del 50%, indicando una comprensión y despliegue relativamente sólidos en estas áreas.

No obstante, el proceso de revisión de la adecuación y eficacia del sistema muestra un nivel del 30%, señalando oportunidades para fortalecer este proceso crucial. Por otro lado, los aspectos de diseño y desarrollo, control de producción y prestación de servicios, liberación de productos y servicios, y control de las actividades de producción y servicio presentan un progreso bajo del 0%. Además, los procesos relacionados con la propiedad del cliente, el manejo de productos no conformes y las acciones correctivas y preventivas exhiben un nivel del 30%.

- Capítulo 8. Operación

Tabla 16. Lista de verificación - Capítulo 8. Operación

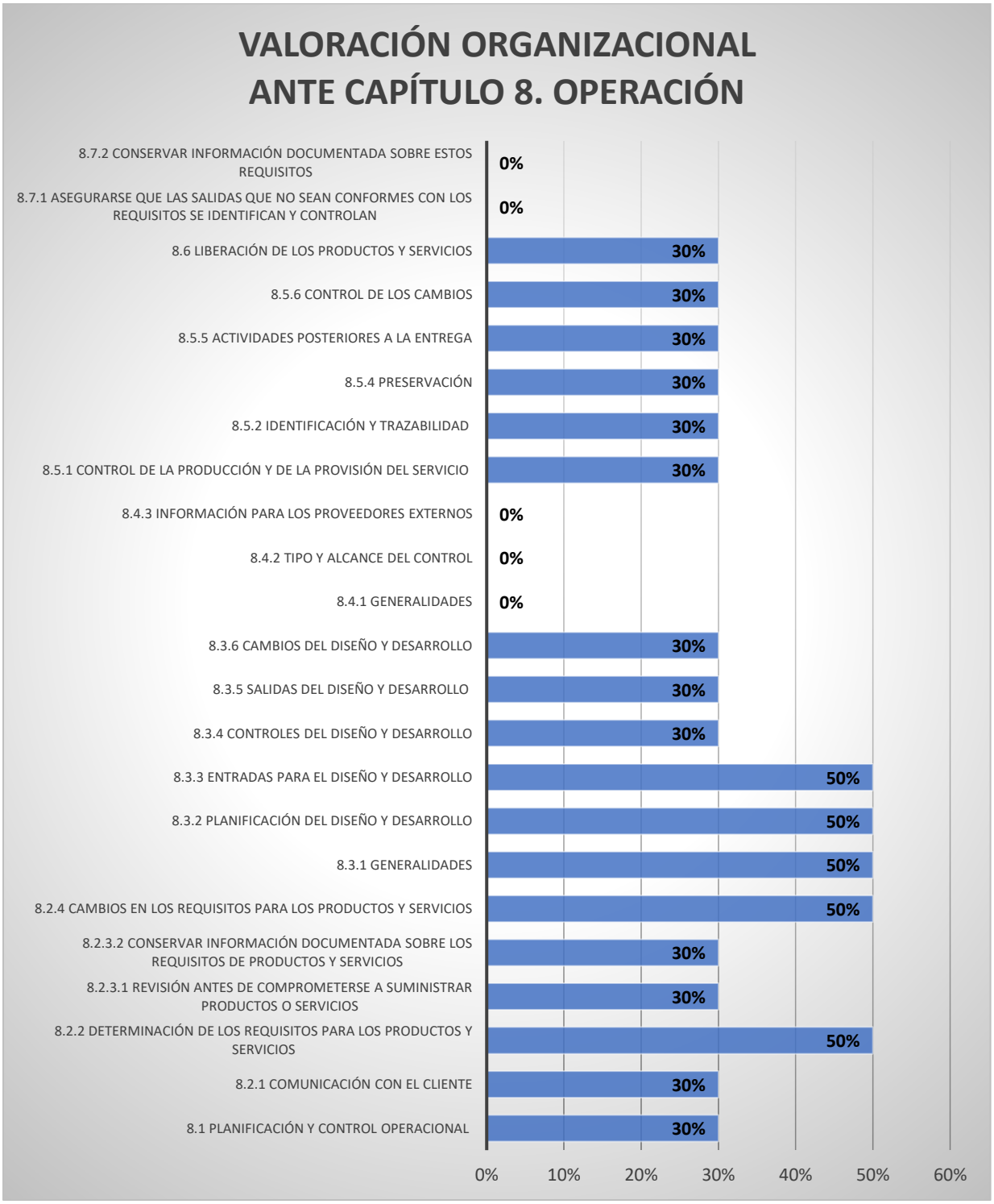
Capítulo de norma	Punto de norma	Valoración
8.Operación	8.1 Planificación y control operacional	30%
8.Operación	**8.2 Requisitos para los productos y servicios**	
8.Operación	8.2.1 Comunicación con el cliente	30%
8.Operación	8.2.2 Determinación de los requisitos para los productos y servicios	50%
8.Operación	**8.2.3 Revisión de los requisitos para los productos y servicios**	
8.Operación	8.2.3.1 Revisión antes de comprometerse a suministrar productos o servicios	30%
8.Operación	8.2.3.2 Conservar información documentada sobre los requisitos de productos y servicios	30%
8.Operación	8.2.4 Cambios en los requisitos para los productos y servicios	50%
8.Operación	**8.3 Diseño y desarrollo de los productos y servicios**	
8.Operación	8.3.1 Generalidades	50%
8.Operación	8.3.2 Planificación del diseño y desarrollo	50%
8.Operación	8.3.3 Entradas para el diseño y desarrollo	50%

Continúa Tabla 16 en la siguiente página →

Capítulo de norma	Punto de norma	Valoración
8.Operación	8.3.4 Controles del diseño y desarrollo	30%
8.Operación	8.3.5 Salidas del diseño y desarrollo	30%
8.Operación	8.3.6 Cambios del diseño y desarrollo	30%
8.Operación	**8.4 Control de los procesos, productos y servicios suministrados externamente**	
8.Operación	8.4.1 Generalidades	0%
8.Operación	8.4.2 Tipo y alcance del control	0%
8.Operación	8.4.3 Información para los proveedores externos	0%
8.Operación	**8.5 Producción y provisión del servicio**	
8.Operación	8.5.1 Control de la producción y de la provisión del servicio	30%
8.Operación	8.5.2 Identificación y trazabilidad	30%
8.Operación	8.5.4 Preservación	30%
8.Operación	8.5.5 Actividades posteriores a la entrega	30%
8.Operación	8.5.6 Control de los cambios	30%
8.Operación	8.6 Liberación de los productos y servicios	30%
8.Operación	**8.7 Control de las salidas no conformes**	
8.Operación	8.7.1 Asegurarse que las salidas que no sean conformes con los requisitos se identifican y controlan	0%
8.Operación	8.7.2 Conservar información documentada sobre estos requisitos	0%

Fuente: elaboración propia

Figura 19. Capítulo 8. Operación – resultados



Fuente: elaboración propia

Análisis: El resultado promedio fue del 28% en el capítulo 8 “operación” de la normativa ISO 9001:2015, revela una diversidad de resultados en los diferentes aspectos. Se han alcanzado niveles del 50% en múltiples áreas, incluyendo la determinación de requisitos para productos y servicios, el diseño y desarrollo de productos y servicios, así como la evaluación de proveedores y el control de servicios suministrados externamente.

Además, los procesos relacionados con el control de producción y provisión de servicios, la identificación y trazabilidad de productos y servicios, y la propiedad del cliente han logrado igualmente un nivel del 50%. Sin embargo, otras áreas como la revisión de diseño y desarrollo, la validación de procesos y el control de cambios alcanzan un nivel del 30%. Aunque existen resultados bajos del 0% en áreas como la información post entrega a los clientes y la liberación de productos y servicios, en conjunto, estos resultados subrayan la necesidad de mejorar la planificación y el control de procesos.

- Capitulo 9. Evaluación del desempeño

Tabla 17. Lista de verificación - Capítulo 9. Evaluación del desempeño

Capítulo de norma	Punto de norma	Valoración
9. Seguimiento y evaluación	**9, Evaluación del desempeño**	
9. Seguimiento y evaluación	**9.1 Seguimiento, medición, análisis y evaluación**	
9. Seguimiento y evaluación	9.1.1 Generalidades (indicadores de desempeño)	0%
9. Seguimiento y evaluación	9.1.2 Satisfacción del Cliente	0%
9. Seguimiento y evaluación	9.1.3 Análisis y evaluación	0%
9. Seguimiento y evaluación	**9.2 Auditoría interna**	
9. Seguimiento y evaluación	9.2.1 Realizar auditorías internas planificadas	0%
9. Seguimiento y evaluación	9.2.2 Establecer programas de auditoría, definir criterios de auditorías y alcance, seleccionar a los auditores…	0%
9. Seguimiento y evaluación	**9.3 Revisión por la dirección**	
9. Seguimiento y evaluación	9.3.1 Generalidades	0%

Continúa Tabla 17 en la siguiente página →

Capítulo de norma	Punto de norma	Valoración
9. Seguimiento y evaluación	9.3.2 Entradas de la revisión por la dirección	0%
9. Seguimiento y evaluación	9.3.3 Salidas de la revisión por la dirección	0%

Fuente: elaboración propia

Figura 20. Capítulo 9. Seguimiento y evaluación – resultados

Fuente: elaboración propia

Análisis: El resultado promedio fue del 0% en el capítulo 9 “seguimiento y evaluación” de la normativa ISO 9001:2015, lo cual refleja resultados consistentemente bajos en todas las áreas evaluadas. Tanto la evaluación del desempeño del sistema de gestión como la auditoría interna, la revisión por la dirección y la mejora continua han alcanzado un nivel del 0%.

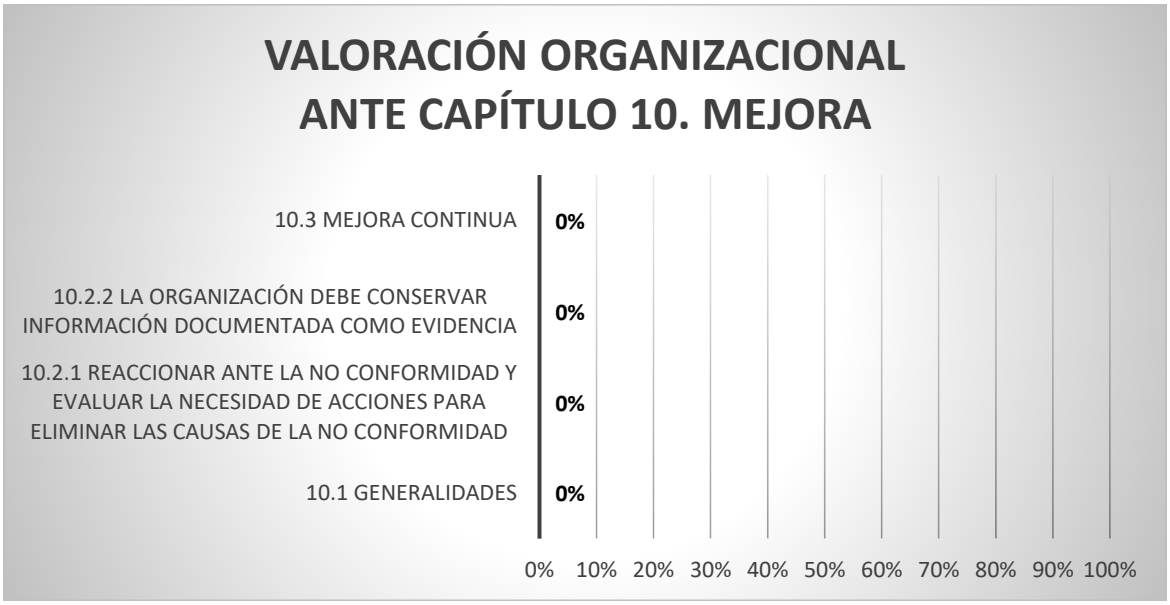
- Capítulo 10. Evaluación del desempeño

Tabla 18. Lista de verificación - Capítulo 10. Mejora

Capítulo de norma	Punto de norma	Valoración
10. Mejora	10.1 Generalidades	0%
10. Mejora	**10.2 No conformidades y acción correctiva**	
10. Mejora	10.2.1 Reaccionar ante la no conformidad y evaluar la necesidad de acciones para eliminar las causas de la no conformidad	0%
10. Mejora	10.2.2 La organización debe conservar información documentada como evidencia	0%
10. Mejora	10.3 Mejora continua	0%

Fuente: elaboración propia

Figura 21. Capítulo 10. Mejora – resultados



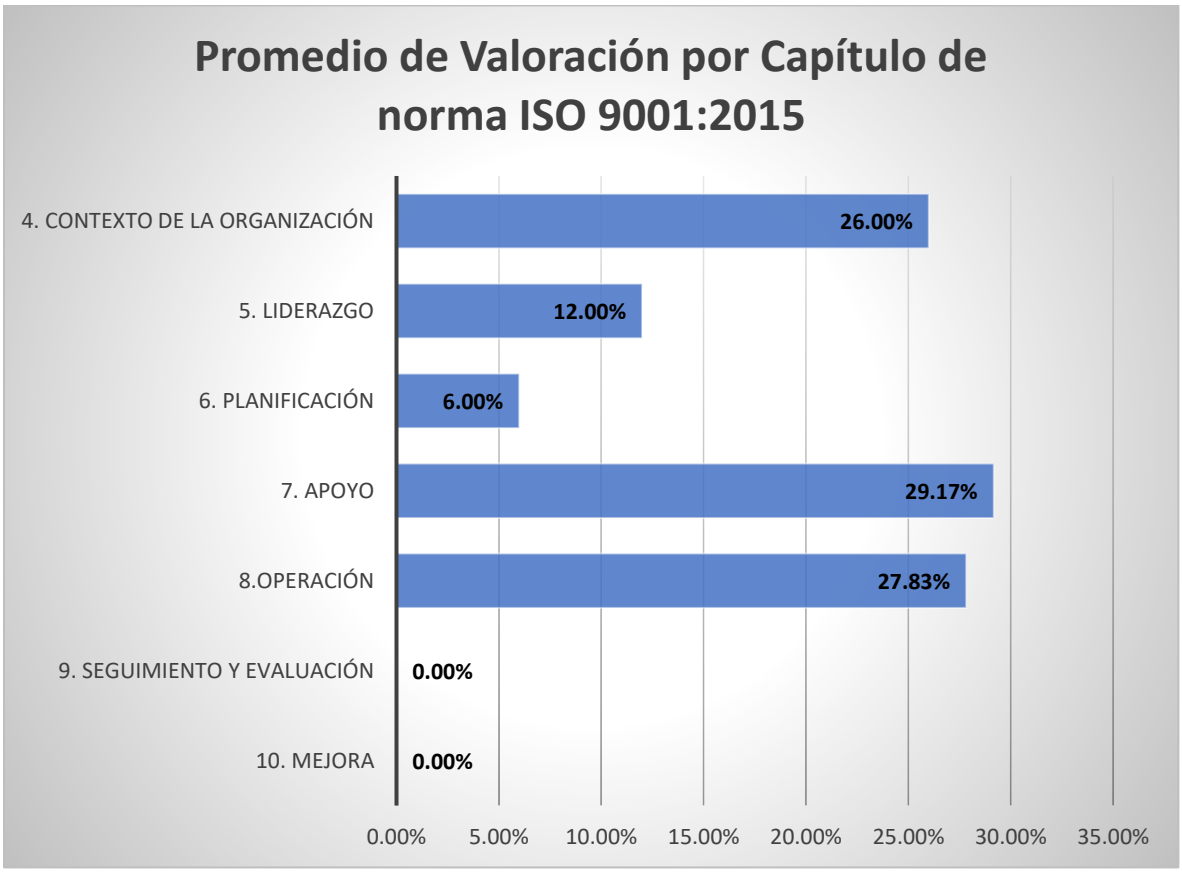
Fuente: elaboración propia

Análisis: El resultado promedio fue del 0% en el capítulo 10 “mejora” de la normativa ISO 9001:2015, reveló un bajo rendimiento en todas las áreas evaluadas, tanto la mejora continua del sistema de gestión, la no conformidad y la acción correctiva, así como la acción preventiva, reflejaron un nivel del 0%.

Estos resultados señalan la necesidad de implementar un enfoque más sólido en la detección, corrección y prevención de problemas en la organización.

- Resultado de todos los capítulos

Figura 22.– consolidado de resultados



Fuente: elaboración propia

Análisis final: El resultado promedio de todos los capítulos de la normativa ISO 9001:2015 es de 14.4%. Mientras el capítulo 4 obtuvo un 26% indicando cierto entendimiento, pero con margen para mejoras, el capítulo 5 marcó un 12% apuntando a desafíos en su implementación. En el capítulo 6 se registró un 6%, resaltando áreas cruciales que requieren atención.

El capítulo 7 alcanzó un 29.17%, sugiriendo un progreso mayor pero aun necesitando mejoras. El capítulo 8 llegó al 27.83%, demostrando un nivel medio de implementación. Por otro lado, los capítulos 9 y 10, ambos con un 0%, indican la urgencia de enfocar esfuerzos en la implementación y mejora de estos aspectos.

ii. Resultados de variable: Satisfacción de las necesidades y expectativas de los clientes (Variable Nro. 2)

Instrumento: cuestionario.

Se diseñó una encuesta que se aplicó a 381 clientes, dicho instrumento se realizó a través de un formulario digital (Google Forms) el cual se solicitó completar a los asegurados que visitaban las instalaciones de la aseguradora, en dicha actividad se les invitaba a compartir su correo electrónico para enviarle la encuesta de satisfacción, el proceso llenado de clientes se llevó a cabo durante 2 meses, en tres ocasiones ambos investigadores nos abocamos a las instalaciones de la aseguradora, y las demás ocasiones en servicio al cliente se les comentaba sobre la encuesta. Dicha encuesta estaba conformada por 7 preguntas, estas interrogantes tenían el objetivo de conocer la percepción que tenían los clientes de Aseguradora ABANK con respecto a sus servicios. (Ver Apéndice 15, para visualizar una muestra de las encuestas digitales realizadas y el correo enviado a los asegurados). Los resultados obtenidos se presentan a continuación:

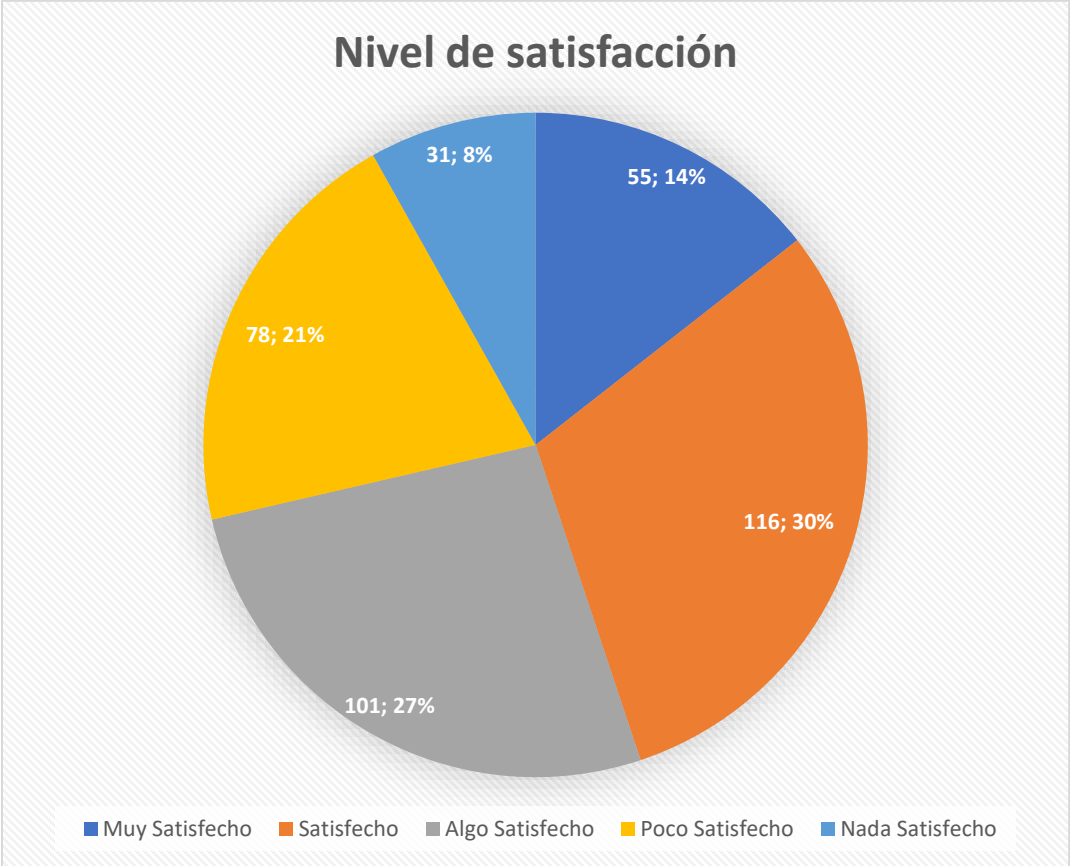
1) ¿Qué calificación le darías a los servicios y cobertura que has recibido como asegurado(a)?

Tabla 19. Opinión de los clientes sobre los servicios y cobertura de la aseguradora

Nivel de satisfacción	Cantidad de clientes	Porcentaje
Muy Satisfecho	55	14.4%
Satisfecho	116	30.4%
Algo Satisfecho	101	26.5%
Poco Satisfecho	78	20.5%
Nada Satisfecho	31	8.1%
Total	381	100%

Fuente: elaboración propia

Figura 23. Nivel de satisfacción con respecto a los servicios y cobertura de Aseguradora ABANK



Fuente: elaboración propia

Análisis: De acuerdo con los resultados de la encuesta realizada sobre la satisfacción de los clientes con respecto a los servicios y coberturas de la aseguradora, de un total de 381 clientes encuestados, un notable 14.4% expresó estar "muy satisfecho" con los servicios proporcionados. Además, un significativo 30,4% indicó sentirse "satisfecho", lo que refleja un nivel de satisfacción generalmente positivo.

Por otro lado, un 26,5% de los encuestados manifestó estar "algo satisfecho", mientras que un 20,5% señaló estar "poco satisfecho". Es importante destacar que un 8.1% de los clientes indicaron que están "nada satisfechos".

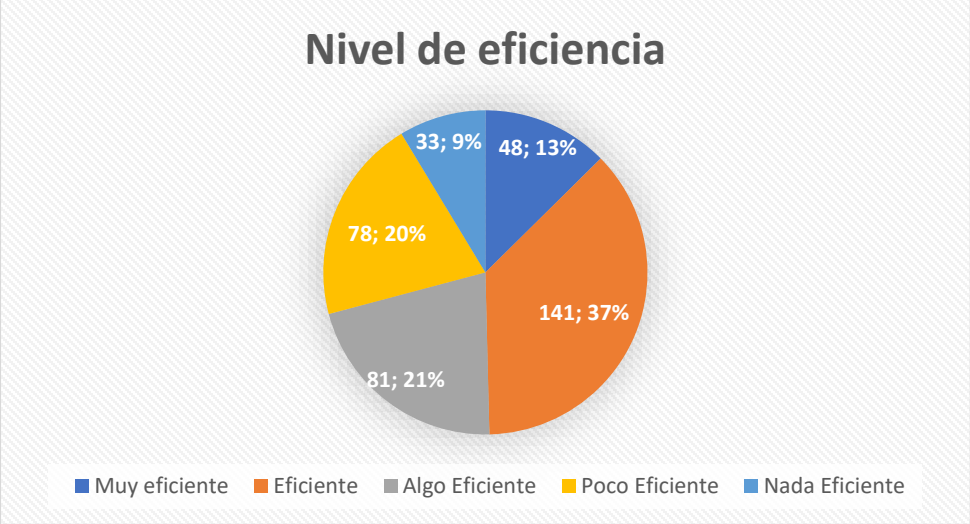
2) ¿Cómo calificarías la eficiencia de la atención al cliente proporcionada por la compañía de seguros?

Tabla 20. Opinión sobre la eficiencia de la atención al cliente proporcionada por la aseguradora

Nivel de eficiencia	Cantidad de clientes	Porcentaje
Muy eficiente	48	12.6 %
Eficiente	78	20.5%
Algo Eficiente	141	37%
Poco Eficiente	81	21.3%
Nada Eficiente	33	8.7%
Total	381	100%

Fuente: elaboración propia

Figura 24. Nivel de la eficiencia de la atención al cliente proporcionada por la aseguradora



Fuente: elaboración propia

Análisis: Según los resultados de la encuesta sobre el nivel de eficiencia en la atención al cliente, basados en las respuestas de 381 clientes encuestados, se destaca que un 12.6% de los participantes consideran que la atención al cliente era "muy eficiente". Asimismo, un 20.5% de los encuestados opinaron que era "eficiente", lo que indica un nivel positivo de satisfacción en cuanto a la eficiencia percibida en el servicio.

Por otro lado, un considerable 37% de los clientes manifestó que la atención era "algo eficiente", mientras que un 21,3% la calificó como "poco eficiente". Es importante señalar que un 8,7% de los encuestados opinó que la atención al cliente era "nada eficiente".

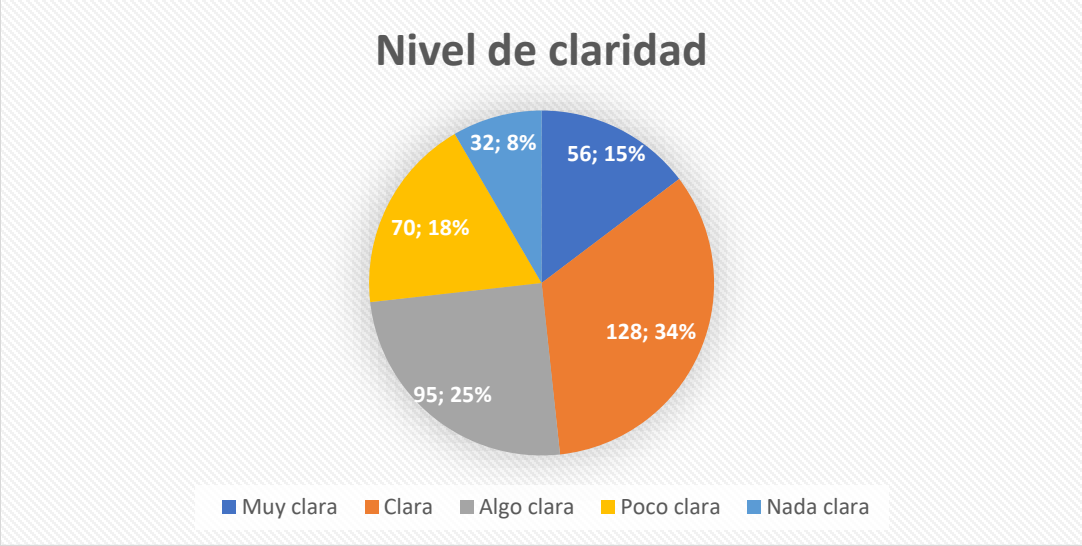
3) ¿Qué puntuación le darías a la claridad y transparencia de la información proporcionada sobre los beneficios y condiciones de tu póliza de seguro?

Tabla 21. Opinión sobre la claridad y transparencia de la información proporcionada sobre los beneficios y condiciones de tu póliza de seguro

Nivel de claridad	Cantidad de clientes	Porcentaje
Muy clara	56	14.7%
Clara	95	24.9%
Algo clara	128	33.6%
Poco clara	70	18.4%
Nada clara	32	8.4%
Total	381	100%

Fuente: elaboración propia

Figura 25. Nivel de claridad y transparencia de la información proporcionada sobre los beneficios y condiciones de tu póliza de seguro



Fuente: elaboración propia

Análisis: Según la opinión de 381 clientes acerca de la claridad y transparencia de la información proporcionada sobre los beneficios y condiciones de su póliza de seguro, los resultados muestran una diversidad de percepciones.

Un 14.7% (56 personas) encontró que la información era muy clara, lo que denota un alto nivel de satisfacción en cuanto a la comprensión de los detalles de la póliza. El 24.9% (95 personas) la calificó como clara, lo que sugiere una buena transparencia, aunque posiblemente con espacio para mejoras. Por otro lado, el 33.6% (128 personas) la pareció algo clara, indicando cierta ambigüedad o falta de claridad en algunos puntos.

Sin embargo, el 18.4% (70 personas) la percibió como poco clara, señalando una necesidad de mejorar la comunicación de ciertos aspectos de la póliza. Finalmente, el 8.4% (32 personas) la vio como nada clara, lo que destaca un área crítica que requiere atención inmediata para asegurar que los clientes comprendan completamente los beneficios y condiciones de su seguro.

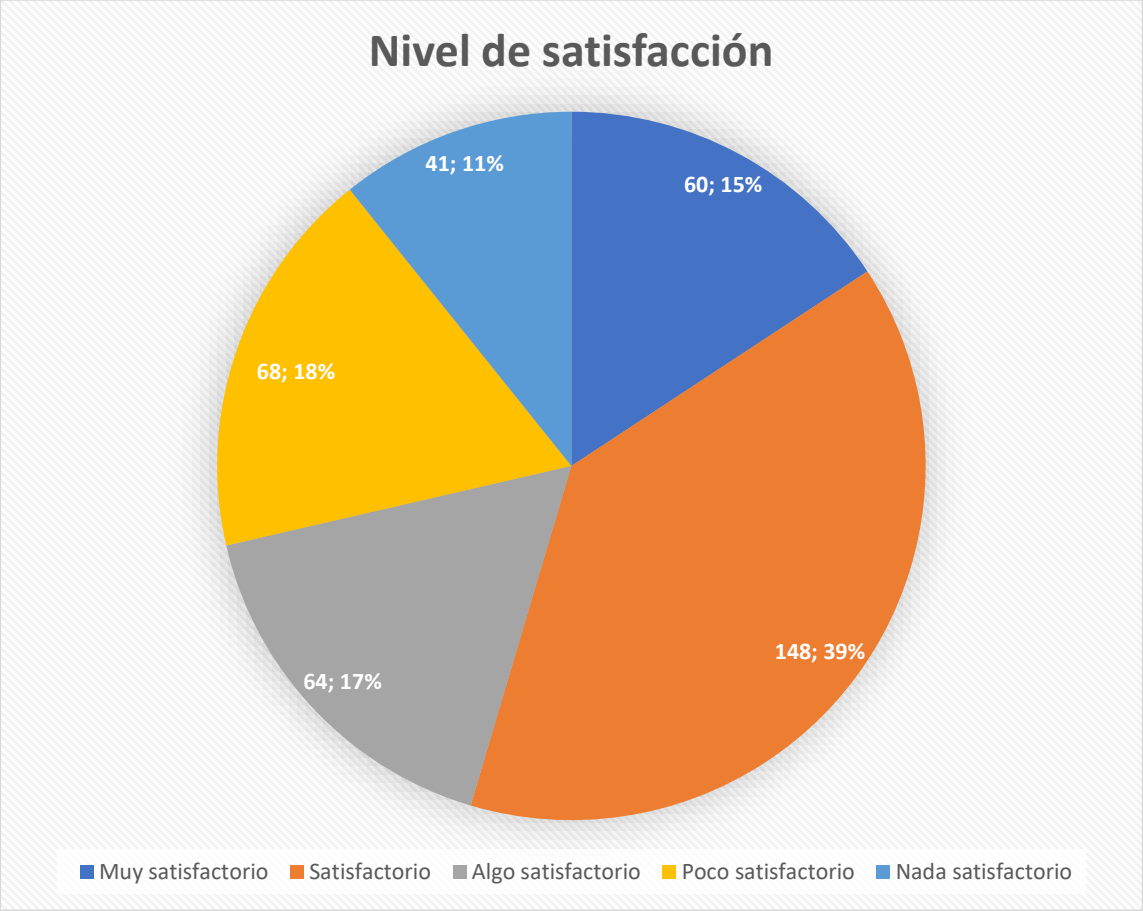
4) ¿Qué calificación le darías al manejo de problemas o dificultades al presentar una reclamación o solicitar un reembolso por parte de Aseguradora ABANK?

Tabla 22. Opinión sobre el manejo de problemas o dificultades al presentar una reclamación o solicitar un reembolso por parte de Aseguradora ABANK

Nivel de satisfacción	**Cantidad de clientes**	**Porcentaje**
Muy satisfactorio	60	15.7%
Satisfactorio	148	38.8%
Algo satisfactorio	64	16.8%
Poco satisfactorio	68	17.9%
Nada satisfactorio	41	10.8%
Total	381	100%

Fuente: elaboración propia

Figura 26. Nivel de satisfacción sobre el manejo de problemas o dificultades al presentar una reclamación o solicitar un reembolso por parte de Aseguradora ABANK



Fuente: elaboración propia

Análisis: De acuerdo con la opinión de 381 encuestados en relación al manejo de problemas o dificultades al presentar una reclamación o solicitar un reembolso por parte de Aseguradora ABANK, los resultados arrojan una variedad de percepciones. Un notable 15,7% (60 encuestados) expresó que la experiencia fue muy satisfactoria, lo que denota un alto nivel de satisfacción en la gestión de sus inquietudes.

Además, un 38.8% (148 encuestados) la consideraron satisfactoria, lo que sugiere que la aseguradora ha logrado mantener un estándar aceptable en la resolución de problemas. Por otro lado, un 16.8% (64 encuestados) la calificaron como algo satisfactorio, indicando que hay margen para mejorar en ciertos aspectos. Sin embargo, un 17.9% (68 encuestados) la percibieron como poco satisfactoria.

Finalmente, un 10.8% (41 encuestados) la catalogaron como nada satisfactoria, resaltando la urgencia de implementar cambios significativos para garantizar una experiencia más positiva para los asegurados al enfrentar problemas o dificultades. Estos datos resaltan la importancia de seguir trabajando en la mejora continua de la atención al cliente en Aseguradora ABANK.

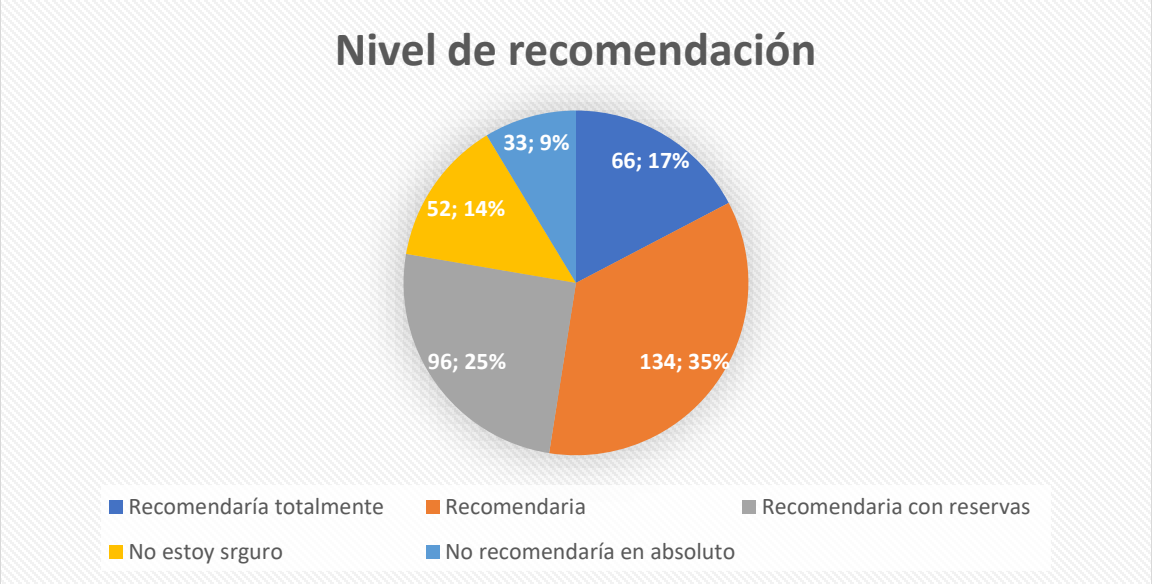
5) ¿Recomendarías los servicios de Aseguradora ABANK a otras personas?

Tabla 23. Opinión sobre recomendación de los servicios de Aseguradora ABANK

Nivel de recomendación	Cantidad de clientes	Porcentaje
Recomendaría totalmente	66	17.3%
Recomendaría	134	35.2%
Recomendaría con reservas	96	25.2%
No estoy seguro	52	13.6%
No recomendaría en absoluto	33	8.7%
Total	381	100%

Fuente: elaboración propia

Figura 27. Nivel de recomendación sobre los servicios de Aseguradora ABANK a otras personas



Fuente: elaboración propia

Análisis: Según las respuestas de los 381 encuestados acerca de si recomendasen los servicios de Aseguradora ABANK a otras personas, se revela una amplia diversidad de opiniones.

Un total de 66 encuestados, que representan el 17.3%, manifestaron que recomendarían los servicios de la aseguradora de manera entusiasta y sin reservas. Además, 134 personas, equivalente al 35.2%, afirmaron que definitivamente los recomendarían, lo que indica una satisfacción considerable con los servicios brindados. Por otro lado, 96 encuestados, el 25.2%, expresaron que recomendarían los servicios, pero con algunas reservas, señalando posibles áreas de mejora. Un grupo de 52 personas, un 13.6%, se mostró indeciso reflejando la necesidad de aclaración o mejoras adicionales en su experiencia.

Finalmente, 33 encuestados, que equivalen al 8,7%, indicaron que no recomendarían en absoluto los servicios de la aseguradora, resaltando la importancia de abordar sus preocupaciones y desafíos para fortalecer la satisfacción del cliente. Estos resultados proporcionan información valiosa para Aseguradora ABANK en su esfuerzo continuo por mejorar y adaptar sus servicios a las expectativas de sus clientes.

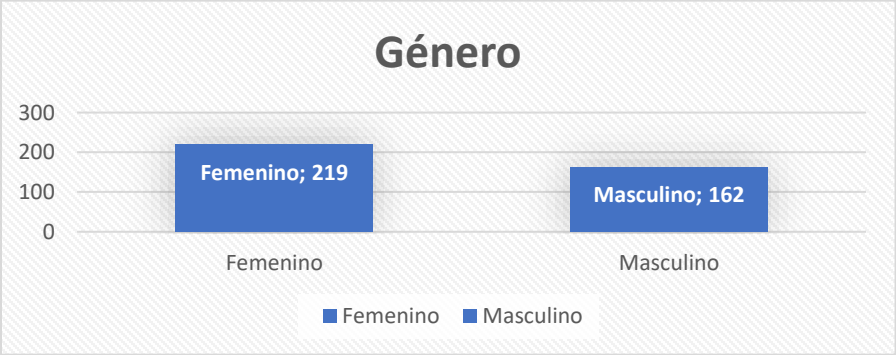
6) Por temas estadísticos, selecciona tu género

Tabla 24. Distribución de género de personas encuestadas

Genero	Cantidad de clientes
Femenino	219
Masculino	162

Fuente: elaboración propia

Figura 28. Gráfica de distribución de personas encuestadas



Fuente: elaboración propia

Análisis: De un total de 381 asegurados encuestados, se observa una distribución por género donde el 42.5% (162 personas) son hombres y el 57.5% (219 personas) son mujeres. Esta muestra equitativa entre géneros nos brinda una perspectiva diversa y representativa de opiniones y experiencias, asegurando una base sólida para la toma de decisiones informadas y el análisis de los resultados de la encuesta.

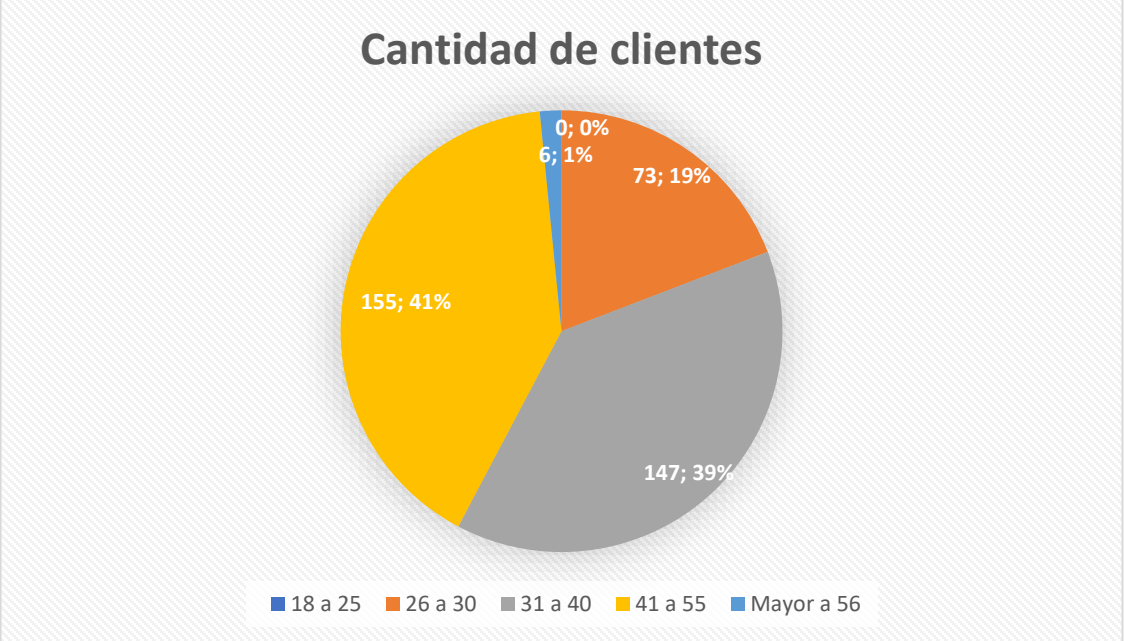
7) Por temas estadísticos, selecciona el rango de edad en el que te encuentras, por favor:

Tabla 25. Rango de edades de personas encuestadas

Edades (años)	Cantidad de clientes	Porcentaje
18 a 25	0	0%
26 a 30	73	19.1%
31 a 40	147	38.6%
41 a 55	155	40.7%
Mayor a 56	6	1.6%
Total	381	100%

Fuente: elaboración propia

Figura 29. Gráfica de rango de edades de personas encuestadas



Fuente: elaboración propia

Análisis: De un total de 381 clientes encuestados. En particular, no se registraron participantes en el rango de edad de 18 a 25 años. En cambio, 73 clientes, que representan un 19,2% del total, se ubicaron en el grupo de edades de 26 a 30 años, mientras que 147 clientes, equivalente al 38,6%, se centró en el grupo de 31 a 40 años. Un grupo aún más numeroso de 155 clientes, que corresponde al 40,7%, se ubicó en edades de 41 a 55 años. Un grupo más reducido de 6 clientes, que constituye el 1,6%, pertenece a los mayores de 56 años.

iii. Resultados de variable: Información documental existente (Variable Nro. 3)

Instrumento: lista de verificación.

✓ **Identificación de información documentada de la organización**

La lista de verificación se utilizó para verificar la información documentada de Aseguradora ABANK en contraste a los requisitos de la normativa ISO 9001:2015 e ISO/IEC 27001:2022. La plantilla utilizada se estructuró de tal forma que abarque cada uno de los capítulos del documento normativo partiendo del capítulo 4 "Contexto de la organización" hasta el capítulo 10 "Mejora continua". El llenado de éste se realizó al hacer contacto con la unidad de procesos y la gerencia de tecnología de la aseguradora y realizando las preguntas correspondientes por medio de una sesión de entrevista estructurada.

La lista de verificación se realizó a: Analista de procesos Senior. y Gerente de Tecnología.

Tabla 26. Lista de información documentada en contraste a ISO 9001:2015

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
4. Contexto de la Organización	4.1 Comprensión de la organización y de su contexto	N/A	N/A	No se requiere información documental según norma.
4. Contexto de la Organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	N/A	N/A	No se requiere información documental según norma.
4. Contexto de la Organización	4.3 Determinación del alcance del sistema de gestión de la calidad	¿Se cuenta con un alcance?	N/A	**No se cumple** – la aseguradora no posee un alcance para el Sistema de Gestión de Calidad.

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
4. Contexto de la Organización	4.4 Sistema de gestión de la calidad y sus procesos			
4. Contexto de la Organización	4.4.1 Determinar los procesos necesarios para la organización	N/A	N/A	No se requiere información documental según norma.
4. Contexto de la Organización	4.4.2 Mantener y conservar información documentada	¿Cuenta con los procesos de la organización?	¿Cuenta con registros de los procesos?	**Cumple medianamente bien** – la aseguradora cuenta con procesos organizacionales, sin embargo muchos de ellos se encuentran desactualizados o sin haberse creado.
5. Liderazgo	5.1 Liderazgo y compromiso			
5. Liderazgo	5.1.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
5. Liderazgo	5.1.2 Enfoque al cliente	N/A	N/A	No se requiere información documental según norma.
5. Liderazgo	5.2 Política			
5. Liderazgo	5.2.1 Establecimiento de la política de la calidad	¿Se tiene una política del SG?	N/A	**No se cumple** – la aseguradora no posee una política para el Sistema de Gestión de Calidad.
5. Liderazgo	5.2.2 Comunicación de la política de la calidad	N/A	N/A	No se requiere información documental según norma.
5. Liderazgo	5.3 Roles, responsabilidades y autoridades en la organización	N/A	N/A	No se requiere información documental según norma.
6. Planificación	6.1 Acciones para abordar riesgos y oportunidades			
6. Planificación	6.1.1 Al planificar el SGC la organización debe considerar que se puedan lograr los resultados previstos, aumentar defectos deseables, mejora.	N/A	N/A	No se requiere información documental según norma.

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
6. Planificación	6.1.2 Planificar las acciones para abordar riesgos y oportunidades	N/A	N/A	No se requiere información documental según norma.
6. Planificación	6.2 Objetivos de la calidad y planificación para lograrlos			
6. Planificación	6.2.1 Establecer objetivos de calidad	¿Cuenta con objetivos de calidad y sus planes?	N/A	**No se cumple** – la aseguradora no posee objetivos de calidad, por lo tanto tampoco planes para alcanzarlos.
6. Planificación	6.2.2 Al determinar los objetivos se debe planificar: qué se hará, recursos, responsables, cuándo se finalizará, evaluación de resultados	N/A	N/A	No se requiere información documental según norma.
6. Planificación	6.3 Planificación de los cambios	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.1 Recursos			
7. Apoyo	7.1.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.1.2 Personas	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.1.3 Infraestructura	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.1.4 Ambiente para la operación de los procesos	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.1.5 Recursos de seguimiento y medición			
7. Apoyo	7.1.6 Conocimientos de la organización	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.2 Competencia	N/A	¿Se tienen perfiles de puesto?	**Cumple medianamente bien** – la aseguradora cuenta con perfiles de puesto para algunos cargos, pero no todos se encuentran actualizados

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
				o finalizado su documentación.
7. Apoyo	7.3 Toma de conciencia	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.4 Comunicación	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.5.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.5.2 Creación y actualización	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.5.3 Control de la información documentada			
7. Apoyo	7.5.3.1 Esté disponible y sea idónea para su uso, está protegida adecuadamente.	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.5.3.2 Distribución, acceso, recuperación y uso, almacenamiento y preservación, control de cambios, conservación y disposición.	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.1 Planificación y control operacional	¿Cuenta con controles?	¿Se tienen registros de las operaciones?	**Cumple medianamente bien** – la aseguradora cuenta con control de la operación; sin embargo, estos controles no se encuentran documentados de forma oficial, no son comunicados a toda la organización ni existe un seguimiento sobre ellos. Se lleva el registro para la mayoría de operaciones, pero no en su totalidad, estos registros no tienen

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
				mayor impacto en el negocio que para llevar registrada el día a día de la aseguradora.
8.Operación	8.2 Requisitos para los productos y servicios			
8.Operación	8.2.1 Comunicación con el cliente	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.2.2 Determinación de los requisitos para los productos y servicios	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.2.3 Revisión de los requisitos para los productos y servicios			
8.Operación	8.2.3.1 Revisión antes de comprometerse a suministrar productos o servicios	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.2.3.2 Conservar información documentada sobre los requisitos de productos y servicios	N/A	¿Se tiene un check list de cumplimiento de requisitos?	**Cumple medianamente bien** – la aseguradora cuenta con documentos como presentaciones y otros documentos no oficiales en los que se plasman los requisitos de los clientes, de forma informal en el proceso de creación de seguros.
8.Operación	8.2.4 Cambios en los requisitos para los productos y servicios	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.3 Diseño y desarrollo de los productos y servicios			
8.Operación	8.3.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.3.2 Planificación del diseño y desarrollo	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.3.3 Entradas para el diseño y desarrollo	N/A	Entradas del diseño y desarrollo	**Cumple medianamente bien** – la aseguradora define las entradas del diseño y desarrollo en

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
				documentos no oficiales.
8.Operación	8.3.4 Controles del diseño y desarrollo	N/A	Controles de diseño y desarrollo	**Cumple medianamente bien** – la aseguradora define los controles del diseño y desarrollo en documentos no oficiales.
8.Operación	8.3.5 Salidas del diseño y desarrollo	N/A	Salidas del diseño y desarrollo	**Cumple medianamente bien** – la aseguradora define las salidas del diseño y desarrollo en documentos no oficiales.
8.Operación	8.3.6 Cambios del diseño y desarrollo	N/A	Cambios del diseño y desarrollo	**Cumple medianamente bien** – la aseguradora define los cambios del diseño y desarrollo en documentos no oficiales.
8.Operación	8.4 Control de los procesos, productos y servicios suministrados externamente			
8.Operación	8.4.1 Generalidades	N/A	Evaluaciones de proveedores	**No se cumple** – la aseguradora no posee documentación sobre evaluación de proveedores.
8.Operación	8.4.2 Tipo y alcance del control	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.4.3 Información para los proveedores externos	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.5 Producción y provisión del servicio			
8.Operación	8.5.1 Control de la producción y de la provisión del servicio	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.5.2 Identificación y trazabilidad	N/A	Trazabilidad	**Cumple medianamente bien** – la aseguradora realiza registros de información

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
				en archivos de Excel y otros tipos de documentación con alto riesgo de variación, no existen los medios adecuados y fidedignos que garanticen la información.
8.Operación	8.5.4 Preservación	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.5.5 Actividades posteriores a la entrega	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.5.6 Control de los cambios	N/A	¿Se tiene lo resultados de la revisión de los cambios?	**Cumple medianamente bien** – la aseguradora define las revisiones de cambios en documentos no oficiales ni adecuadamente registrados.
8.Operación	8.6 Liberación de los productos y servicios	N/A	¿Se cuenta con un documento de Liberación de los productos?	**Cumple medianamente bien** – la aseguradora define las liberaciones de productos en documentos no oficiales ni adecuadamente registrados.
8.Operación	8.7 Control de las salidas no conformes			
8.Operación	8.7.1 Asegurarse que las salidas que no sean conformes con los requisitos se identifican y controlan	N/A	N/A	No se requiere información documental según norma.
8.Operación	8.7.2 Conservar información documentada sobre estos requisitos	N/A	¿se cuenta con documentos de salidas no conformes, No conformidades?	**No se cumple** – la aseguradora no posee documentación salidas no conformes.
9. Seguimiento y evaluación	9 evaluación del desempeño			

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
9. Seguimiento y evaluación	9.1 Seguimiento, medición, análisis y evaluación			
9. Seguimiento y evaluación	9.1.1 Generalidades	N/A	¿Se cuentan con indicadores de desempeño?	**No se cumple** – la aseguradora no posee indicadores de desempeño para sus procesos.
9. Seguimiento y evaluación	9.1.2 Satisfacción del Cliente	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.1.3 Análisis y evaluación	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.2 Auditoría interna			
9. Seguimiento y evaluación	9.2.1 Realizar auditorías internas planificadas	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.2.2 Establecer programas de auditoría, definir criterios de auditorías y alcance, seleccionar a los auditores…	N/A	¿Se cuenta con un Programa, plan, informe, check list de auditoría?	**No se cumple** – la aseguradora no realiza auditorías de calidad.
9. Seguimiento y evaluación	9.3 Revisión por la dirección			
9. Seguimiento y evaluación	9.3.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.3.2 Entradas de la revisión por la dirección	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.3.3 Salidas de la revisión por la dirección	N/A	¿Se tiene evidencia de los resultados de la revisión por la dirección?	**No se cumple** – la aseguradora no realiza revisiones por la Alta dirección.
10. Mejora	10 Mejora			
10. Mejora	10.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
10. Mejora	10.2 No conformidades y acción correctiva			

Continúa Tabla 26 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO 9001:2015
10. Mejora	10.2.1 Reaccionar ante la no conformidad y evaluar la necesidad de acciones para eliminar las causas de la no conformidad	N/A	N/A	No se requiere información documental según norma.
10. Mejora	10.2.2 La organización debe conservar información documentada como evidencia	N/A	¿Se cuenta con planes de acción NC?	**No se cumple** – la aseguradora no posee documentación de No conformidades.
10. Mejora	10.3 Mejora continua	N/A	N/A	No se requiere información documental según norma.

Fuente: elaboración propia

Tabla 27. Lista de información documentada en contraste a ISO/IEC 27001:2022

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO/IEC 27001:2022
4. Contexto de la organización	4.1 Comprensión de la organización y de su contexto	N/A	N/A	No se requiere información documental según norma.
4. Contexto de la organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	N/A	N/A	No se requiere información documental según norma.
4. Contexto de la organización	4.3 Determinación del alcance del sistema de gestión de la SI	¿Se cuenta con un alcance?	N/A	**No se cumple** – la aseguradora no posee un alcance para el Sistema de Gestión de Calidad.
4. Contexto de la organización	4.4 Sistema de gestión de SI	N/A	N/A	No se requiere información documental según norma.
5. Liderazgo	5.1 Liderazgo y compromiso	N/A	N/A	No se requiere información documental según norma.
5. Liderazgo	5.2 Política	¿Se cuenta con una política del SGSI?	N/A	**No se cumple** – la aseguradora no posee una política para el Sistema de Gestión de Seguridad de la Información.

Continúa Tabla 27 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO/IEC 27001:2022
5. Liderazgo	5.3 Funciones, responsabilidades y autoridades de la organización	N/A	N/A	No se requiere información documental según norma.
6. Planificación	6.1 Acciones para abordar riesgos y oportunidades			
6. Planificación	6.1.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
6. Planificación	6.1.2 Evaluación de riesgos de SI	N/A	N/A	No se requiere información documental según norma.
6. Planificación	6.1.3 Tratamiento de RI de SI	¿Se tiene un procedimiento para el tratamiento de RI y controles?	N/A	**No se cumple** – la aseguradora no posee procedimientos para riesgos y los controles.
6. Planificación	6.2 Objetivos de la SI y planificación para lograrlos	¿Se cuenta con objetivos de Seguridad de la información y sus planes?	N/A	**No se cumple** – la aseguradora no posee objetivos de Seguridad de la información, por lo tanto tampoco planes para alcanzarlos.
6. Planificación	6.3 Planificación de los cambios	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.1 Recursos	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.2 Competencia	N/A	¿Se cuentan con perfiles de puesto?	**Cumple medianamente bien** – la aseguradora cuenta con perfiles de puesto para algunos cargos, pero no todos se encuentran actualizados o finalizado su documentación.
7. Apoyo	7.3 Toma de conciencia	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.4 Comunicación	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.5.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
7. Apoyo	7.5.2 Creación y actualización	N/A	N/A	

Continúa Tabla 27 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO/IEC 27001:2022
7. Apoyo	7.5.3 Control de información documentada	N/A	N/A	No se requiere información documental según norma.
8. Operación	8.1 Planificación y control operacional	¿Se tiene Controles?	¿Se cuenta con registros de operaciones?	**Cumple medianamente bien** – la aseguradora cuenta con control de la operación; sin embargo, estos controles no se encuentran documentados de forma oficial, no son comunicados a toda la organización ni existe un seguimiento sobre ellos. Se lleva el registro para la mayoría de operaciones pero no en su totalidad, estos registros no tienen mayor impacto en el negocio que para llevar registrada el día a día de la aseguradora.
8. Operación	8.2 Evaluación de RI de SI	¿Se tiene resultados de la evaluación de RI?	N/A	**Cumple medianamente bien** – la aseguradora cuenta con procedimientos generales para evaluar los riesgos de la organización. Sin embargo, no se comunican y oficializan ante toda la operación para tomarlos como insumo estratégico.
8. Operación	8.3 Tratamiento de RI de SI	¿Se cuenta con Resultados del tratamiento de RI?	N/A	**Cumple medianamente bien** – la aseguradora cuenta procedimientos generales para el tratamiento de riesgos organizacionales, sin embargo, no se da un seguimiento oportuno e integral en conjunto al personal de la organización y todos los procesos del negocio.
9. Seguimiento y evaluación	9. Evaluación del desempeño			

Continúa Tabla 27 en la siguiente página →

Capítulo de norma	Punto de norma	Información documentada a mantener (Documentos)	Información documentada a conservar (registros)	Valoración de cumplimiento ante ISO/IEC 27001:2022
9. Seguimiento y evaluación	9.1 Seguimiento, medición, análisis y evaluación	N/A	¿Se cuenta con indicadores de desempeño?	**No se cumple** – la aseguradora no posee indicadores de desempeño para sus procesos.
9. Seguimiento y evaluación	9.2 Auditoría interna			
9. Seguimiento y evaluación	9.2.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.2.2 Programa de auditoría interna	N/A	¿Se cuenta con Programa, plan, informe, check list de auditoría?	**No se cumple** – la aseguradora no realiza auditorías de vinculadas a Seguridad de la Información.
9. Seguimiento y evaluación	9.3 Revisión por la dirección			
9. Seguimiento y evaluación	9.3.1 Generalidades	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.3.2 Entradas de la revisión por la dirección	N/A	N/A	No se requiere información documental según norma.
9. Seguimiento y evaluación	9.3.3 Resultados de la revisión por la dirección	N/A	¿Se evidencia de los resultados de la revisión por la dirección?	**No se cumple** – la aseguradora no realiza revisiones por la Alta dirección.
10. Mejora	10 Mejora			
10. Mejora	10.1 Mejora continua	N/A	N/A	No se requiere información documental según norma.
10. Mejora	10.2 No conformidades y acción correctiva	N/A	Planes de acción NC	**No se cumple** – la aseguradora no posee documentación de No conformidades.

Fuente: elaboración propia

iv. Resultados de variable: Grado de conformidad con respecto a requisitos de Seguridad de la Información según ISO/IEC 27001:2022. (Variable Nro. 4)

- ✓ **Identificación del cumplimiento de la organización ante los requisitos de normativa ISO/IEC 27001:2022**

Instrumento: lista de verificación y guía de entrevista

La lista de verificación se empleó para evaluar el nivel de cumplimiento de la situación actual de Aseguradora ABANK en contraposición a los lineamientos de la norma ISO 27001:2022. El formato utilizado fue estructurado de manera que englobe la totalidad de los 7 segmentos del texto reglamentario, comenzando desde la sección 4 "Contexto de la organización" y llegando hasta el apartado 10 "Mejora continua". El llenado de dicho formato fue llevado a cabo al interactuar con el equipo de seguridad de la información y continuidad del negocio realizando las cuestiones correspondientes. (Ver Apéndice 16 para visualizar la plantilla completa de la lista de verificación y guía de entrevista usada).

- Capítulo 4. Contexto de la organización

Tabla 28. Lista de verificación - Capítulo 4. Contexto de la organización

Capítulo de norma	Punto de norma	Descripción	Valoración
4. Contexto de la Organización	4.1 Comprensión de la organización y de su contexto	En términos metodológicos, la identificación de factores internos y externos ha demostrado ser superficial y carente de un enfoque analítico adecuado. Además, los ejemplos documentales presentan carencias en la representación precisa de los elementos clave relacionados con la organización y su contexto. La aseguradora no posee una metodología o proceso específico para la realización periódica de dichas evaluaciones de su contexto. Recientemente la organización realizó un análisis FODA el cual no contempla todos los escenarios descritos en los párrafos anteriores.	30%
4. Contexto de la Organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%
4. Contexto de la Organización	4.3 Determinación del alcance del sistema de gestión de la SI	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%
4. Contexto de la Organización	4.4.2 Mantener y conservar información documentada	Se observa una falta de rigurosidad en la identificación y clasificación de la información relevante para la organización.	50%

Continúa Tabla 28 en la siguiente página →

Capítulo de norma	Punto de norma	Descripción	Valoración
		Las acciones utilizadas para el mantenimiento y conservación de documentos parecen carecer de la sistematicidad necesaria, reflejando debilidades en la gestión de registros clave de la aseguradora. Además, los ejemplos documentales presentan limitaciones en la demostración clara de las prácticas y procedimientos utilizados para asegurar la integridad y disponibilidad de la información documentada.	

Fuente: elaboración propia

Figura 30. Capítulo 4. Contexto de la organización--Resultados

Fuente: elaboración propia

Análisis: El resultado del Capítulo 4 de la norma ISO 27001:2022 refleja un resultado variado. Mientras que el apartado 4.1 ha alcanzado un nivel del 30%, indicando un progreso inicial en la planificación del sistema de gestión, los apartados 4.2 y 4.3 muestran un 0%.

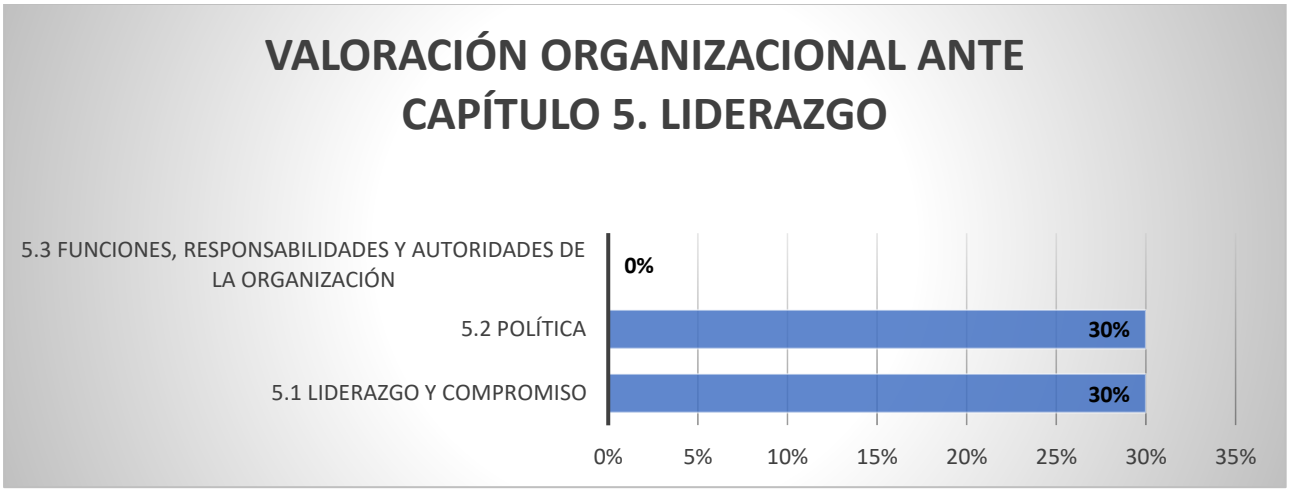
Sin embargo, el apartado 4.4.2 destaca con un 50%, indicando que se ha avanzado significativamente en la evaluación de riesgos y oportunidades relacionadas con la temática.

Tabla 29. Lista de verificación - Capítulo 5. Liderazgo

Capítulo de norma	Punto de norma	Descripción	Valoración
5. Liderazgo	5.1 Liderazgo y compromiso	Las técnicas empleadas para abordar este requisito son insuficientes, reflejando debilidades en la interpretación y aplicación de los mismos La alta dirección no refleja un compromiso suficiente para reflejar un liderazgo ante los principios de la normativa ISO/IEC 27001:2022.	30%
5. Liderazgo	5.2 Política	En la organización ha establecido una política no documentada sobre seguridad de la información y continuidad del negocio, dicho documento no es oficial y no se ha comunicado ante la organización.	30%
5. Liderazgo	5.3 Funciones, responsabilidades y autoridades de la organización	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%

Fuente: elaboración propia

Figura 31. Capítulo 5. Liderazgo--Resultados



Fuente: elaboración propia

Análisis: El resultado del Capítulo 5 de la norma ISO 27001:2022 presenta una diversidad de resultados en lo que respeta a la gestión de roles y responsabilidades en seguridad de la información. En el apartado 5.1, se ha logrado un avance del 30%, indicando que se han identificado roles clave, pero aún se necesita mayor claridad en sus responsabilidades.

De manera similar, el apartado 5.2 también muestra un nivel del 30%, señalando que se han asignado algunas responsabilidades relacionadas con la gestión de activos de información. Sin embargo, el apartado 5.3 muestra un 0%, lo que indica que la supervisión y revisión de roles y responsabilidades aún no se ha abordado.

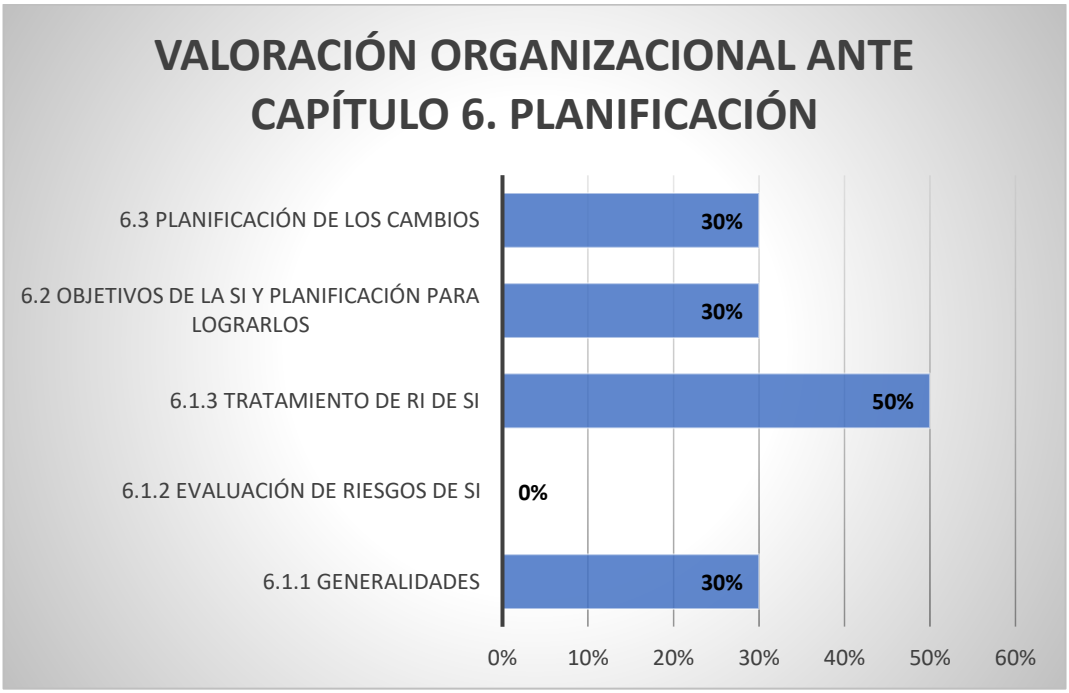
Tabla 30. Lista de verificación - Capítulo 6. Liderazgo

Capítulo de norma	Punto de norma	Descripción	Valoración
6. Planificación	**6.1 Acciones para abordar riesgos y oportunidades**		
6. Planificación	6.1.1 Generalidades	Metodológicamente, la planificación para lograr resultados previstos y aumentar defectos deseables parece ser superficial y carente de un enfoque detallado, esto se ve reflejado en que los riesgos y oportunidades no son acordes al contexto de la aseguradora y sus procesos.	30%
6. Planificación	6.1.2 Evaluación de riesgos de SI	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%
6. Planificación	6.1.3 Tratamiento de RI de SI	La aseguradora realiza acciones para dar tratamiento de las actividades sospechosas y riesgos mapeados en la organización, sin embargo, este seguimiento es reactivo y no proactivo, por lo que no existe un procedimiento o metodología de seguimiento y desarrollo de dichos tratamientos.	50%
6. Planificación	6.2 Objetivos de la SI y planificación para lograrlos	Se han definido objetivos para la seguridad e la información, pero no se encuentran documentados ni existe un plan para que la aseguradora los alcance.	30%
6. Planificación	6.3 Planificación de los cambios	La aseguradora desarrolla de forma genérica iniciativas de gestión de cambios, sin embargo, no está documentado ni existe un procedimiento estandarizado que estandarice y guíe a la organización para lograr una efectiva gestión del cambio adecuadamente organizada.	30%

Fuente: elaboración propia

Continúa Tabla 30 en la siguiente página →

Figura 32. Capítulo 6. Planificación--Resultados



Fuente: elaboración propia

Análisis: El resultado del Capítulo 6 de la norma ISO 27001:2022 refleja un enfoque mixto en la gestión de actividades de soporte. En el apartado 6.1.1, se ha logrado un progreso del 30%, lo que indica una iniciación en la definición de recursos y competencias necesarias para la implementación de la seguridad de la información. Sin embargo, el apartado 6.1.2 muestra un 0%, lo que sugiere que la identificación de competencias específicas aún no ha sido abordada y es posible mejorar esta área.

Por otro lado, el apartado 6.1.3 destaca con un 50%, lo que señala un avance sustancial en la definición de la competencia, capacitación y conciencia del personal relacionado con la seguridad de la información. Además, los apartados 6.2 y 6.3 registran un nivel del 30%.

Tabla 31. Lista de verificación - Capítulo 7. Apoyo

Capítulo de norma	Punto de norma	Descripción	Valoración
7. Apoyo	7.1 Recursos	La aseguradora realiza gestiones para la planificación de los recursos de la organización, sin embargo, no se posee ningún registro sobre tal planificación, ni tampoco algún mecanismo que evidencie el seguimiento al mismo.	50%

Continúa Tabla 31 en la siguiente página →

Capítulo de norma	Punto de norma	Descripción	Valoración
7. Apoyo	7.2 Competencia	En cuanto a competencia sobre el personal orientado a la seguridad de la información, la aseguradora procura garantizar la idoneidad de sus colaboradores; sin embargo, no se posee una metodología o mecanismo para desarrollar a dicho personal. De igual forma no se posee información documentada que lo evidencie.	50%
7. Apoyo	7.3 Toma de conciencia	La aseguradora desarrolla campañas de concientización y conocimiento sobre seguridad de la información, sin embargo, esto se realiza sin establecer una calendarización o metodología que garantice el éxito del programa a largo plazo.	50%
7. Apoyo	7.4 Comunicación	Se observa que existen comunicaciones sobre los acontecimientos sobre seguridad e la información de forma particular, debido a que la comunicación no es proactiva, sino reactiva y sin seguimiento a lo largo del tiempo. Actualmente la comunicación se realiza básicamente por medio de correo electrónico.	50%
7. Apoyo	7.5.1 Generalidades	Se identifican áreas donde la documentación puede ser más completa y detallada, especialmente en lo que respecta a la determinación de la información documentada necesaria para la eficacia del Sistema de Gestión de la Seguridad de la Información.	30%
7. Apoyo	7.5.2 Creación y actualización	La evidencia recopilada refleja la existencia de procedimientos documentados, sin embargo, se identifican deficiencias en la actualización regular y la revisión de la documentación para asegurar su pertinencia y vigencia. No existen procesos documentados y comunicados entre el personal de la aseguradora para establecer una ruta clara de gestión de la documentación en la organización.	30%
7. Apoyo	7.5.3 Control de información documentada	La evidencia recopilada indica que, si bien existe documentación disponible, la accesibilidad y su idoneidad para su uso no están completamente garantizadas. Se observan deficiencias en los mecanismos de protección y en la disponibilidad oportuna de la documentación necesaria. No existe un sitio (por ejemplo, intranet) para alojar documentos y que estos sean de accesibilidad para todo el personal de la aseguradora; actualmente cada área y colaborador de la organización resguarda la información en sus computadoras personales. A excepción documentos o registros operaciones resguardados en carpetas compartidas.	30%

Fuente: elaboración propia

Figura 33. Capítulo 7. Apoyo—Resultados

Fuente: elaboración propia

Análisis: El resultado del Capítulo 7 de la norma ISO 27001:2022 muestra un avance constante en la planificación y la gestión de soporte a la seguridad de la información.

Los apartados 7.1, 7.2, 7.3 y 7.4 todos registran un nivel del 50%, lo que indica un sólido progreso en la definición y el control de los recursos necesarios para mantener el sistema de gestión de seguridad de la información.

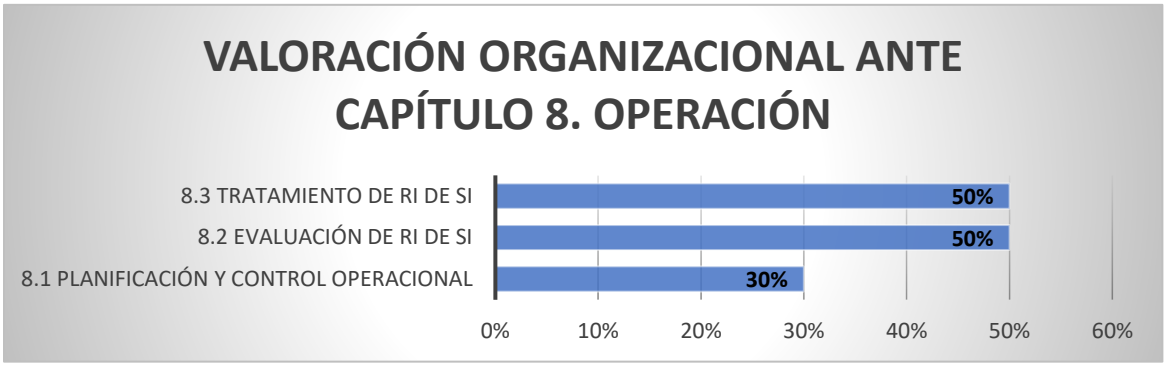
Sin embargo, los apartados 7.5.1, 7.5.2 y 7.5.3 muestran un nivel del 30%.

Tabla 32. Lista de verificación - Capítulo 8. Operación

Capítulo de norma	Punto de norma	Descripción	Valoración
8. Operación	8.1 Planificación y control operacional	La evidencia recopilada indica que, si bien existen procedimientos documentados para la planificación y control operacional, se identifican áreas donde la planificación no se alinea completamente con los objetivos estratégicos de la organización. Además, se observa una falta de mecanismos efectivos de control operacional para asegurar la consistencia en la ejecución de procesos clave.	30%
8. Operación	8.2 Evaluación de RI de SI	Existen en la aseguradora mecanismos para la evaluación de los riesgos según las normativas de los entes reguladores, sin embargo, no existen evidencia documental del seguimiento a lo largo del tiempo sobre dichas evaluaciones relacionadas a seguridad de la información.	50%
8. Operación	8.3 Tratamiento de RI de SI	Se realizan acciones específicas para el tratamiento de riesgos relacionados con seguridad de la información, sin embargo, no se posee evidencia documental de seguimiento proactivo a dichos planes de acción.	50%

Fuente: elaboración propia

Figura 34. Capítulo 8. Operación—Resultados



Fuente: elaboración propia

Análisis: El resultado del Capítulo 8 de la norma ISO 27001:2022 revela un enfoque variado en la planificación y control de las operaciones relacionadas con la seguridad de la información. El apartado 8.1 muestra un nivel del 30%, lo que indica que la organización ha considerado la planificación de operaciones, pero aún necesita desarrollarse en esta área.

Por otro lado, los apartados 8.2 y 8.3 exhiben un nivel del 50%.

Tabla 33. Lista de verificación - Capítulo 9. Seguimiento y evaluación

Capítulo de norma	Punto de norma	Descripción	Valoración
9. Seguimiento y evaluación	**9. Evaluación del desempeño**		
9. Seguimiento y evaluación	9.1 Seguimiento, medición, análisis y evaluación	Para seguridad de la información se poseen indicadores de medición que ayudan a entender el contexto de la operación de cara a este aspecto, sin embargo, se ha observado que no se posee evidencia de seguimientos oportunos, además, no existe un mecanismo de acción a seguir para los incumplimientos y demás tipo de situaciones que evidencien alerta ante la seguridad de la información.	30%
	9.2 Auditoría interna		
9. Seguimiento y evaluación	9.2.1 Generalidades	Se considera en la organización la realización de auditorías para la seguridad de la información de forma reactiva; no existe un programa específico o un mecanismo que garantice la evaluación periódica y efectiva a este aspecto. De igual forma no existe documentación que respalde esta actividad.	50%
9. Seguimiento y evaluación	9.2.2 Programa de auditoría interna	Se ejecutan sesiones de revisión, con enfoque de auditoría, pero no poseen la rigidez e integridad de una auditoría formal, no se documenta adecuadamente ni se da el seguimiento oportuno.	50%

Continúa Tabla 33 en la siguiente página →

	9.3 Revisión por la dirección		
9. Seguimiento y evaluación	9.3.1 Generalidades	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%
9. Seguimiento y evaluación	9.3.2 Entradas de la revisión por la dirección	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%
9. Seguimiento y evaluación	9.3.3 Resultados de la revisión por la dirección	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%

Fuente: elaboración propia

Figura 35. Capítulo 9. Seguimiento y evaluación--Resultados

Fuente: elaboración propia

Análisis: El resultado del Capítulo 9 de la norma ISO 27001:2022 indica una gestión diversa en el seguimiento y evaluación de la seguridad de la información. En el apartado 9.1 se ha alcanzado un nivel del 30%, señalando un comienzo en la planificación de actividades.

Los apartados 9.2.1 y 9.2.2 registran un nivel del 50%, indicando un progreso en la identificación de los indicadores clave de desempeño y en la implementación de procesos de seguimiento. Los apartados 9.3.1, 9.3.2 y 9.3.3 reflejan un 0%.

Tabla 34. Lista de verificación - Capítulo 10. Mejora

Capítulo de norma	Punto de norma	Nivel de cumplimiento	Valoración
	10 Mejora		
10. Mejora	10.1 Mejora continua	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%
10. Mejora	10.2 No conformidades y acción correctiva	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.	0%

Fuente: elaboración propia

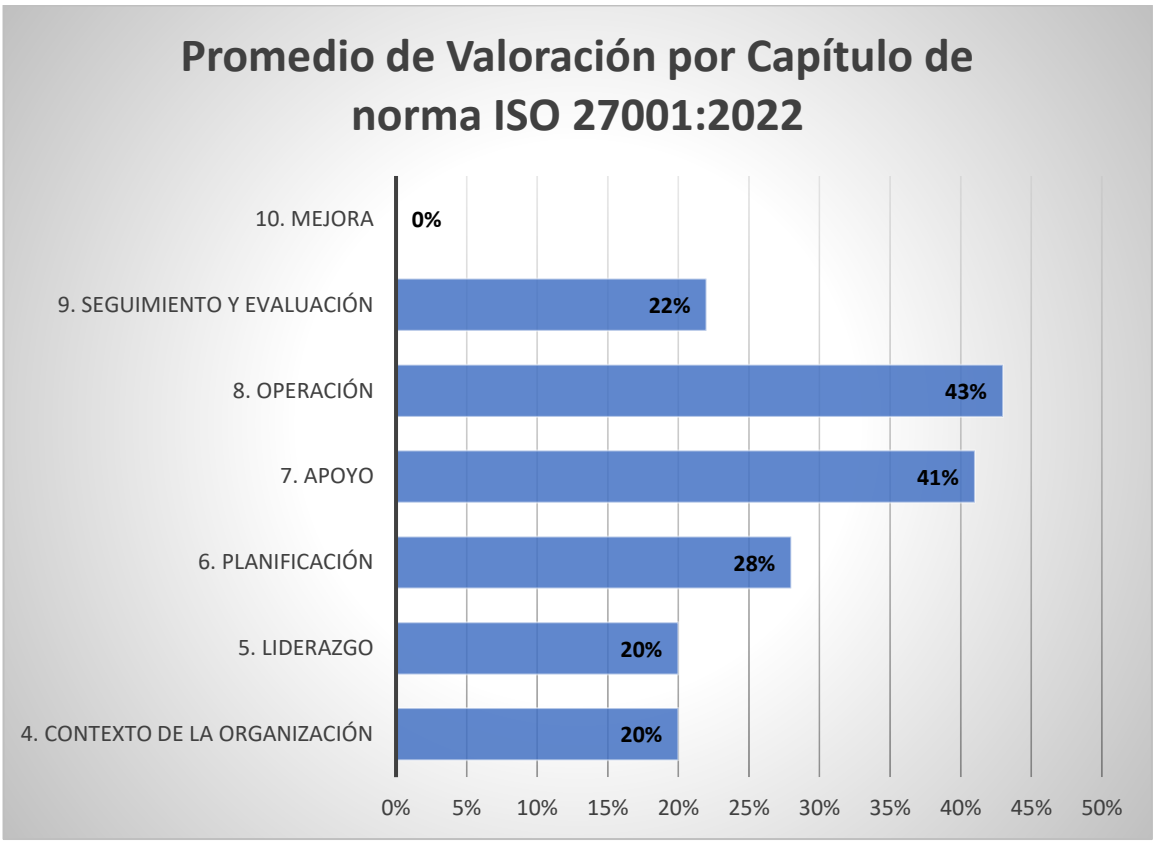
Figura 36. Capítulo 10. Mejora--Resultados

Fuente: elaboración propia

Análisis: El resultado del Capítulo 10 de la norma ISO 27001:2022 indica un desafío importante en la gestión de la mejora continua de la seguridad de la información. Los apartados 10.1 y 10.2 registran un 0% , lo que refleja una falta de enfoque en la identificación de oportunidades de mejora y en la implementación de acciones correctivas y preventivas relacionadas con la seguridad de la información.

- Resultado de todos los capítulos

Figura 37.– consolidado de resultados



Fuente: elaboración propia

Análisis El resultado de la norma ISO 27001:2022 revela un promedio general de 29% en todos los capítulos, indicando que la organización tiene un trabajo significativo por delante para fortalecer su sistema de gestión de seguridad de la información.

Los capítulos 4 y 5, relacionados con roles y responsabilidades y la planificación de la seguridad de la información, registran un 20% respectivamente. El Capítulo 6, que aborda las actividades de soporte, refleja un 28%. El Capítulo 7, centrado en el soporte, alcanzó un 41%. El Capítulo 8, relacionado con la operación, presenta un nivel del 43%, indicando un progreso en la gestión de operaciones de seguridad. El Capítulo 9, enfocado en el seguimiento y evaluación, alcanzó un nivel de 22%, destacando una necesidad de mejorar en la evaluación y seguimiento de la seguridad de la información. El Capítulo 10, centrado en la mejora continua, registró un preocupante 0%.

✓ **Identificación de los activos de la información**

La matriz de activos de información se construyó a partir de una serie de entrevistas realizadas al personal de Aseguradora ABANK (Desarrollador Senior de la Gerencia de tecnología y al Encargado de seguridad de la información y continuidad del negocio perteneciente a la Unidad de Riesgos). Se identificaron 14 activos críticos para la organización, dentro de los cuales se encuentran algunos vinculados directamente a temas tecnológicos, como otros casos relacionados a la información tangible de la organización.

Tabla 35. Matriz de activos de información

Nro.	Activo de Información	Descripción	Ubicación Física	Propietario	Valor del Activo	Clasificación
1	Base de Datos de Clientes	Datos personales de asegurados y beneficiarios.	Servidores internos - SISE 3G	Tecnología	Alto	Confidencial
2	Datos de Siniestros	Información sobre siniestros y reclamaciones.	Servidores internos - SISE 3G	Tecnología	Alto	Confidencial
3	Datos de Proveedores	Información sobre proveedores y acuerdos.	Servidores internos - SISE 3G	Tecnología	Medio	Confidencial
4	Portal de Clientes	Plataforma en línea para clientes.	Servidores web externos	Tecnología	Alto	Confidencial
5	Página WEB	Plataforma en línea para clientes.	Servidores web externos	Tecnología	Alto	No confidencial
6	Registros de Auditoría	Registros de auditorías internas y externas.	Archivo Digital	Auditoría interna	Alto	Confidencial
7	Políticas y Procedimientos	Documentación de políticas y procedimientos internos.	Archivo Digital	Riesgos y procesos	Medio	Confidencial
8	Datos de Empleados	Información personal y laboral de empleados.	Servidores internos	Recursos humanos	Alto	Confidencial
9	Documentos Regulatorios	Documentos relacionados con regulaciones del sector.	Archivo Digital	Cumplimiento y riesgos	Medio	Confidencial
10	Archivos	Expedientes de asegurados	Archivo digital Servicio de almacenami	Emisión/ Administración - Archivo	Alto	Confidencial

Continúa Tabla 35 en la siguiente página →

Nro.	Activo de Información	Descripción	Ubicación Física	Propietario	Valor del Activo	Clasificación
			ento físico - Externo			
11	Marca	Documentos de marca comercial aspectos de mercadeo y comunicaciones	Archivo Digital	Comercial	Alto	Confidencial
12	Sistema de Respaldo	Copias de seguridad de datos críticos.	Torre Quattro sitio principal (Servidores host)	Tecnología	Alto	Confidencial
13	Comunicaciones y aplicaciones	- Internet dedicado - Servidor de aplicaciones CORE de seguros SISE - Correo Outlook (office 365) - Servidor telefonía IVR (Respuesta de voz interactiva) servidor físico - Servidor aplicaciones de seguridad (antivirus FortiClient EMS) - Servidores de prueba - SQL Desarrollo - Aplicaciones Desarrollo - Estaciones de trabajo (Nivel 1)	Servidores internos	Tecnología	Alto	Confidencial
14	Bases de datos y conexión (servidores internos)	- Servidor Controlador de Dominio (PDC) DOM01 - Servidor Controlador de Dominio (SDC) DOM02 - Base de datos SQL - Dispositivos de almacenamiento (VSAN 140, 41 y 42) - Software de recuperación de datos (DRP)	Servidores internos	Tecnología	Alto	Confidencial

Fuente: elaboración propia

- ✓ **Identificación de los controles de seguridad de la información**
  - Controles organizacionales

A continuación, se presenta la lista de verificación utilizada para verificar el contexto actual de Aseguradora ABANK en contraste a los requisitos de la normativa ISO/IEC 27001:2022, la recolección de la información se realizó, por medio de 3 sesiones, a través de entrevistas al Desarrollador Senior de la Gerencia de tecnología y al Encargado de seguridad de la información y continuidad del negocio perteneciente a la Unidad de Riesgos.

Tabla 36. Lista de verificación – Controles organizacionales. ISO/IEC 27001:2022

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
A.5.1	Políticas de seguridad de la información ¿Poseen una política de seguridad de la información?	La política de seguridad de la información y las políticas de temas específicos deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	Se cumple en su totalidad	Se tiene una política de seguridad de la información	100%
A.5.2	Roles y responsabilidades de seguridad de la información ¿Tienen adecuadamente definidos los roles y responsabilidades?	Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.	Se cumple en su totalidad	En la política de seguridad de la información se han determinado los roles y responsabilidades	100%
A.5.3	Segregación de deberes ¿Existe una segregación de deberes en la organización?	Deben separarse los deberes y las áreas conflictivos de responsabilidad.	Se cumple en su totalidad	Se tienen todos los accesos a sistemas perfilados por usuarios	100%
A.5.4	Responsabilidades de gestión ¿Se realizan actividades de responsabilización sobre la gestión de la seguridad de la información?	La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.	Se cumple en su totalidad	Se realizan actividades de concientización por parte de la gerencia	100%
A.5.5	Contacto con autoridades ¿Se tiene un mapeo y contacto con las autoridades o entes	La organización deberá establecer y mantener contacto con las autoridades pertinentes.	Se cumple en su totalidad	Se tiene contacto con entes reguladores (SSF) y otros relacionados	100%

Continúa Tabla 36 en la siguiente página →

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
	reguladores de la organización?				
A.5.6	Contacto con grupos de interés especial ¿Existe contacto con grupos de interés especial, como revistas tecnológicas, de ciberseguridad, etc.?	La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.	Se cumple en su totalidad	La organización se encuentra suscrita a medios de información y foros de tecnológicos como Infosecurity Magazine	100%
A.5.7	Inteligencia de amenazas ¿Se realizan acciones específicas para mejorar y gestionar la inteligencia y aprendizaje sobre amenazas?	La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para generar información sobre amenazas.	Se tiene una noción vaga del cumplimiento a requisito	No se le da seguimiento al registro de amenazas	
A.5.8	Seguridad de la información en la gestión de proyectos. ¿Existen mecanismos para controlar la seguridad de la información en el desarrollo de proyectos?	La seguridad de la información se integrará en la gestión de proyectos.	Se cumple en su totalidad	Todos los proyectos incluyen valoraciones sobre aspectos de Seguridad de la información	100%
A.5.9	Inventario de información y otros activos asociados ¿Se lleva un inventario de activos de la información adecuado?	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.	Cumple medianamente bien	Se tiene un inventario, pero no se le da seguimiento	50%
A.5.10	Uso aceptable de la información y otros activos asociados ¿Se documentan e implementan reglas para el uso adecuado de los	Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.	Se tiene una noción vaga del cumplimiento a requisito	No se tienen instructivos o manuales para el manejo de la seguridad de la información, solamente se tienen apartados genéricos en la política de seguridad de la información	30%

Continúa Tabla 36 en la siguiente página →

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
	activos de la información?				
A.5.11	Devolución de activos ¿Existe un mecanismo para la devolución de activos?	El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización en su posesión al momento del cambio o terminación de su empleo, contrato o acuerdo.	No se cumple en su totalidad	No se cumple	0%
A.5.12	Clasificación de la información ¿Se realizan gestiones para la clasificación de la información?	La información se clasificará de acuerdo con la seguridad de la información y las necesidades de la organización basadas en la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.	Se tiene una noción vaga del cumplimiento a requisito	Se tiene una clasificación genérica en la política de seguridad de la información, solamente detalla que existen "documentos confidenciales" y "documentos no confidenciales"	30%
A.5.13	Etiquetado de información ¿Existe un mecanismo para el etiquetado de la información?	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Se tiene una noción vaga del cumplimiento a requisito	En algunos casos como en los servidores físicos y equipos de cómputo sí se implementan etiquetas, pero no en todo tipo de equipos y no se lleva control sobre ello.	30%
A.5.14	Transferencia de información ¿Existe gestiones adecuadas la transferencia de información?	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	No se cumple en su totalidad	No cumple	0%
A.5.15	Control de acceso ¿Se tiene un protocolo o mecanismo de Control de acceso?	Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros	Se tiene una noción vaga del cumplimiento a requisito	Se tiene control de acceso en ciertas áreas como de servidores, pero no para toda las áreas que involucren activos de	30%

Continúa Tabla 36 en la siguiente página →

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
		activos asociados en función de los requisitos de seguridad empresarial y de la información.		información confidenciales	
A.5.16	Gestión de identidad ¿Se gestiona la identificación y trazabilidad de las entidades que usan el software de la aseguradora?	Se gestionará el ciclo de vida completo de las identidades.	No se cumple en su totalidad	No cumple	0%
A.5.17	Información de autenticación ¿Existen mecanismos de información de autenticación?	La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	No se cumple en su totalidad	No cumple	0%
A.5.18	Derechos de acceso ¿Existen protocolos o mecanismos para gestionar los Derechos de acceso?	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.	Se tiene una noción vaga del cumplimiento a requisito	Los derechos de acceso se han descrito en política, pero no se da seguimiento ni cumplimiento en su totalidad	30%
A.5.19	Seguridad de la información en las relaciones con los proveedores ¿Se garantiza la seguridad de la información con respecto a los proveedores y/o partes interesadas?	Se deben definir e implementar procesos y procedimientos para gestionarlos riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.	Se tiene una noción vaga del cumplimiento a requisito	No existen procesos para el control de la seguridad de la información con proveedores, solamente se trata a nivel verbal y de contrato de forma genérica	30%

Continúa Tabla 36 en la siguiente página →

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
A.5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores ¿Se aborda la seguridad de la información en los acuerdos de servicios?	Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor.	Cumple medianamente bien	Se plasman de forma genérica, en algunas ocasiones, en los contratos	50%
A.5.22	Supervisión, revisión y gestión del cambio de servicios de proveedores ¿Se poseen mecanismos para la administración y monitoreo de cambios en servicios realizados por parte de proveedores?	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.	No se cumple en su totalidad	No cumple	0%
A.5.23	Seguridad de la información para el uso de servicios en la nube ¿Se poseen mecanismos o protocolos para la seguridad de la información en la nube?	Procesos de adquisición, uso, gestión y salida de servicios en las nubes establecerán de acuerdo con los requisitos de seguridad de la información de la organización.	No se cumple en su totalidad	No cumple	0%
A.5.24	Incidente de seguridad de la información, planificación y preparación de la gestión a realizar ¿Existe algún mecanismo para la gestión de incidentes?	La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando la información. Procesos, roles y responsabilidades de gestión de incidentes de seguridad.	Se cumple en su totalidad	Se atienden los incidentes según plan de recuperación y atención ante incidentes tecnológicos	100%

Continúa Tabla 36 en la siguiente página →

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
A.5.25	Evaluación y decisión sobre eventos de seguridad de la información ¿Se poseen alternativas para la evaluación sobre eventos de seguridad de la información?	La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.	Cumple medianamente bien	Se evalúan al haber ocurrido, pero no se da seguimiento	50%
A.5.26	Respuesta a la seguridad de la información incidentes ¿Existen procedimientos o mecanismos para la respuesta ante incidentes?	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Se cumple en su totalidad	Se responde de acuerdo al Plan de Recuperación de Desastres DRP	100%
A.5.27	Aprender de los incidentes de seguridad de la información ¿Se aprende sobre los incidentes de seguridad de la información, de qué manera?	El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información.	Se cumple en su totalidad	Se analizan los incidentes y se plantean planes de acción de mejora	100%
A.5.28	Recolección de evidencia ¿Se realizan acciones para la recolección de evidencia ante eventos de seguridad de la información?	La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	Cumple medianamente bien	No se tienen procedimientos oficializados	50%
A.5.29	Seguridad de la información durante la interrupción ¿Se garantiza la seguridad de la información ante interrupciones?	La organización debe planificar cómo mantener la seguridad de la información a un nivel apropiado durante la interrupción.	Cumple medianamente bien	No se lleva planificación sobre la recuperación a nivel detallado	50%

Continúa Tabla 36 en la siguiente página →

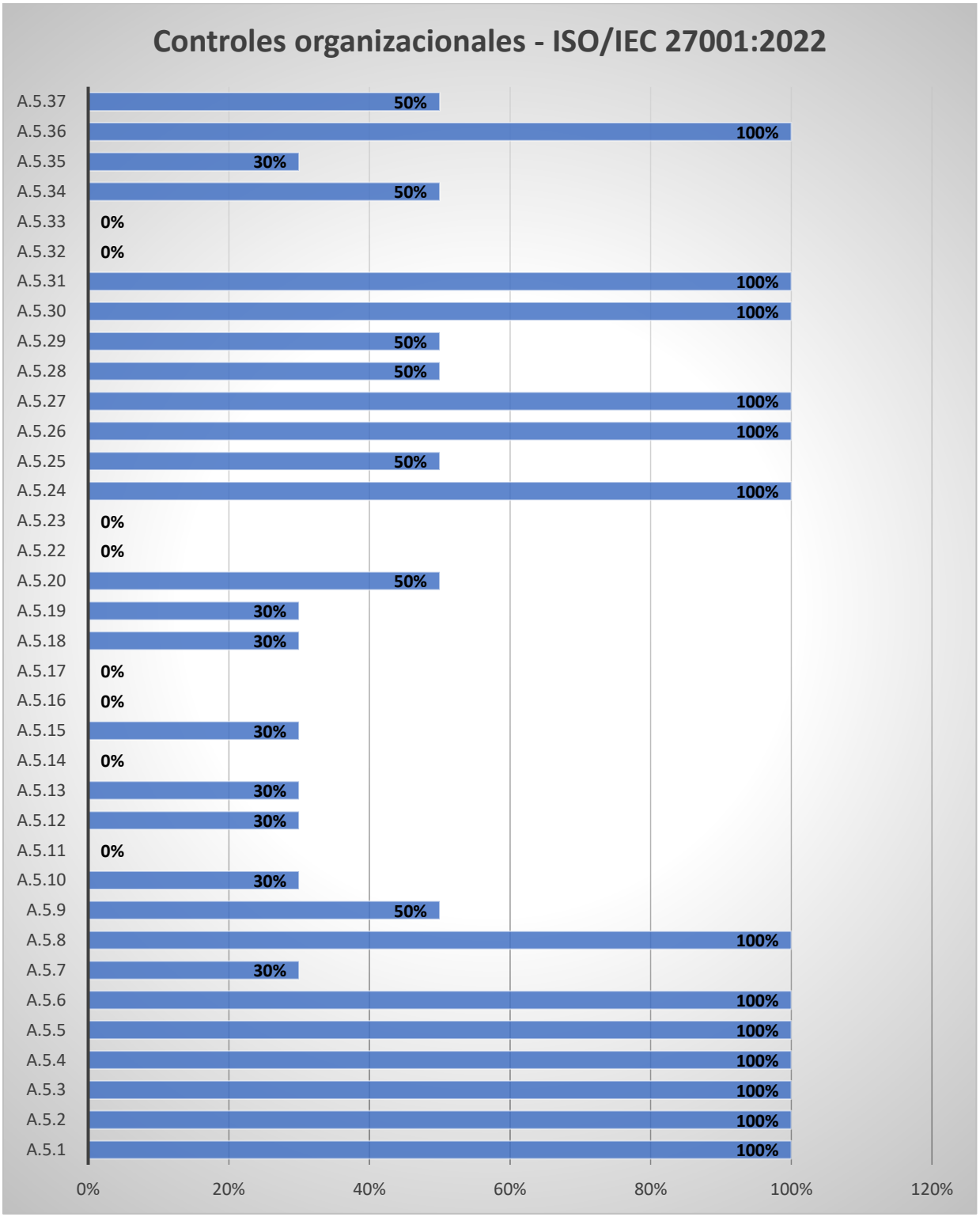
Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
A.5.30	Preparación de las TIC para la continuidad del negocio ¿Existe un mecanismo para preparar las TIC ante aspectos de Continuidad del Negocio?	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	Se cumple en su totalidad	Se implementa por medio de un programa anual	100%
A.5.31	Legales, estatutarias, reglamentarias y requisitos contractuales ¿Se cuenta documentación sobre políticas, códigos de seguridad y otros documentos regulatorios que apliquen a la aseguradora?	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.	Se cumple en su totalidad	Se cumple con las normativas nacionales orientadas a seguridad de la información (NRP-23)	100%
A.5.32	Derechos de propiedad intelectual ¿Existen acciones ante la protección de la propiedad intelectual referente a seguridad de la información?	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.	No se cumple en su totalidad	No se cumple	0%
A.5.33	Protección de registros ¿Se realizan acciones para la protección de registros?	Los registros se protegerán contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	No se cumple en su totalidad	No se cumple	0%
A.5.34	Privacidad y protección de la persona toda la información identificable (PII) ¿Existen mecanismos para la privacidad y protección de PII (Información de	La organización debe identificar y cumplir los requisitos relativos a la preservación de la privacidad y la protección de la PII de acuerdo con leyes y reglamentos y requisitos contractuales.	Cumple medianamente bien	Se da cumplimiento a requisitos normativos, no en su totalidad a otros tipos (contractuales, etc.)	50%

Continúa Tabla 36 en la siguiente página →

Nro.	Elemento/Pregunta	Descripción	Cumplimiento	Detalle	Valoración
	identificación personal)?				
A.5.35	Revisión independiente de información de seguridad ¿Existen acciones de revisión independiente sobre la seguridad de la información?	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.	Se tiene una noción vaga del cumplimiento a requisito	No se realizan auditorías de tecnología focalizadas; solamente se reciben aleatoriamente y no frecuentemente auditoría externa regulatoria por parte de la Súper Intendencia del Sistema Financiero.	30%
A.5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información ¿Se da cumplimiento a políticas, normas, etc. relacionadas a seguridad de la información de la aseguradora?	El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos del tema se revisará periódicamente.	Se cumple en su totalidad	Se revisa, se da seguimiento y se concientiza sobre el tema	100%
A.5.37	Procedimientos operativos documentados ¿Se poseen procedimientos operativos documentados en cuanto a la seguridad de la información?	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.	Cumple medianamente bien	No se tiene procedimientos documentados, solo se realizan las acciones de forma verbal y con documentos no formales.	50%

Fuente: elaboración propia

Figura 38. Apartado 5. Controles organizacionales – ISO/IEC 27001:2022



Fuente: elaboración propia

Análisis final: El cumplimiento promedio del 53% en el apartado de "Controles organizacionales" según la norma ISO/IEC 27001:2022 es un logro significativo para una organización de seguros. Esto indica que la empresa ha implementado y mantenido un conjunto sólido de controles organizacionales diseñados para proteger la confidencialidad, integridad y disponibilidad de la información crítica de sus clientes y operaciones.

- Controles de personas

Tabla 37. Lista de verificación – Controles de personas. ISO/IEC 27001:2022

Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
A.6.1	Poner en pantalla (Screening) ¿Se cuenta con un mecanismo para evaluar e identificar a los aspirantes o candidatos a cargos dentro de la aseguradora?	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.	Se tiene una noción vaga del cumplimiento a requisito	Se analizan temas de seguridad de la información de forma genérica en los aspirantes a cargos relacionados con IT.	30%
A.6.2	Términos y condiciones de empleo ¿En los acuerdos de contratación se contempla temas de seguridad de la información?	Los acuerdos contractuales de trabajo deberán expresar el personal y responsabilidades de la organización para la seguridad de la información.	Cumple medianamente bien	Se contempla en los contratos laborales temas de seguridad de la información de forma genérica	50%
A.6.3	Conciencia de seguridad de la información, educación y formación ¿Se hace conciencia al personal de la organización sobre temas relacionados a	El personal de la organización y las partes interesadas relevantes recibirán conciencia, educación y capacitación apropiadas sobre la seguridad de la información y actualizaciones periódicas de la política	Cumple medianamente bien	Se procura concientizar sobre el tema pero no constantemente	50%

Continúa Tabla 37 en la siguiente página →

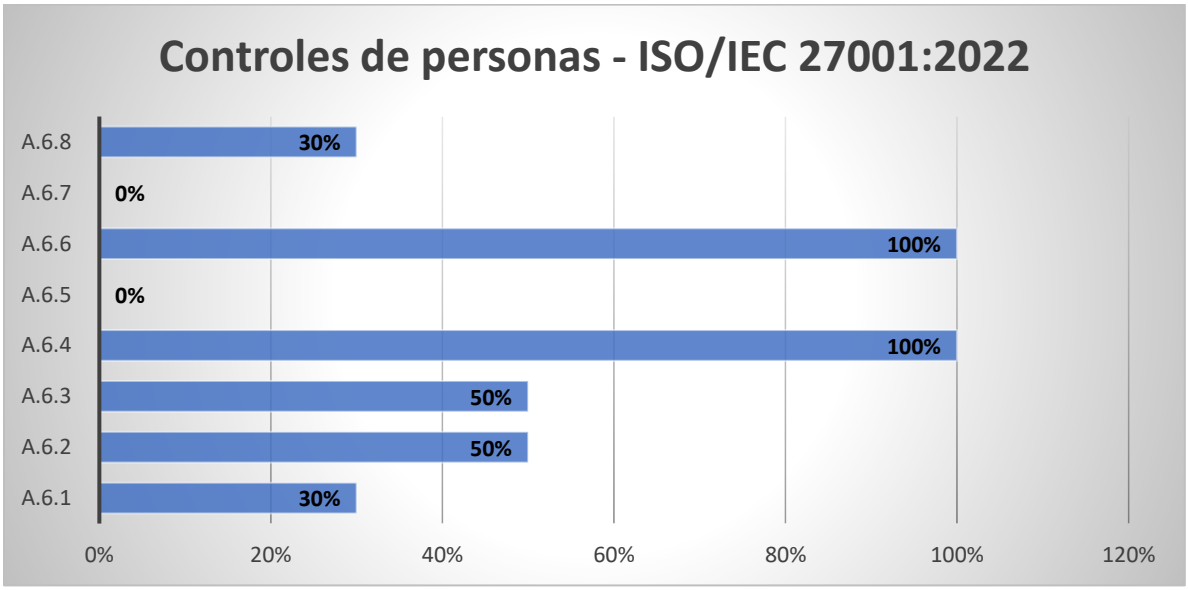
Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
	seguridad de la información?	de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral.			
A.6.4	Proceso Disciplinario ¿Existen procesos disciplinarios para colaboradores de la organización que no respeten o violenten las políticas de la seguridad de la información?	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.	Se cumple en su totalidad	Se realizan acciones ante violaciones de seguridad de la información	100%
A.6.5	Responsabilidades después de la terminación o cambio de empleo ¿Se ejecutan acciones o protocolos específicos para garantizar la seguridad de la información luego de la terminación de los contratos?	Responsabilidades y deberes de seguridad de la información que siguen siendo válidos después la terminación o el cambio de empleo se definirán, ejecutarán y comunicarán al personal pertinente y otras partes interesadas.	No se cumple en su totalidad	No cumple	0%
A.6.6	Confidencialidad o no divulgación acuerdos ¿Existen mecanismos para garantizar la confidencialidad y privacidad de la seguridad de la organización en la aseguradora?	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deberán ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.	Se cumple en su totalidad	Se firman acuerdos de confidencialidad para personal que ingresa	100%
A.6.7	Trabajo remoto ¿Existe mecanismos de control de trabajo remoto?	Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la	No se cumple en su totalidad	No cumple	0%

Continúa Tabla 37 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
		información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.			
A.6.8	Reporte de eventos de seguridad de la información ¿Existen formas en las que se gestionan y ejecutan reportes sobre eventos de seguridad de la información?	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través decanales de manera oportuna.	Se tiene una noción vaga del cumplimiento a requisito	No se tiene un mecanismo formal, solo de forma verbal	30%

Fuente: elaboración propia

Figura 39. Apartado 6. Controles de personas – ISO/IEC 27001:2022



Fuente: elaboración propia

Análisis final: El cumplimiento promedio del 45% en el apartado de "Controles de personas" según la norma ISO/IEC 27001:2022 plantea desafíos y áreas de mejora significativas para una organización de seguros. Este nivel de cumplimiento sugiere que la empresa necesita fortalecer sus políticas y prácticas relacionadas con la gestión y supervisión de su personal en lo que respecta a la seguridad de la información.

Es fundamental que la organización invierta en la formación y concienciación de su equipo, establezca controles más sólidos para la gestión de contraseñas y el acceso a datos sensibles, y promueva una cultura de seguridad robusta entre sus empleados. Dado que la seguridad de la información es esencial en el sector de seguros, abordar estas deficiencias en los controles de personas es crucial para garantizar la protección de los activos.

- Controles físicos

Tabla 38. Lista de verificación – Controles físicos. ISO/IEC 27001:2022

Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
A.7.1	Perímetros físicos de seguridad ¿Se han establecido mecanismos físicos de seguridad=	Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.	Se tiene una noción vaga del cumplimiento a requisito	Se tienen perímetros de seguridad solamente para área de servidores físicos, no para los demás activos de información	30%
A.7.2	Entrada física ¿Existen controles de entrada física?	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.	No se cumple en su totalidad	No cumple	0%
A.7.3	Protección de oficinas, salas e instalaciones ¿Existen mecanismos de protección de oficinas, salas e instalaciones?	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.	Se cumple en su totalidad	Existe seguridad en ingreso a salas y oficinas	100%
A.7.4	Monitoreo de seguridad física ¿Se realizan gestiones para el adecuado monitoreo de seguridad física?	Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.	Se cumple en su totalidad	Se monitorea a través de cámaras de vigilancia	100%
A.7.5	Protección contra amenazas físicas y ambientales.	Protección contra amenazas físicas y ambientales, tales como deben diseñarse e	Se cumple en su totalidad	Se cumple con requisitos normativos con respecto a seguridad ante	100%

Continúa Tabla 38 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
	¿Cómo se asegura la empresa contra amenazas físicas y ambientales en sus instalaciones y operaciones?	implementarse desastres y otras amenazas físicas intencionales o no intencionales a la infraestructura.		amenazas físicas y ambientales. Existe un comité de Seguridad Ocupacional	
A.7.6	Trabajar en áreas seguras ¿Qué medidas se implementan para garantizar un entorno de trabajo seguro en todas las áreas de la empresa?	Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.	Se cumple en su totalidad	Se han estructurado adecuadamente las áreas de trabajo, en cumplimiento a normativas y leyes vigentes que lo regulan.	100%
A.7.7	Escritorio y pantalla despejada ¿Existen mecanismos para gestionar variables como escritorio y pantalla despejada para mantener la limpieza y evitar la exposición de información crítica?	Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.	No se cumple en su totalidad	No se cumple	0%
A.7.8	Emplazamiento y protección de equipos ¿Qué medidas se toman para garantizar el emplazamiento adecuado y la protección de los equipos críticos en la empresa?	El equipo se colocará de forma segura y protegida.	Cumple medianamente bien	Se cumple, pero sin un seguimiento adecuado o para todos los casos que lo ameriten, no existen procedimientos específicos	50%
A.7.9	Seguridad de los activos fuera de las instalaciones ¿Qué protocolos existen para garantizar la seguridad de los	Se protegerán los activos fuera del sitio.	Se tiene una noción vaga del cumplimiento a requisito	No se tiene un control y seguimiento específico para estos casos, pero sí se considera a nivel verbal	30%

Continúa Tabla 38 en la siguie

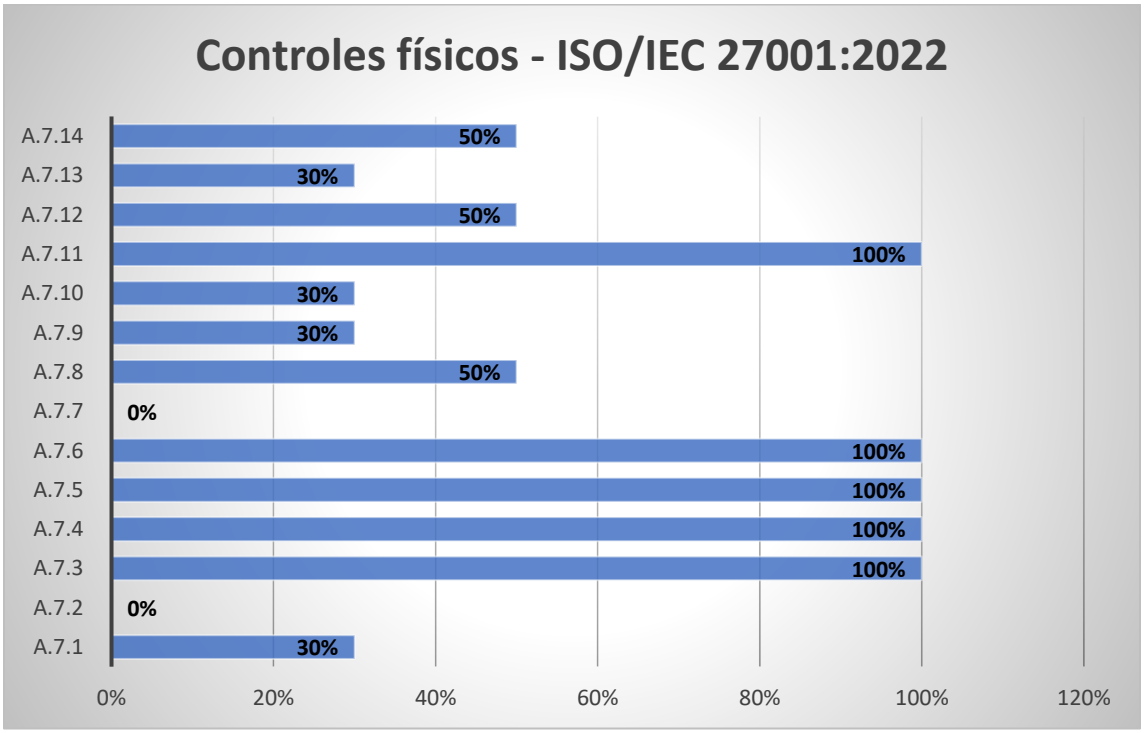
Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
	activos cuando se encuentran fuera de las instalaciones de la empresa?				
A.7.10	Medios de almacenamiento ¿Cómo se asegura la protección y la integridad de los datos almacenados en los diferentes medios de almacenamiento utilizados por la empresa?	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	Se tiene una noción vaga del cumplimiento a requisito	No se tienen procedimientos o metodologías documentadas para su gestión, solo a nivel verbal	30%
A.7.11	Utilidades de apoyo ¿Qué medidas se implementan para garantizar la seguridad y disponibilidad de las utilidades de apoyo críticas para las operaciones de la empresa?	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.	Se cumple en su totalidad	Se cuenta con planta eléctrica, servidores de contingencia y otros medios para atender emergencias por fallos o incidentes	100%
A.7.12	Seguridad del cableado ¿Qué medidas se toman para asegurar la seguridad y la integridad del cableado utilizado en las instalaciones de la empresa?	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.	Cumple medianamente bien	Algunos cableados de red de la organización se protegen, no adecuadamente algunos o no en su totalidad	50%
A.7.13	Mantenimiento de equipo ¿Cómo se gestiona y lleva a cabo el mantenimiento del equipo para	El equipo se mantendrá correctamente para garantizar la disponibilidad, la integridad y	Se tiene una noción vaga del cumplimiento a requisito	Se da mantenimiento correctivo, no preventivo. No se lleva un control sobre estas actividades	30%

Continúa Tabla 38 en la siguiente

Nro.	Elemento	Descripción	Cumplimiento	Detalle	Valoración
	garantizar su funcionamiento óptimo y seguro?	confidencialidad de la información.			
A.7.14	Eliminación segura o reutilización de equipos ¿Cuáles son los procedimientos establecidos para garantizar la eliminación segura o la reutilización adecuada de equipos obsoletos o fuera de servicio?	Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.	Cumple medianamente bien	No se siguen procedimientos o metodologías específicas, solamente se realiza por costumbre	50%

Fuente: elaboración propia

Figura 40. Apartado 7. Controles físicos – ISO/IEC 27001:2022



Fuente: elaboración propia

Análisis final: El cumplimiento promedio del 55% en el apartado de "Controles físicos" según la norma ISO/IEC 27001:2022 es un indicativo positivo para una organización de seguros. Esto implica que la empresa ha implementado una serie de medidas sólidas para proteger sus instalaciones y activos físicos relacionados con la seguridad de la información. Estos controles incluyen aspectos como la protección de servidores, la gestión de accesos a las áreas críticas, la monitorización de sistemas de seguridad, entre otros.

Este nivel de cumplimiento refleja un compromiso con la seguridad física de los datos, lo que es esencial en el sector de seguros donde la confidencialidad y la integridad de la información son de suma importancia para garantizar la confianza de los clientes y el cumplimiento normativo.

- Controles tecnológicos

Tabla 39. Lista de verificación – Controles tecnológicos. ISO/IEC 27001:2022

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
A.8.1	Dispositivos de punto final de usuario ¿Cómo se asegura la protección y el control de los dispositivos de punto final de usuario en la red de la empresa?	Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.	Cumple medianamente bien	Se cuenta con protección de antivirus, reglas de restricción de red, entre otros	50%
A.8.2	Derechos de acceso privilegiado ¿Cómo se gestionan y controlan los derechos de acceso privilegiado a sistemas y datos críticos dentro de la empresa?	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	Se cumple en su totalidad	Se tienen accesos de usuarios perfilados	100%
A.8.3	Restricción de acceso a la información ¿Qué medidas se implementan para restringir el acceso no autorizado a la información confidencial de la empresa?	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.	Se cumple en su totalidad	Se cuenta con doble factor de autenticación, reglas de red, entre otros según política de seguridad de la información	100%

Continúa Tabla 39 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
A.8.4	Acceso al código fuente ¿Cómo se controla y gestiona el acceso al código fuente de los sistemas de la empresa para garantizar su seguridad e integridad?	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.	Se cumple en su totalidad	Se poseen protocolos seguros de acceso a códigos fuentes de sistemas	100%
A.8.5	Autenticación segura ¿Qué métodos de autenticación segura se emplean para verificar la identidad de los usuarios que acceden a los sistemas y datos sensibles de la empresa?	Se implementarán tecnologías y procedimientos de autenticación segura basada en las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.	Se tiene una noción vaga del cumplimiento a requisito	Se posee doble factor de autenticación, pero no se tiene documentación o control específico para seguimiento.	30%
A.8.6	Gestión de capacidad ¿Cómo se gestiona y planifica la capacidad de los recursos informáticos para garantizar un rendimiento óptimo y prevenir sobrecargas en los sistemas de la empresa?	El uso de los recursos se controlará y ajustará de acuerdo con las normas vigentes y requisitos de capacidad esperados.	Se cumple en su totalidad	Se ajustan y gestionan los recursos tecnológicos con forme a los requisitos de normativas y leyes (NRP-23)	100%
A.8.7	Protección contra malware ¿Qué medidas se implementan para proteger los sistemas de la empresa contra malware y otras amenazas cibernéticas?	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	Cumple medianamente bien	Se concientiza al personal, pero no de forma constante y periódica	50%
A.8.8	Gestión de vulnerabilidades técnicas ¿Cómo se lleva a cabo la gestión de vulnerabilidades técnicas en los sistemas de la empresa para identificar, evaluar y mitigar posibles	Información sobre vulnerabilidades técnicas de los sistemas de información a partir del uso, la exposición de la organización a tales vulnerabilidades será evaluadas y se tomarán las medidas apropiadas.	Cumple medianamente bien	Se identifican vulnerabilidades de forma reactiva, no se poseen documentación ni controles para su seguimiento	50%

Continúa Tabla 39 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
	riesgos de seguridad?				
A.8.9	Gestión de la configuración ¿Cómo se gestiona y controla la configuración de los sistemas y dispositivos de la empresa para garantizar su seguridad y coherencia?	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, supervisarse y revisarse.	No se cumple en su totalidad	No cumple	0%
A.8.10	Eliminación de información ¿Cuáles son los procedimientos establecidos para garantizar la eliminación segura y completa de información confidencial cuando ya no es necesaria?	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.	Se cumple en su totalidad	Se elimina información según política organización y según normativas y leyes nacionales	100%
A.8.11	Enmascaramiento de datos ¿Qué prácticas se aplican para enmascarar datos confidenciales y proteger la privacidad de la información durante pruebas y desarrollo de software?	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.	Se tiene una noción vaga del cumplimiento a requisito	Se realiza enmascaramiento de datos y red, pero no se llevan un control documentado sobre ello	30%
A.8.12	Prevención de fuga de datos ¿Qué medidas se toman para prevenir la fuga de datos sensibles fuera de la red de la empresa?	Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	No se cumple en su totalidad	No se cumple	0%
A.8.13	Copia de seguridad de la información ¿Cómo se asegura la realización regular y la integridad de las copias de	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán regularmente de acuerdo con la	Se cumple en su totalidad	Se realizan copias de seguridad por medio de nube y servidores virtuales	

Continúa Tabla 39 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
	seguridad de la información crítica de la empresa?	política específica de copias de seguridad.			
A.8.14	Redundancia de las instalaciones de procesamiento de información ¿Qué medidas se implementan para garantizar la redundancia de las instalaciones de procesamiento de información y minimizar el riesgo de interrupciones del servicio?	Las instalaciones de procesamiento de información se implementarán con redundancia suficiente para cumplir con los requisitos de disponibilidad.	Se cumple en su totalidad	Se poseen servidores y sistemas alternos en casos de contingencia y/o falla	100%
A.8.15	Inicio sesión ¿Qué medidas se aplican para asegurar la autenticación segura y el registro adecuado de inicio de sesión de los usuarios en los sistemas de la empresa?	Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.	Se tiene una noción vaga del cumplimiento a requisito	Se implementan controles de inicio de sesión, pero no se deja registro sobre ello, en alguna base de datos o bitácora	30%
A.8.16	Actividades de seguimiento ¿Cómo se registran y supervisan las actividades de los usuarios en los sistemas de la empresa para garantizar la seguridad y la integridad de los datos?	Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se tomarán las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.	No se cumple en su totalidad	No se cumple	0%
A.8.17	Sincronización de reloj ¿Cómo se asegura la sincronización precisa de los relojes en los sistemas de la empresa para garantizar la integridad de los registros y la coordinación de eventos?	Los relojes de los sistemas de procesamiento de información utilizados por la organización se sincronizarán con las fuentes de tiempo aprobadas.	Se cumple en su totalidad	Se sincroniza reloj según hora mundial de internet en concordancia con la zona horaria	100%

Continúa Tabla 39 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
A.8.18	Uso de programas de utilidad privilegiados ¿Cómo se controla y supervisa el uso de programas de utilidad privilegiados para garantizar su uso apropiado y evitar posibles riesgos de seguridad?	El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.	Se cumple en su totalidad	Se tienen controles de usuarios según perfil	100%
A.8.19	Instalación de software en sistemas operativos ¿Cuáles son los procedimientos establecidos para la instalación de software en los sistemas operativos de la empresa, y cómo se asegura la conformidad con las políticas de seguridad?	Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	Se cumple en su totalidad	Se realizan controles de seguridad de la información para controlar las instalaciones de software en equipo tecnológico de la aseguradora	100%
A.8.20	Seguridad en redes ¿Qué medidas se implementan para garantizar la seguridad de las redes de la empresa contra accesos no autorizados y amenazas cibernéticas?	Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.	Se cumple en su totalidad	Se poseen protocolos actualizados de seguridad	100%
A.8.21	Seguridad de los servicios de red. ¿Cómo se asegura la seguridad de los servicios de red para proteger la integridad y confidencialidad de los datos transmitidos y recibidos?	Mecanismos de seguridad, niveles de servicio y requisitos de servicio de la red deben ser identificados, implementados y monitoreados.	Se tiene una noción vaga del cumplimiento a requisito	Se posee controles de seguridad de red, pero los softwares con los que cuenta en la actualidad la empresa no permiten dar seguimiento o tracking a todas las gestiones que controlan	30%
A.8.22	Segregación de redes ¿Qué medidas se toman para asegurar la	Los grupos de servicios de información, usuarios y sistemas de información deben	Se cumple en su totalidad	Existen protocolos de segregación en todas las redes	100%

Continúa Tabla 39 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
	adecuada segregación de redes y prevenir el acceso no autorizado entre diferentes segmentos de la red de la empresa?	estar segregados en las redes de la organización.		internas de la aseguradora	
A.8.23	Filtrado web ¿Qué políticas y herramientas se utilizan para implementar un filtrado web efectivo y proteger la red de la empresa contra contenido malicioso y no deseado?	El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.	Se cumple en su totalidad	Se implementan reglas de filtrado WEB en todos los equipos de la organización según perfil de usuario	100%
A.8.24	Uso de criptografía ¿Cómo se utiliza la criptografía para proteger la confidencialidad y la integridad de los datos sensibles de la empresa?	Reglas para el uso efectivo de la criptografía, incluida la clave criptográfica debe ser definida e implementada.	Se tiene una noción vaga del cumplimiento a requisito	No se utiliza criptografía para toda infraestructura de la organización	30%
A.8.25	Ciclo de vida de desarrollo seguro ¿Cuáles son las prácticas y procesos implementados para garantizar un ciclo de vida de desarrollo seguro en los proyectos de software de la empresa?	Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.	Se tiene una noción vaga del cumplimiento a requisito	No se tiene una metodología específica documentada, solamente a nivel verbal se contempla en ciclo de vida del desarrollo de software	30%
A.8.26	Requisitos de seguridad de la aplicación ¿Cómo se asegura que los requisitos de seguridad de las aplicaciones sean identificados, documentados y cumplidos durante el desarrollo y mantenimiento de software?	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.	Se tiene una noción vaga del cumplimiento a requisito	Se identifican a nivel verbal, pero no se documenta y se les da seguimiento	30%
A.8.27	Arquitectura segura del sistema	Se deben establecer principios para la ingeniería de sistemas	Se tiene una noción vaga del	Se identifican a nivel verbal, pero no se documenta	30%

Continúa Tabla 39 en la siguiente página →

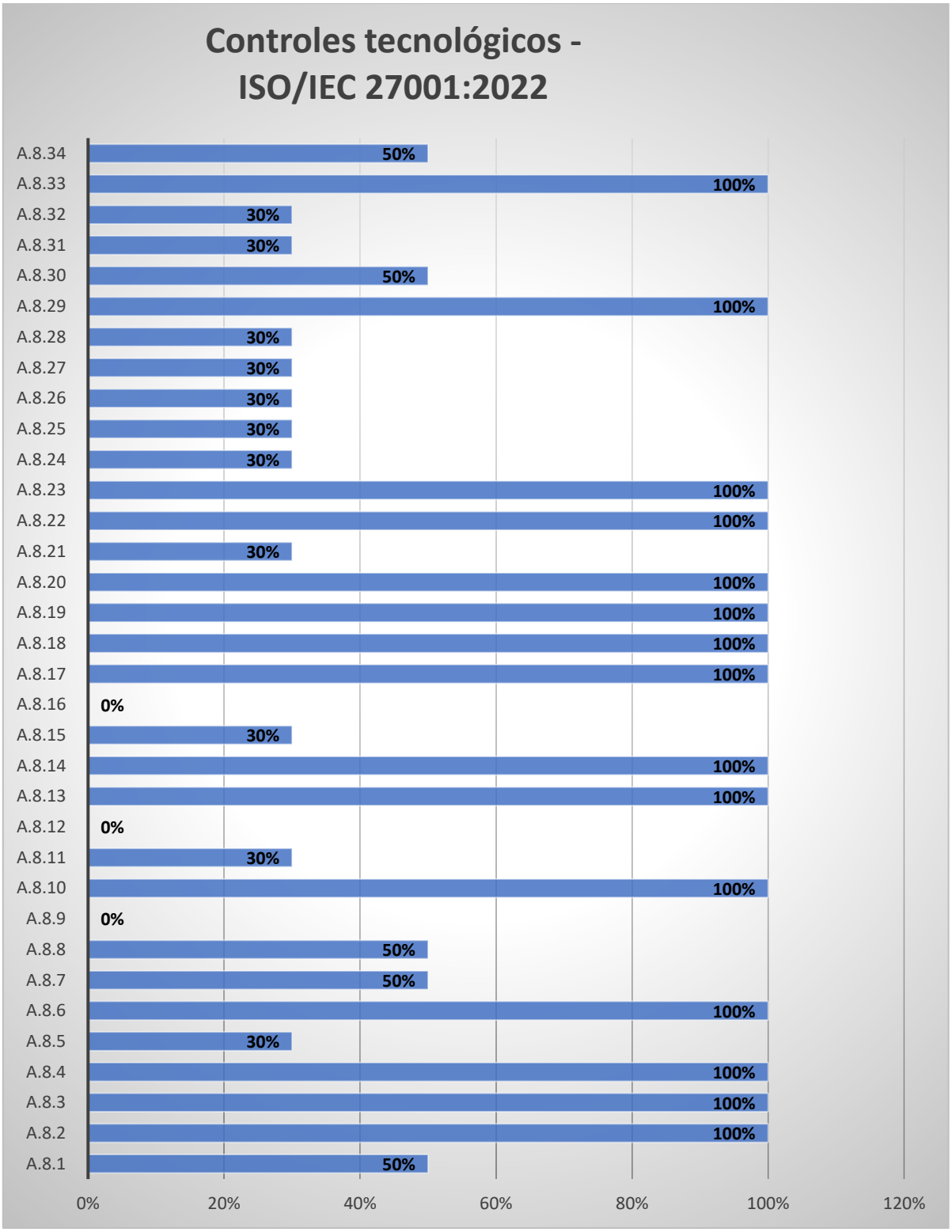
Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
	y principios de ingeniería ¿Qué principios de ingeniería se siguen para garantizar una arquitectura segura del sistema, y cómo se aplican en el diseño y desarrollo de sistemas de la empresa?	seguros, documentados, mantenido y aplicado a cualquier desarrollo de sistema de información actividades.	cumplimiento a requisito	y se les da seguimiento	
A.8.28	Codificación segura ¿Qué medidas se toman para garantizar la codificación segura de las aplicaciones y sistemas de la empresa, minimizando así las vulnerabilidades de seguridad?	Los principios de codificación segura se aplicarán al desarrollo de software.	Se tiene una noción vaga del cumplimiento a requisito	Se identifican a nivel verbal, pero no se documenta y se les da seguimiento	30%
A.8.29	Pruebas de seguridad en desarrollo y aceptación ¿Qué métodos se emplean para realizar pruebas de seguridad durante el desarrollo y la aceptación de sistemas y aplicaciones?	Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.	Se cumple en su totalidad	Se aplican pruebas de desarrollo tanto en ambiente de pruebas como en desarrollo para garantizar la seguridad de la información y el cumplimiento exitoso al desarrollo realizado	100%
A.8.30	Desarrollo subcontratado ¿Cómo se asegura que el desarrollo subcontratado cumpla con los estándares de seguridad y las políticas de la empresa?	La organización debe dirigir, monitorear y revisar las actividades relacionadas al desarrollo de sistemas subcontratados.	Cumple medianamente bien	No se da seguimiento a nivel documentado, solo a nivel verbal	50%
A.8.31	Separación de desarrollo, prueba y entornos de producción ¿Cómo se garantiza la separación	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.	Se tiene una noción vaga del cumplimiento a requisito	Se posee ambos ambientes, pero no se gestionan a nivel de un enfoque de seguridad de la información	30%

Continúa Tabla 39 en la siguiente página →

Nro.	Elemento	Descripción	Cumplimento	Detalle	Valoración
	efectiva entre los entornos de desarrollo, prueba y producción para minimizar los riesgos de seguridad y garantizar la integridad de los sistemas?				
A.8.32	Gestión del cambio ¿Cómo se gestionan y documentan los cambios en los sistemas y procesos de la empresa para garantizar la seguridad y la continuidad del negocio?	Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.	Se tiene una noción vaga del cumplimiento a requisito	No se realizan acciones de gestión de cambio seguras bajo procedimientos específicos, solamente a nivel verbal	30%
A.8.33	Información de prueba ¿Cómo se asegura la protección de la información de prueba para evitar la exposición de datos sensibles durante las pruebas de sistemas y aplicaciones?	La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.	Se cumple en su totalidad	Se realizan resguardos seguros de resultados de pruebas funcionales	100%
A.8.34	Protección de los sistemas de información durante las pruebas de auditoría ¿Qué medidas se implementan para proteger la integridad y la confidencialidad de los sistemas de información durante las pruebas de auditoría?	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de sistemas operativos se planificarán y acordarán entre el probador y la dirección adecuada.	Cumple medianamente bien	Se realizan monitoreos esporádicos y sin planificación específica para la protección de pruebas de auditoría	50%

Fuente: elaboración propia

Figura 41. Apartado 8. Controles tecnológicos – ISO/IEC 27001:2022



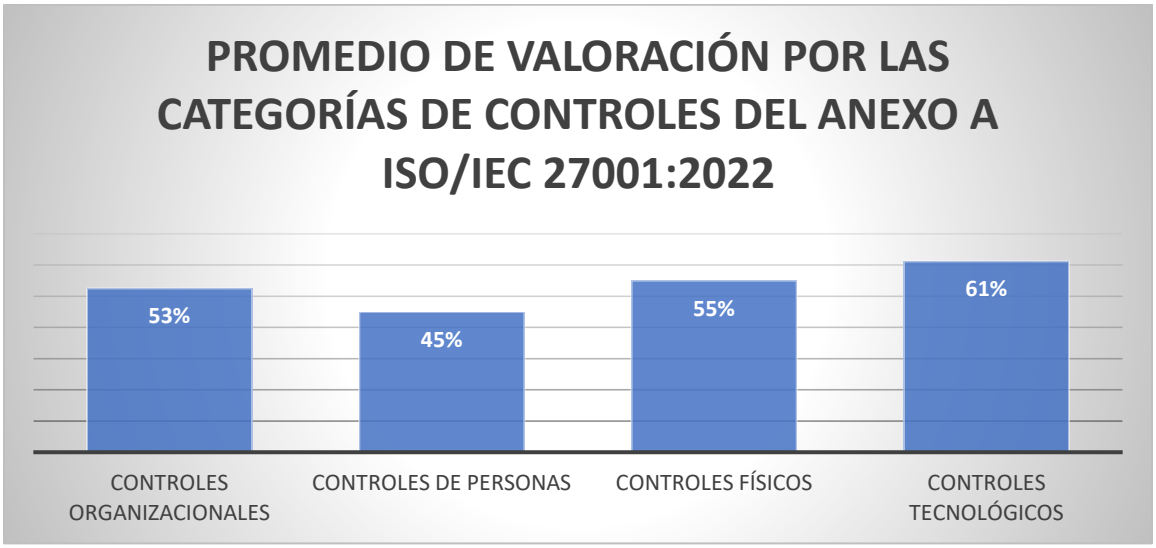
Fuente: elaboración propia

Análisis final: El cumplimiento promedio del 61% en el apartado de "Controles tecnológicos" según la norma ISO/IEC 27001:2022 es un logro alentador para una organización de seguros. Esto indica que la empresa ha implementado una amplia gama de controles tecnológicos para salvaguardar la seguridad de su infraestructura de tecnología de la información.

Estos controles pueden incluir medidas como firewalls robustos, detección de intrusiones, cifrado de datos, gestión de parches y actualizaciones, entre otros. Un cumplimiento del 61% demuestra un sólido compromiso con la protección de la información y la mitigación de riesgos cibernéticos en un sector donde la confidencialidad y la disponibilidad de datos son cruciales. Esto contribuye a fortalecer la posición de la organización en un entorno empresarial cada vez más digitalizado y su capacidad para brindar un servicio seguro y confiable a sus clientes.

- Resultado de todos los controles Anexo A, ISO/IEC 27001:2022

Figura 42.– Consolidado de resultados



Fuente: elaboración propia

Análisis final: El resultado del promedio de todas las categorías del Anexo A (Controles de seguridad de la información) de la normativa ISO/IEC 27001:2015 es de 53%, la evaluación arrojó una imagen variada pero globalmente positiva de la postura de seguridad de nuestra organización. Los controles organizacionales, con un cumplimiento del 53%, indican un esfuerzo sólido en la gestión y las políticas de seguridad.

Por otro lado, existe margen para mejorar en el ámbito de los controles de personas, donde alcanzamos un 45%. Esto sugiere la necesidad de un mayor énfasis en la formación y concienciación de los empleados. Por otro lado, los controles físicos, con un cumplimiento del 55%, y los controles tecnológicos, con un impresionante 61%, reflejan una infraestructura de seguridad sólida en términos de protección física y cibernética.

3.12.2 Resumen de los resultados

Finalmente, el presente capítulo ha proporcionado los fundamentos metodológicos para llevar a cabo el trabajo de graduación. Se ha establecido el tipo de investigación realizado, la población y muestra seleccionada, así como los métodos, técnicas e instrumentos utilizados para recopilar y analizar los datos, los cuales son fundamentales para garantizar la validez y la confiabilidad de los resultados de la investigación.

Con el marco metodológico establecido, se sientan las bases para adentrarnos en el siguiente capítulo, donde se abordará el control administrativo del trabajo de graduación, permitiendo así una comprensión más profunda y detallada del proceso de esta investigación.

Tabla 40. Resumen de resultados obtenidos por variables

#	Variable	Indicadores a evaluar	Resultados/hallazgos	Meta ideal
1	Grado de conformidad con respecto a requisitos de Calidad	Identificación del cumplimiento de la organización ante los requisitos de normativa ISO 9001:2015 (Cualitativo)	Se tiene noción vaga del cumplimiento a requisitos de la normativa ISO 9001:2015. El resultado de la evaluación indica que la aseguradora ha comenzado a implementar medidas para cumplir con los requisitos de calidad, pero aún tiene un largo camino por recorrer para lograr una conformidad completa con la norma ISO 9001:2015.	N/A
		(Requisitos cumplidos ante ISO 9001:2015/ Total de requisitos requeridos por ISO 9001:2015) *100 (Cuantitativo)	14.4%	100%
2	Satisfacción de las necesidades y expectativas de los clientes	Identificación de necesidades y expectativas de Clientes (Cualitativo)	Los asegurados buscan que se cumplan sus necesidades y expectativas con respecto a: - Mejorar la calidad de los servicios y brindar una experiencia más satisfactoria a los asegurados. - Continuar esforzándose por mejorar la eficiencia en la atención al cliente. - Trabajar en la mejora de la claridad y transparencia de la información. - Necesidad de atención y mejora en el proceso de recuperación.	N/A
		(Número de clientes (asegurados) Muy satisfechos y satisfechos/Total de	44.8%	100%

Continúa Tabla 40 en la siguiente página →

#	Variable	Indicadores a evaluar	Resultados/hallazgos	Meta ideal
		encuestados) *100 (Cuantitativo)		
3	Información documental existente	Identificación de información documentada de la organización (Cualitativo)	**ISO 9001:2015:** se tomaron en consideración 5 elementos de información documentada a mantener y 17 a conservar, esta información de la normativa se contrastó con la realidad de la organización y como resultado se obtuvo que son muy pocos de los documentos que se poseen por parte de la aseguradora que respaldan el cumplimiento ante la normativa, entre los documentos que no se poseen son alcance, política, evaluación de proveedores, indicadores de desempeño, entre otros. En cuanto a documentos a los que se cumple medianamente bien se encuentran los controles organizacionales, procesos, perfiles de puesto, registro de las operaciones, entre otros. Sin embargo, ningún documento se observa que se cumple en su totalidad. **ISO/IEC 27001:2022:** en cuanto a la normativa de seguridad de la información se consideraron 7 documentos a mantener y 6 a conservar, de ellos en resumen no se cumple con el alcance, política, procedimiento de tratamiento de riesgos; dentro de los que se cumple medianamente bien se tiene controles de seguridad de la información, resultados de la evaluación de riesgos, entre otros. Sin embargo, ningún documento se observa que se cumple en su totalidad.	N/A
		(Información documentada de la organización/ información documentada requerida por ISO 9001:2015 e ISO/IEC 27001:2022) * 100 (Cuantitativo)	Información documentada a mantener **ISO 9001:2015** 20% **ISO/IEC 27001:2022** 21%	Información documentada a mantener **ISO 9001:2015** 100% **ISO/IEC 27001:2022** 100%
			Información documentada a conservar **ISO 9001:2015** 32% **ISO/IEC 27001:2022** 17%	Información documentada a conservar **ISO 9001: 2015** 100% **ISO/IEC 27001:2022** 100%
4	Grado de conformidad con respecto a requisitos de Seguridad de la información	Identificación del cumplimiento de la organización ante los requisitos de normativa ISO/IEC 27001:2022 (Mixto)	29%	100%
			Los resultados destacan la necesidad de un enfoque más sólido en la mejora continua y en la gestión de roles y responsabilidades para fortalecer el sistema de gestión de seguridad de la información de acuerdo con la norma ISO/IEC 27001:2022.	N/A
		Identificación de los activos de información (Cualitativo)	Se identificaron 14 activos de información críticos para aseguradora ABANK, entre ellos algunos relacionados a bases de datos, página WEB, sistema de respaldo, entre otros. Estos	N/A

Continúa Tabla 40 en la siguiente página →

#	Variable	Indicadores a evaluar	Resultados/hallazgos	Meta ideal
			elementos se clasificaron por su ubicación física, propietario, valor cualitativo del activo y su confidencialidad.	
		Identificación de controles de seguridad de la información	Se valuaron 93 controles de seguridad de la información según ISO/IEC 27001:2022 con respecto al contexto actual de seguridad de la información. Los resultados del análisis destacan la necesidad de un enfoque más sólido en la mejora continua y en la gestión de roles y responsabilidades para fortalecer el sistema de gestión de seguridad de la información de acuerdo con la norma ISO 27001:2022.	N/A
		(Controles de seguridad de seguridad de la información cumplidos/ Total de controles de seguridad de la información según ISO/IEC 27001:2022) *100	53%	100%

Fuente: elaboración propia

CAPÍTULO IV. PROPUESTA DE DISEÑO DEL SISTEMA INTEGRADO DE GESTIÓN

4.1 Introducción

A partir los resultados de la investigación realizada, se ha formulado una propuesta para integrar el sistema de gestión que combina las normativas ISO 9001:2015 e ISO/IEC 27001:2022. Esta iniciativa tiene como objetivo primordial garantizar que la compañía cumpla con estándares de calidad y seguridad de la información que mitiguen los riesgos que representa la situación problemática de la compañía. Al considerar esta propuesta, Aseguradora ABANK podrá optimizar sus procesos internos, mejorar la satisfacción del cliente, y fortalecer sus medidas de seguridad de la información.

4.2 Propuesta del diseño del Sistema Integrado de Gestión (SIG)

A continuación, se presenta la "Guía para el Diseño de un Sistema Integrado de Gestión", desarrollada específicamente para la Aseguradora ABANK, conforme a las normas ISO 9001:2015 e ISO IEC 27001:2022. Este documento ha sido diseñado con procedimientos, directrices y protocolos operativos adaptados a las características y necesidades particulares de ABANK, con el objetivo de asegurar que la organización cumpla no solo con los requisitos normativos, sino también con los objetivos estratégicos específicos de la empresa.

La propuesta busca proporcionar a ABANK un marco sólido para gestionar la calidad de sus productos y servicios, así como para garantizar la seguridad de la información, en línea con las normativas internacionales. Los puntos clave incluyen:

1. Optimización de la Gestión por Procesos y Control Documental: Se propuso la reestructuración de los procesos organizacionales para mejorar su eficiencia, con un enfoque en la implementación de controles robustos para la información documentada, asegurando su alineación con las expectativas de los clientes y partes interesadas. Esto incluye la estandarización de procedimientos para el manejo de documentos y la creación de un sistema de gestión de calidad que permita una trazabilidad efectiva.

2. Fortalecimiento de la Seguridad de la Información: Se integrarán medidas de seguridad para proteger los datos sensibles, tanto en bases de datos físicas como en la nube. Esto incluye la propuesta de desarrollo de políticas de control para la transferencia de información, el trabajo remoto y el acceso a áreas críticas, de acuerdo con los requisitos de la norma ISO IEC 27001:2022.

Componentes Clave del Estudio: Como parte de este trabajo investigativo, se desarrollaron los siguientes componentes esenciales para la implementación del Sistema Integrado de Gestión:

- **Manual del Sistema Integrado de Gestión de Calidad:** Una compilación detallada que integra las normativas ISO 9001:2015 para el Sistema de Gestión de Calidad y ISO/IEC 27001:2022 para el Sistema de Gestión de Seguridad de la Información.
- **Plan de Implementación del SIG:** Un análisis que describe las etapas, recursos y cronograma para la implementación del Sistema Integrado de Gestión.
- **Evaluación del Contexto Organizacional:** Un estudio exhaustivo del contexto interno y externo de ABANK, que identifica los factores que afectan la capacidad de la organización para lograr sus objetivos estratégicos.
- **Enfoque y Evaluación de Riesgos:** Un enfoque estructurado para la identificación, análisis y mitigación de riesgos, asegurando que los riesgos más críticos sean gestionados de manera efectiva.
- **Matriz de Partes Interesadas:** Un análisis que identifica y evalúa a las partes interesadas clave, junto con sus necesidades y expectativas, para asegurar que se consideren adecuadamente en la planificación estratégica.
- **Manual de Procedimientos:** Documentación de los procedimientos operativos estándar que soportarán la implementación del Sistema Integrado de Gestión.
- **Manual de Interpretación y Aplicación de Controles de Seguridad de la Información:** Una guía detallada para la interpretación, implementación y monitoreo de los controles de seguridad de la información, en conformidad con los requisitos de ISO/IEC 27001:2022.

Para llevar a cabo esta implementación, se propone la creación de un comité de integración que será responsable de la planificación, supervisión y asignación de recursos necesarios para la integración efectiva de las normas ISO.

Este comité trabajará en estrecha colaboración con las áreas clave de la organización, asegurando que las mejoras se implementen de manera coherente con las operaciones actuales de ABANK y que se mantenga un enfoque continuo en la excelencia operativa y la satisfacción del cliente.

4.2.1 Conformación de un comité del Sistema Integrado de Gestión

En el contexto de una organización aseguradora, la conformación de un comité de integración y desarrollo para un sistema integra do de gestión que cumpla con las normas ISO 9001:2015 e ISO/IEC 27001:2022 es una iniciativa estratégica de suma importancia. La conformación de este comité garantiza un enfoque unificado en la planificación, implementación y mejora continua de ambos sistemas, permitiendo a la organización aseguradora mitigar riesgos, mantener la confianza de los clientes y cumplir con los requisitos legales y regulatorios. Además, promueve una cultura de calidad y seguridad en toda la organización.

Objetivo de comité de integración y desarrollo del SIG: planificar, implementar y dar seguimiento al desarrollo en la práctica del Sistema Integrado de Gestión ISO 9001:2015 e ISO/IEC 27001:2022.

Objetivos específicos del comité:

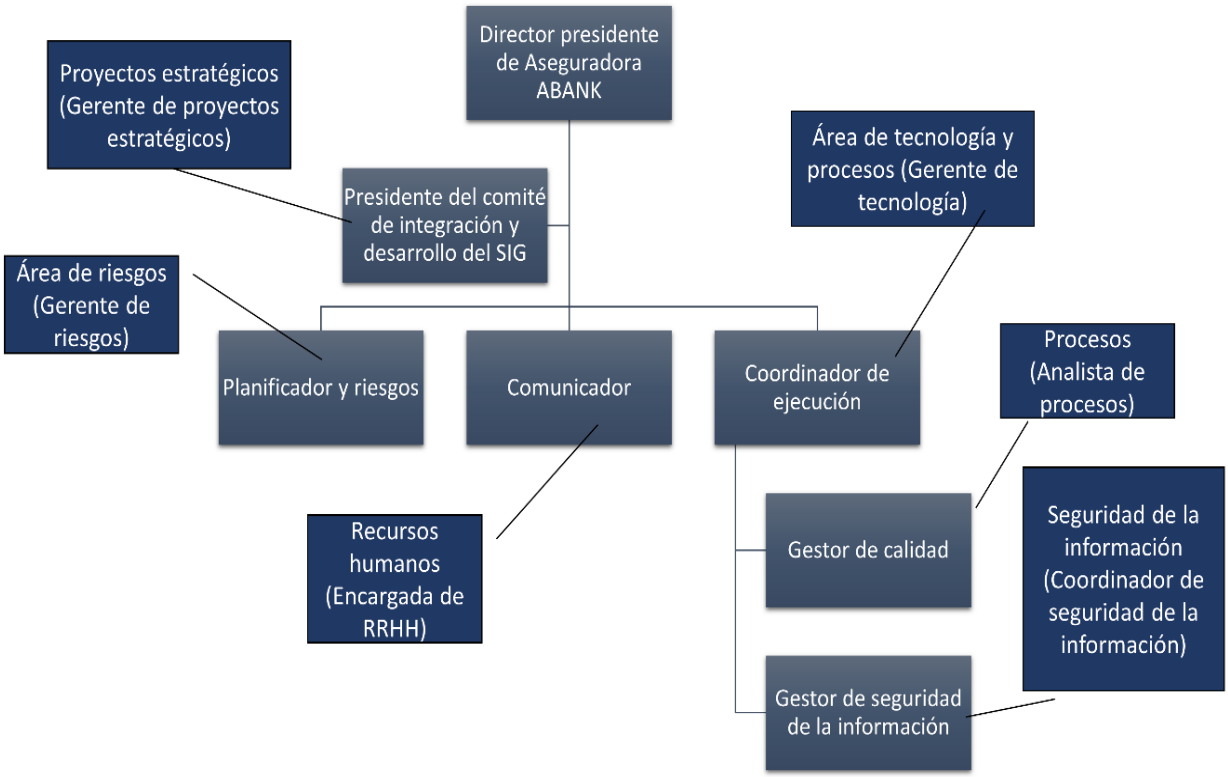
- Plan de implementación: Dar seguimiento y controlar el desarrollo del plan de implementación del Sistema Integrado de Gestión.
- Formación y Concienciación: Organizar programas de formación y concienciación para el personal, asegurando que todos comprendan sus roles y responsabilidades en la implementación y mantenimiento del SIG.
- Realizar Auditorías Internas: Planificar y llevar a cabo auditorías internas regulares para evaluar el desempeño del SIG y garantizar el cumplimiento de los estándares establecidos.
- Gestión de Documentación: Supervisar la gestión de la documentación relacionada con el SIG, incluyendo la revisión y actualización de manuales, procedimientos y registros.
- Mejora Continua: Fomentar una cultura de mejora continua, identificando oportunidades para optimizar procesos, reducir costos, mejorar la satisfacción del cliente y fortalecer la seguridad de la información.

- Comunicación: Establecer un sistema de comunicación efectivo para informar a la alta dirección y otras partes interesadas sobre el progreso y los resultados del SIG.
- Cumplimiento Regulatorio: Asegurarse de que la organización cumpla con todas las regulaciones y requisitos legales aplicables en relación con la calidad y la seguridad de la información.
- Preparación para Auditorías Externas: Coordinar la preparación y respuesta a auditorías externas por parte de organismos de certificación o entidades reguladoras.
- Promover la Conciencia del SIG: Incentivar la comprensión y adhesión de todos los miembros de la organización a los principios y objetivos del SIG.

4.2.2 Estructuración del comité de integración y desarrollo del SIG

El comité de integración y desarrollo del SIG estará compuesto por áreas funcionales clave de Aseguradora ABANK, incluidas tecnología, riesgos, recursos humanos y proyectos estratégicos. La Figura 43 detalla los roles específicos de cada miembro del comité.

Figura 43. Estructura del comité de implementación y desarrollo del SIG



Fuente: Elaboración propia

A continuación, se presenta la Tabla 41., en la cual se describe las funciones principales de cada uno de los miembros de Comité de implementación y desarrollo:

Tabla 41. Funciones principales de cada uno de los miembros de Comité de implementación y desarrollo

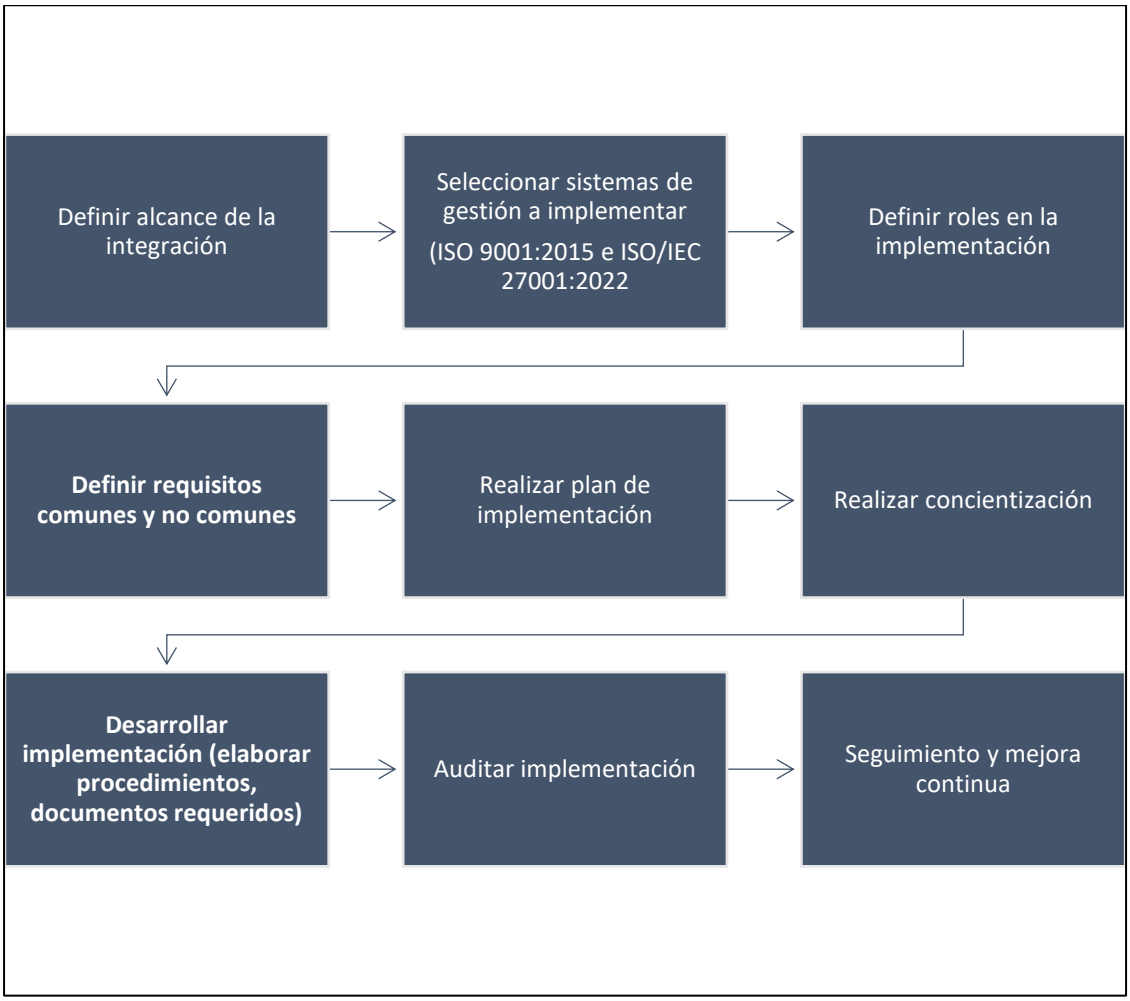
#	Rol dentro del comité	Área a la que se vincula	Descripción
1	Director presidente de Aseguradora ABANK	Presidencia	Ejerce liderazgo sobre el comité y las acciones estratégicas que se implementen a partir de SIG.
2	Presidente del comité de implementación y desarrollo del SIG	Proyectos estratégicos	Lidera las actividades planificadas de todo el comité, además rinde cuenta ante la alta dirección sobre el progreso del SIG.
3	Planificador y riesgos	Riesgos	Participa directamente en la planificación y análisis de riesgos de la implementación y de las actividades post implementación.
4	Comunicador	Recursos humanos	Comunica y concientiza a toda la organización sobre la cultura del SIG y su repercusión en el negocio.
5	Coordinador de ejecución	Tecnología y procesos	Coordina y lidera el desarrollo de los planes de acción y las actividades operativas en la implementación y el desarrollo del SIG en la organización.
6	Gestor de calidad	Procesos	Desarrolla actividades operativas en conjunto con otros miembros de la organización. Se desarrollan manuales, procedimientos, participa directamente en talleres, actividades de concientización, entre otros.
7	Gestor de la seguridad de la información	Seguridad de la información	Desarrolla actividades de seguridad de la información, lleva el control administrativo del SIG relacionado a seguridad de la información (activos de la información, seguimiento y gestión de los controles de seguridad de la información, entre otros).

Fuente: elaboración propia

4.2.3 Etapas de la implementación del Sistema Integrado de Gestión

Las actividades por realizar para el desarrollo del Sistema Integrado de Gestión se han plasmado en la siguiente Figura *44*, la cual ejemplifica las características más relevantes de la integración según la normativa PAS 99 versión 2012:

Figura 44. Etapas de la implementación del SIG



Fuente: Elaboración propia

Cada una de las etapas reflejadas en el esquema anterior son la base para la adecuada implementación, el éxito de cada una de ellas depende del compromiso y empoderamiento de cada miembro del Comité de implementación y desarrollo del SIG, así como de la alta dirección y de todos los colaboradores de Aseguradora ABANK.

A continuación, en la Tabla *42*, se presenta un desglose detallado de cómo se llevará a cabo la implementación del SIG en ABANK, estructurada en etapas y fases que abarcan desde el prediagnóstico hasta la certificación final. Esta estructura permitirá una ejecución organizada y coherente, asegurando que todos los aspectos del SIG sean abordados de manera eficiente y efectiva.

Tabla 42. Hoja de ruta para la implementación del Sistema Integrado de Gestión

Etapa	Fase	Acción	Responsable
0. Etapa de Pre-Diagnóstico	Fase 0. Contacto Inicial con Cliente	Establecer comunicación con el cliente para entender necesidades y expectativas.	Consultores del SIG
I. Etapa de Diagnóstico o Evaluación Inicial	Fase I. Concientización	Realizar sesiones de concientización y establecer un equipo interno para el SIG.	Consultores del SIG y equipo interno
	Fase II. Análisis del Contexto de la Organización	Evaluar el entorno interno y externo, identificar factores críticos y regulaciones.	Consultores del SIG y equipo interno
	Fase III. Evaluación del Nivel de Madurez de la Organización	Evaluar el nivel actual de madurez en términos de gestión y procesos.	Consultores del SIG
II. Etapa de Planificación y Diseño del SIG	Fase IV. Diseño del SIG	Diseñar la estructura del SIG y definir procesos, responsabilidades y recursos.	Consultores del SIG y equipo interno
III. Etapa de Documentación del SIG	Fase V. Establecimiento de Política del SIG y Objetivos	Desarrollar una política del SIG y establecer objetivos claros y medibles.	Alta dirección y equipo del SIG
	Fase VI. Estandarización de Procesos del SIG	Documentar procesos estándar, procedimientos operativos y guías de trabajo.	Equipo del SIG
	Fase VII. Identificación de Riesgos y Controles del SIG	Identificar riesgos asociados y definir controles para mitigar estos riesgos.	Equipo del SIG
	Fase VIII. Identificación de Clientes y Partes Interesadas	Identificar y analizar las partes interesadas clave y gestionar sus expectativas.	Consultores del SIG y equipo interno
	Fase IX. Desarrollo del Manual del SIG	Crear un manual del SIG que documente todos los procesos, políticas y procedimientos.	Equipo del SIG
IV. Etapa de Implantación del SIG	Fase X. Capacitación de la Implantación	Capacitar al personal en la implementación del SIG y realizar talleres.	Consultores del SIG y equipo interno
	Fase XI. Prueba Piloto	Realizar una prueba piloto del SIG en un área o proceso específico y evaluar el desempeño.	Equipo del SIG
	Fase XII. Apoyo en la Implantación del SIG	Proporcionar apoyo continuo durante la implementación completa y resolver problemas.	Consultores del SIG y equipo interno
V. Etapa de Evaluación del SIG	Fase XIII. Evaluación del SIG (Auditoría)	Realizar una auditoría interna del SIG para evaluar su efectividad y cumplimiento.	Consultores del SIG y equipo interno
	Fase XIV. Apoyo en la Gestión de Hallazgos	Apoyar en la gestión y resolución de hallazgos de la auditoría e implementar acciones correctivas.	Equipo del SIG

Continúa Tabla 42 en la siguiente página →

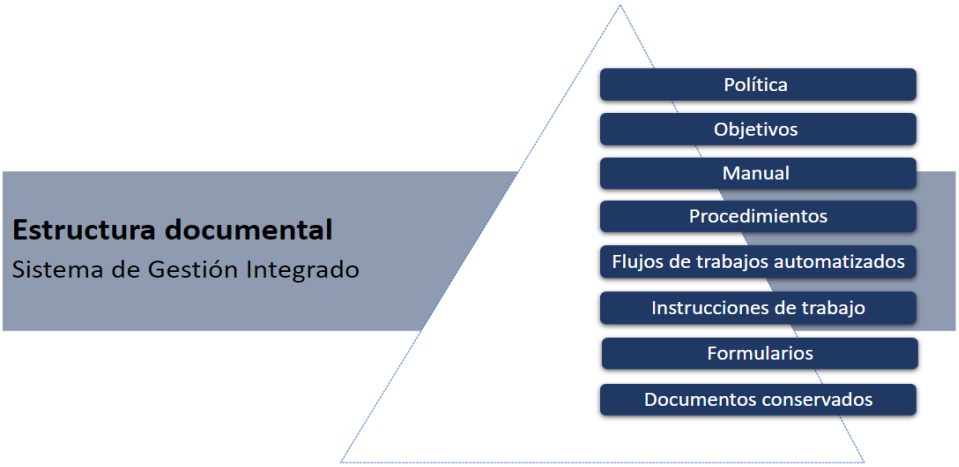
Etapa	Fase	Acción	Responsable
	Fase XV. Re-evaluación del Nivel de Madurez de la Organización	Re-evaluar el nivel de madurez tras la implementación del SIG y comparar con la evaluación inicial.	Consultores del SIG
VI. Etapa de Mantenimiento y Mejora del SIG	Fase XVI. Empoderamiento en Mejora Continua	Fomentar una cultura de mejora continua y establecer mecanismos para la retroalimentación.	Equipo del SIG
	Fase XVII. Revisión por la Dirección	Realizar revisiones periódicas del SIG para asegurar la alineación con los objetivos estratégicos.	Alta dirección
VII. Etapa de Certificación del SIG	Fase XVIII. Acompañamiento en la Certificación	Apoyar el proceso de certificación con un organismo acreditado y asistir a la auditoría.	Consultores del SIG y equipo interno

Fuente: Elaboración propia

4.2.4 Estructura documental del Sistema Integrado de Gestión

Es importante considerar la estructura documental según la norma ISO 10013:2021 porque esta norma proporciona directrices específicas para la elaboración y el mantenimiento de la documentación de un sistema de gestión. ISO 10013:2021 se centra en la documentación de sistemas de gestión en general y no está vinculada a una norma específica, lo que la hace aplicable a una amplia variedad de sistemas de gestión, incluyendo aquellos basados en ISO 9001 (calidad) e ISO/IEC 27001 (seguridad de la información), entre otros. A continuación, se describe el detalle de la estructura documental según ISO 10013:2021, ver Figura *45*:

Figura 45. Pirámide documental



Fuente: Adaptado de ISO 10013:2021

A partir de los documentos ideales que deben formar parte de la estructura de un Sistema Integrado de Gestión, según ISO 10013:2021, se resumió y priorizaron en la Tabla *43* de la misma manera se definen los documentos que serán parte los entregables de la presente investigación:

Tabla 43. Estructura documental

Nro.	Estructura documental	Detalle	Entregable de investigación
1	Política	Política del SIG	SI
2	Objetivo	Objetivos y alcance del SIG	SI
3	Manual	Manual del SIG	SI
4	Manual	Manual de interpretación y aplicación de controles de seguridad de la información según ISO/IEC 27001:2022	SI
5	Procedimientos	Procedimientos requeridos por el SIG	SI
6	Formularios	Formularios	NO*
7	Registros	Registros de la operación del negocio	NO*

Fuente: Elaboración propia

*Nota: los documentos que no serán parte de los entregables se consideran así debido que su naturaleza proviene directamente de la operatividad y estrategias propias de la aseguradora.

La estructura detallada en la Tabla *43*, revela que el Manual es el documento fundamental que integra a los demás, por lo que a continuación se muestra los documentos específicos que serán parte del contenido de este, ver Tabla 44.

Tabla 44. Detalle de documentación de la organización

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
SIG	4. Contexto de la Organización	4.1 Comprensión de la organización y de su contexto	FODA	SIG-4-01-MA
SIG	4. Contexto de la Organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Matriz de partes interesadas	SIG-4-02-MA
SIG	4. Contexto de la Organización	4.3 Determinación del alcance del sistema de gestión de la calidad	Alcance	N/A
	4. Contexto de la Organización	**4.4 Sistema de gestión de la calidad y sus procesos**		
ISO 9001:2015	4. Contexto de la Organización	4.4.1 Determinar los procesos necesarios para la organización	Mapa de procesos	SIG-4-04-INF

Continúa Tabla 44 en la siguiente página →

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
ISO 9001:2015	4. Contexto de la Organización	4.4.2 Mantener y conservar información documentada	Registros de los procesos	N/A
	5. Liderazgo	**5.1 Liderazgo y compromiso**		
SIG	5. Liderazgo	5.1.1 Generalidades	Concientización de la alta dirección	N/A
ISO 9001:2015	5. Liderazgo	5.1.2 Enfoque al cliente	Concientización de la alta dirección	N/A
	5. Liderazgo	**5.2 Política**		
SIG	5. Liderazgo	5.2.1 Establecimiento de la política del SIG	Política del SIG	SIG-5-01-PO
ISO 9001:2015	5. Liderazgo	5.2.2 Comunicación de la política del SIG	Comunicación del SIG	N/A
SIG	5. Liderazgo	5.3 Roles, responsabilidades y autoridades en la organización	Roles y responsabilidades	N/A
	6. Planificación	**6.1 Acciones para abordar riesgos y oportunidades**		
SIG	6. Planificación	6.1.1 Al planificar el SIG la organización debe considerar que se puedan lograr los resultados previstos, aumentar defectos deseables, mejora.	Planificación del SIG	N/A
SIG	6. Planificación	6.1.2 Planificar las acciones para abordar riesgos y oportunidades Evaluar riesgos de seguridad de la información	Matriz de riesgos	SIG-6-01-MA
ISO/IEC 27001:2022	6. Planificación	6.1.3 Tratamiento de riesgos de seguridad de la información Nota: cubre también punto 8.2 y 8.3 de la presente norma.	Procedimiento de tratamiento de riesgos de calidad Procedimiento de tratamiento de riesgos de seguridad de la información	SIG-6-02-PRO SIG-6-03 PRO
	6. Planificación	**6.2 Objetivos de la calidad y planificación para lograrlos**		
SIG	6. Planificación	6.2.1 Establecer objetivos del SIG	Objetivos del SIG y sus planes	SIG-6-03-PO
SIG	6. Planificación	6.2.2 Al determinar los objetivos se debe planificar: qué se hará,	Planificación de objetivos	

Continúa Tabla 44 en la siguiente página →

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
		recursos, responsables, cuándo se finalizará, evaluación de resultados		
SIG	6. Planificación	6.3 Planificación de los cambios	Gestión de cambios	N/A
	7. Apoyo	**7.1 Recursos**		
SIG	7. Apoyo	7.1.1 Generalidades	Determinación y gestión de recursos	N/A
ISO 9001:2015	7. Apoyo	7.1.2 Personas	Determinación y gestión de recursos	N/A
ISO 9001:2015	7. Apoyo	7.1.3 Infraestructura	Determinación y gestión de recursos	N/A
ISO 9001:2015	7. Apoyo	7.1.4 Ambiente para la operación de los procesos	Determinación y gestión de recursos	N/A
ISO 9001:2015	7. Apoyo	7.1.6 Conocimientos de la organización	Información documentada de la organización	N/A
SIG	7. Apoyo	7.2 Competencia	Procedimiento de reclutamiento y selección	SIG-7-01-PRO
SIG	7. Apoyo	7.2 Competencia	Procedimiento para la gestión del desarrollo del trabajador	SIG-7-02-PRO
SIG	7. Apoyo	7.3 Toma de conciencia	Campañas de concientización	N/A
SIG	7. Apoyo	7.4 Comunicación	Matriz de comunicación	SIG-7-02-MA
SIG	7. Apoyo	7.5.1 Generalidades	Manual del SG	SIG-01-01
SIG	7. Apoyo	7.5.2 Creación y actualización	Procedimiento de información documentada	SIG-7-03-PRO
	7. Apoyo	7.5.3 Control de la información documentada		
SIG	8.Operación	8.1 Planificación y control operacional	Planificación de la operación	N/A
	8.Operación	**8.2 Requisitos para los productos y servicios**		
ISO 9001:2015	8.Operación	8.2.1 Comunicación con el cliente	Protocolo de comunicación con cliente	N/A
ISO 9001:2015	8.Operación	8.2.2 Determinación de los requisitos para los productos y servicios	Planificación de los requisitos	N/A

Continúa Tabla 44 en la siguiente página →

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
	8.Operación	**8.2.3 Revisión de los requisitos para los productos y servicios**		
ISO 9001:2015	8.Operación	8.2.3.1 Revisión antes de comprometerse a suministrar productos o servicios	Controles (previos al procesamiento de los servicios/productos)	N/A
ISO 9001:2015	8.Operación	8.2.3.2 Conservar información documentada sobre los requisitos de productos y servicios	Check list de cumplimiento de requisitos	N/A
ISO 9001:2015	8.Operación	8.2.4 Cambios en los requisitos para los productos y servicios	Control de cambios en los requisitos	N/A
	8.Operación	**8.3 Diseño y desarrollo de los productos y servicios**		
ISO 9001:2015	8.Operación	8.3.1 Generalidades	Procedimiento de diseño y desarrollo de productos/servicios	SIG-8-05-PRO
ISO 9001:2015	8.Operación	8.3.2 Planificación del diseño y desarrollo	Procedimiento de diseño y desarrollo de productos/servicios	
ISO 9001:2015	8.Operación	8.3.3 Entradas para el diseño y desarrollo	Procedimiento de diseño y desarrollo de productos/servicios	
ISO 9001:2015	8.Operación	8.3.4 Controles del diseño y desarrollo	Procedimiento de diseño y desarrollo de productos/servicios	
ISO 9001:2015	8.Operación	8.3.5 Salidas del diseño y desarrollo	Procedimiento de diseño y desarrollo de productos/servicios	
ISO 9001:2015	8.Operación	8.3.6 Cambios del diseño y desarrollo	Procedimiento de diseño y desarrollo de productos/servicios	

Continúa Tabla 44 en la siguiente página →

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
			Cambios del diseño y desarrollo	
	8.Operación	**8.4 Control de los procesos, productos y servicios suministrados externamente**		
ISO 9001:2015	8.Operación	8.4.1 Generalidades	Procedimiento para la evaluación de proveedores	SIG-8-06-PRO
ISO 9001:2015	8.Operación	8.4.2 Tipo y alcance del control	Política de proveedores externos	N/A
ISO 9001:2015	8.Operación	8.4.3 Información para los proveedores externos	Política de proveedores externos/matriz de comunicaciones	
	8.Operación	**8.5 Producción y provisión del servicio**		
ISO 9001:2015	8.Operación	8.5.1 Control de la producción y de la provisión del servicio	Controles de la operación	N/A
ISO 9001:2015	8.Operación	8.5.2 Identificación y trazabilidad	Registros de trazabilidad (ERP)	N/A
ISO 9001:2015	8.Operación	8.5.4 Preservación	Registros de trazabilidad (ERP)	N/A
ISO 9001:2015	8.Operación	8.5.5 Actividades posteriores a la entrega	Procedimientos de servicios post venta	SIG-8-07-PRO
ISO 9001:2015	8.Operación	8.5.6 Control de los cambios	Registros de trazabilidad (ERP) Resultados de la revisión de los cambios	N/A
ISO 9001:2015	8.Operación	8.6 Liberación de los productos y servicios	Liberación de los productos	N/A
	8.Operación	**8.7 Control de las salidas no conformes**		
ISO 9001:2015	8.Operación	8.7.1 Asegurarse que las salidas que no sean conformes con los requisitos se identifican y controlan	Procedimiento de NC	SIG-8-08-PRO

Continúa Tabla 44 en la siguiente página →

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
ISO 9001:2015	8.Operación	8.7.2 Conservar información documentada sobre estos requisitos	Planes de acción NC Salidas no conformes, No conformidades	N/A
	9. Seguimiento y evaluación	**9, Evaluación del desempeño**		
	9. Seguimiento y evaluación	**9.1 Seguimiento, medición, análisis y evaluación**		
SIG	9. Seguimiento y evaluación	9.1.1 Generalidades	Procedimiento de Indicadores de desempeño	SIG-9-08-PRO
ISO 9001:2015	9. Seguimiento y evaluación	9.1.2 Satisfacción del Cliente	Procedimiento para evaluación de la satisfacción del Cliente	SIG-9-09-PRO
ISO 9001:2015	9. Seguimiento y evaluación	9.1.3 Análisis y evaluación	Análisis de indicadores de desempeño	N/A
	9. Seguimiento y evaluación	**9.2 Auditoría interna**		
SIG	9. Seguimiento y evaluación	9.2.1 Realizar auditorías internas planificadas	Procedimiento de auditoría interna	SIG-9-10-PRO
	9. Seguimiento y evaluación	9.2.2 Establecer programas de auditoría, definir criterios de auditorías y alcance, seleccionar a los auditores.	Programa, plan, informe, check list de auditoría	SIG-9-01-PLAN
	9. Seguimiento y evaluación	**9.3 Revisión por la dirección**		
SIG	9. Seguimiento y evaluación	9.3.1 Generalidades	Procedimiento de la revisión por la dirección	SIG-9-11-PRO
SIG	9. Seguimiento y evaluación	9.3.2 Entradas de la revisión por la dirección		
SIG	9. Seguimiento y evaluación	9.3.3 Salidas de la revisión por la dirección		
	10. Mejora	**10 Mejora**		
SIG	10. Mejora	10.1 Generalidades	Mejora continua	N/A
	10. Mejora	**10.2 No conformidades y acción correctiva**		
SIG	10. Mejora	10.2.1 Reaccionar ante la no conformidad y evaluar la necesidad de acciones para eliminar	Procedimiento de NC y acciones correctivas	SIG-10-12-PRO

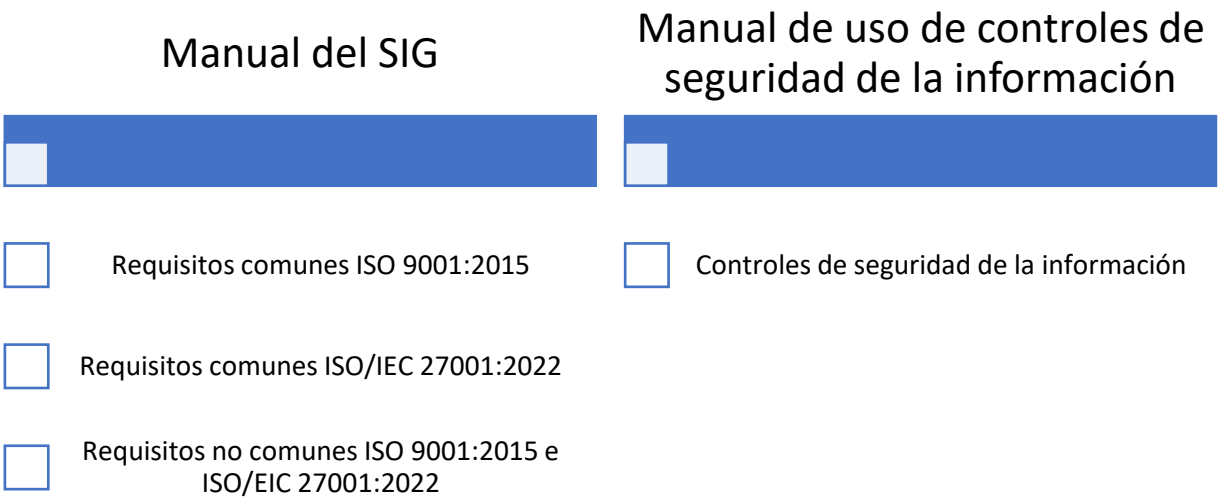
Continúa Tabla 44 en la siguiente página →

Sistema de gestión que aplica	Capítulo de norma	Punto de norma	Documento	Código de documento
		las causas de la no conformidad		
SIG	10. Mejora	10.2.2 La organización debe conservar información documentada como evidencia		
SIG	10. Mejora	10.3 Mejora continua	Mejora continua	N/A

Fuente: elaboración propia

En la integración de los requisitos de ambos Sistemas de Gestión, se realizó una separación entre los documentos comunes y no comunes, por lo que se entregan dos documentos con la configuración siguiente, ver Figura 46:

Figura 46. Pirámide documental



Fuente: elaboración propia

4.3 Manual del Sistema Integrado de Gestión

MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN DE CALIDAD DE ACUERDO CON LAS NORMATIVAS ISO 9001:2015 SISTEMA DE GESTIÓN DE CALIDAD E ISO/IEC 27001:2022 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Septiembre 2024

Presentado por:

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

MUÑOZ SOSA, NORA NATHALY

RODAS LAÍNEZ, GUSTAVO MANUEL

Para:

Aseguradora ABANK

ÍNDICE

INTRODUCCIÓN

En un entorno empresarial cada vez más competitivo y en constante evolución, la búsqueda de la excelencia en la gestión se ha convertido en un objetivo fundamental para las organizaciones. Aseguradora ABANK, comprometida con la satisfacción de sus clientes y la protección de la información confidencial, ha decidido implementar un Sistema Integrado de Gestión (SIG) que abarca dos pilares esenciales: la calidad y la seguridad de la información.

Este manual tiene como objetivo proporcionar una guía detallada sobre el Sistema Integrado de Gestión (SIG) de Aseguradora ABANK. El SIG se desarrolla conforme a las normas y estándares reconocidos internacionalmente, para asegurar que la organización cumpla con sus compromisos de calidad y seguridad de la información.

A lo largo de este manual, encontrará información esencial sobre los procesos, políticas y procedimientos que rigen nuestro SIG, así como las responsabilidades de cada miembro de la organización en su implementación y mantenimiento. Además, se describen las herramientas y recursos disponibles para apoyar la gestión de calidad y la seguridad de la información.

Este manual no solo es una referencia para nuestros empleados, sino también una muestra de nuestro compromiso con la transparencia y la mejora continua. Aseguradora ABANK se esfuerza por mantener los más altos estándares de calidad en sus productos y servicios, al tiempo que garantiza la confidencialidad, integridad y disponibilidad de la información de nuestros clientes y colaboradores.

A través de la implementación de este Sistema Integrado de Gestión, Aseguradora ABANK busca fortalecer su posición en el mercado, promover la confianza de sus clientes y colaboradores, y contribuir al logro de sus objetivos estratégicos.

GENERALIDADES

Aseguradora ABANK nace como parte de una iniciativa de inversión salvadoreña del grupo Perinversiones S.A. De C.V., La aseguradora, antes conocida como Seguros Vivir, tenía origen dominicano, pero en 2019 fue comprada en su totalidad por ABANK, estrategia financiera de la cual hoy en día es parte.

Aseguradora ABANK es una empresa innovadora, orientada a brindar la excelencia en el servicio y especializada en los ramos de personas, ofreciendo ventajas y valores agregados a nuestros clientes, con amplia experiencia y enfoque en el mercado de aseguramiento de salud.

El conglomerado ABANK, en El Salvador, posee 29 sucursales que cubren la mayor parte del territorio nacional y una sede central ubicada en Boulevard Merliot, Urbanización Jardines de La Hacienda, edificio Spatium, Antiguo Cuscatlán, La Libertad.

DEFINICIONES

- **Acción correctiva:** Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.
- **Acción preventiva:** Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente indeseable.
- **Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencia de la auditoria y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de la auditoria.
- **Evidencia de auditoria:** Son registros, declaraciones de hechos o cualquier otra información pertinente a los criterios de auditoría y que son verificables.
- **Evidencia objetiva:** Datos que respaldan la existencia o veracidad de algo.
- **No conformidad:** Incumplimiento de un requisito.
- **Proceso:** Se define como “conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforma elementos de entradas en resultados.
- **Producto:** Se define como el resultado de un proceso.

- **Programa de la auditoria:** Conjunto de una o más auditorias planificadas para un período de tiempo determinado y dirigida para un propósito específico.
- **Plan de auditoria:** Descripción de las actividades y detalles a desarrollarse durante una auditoria.
- **Requisito:** Necesidad o expectativa establecida, generalmente implícita u obligatoria.
- **Trazabilidad:** Capacidad de seguir el recorrido de un alimento a través de la(s) etapa(s) especificada(s) de producción, procesamiento y distribución.

VALORES, VISIÓN Y MISIÓN DE ASEGURADORA ABANK

Valores

Innovación, integridad, servicio, confianza, positivismo, compromiso.

Visión

Ser la aseguradora líder en salud de El Salvador.

Misión

Elevar la calidad de vida de nuestros clientes, brindando coberturas de salud con productos innovadores, a través de una red de atención médica de alta calidad y un servicio confiable.

SISTEMA INTEGRADO DE GESTIÓN

4.Contexto de la organización

En Aseguradora ABANK, consideramos fundamental comprender el contexto en el que operamos para orientar eficazmente nuestros esfuerzos hacia la excelencia en calidad y seguridad de la información. Nuestro compromiso con la satisfacción del cliente y la protección de datos se refleja en todas las áreas de nuestra operación.

Este capítulo aborda la comprensión de nuestra organización y su entorno, así como la identificación de las partes interesadas y la determinación del alcance de nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información. Entendemos que el éxito de nuestro SIG depende en gran medida de nuestra capacidad para adaptarnos y responder de manera efectiva a un entorno en constante evolución, cumplir con las regulaciones y normativas vigentes, y superar las expectativas de todas nuestras partes interesadas.

4.1 Comprensión de la organización y su contexto

En Aseguradora ABANK, reconocemos la importancia de comprender el contexto en el que operamos y cómo este contexto influye en nuestros objetivos estratégicos en términos de calidad y seguridad de la información. Para lograr esto, realizamos un análisis continuo de nuestro entorno organizacional, incluyendo factores internos y externos que puedan impactar nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información.

Para mayor detalle, se ha establecido un análisis PESTEL (SIG-4-01-MA, Ver Apéndice 7).

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

En Aseguradora ABANK, damos gran importancia a la identificación y comprensión de las necesidades y expectativas de todas las partes interesadas relevantes para nuestro SIG de Calidad y Seguridad de la Información. Estas partes aceptables incluyen a nuestros valiosos clientes, nuestros empleados, los reguladores, los accionistas y otros actores que tienen un interés en nuestros servicios y en la protección de la información.

Para mayor detalle, ver matriz de partes interesadas (SIG-4-02-MA, Ver Apéndice 8).

4.3 Determinación del alcance del sistema de gestión integrada.

El alcance de nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información comprende de manera integral todas las actividades y procesos de Aseguradora ABANK. Esto incluye, pero no se limita a:

La ubicación geográfica Aseguradora ABANK, sede central ubicada en: Boulevard Merliot, Urbanización Jardines de la Hacienda, Lote 5 y 6, Zona Comercial Z.C 5, Antiguo Cuscatlán. La Libertad, El Salvador, C.A.

Aplica para los siguientes procesos:

- Mercadeo y comunicaciones
- Gestión estratégica
- Control interno
- Auditoría
- Gestión de calidad
- Comercialización
- Suscripción
- Reaseguro
- Gestión de la emisión
- Cobranza y tesorería
- Ciclo de siniestros
- Servicio post venta
- Tecnología

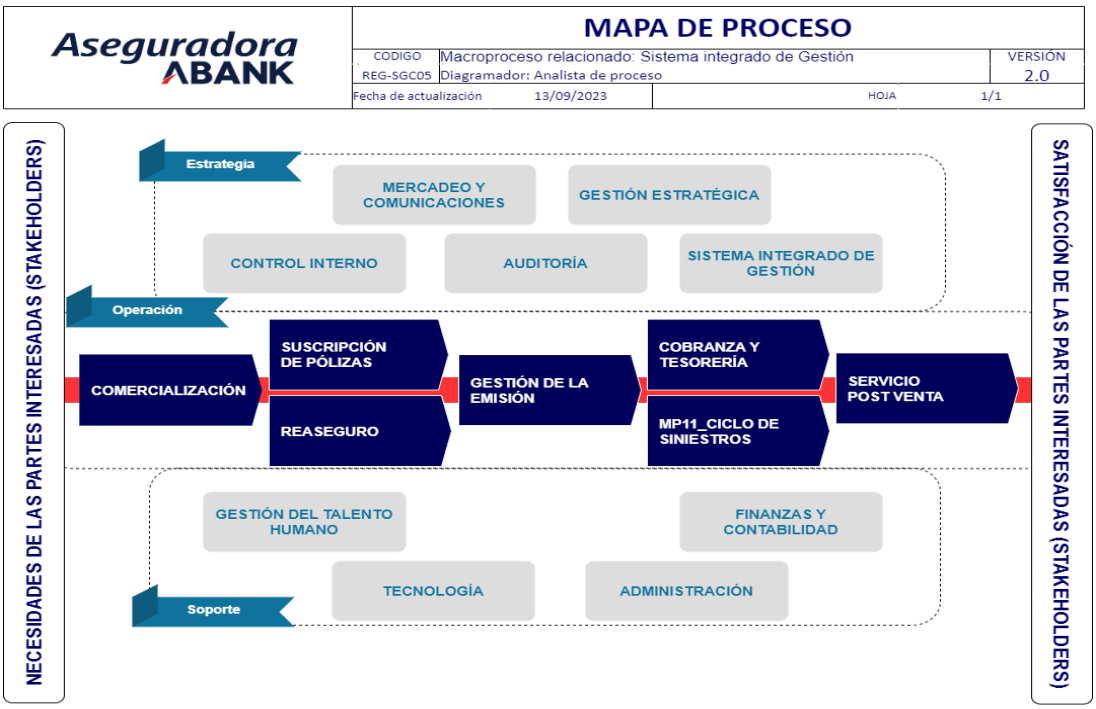
Y aplica para los productos:

- Seguros de gastos médicos (salud)
- Seguros de vida

4.4.1 Determinar los procesos necesarios para la organización

En Aseguradora ABANK, hemos llevado a cabo una evaluación exhaustiva para determinar los procesos necesarios para nuestro Sistema de Gestión de la Calidad y Seguridad de la Información (SIG). Esta determinación se basa en la comprensión de las necesidades y expectativas de nuestras partes interesadas, los requisitos de las normas ISO 9001:2015 e ISO 27001:2013, y nuestro compromiso con la calidad y la seguridad de la información. Los procesos identificados como necesarios para el funcionamiento de nuestro SIG se documentan y gestionan de manera integral para asegurar que contribuyan a la consecución de nuestros objetivos.

Figura 47. Mapa de proceso actualizado (cód.)



Fuente: elaboración propia.

4.4.2 Mantener y conservar información documentada

En Aseguradora ABANK, reconocemos la importancia de mantener y conservar la información documentada de manera adecuada como parte esencial de nuestro Sistema de Gestión de la Calidad y Seguridad de la Información (SIG). Esto implica la gestión de documentos y registros que son críticos para la operación de nuestro SIG y para el cumplimiento de los requisitos de las normas ISO 9001:2015 e ISO 27001:2013.

Documentos: Identificamos, controlamos y mantenemos los documentos necesarios para respaldar la planificación, operación y control efectivo de nuestros procesos relacionados con la calidad y seguridad de la información. Estos documentos incluyen políticas, procedimientos, instrucciones de trabajo y otros documentos relevantes.

Registros: Mantenemos registros de nuestras actividades y resultados para demostrar el cumplimiento de nuestros requisitos, así como para evaluar el rendimiento y la eficacia de nuestro SIG. Estos registros son conservados de acuerdo con los plazos establecidos y protegidos para su integridad y confidencialidad.

La gestión adecuada de la información documentada contribuye significativamente a la transparencia, el control y la mejora continua de nuestro SIG en términos de calidad y seguridad de la información.

Toda la información referente a la gestión por procesos de la organización se resguarda en la intranet organizacional:

Sharepoint.com/Aseguradora ABANK/Sistema integrado de gestión.

5. Liderazgo

En Aseguradora ABANK, el liderazgo y el compromiso de la alta dirección son fundamentales para guiar y respaldar nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información. Este apartado se enfoca en la responsabilidad y el compromiso de nuestra alta dirección en la dirección estratégica y operativa del SIG, garantizando que se establezcan los fundamentos necesarios para la mejora continua de la calidad y la seguridad de la información en toda la organización.

5.1 Liderazgo y compromiso

5.1.1 Generalidades

La alta dirección de Aseguradora ABANK demuestra su liderazgo y compromiso con nuestro SIG de Calidad y Seguridad de la Información al:

- Establecer una política integral de calidad y seguridad de la información que refleje nuestra orientación hacia la excelencia en ambos aspectos.
- Asegurar que la política sea comunicada, entendida y aceptada en todos los niveles de la organización.
- Asignar roles y responsabilidades específicas relacionadas con la calidad y la seguridad de la información dentro de la alta dirección, garantizando una supervisión efectiva.
- Proporcionar recursos adecuados para la implementación, mantenimiento y mejora continua del SIG.
- Liderar mediante el ejemplo, demostrando un compromiso personal con la calidad y la seguridad de la información y fomentando una cultura organizacional que valore estos aspectos.

5.1.2 Enfoque al cliente

En Aseguradora ABANK, el enfoque al cliente es una piedra angular de nuestro compromiso con la calidad y la seguridad de la información. Para asegurar que cumplimos con las expectativas de nuestros clientes, nos comprometemos a:

- Comprender las necesidades y expectativas de nuestros clientes, teniendo en cuenta sus comentarios y retroalimentación.
- Integrar los requisitos del cliente en nuestros procesos y servicios, asegurando que se reflejen en nuestra política de calidad y seguridad de la información.
- Monitorear y evaluar continuamente la satisfacción del cliente y tomar medidas para mejorar y corregir cuando sea necesario.
- Asegurar la confidencialidad y la integridad de la información del cliente

5.2 Política de calidad y seguridad de la información

En Aseguradora ABANK, nuestra política de la calidad y seguridad de la información refleja nuestro compromiso inquebrantable con la excelencia en la prestación de servicios de seguros y la protección de la información. Nuestra política establece los principios fundamentales que guían nuestras acciones y decisiones en relación con la calidad y la seguridad de la información. Esta política se comunica a todos los empleados y partes interesadas relevantes y está disponible públicamente para garantizar la transparencia.

5.2.1 Establecimiento de la política

Nuestra política de la calidad y seguridad de la información se ha establecido con la participación de la alta dirección, a continuación, se expone:

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN

Como organización nos comprometemos a establecer, implementar y mantener un Sistema Integrado de Gestión de Calidad y Seguridad de la Información (SIG) conforme a los requisitos de las normas ISO 9001:2015 e ISO/IEC 27001:2022. Esta política está alineada con el propósito de la organización, que es proporcionar servicios de seguros de alta calidad, mientras se garantiza la protección de la información sensible y la satisfacción de nuestros clientes. En consonancia con nuestra dirección estratégica, esta política busca impulsar la excelencia operativa, fortalecer la confianza de nuestros clientes y cumplir con todas las obligaciones legales y normativas.

Marco de Referencia para Objetivos

La política del SIG proporciona un marco de referencia esencial para el establecimiento, revisión y cumplimiento de los objetivos de calidad y de seguridad de la información. Estos objetivos son medibles, alcanzables y alineados con nuestra visión de ser líderes en el sector asegurador, ofreciendo productos y servicios que satisfagan las expectativas de nuestros clientes y protejan la integridad, confidencialidad y disponibilidad de la información.

Compromiso con los Requisitos Aplicables

ABANK se compromete a cumplir con todos los requisitos aplicables en materia de calidad y seguridad de la información, incluidos aquellos impuestos por las normas ISO 9001:2015 e ISO/IEC 27001:2022, así como otros requisitos legales, regulatorios y contractuales que sean relevantes para nuestras operaciones. Este compromiso es fundamental para mantener la confianza de nuestros clientes, socios y partes interesadas.

Compromiso de Mejora Continua

La alta dirección de ABANK se compromete a la mejora continua del Sistema de Gestión de la Calidad y del Sistema de Gestión de Seguridad de la Información. Esto se logra a través de la evaluación continua de nuestros procesos, la implementación de acciones correctivas y preventivas, y la promoción de una cultura organizacional orientada a la innovación y la excelencia.

Revisión de la Política

Esta política se revisa anualmente o cuando sea necesario para garantizar que siga siendo adecuada y efectiva para nuestra organización.

Jaime García-Prieto

Versión 01 SIG-5-01-PO Director Presidente

5.2.2 Comunicación de la política

Nuestra política de calidad y seguridad de la información se comunica de manera efectiva a través de todos los niveles de la organización. Además, se asegura de que se comprende y se acepta en todos los niveles y áreas de Aseguradora ABANK.

La política se revisa periódicamente para garantizar su relevancia continua y su alineación con nuestros objetivos estratégicos y las necesidades cambiantes de nuestras partes interesadas.

5.3 Roles, responsabilidades y autoridades en la organización

En Aseguradora ABANK, la asignación clara de roles, responsabilidades y autoridades es esencial para garantizar la efectividad de nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información. Este apartado establece las bases para la gestión de las funciones y tareas relacionadas con la calidad y seguridad de la información en toda la organización.

5.3.1 Responsabilidades y Autoridades de la Alta Dirección

La alta dirección de Aseguradora ABANK asume la máxima responsabilidad en lo que respeta al SIG de Calidad y Seguridad de la Información. Esto incluye:

- Asegurar que se establecerán, implementarán y mantendrán los procesos necesarios para el SIG.
- Garantizar que se asignen los recursos adecuados para el funcionamiento eficaz del SIG.
- Revisar periódicamente el desempeño del SIG y tomar medidas para su mejora continua.
- Aprobar cambios significativos en la política de calidad y seguridad de la información.
- Comunicar la importancia del cumplimiento de los requisitos del SIG y la política correspondiente a toda la organización.

5.3.2 Representante de la Dirección

La alta dirección designa un Representante de la Dirección con la autoridad y el respaldo necesario para:

- Asegurar que se establecerán, implementarán y mantendrán los procesos del SIG.
- Informar a la alta dirección sobre el desempeño del SIG y las oportunidades de mejora.
- Promover la conciencia y la comprensión de los requisitos del SIG en toda la organización.
- Actuar como punto de contacto para cuestiones relacionadas con la calidad y seguridad de la información, tanto interna como externamente.

5.3.3 Responsabilidades en toda la Organización

Cada miembro del personal de Aseguradora ABANK tiene la responsabilidad de:

- Cumplir con los requisitos del SIG y seguir los procedimientos y políticas correspondientes.
- Informar de inmediato sobre cualquier incidente de seguridad de la información o no conformidad con los procedimientos del SIG.
- Contribuir verificablemente a la mejora continua de la calidad y seguridad de la información en sus áreas de trabajo.

5.3.4 Responsabilidades del comité de integración y desarrollo del SIG

Cada miembro del personal de Aseguradora ABANK tiene la responsabilidad de:

a) El comité debe demostrar un liderazgo sólido y un compromiso inquebrantable con la implementación y mejora continua del SIG. Esto incluye establecer políticas, objetivos y directrices claras que reflejen el compromiso de la organización con la calidad y la seguridad de la información.
b) El comité debe participar en la definición de la estrategia general del SIG, alineándola con los objetivos estratégicos de la organización y garantizando que se cumplan los requisitos de ambas normas (ISO 9001 e ISO/IEC 27001).
c) Asegurar que los recursos necesarios, incluyendo personal, tecnología y presupuesto, estén disponibles para la implementación y el mantenimiento efectivo del SIG.
d) Evaluar y revisar periódicamente la política del SIG y los objetivos de calidad y seguridad de la información para garantizar su relevancia y eficacia continua.
e) Supervisar y revisar la gestión de riesgos en ambos aspectos de calidad y seguridad de la información. Esto incluye la identificación de riesgos, la evaluación de su impacto y probabilidad, y la implementación de medidas de mitigación.

f) Garantizar que se establezcan y mantengan procesos de monitoreo y medición para evaluar el desempeño del SIG en relación con los indicadores clave de calidad y seguridad de la información.

g) Supervisar y asegurarse de que se realicen auditorías internas regulares para evaluar la conformidad con los requisitos de las normas y la efectividad del SIG.

h) Facilitar la comunicación efectiva dentro de la organización y con partes interesadas relevantes sobre asuntos relacionados con la calidad y la seguridad de la información.

i) Fomentar una cultura de mejora continua en toda la organización, identificando oportunidades de mejora y promoviendo la implementación de acciones correctivas y preventivas.

j) Asegurarse de que la organización cumple con todas las leyes y regulaciones aplicables relacionadas con la calidad y la seguridad de la información.

k) Evaluar y aprobar cambios importantes en el SIG, asegurando que se realicen de manera controlada y documentada.

l) Coordinar la preparación y la respuesta a auditorías externas por parte de organismos de certificación o entidades reguladoras.

m) Fomentar una cultura organizacional que valore la calidad y la seguridad de la información, involucrando a todos los empleados en la mejora continua.

Estas responsabilidades y autoridades claras garantizan la implementación y mantenimiento efectivo del SIG en todos los niveles de la organización.

6. Planificación

En Aseguradora ABANK, la planificación es una parte esencial de nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información. Este apartado se centra en la planificación estratégica y operativa que respalda la consecución de nuestros objetivos de calidad y seguridad de la información.

6.1 Acciones para abordar riesgos y oportunidades

6.1.1 Generalidades

Nuestra organización identifica, evalúa y aborda sistemáticamente los riesgos y oportunidades relacionados con la calidad y seguridad de la información. Esta evaluación se realiza en función de los objetivos del SIG y toma en cuenta tanto los factores internos como los externos que puedan afectar a la consecución de estos objetivos.

6.1.2 Planificar las acciones para abordar riesgos y oportunidades

Para abordar los riesgos y oportunidades identificados en relación con la calidad y seguridad de la información, Aseguradora ABANK toma medidas específicas que incluyen:

Prevención y Mitigación de Riesgos: Implementamos medidas preventivas y de mitigación para reducir la probabilidad de eventos no deseados que puedan afectar la calidad y seguridad de la información. Esto incluye controles de seguridad de la información, evaluación de riesgos y planes de contingencia.

Explotación de Oportunidades: Identificamos oportunidades que pueden mejorar la calidad y seguridad de la información y tomamos medidas para aprovecharlas plenamente. Esto puede incluir la adopción de nuevas tecnologías, la mejora de procesos o la inversión en capacitación.

Integración en la Planificación Estratégica: Garantizamos que la gestión de riesgos y oportunidades esté integrada en nuestra planificación estratégica, de modo que nuestros objetivos en materia de calidad y seguridad de la información se alineen con nuestra dirección global como organización.

Para mayor detalle, ver matriz de riesgos (SIG-6-01-MA, Ver Apéndice 9).

6.1.3 Tratamiento de riesgos de calidad y seguridad de información

Para el tratamiento de riesgos en Aseguradora ABANK se han diseñado dos procedimientos que abarcan a todo el sistema integrado:

- Procedimientos para tratamiento de riesgos de calidad.
- Procedimiento para tratamiento de riegos de seguridad de la información.

Para mayor detalle, ver procedimiento para tratamiento de riesgos del Sistema Integrado de Gestión (SIG-6-02-PRO y SIG-6-03-PRO Ver Manual de procedimientos, *Apéndice 10*).

En Aseguradora ABANK se ha diseñado un manual de interpretación y aplicación de los controles de seguridad de la información sugeridos por la norma ISO/IEC 27001:2022, en su Anexo A. (Ver Manual de interpretación y aplicación de controles, *Apéndice 11*)

6.2 Objetivos de la calidad y de Seguridad de la Información y planificación para lograrlos

6.2.1 Establecimiento de Objetivos de la Calidad y de Seguridad de la Información

Aseguradora ABANK establece objetivos de calidad y seguridad de la información que son coherentes con nuestra política y alineados con nuestros compromisos y necesidades. Estos objetivos son medibles y tienen en cuenta los requisitos aplicables.

A nivel general los objetivos desarrollados son:

- Mejorar la satisfacción del cliente mediante la optimización de los procesos de atención y resolución de incidencias.
- Garantizar la protección de la información sensible mediante la mejora de las medidas de seguridad y cumplimiento normativo.
- Mejorar la eficiencia operativa mediante la optimización de los procesos internos clave.
- Desarrollar y lanzar nuevos productos y servicios que satisfagan las necesidades

emergentes del mercado.

Para mayor detalle, ver objetivos del SIG y sus planes de acción (SIG-6-03-PO, Ver *Apéndice 12*).

6.2.2 Planificación para Lograr los Objetivos de la Calidad y de Seguridad de la Información

Desarrollamos planes de acción detallados para lograr nuestros objetivos de calidad y seguridad de la información. Estos planes incluyen asignación de recursos, responsabilidades y plazos para garantizar que se alcancen los objetivos establecidos.

Nuestra planificación estratégica y operativa en el ámbito de la calidad y seguridad de la información es un elemento clave para garantizar que Aseguradora ABANK continúe brindando servicios de alta calidad y protegiendo la información de nuestros clientes y partes interesadas.

6.3 Planificación de los cambios

Cuando se producen cambios en la información documentada relacionada con la calidad y seguridad de la información, se siguen procedimientos específicos para gestionar esos cambios. Esto incluye:

Control de Documentos: Se mantiene un control riguroso de la documentación relacionada con la calidad y seguridad de la información, y se asegura que las versiones actuales estén disponibles para las partes interesadas relevantes.

Revisión y Aprobación: Los cambios propuestos en la información documentada pasan por un proceso de revisión y aprobación antes de su implementación.

Comunicación: Se comunica de manera efectiva cualquier cambio relevante en la información documentada a todas las partes interesadas pertinentes.

La planificación de cambios en nuestro SIG es fundamental para garantizar la adaptabilidad y la mejora continua en términos de calidad y seguridad de la información en Aseguradora ABANK.

7. Apoyo

7.1 Recursos

7.1.1 Recursos Generales

Aseguradora ABANK asigna los recursos necesarios para establecer, implementar, mantener y mejorar el SIG de Calidad y Seguridad de la Información. Esto incluye:

- **Recursos humanos:** Contamos con un equipo de profesionales capacitados y comprometidos con la calidad y seguridad de la información.
- **Infraestructura:** Mantenemos una infraestructura tecnológica y física adecuada para respaldar nuestras operaciones de manera segura y eficiente.
- **Recursos financieros:** Garantizamos la disponibilidad de recursos financieros para la inversión en tecnología, formación y otras necesidades relacionadas con el SIG.

7.1.2 Competencia

Nuestro personal recibe la formación y la capacitación necesarias para desempeñar sus funciones de manera competente en lo que respeta la calidad y seguridad de la información. Esto incluye la comprensión de las políticas y procedimientos relevantes, así como la promoción de una cultura organizacional que valore la formación continua y el desarrollo profesional.

Para mayor detalle, ver procedimiento de reclutamiento y selección (SIG-7-01-PRO y procedimiento para la gestión del desarrollo del trabajador SIG-7-02-PRO, Manual de procedimientos *Apéndice 10*).

7.2 Toma de conciencia

7.2.1 Conciencia de los Requisitos

En Aseguradora ABANK, garantizamos que todo el personal es consciente de los requisitos relevantes del SIG de Calidad y Seguridad de la Información. Esto incluye la comprensión de la política de calidad y seguridad de la información, así como de los procedimientos y prácticas asociados.

7.2.2 Comunicación

Fomentamos una comunicación efectiva en toda la organización en lo que respeta la calidad y seguridad de la información. Esto incluye la promoción de la comunicación interna y externa relacionada con el SIG y la garantía de que las partes interesadas relevantes estén informadas de manera adecuada.

7.2.3.1 Comunicación Interna

Fomentamos una comunicación interna efectiva en toda la organización para garantizar que la calidad y la seguridad de la información sean comprendidas y respaldadas por todos los empleados. Esto incluye la promoción de la conciencia sobre los riesgos de seguridad de la información y la importancia de la calidad en todas las actividades.

7.2.3.2 Comunicación Externa

Mantenemos una comunicación efectiva con las partes interesadas externas pertinentes, incluyendo clientes, proveedores y autoridades reguladoras, en lo que respeta a la calidad y seguridad de la

información. Esto puede incluir la comunicación de políticas, compromisos y resultados relacionados con el SIG.

Para mayor detalle, ver matriz de comunicaciones (SIG-7-02-MA, Ver Apéndice 13).

7.3 Información Documentada

7.3.1 Generalidades

Mantenemos y controlamos la información documentada necesaria para el funcionamiento eficaz del SIG de Calidad y Seguridad de la Información. Esto incluye políticas, procedimientos, instrucciones de trabajo y registros que son relevantes para nuestros procesos y actividades.

Todos los documentos relacionados al SIG se encuentran consolidados en el presente manual identificado con la codificación SIG-01-01.

7.3.2 Creación y actualización de la información documentada

La creación, revisión y actualización de la información documentada se gestionan de acuerdo con procedimientos específicos para garantizar su precisión y relevancia.

7.3.3 Control de la Información Documentada

La información documentada se controla rigurosamente para asegurarse de que esté disponible cuando sea necesario y que se mantenga en condiciones legibles y utilizables. Esto incluye la identificación, almacenamiento, protección y recuperación de la información documentada.

Para mayor detalle, ver procedimiento de Control de información documentada (SIG-7-03-PRO, Manual de procedimientos, Apéndice 9).

7.4 Comunicación

El apartado 7 se enfoca en el apoyo necesario para el funcionamiento efectivo del Sistema Integrado de Gestión de Calidad y Seguridad de la Información en Aseguradora ABANK.

8. Operación

El apartado 8 del Manual de Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información se centra en las operaciones que deben llevarse a cabo para lograr los objetivos de calidad y seguridad de la información en Aseguradora ABANK.

8.1 Planificación y Control Operativo

8.1.1 Planificación de la Operación del SIG

Planificamos y controlamos nuestras operaciones relacionadas con la calidad y seguridad de la información de manera eficaz. Esto incluye la planificación de procesos, actividades, recursos y plazos para garantizar que se alcancen los objetivos establecidos en el SIG.

8.1.2 Controles Operativos

Implementamos controles operativos adecuados para garantizar que los procesos relacionados con la calidad y seguridad de la información se ejecuten de acuerdo con los requisitos y los estándares establecidos. Esto incluye la supervisión y medición continua de los procesos para asegurar su eficacia.

8.2 Requisitos para Productos y Servicios

8.2.1 Comunicación con el Cliente

Nos comunicamos de manera efectiva con nuestros clientes para comprender sus requisitos y necesidades en relación con los productos y servicios de seguros. Esto garantiza que proporcionamos servicios que cumplen con las expectativas del cliente y los estándares de calidad.

8.2.2 Determinación de requisitos para productos y servicios

Determinamos y documentamos los requisitos específicos para los productos y servicios de seguros, teniendo en cuenta los requisitos legales y reglamentarios aplicables.

8.3 Diseño y Desarrollo de Productos y Servicios

En Aseguradora ABANK, el diseño y desarrollo de nuestros productos y servicios son fundamentales para asegurar que cumplimos con los requisitos de calidad y seguridad de la información.

Para mayor detalle, ver procedimiento para diseño y desarrollo de productos SIG-8-05-PRO, Manual de procedimientos, Apéndice 9).

8.3.1 Planificación del Diseño y Desarrollo

Planificamos cuidadosamente el diseño y desarrollo de nuestros productos y servicios para garantizar que cumplen con los requisitos específicos de calidad y seguridad de la información. Establecemos objetivos de diseño claros y plazos para el desarrollo.

8.3.2 Entradas para el Diseño y Desarrollo

Recopilamos todas las entradas necesarias para el diseño y desarrollo de nuestros productos y servicios, incluyendo los requisitos del cliente, las especificaciones técnicas y los requisitos legales y reglamentarios aplicables.

8.3.3 Controles del Diseño y Desarrollo

Implementamos controles rigurosos durante el proceso de diseño y desarrollo para asegurar que nuestros productos y servicios cumplan con los estándares de calidad y seguridad de la información. Esto incluye revisión y pruebas de diseño, así como la gestión de cambios.

8.3.4 Salidas del Diseño y Desarrollo

Generamos documentación de diseño y desarrollo que incluye especificaciones técnicas, planos y cualquier otra información relevante para garantizar que nuestros productos y servicios cumplan con los requisitos.

8.4 Control de los Procesos, Productos y Servicios Producidos

8.4.1 Control de Procesos, Productos y Servicios

Controlamos nuestros procesos, productos y servicios de manera efectiva para garantizar que se ajusten a los requisitos de calidad y seguridad de la información. Esto incluye la supervisión, medición y seguimiento continuo de los procesos.

8.4.2 Identificación y trazabilidad

Identificamos y rastreamos nuestros productos y servicios para asegurarnos de que cumplen con los requisitos específicos. Esto garantiza la trazabilidad de nuestros productos y servicios en todo momento.

8.4.3 Propiedad del Cliente y Preservación de Productos y Servicios

Preservamos los productos y servicios de nuestros clientes y partes satisfactorias y garantizamos que no se dañarán ni se deteriorarán durante su almacenamiento o entrega.

8.4.4 Servicios suministrados externamente

Como aseguradora nos esforzamos por gestionar con precisión los procesos, productos y servicios suministrados externamente. Esto significa que seleccionamos cuidadosamente a nuestros proveedores, establecemos criterios de desempeño y calidad, y realizamos auditorías regulares para asegurarnos de que se cumplan nuestros estándares. Esta gestión rigurosa garantiza la calidad y la

fiabilidad de nuestros servicios, lo que a su vez protege los intereses de nuestros valiosos clientes y partes interesadas.

Para mayor detalle, ver procedimiento para evaluación de proveedores SIG-8-06-PRO, Manual de procedimientos, Apéndice 9.

El apartado 8 se centra en las operaciones relacionadas con la calidad y seguridad de la información en Aseguradora ABANK, asegurando que nuestros productos y servicios cumplan con los requisitos y estándares establecidos.

9.Evaluación del desempeño

En Aseguradora ABANK, la evaluación del desempeño es esencial para asegurarnos de que nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información funcione eficazmente y cumpla con sus objetivos. Este apartado se centra en cómo evaluamos y medimos nuestro desempeño en términos de calidad y seguridad de la información.

9.1 Seguimiento, Medición, Análisis y Evaluación

9.1.1 Generalidades

Llevamos a cabo un seguimiento, medición, análisis y evaluación sistemática de nuestro desempeño en relación con la calidad y seguridad de la información. Esto nos permite garantizar que cumplimos con nuestros objetivos y requisitos establecidos.

9.1.2 Evaluación del Cumplimiento Legal y Reglamentario

Evaluar y asegurar el cumplimiento de las leyes y regulaciones relevantes en materia de calidad y seguridad de la información es fundamental en Aseguradora ABANK. Esto incluye la identificación de requisitos legales y reglamentarios aplicables, su seguimiento y su cumplimiento.

9.1.3 Evaluación del Cumplimiento de los Requisitos

Además del cumplimiento legal, evaluamos nuestro desempeño para garantizar que cumplimos con los requisitos del SIG, incluyendo nuestra política de calidad y seguridad de la información, objetivos y procedimientos.

9.1.4 Seguimiento y Medición del Desempeño

Realizamos un seguimiento y medición continua de nuestro desempeño utilizando indicadores claves de desempeño (KPI) específicos para la calidad y seguridad de la información. Esto nos permite identificar áreas de mejora y tomar medidas correctivas cuando sea necesario.

Para mayor detalle, ver procedimiento de evaluación de la satisfacción del cliente SIG-9-09-PRO, Manual de procedimientos, Apéndice 9).

9.2 Auditoría Interna

9.2.1 Auditoría Interna del SIG

Realizamos auditorías internas periódicas de nuestro SIG de Calidad y Seguridad de la Información para evaluar su conformidad y eficacia. Estas auditorías son realizadas por personal competente e independiente.

Para mayor detalle, ver procedimiento de auditoría interna SIG-9-10-PRO, Manual de procedimientos, Apéndice 9).

9.2.2 Resultados de Auditoría Interna

Los resultados de las auditorías internas se documentan y se comunican a la alta dirección ya las partes interesadas pertinentes. Se identifican oportunidades de mejora y se toman medidas

correctivas y preventivas cuando sea necesario para abordar cualquier no conformidad o área de mejora identificada.

9.3 Revisión por la Dirección

9.3.1 Generalidades

La alta dirección de Aseguradora ABANK lleva a cabo revisiones periódicas del SIG de Calidad y Seguridad de la Información para asegurarse de que sigue siendo adecuado, eficaz y alineado con nuestros objetivos. Estas revisiones se basan en datos reales de desempeño y en el análisis de la información documentada.

Para mayor detalle, ver procedimiento revisión por la dirección SIG-9-11-PRO, Manual de procedimientos, Apéndice 9).

9.3.2 Resultados de la Revisión por la Dirección

Los resultados de las revisiones por la dirección se documentan y se utilizan para tomar decisiones informadas sobre la mejora continua del SIG. Se identifican áreas de éxito y se establecen planes de acción para abordar áreas de mejora.

La evaluación del desempeño es una parte fundamental de nuestro enfoque en Aseguradora ABANK para lograr la mejora continua de la calidad y seguridad de la información en nuestro Sistema Integrado de Gestión.

10. Mejora

En Aseguradora ABANK, la mejora continua es un compromiso fundamental en nuestro Sistema Integrado de Gestión (SIG) de Calidad y Seguridad de la Información. Este capítulo se centra en cómo identificamos oportunidades de mejora, implementamos acciones correctivas y preventivas, y aseguramos que nuestros procesos y resultados evolucionen de manera constante.

10.1 Identificación de Oportunidades de Mejora

Estamos comprometidos con la identificación proactiva de oportunidades de mejora en nuestro SIG. Esto incluye:

- Recopilación y análisis de datos de desempeño, tanto internos como externos.
- Evaluación de retroalimentación de clientes y partes interesadas.
- Monitoreo de incidentes de seguridad de la información y no conformidades.
- Análisis de resultados de auditorías internas y revisión por la dirección.

10.2 Acciones Correctivas y Preventivas

10.2.1 Acciones Correctivas

Cuando se identifican no conformidades o se detectan problemas en nuestros procesos o resultados, implementamos acciones correctivas de manera inmediata y eficaz. Nuestro enfoque en acciones correctivas incluye:

- Identificación de la causa raíz del problema.
- Desarrollo de un plan de acción para abordar la causa raíz.
- Implementación de medidas correctivas.
- Monitoreo para garantizar la eficacia de las acciones correctivas.

Para mayor detalle, ver procedimiento tratamiento de No conformidades y Acciones correctivas SIG-10-12-PRO, Manual de procedimientos, Apéndice 9).

10.2.2 Acciones Preventivas

Además de las acciones correctivas, también nos enfocamos en la prevención proactiva de problemas. Identificamos posibles riesgos y oportunidades de mejora antes de que se conviertan en problemas significativos. Nuestro enfoque en acciones preventivas incluye:

- Evaluación de riesgos de seguridad de la información.
- Desarrollo de planes de acción preventiva.
- Implementación de medidas preventivas.
- Monitoreo continuo para evitar la recurrencia de problemas.

10.3 Medición del Desempeño de Mejora

Realizamos un seguimiento y evaluación constante de nuestras acciones de mejora y su impacto en el desempeño del SIG. Esto incluye la medición de resultados, la revisión de indicadores clave de desempeño y la verificación de la efectividad de las acciones implementadas.

10.4 Actualización del SIG

Mantener nuestro SIG actualizado es esencial para asegurar que esté alineado con nuestras metas y objetivos organizacionales. Esto incluye:

- Revisión periódica de la política de calidad y seguridad de la información.
- Evaluación de la idoneidad de los procedimientos y prácticas actuales.
- Ajuste de los objetivos del SIG según sea necesario para reflejar cambios en el entorno operativo o en las expectativas de las partes interesadas.

10.5 Comunicación y Concienciación

Fomentamos la comunicación y concienciación en toda la organización en relación con las mejoras implementadas en el SIG. Esto incluye la difusión de información sobre cambios, logros y lecciones aprendidas.

10.6 Registro de Mejoras

Mantenemos registros detallados de todas las mejoras implementadas en el SIG. Estos registros incluyen:

- Descripción de la mejora.
- Fecha de implementación.
- Responsable de la implementación.
- Resultados medidos y logros alcanzados.

10.7 Reconocimiento y Celebración

Reconocemos y celebramos los logros y mejoras en el SIG de Calidad y Seguridad de la Información. Esto motiva a nuestro equipo y refuerza nuestro compromiso con la mejora continua.

10.8 Revisión de Mejora Continua

De manera regular, llevamos a cabo revisiones formales de la mejora continua en nuestro SIG. Estas revisiones incluyen:

- Evaluación de la eficacia de las acciones de mejora.
- Identificación de nuevas oportunidades de mejora.
- Ajuste de enfoques y estrategias de mejora en función de lecciones aprendidas.

La mejora continua es un pilar fundamental en Aseguradora ABANK y forma parte integral de nuestro enfoque para lograr la excelencia en calidad y seguridad de la información.

CONTROL DE CAMBIOS

Versión	Fecha de edición	Numeral Revisión	Párrafo de numeral Modificado	Adición (A) y/o Eliminación(E)	Texto Modificado.

01					**Creación del documento**

4.4 Plan para la implementación de la propuesta

A continuación, se presenta una propuesta o aproximación para el cronograma de implementación de las diversas etapas consideradas en este documento para el diseño del SIG (ver Tabla *45*). El plazo máximo contemplado es de 13 meses es decir 52 semanas consecutivas, correspondiente a la etapa de gestión por procesos. Una vez cumplido el cronograma propuesto, será necesario considerar el tiempo adicional que Aseguradora ABANK requiera para completar un ciclo completo desde la planificación hasta la toma de acciones para mejorar aquellos aspectos que no cumplan con sus objetivos (Planificar-Hacer-Verificar-Actuar).

Tabla 45. Cronograma para la implementación del SIG en Aseguradora ABANK

Descripción del hito	Entregable	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Mes 13
0. Etapa de prediagnóstico														
Fase 0. Contacto inicial con Cliente	- Propuesta de Anteproyecto													
I. Etapa de diagnóstico o evaluación inicial														
Fase I. Concientización	- Programa de concientización - Talleres de concientización													
Fase II. Análisis del contexto de la organización	FODA													
Fase III. Evaluación del nivel de madurez de la organización	Informe del nivel de madurez de la organización													
II. Etapa de planificación y diseño del SIG														
Fase IV. Diseño del SIG	- Método de integración del SIG - Roles y responsabilidades de la implantación													

Continúa Tabla 45 en la siguiente página →

Descripción del hito	Entregable	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Mes 13
III. Etapa de documentación del SIG														
Fase V. Establecimiento de política del SIG y objetivos	- Política y objetivos del SIG													
Fase VI. Estandarización de procesos del SIG	- Mapa de procesos - Procesos y procedimientos del SIG - Indicadores de desempeño													
Fase VII. Identificación de riesgos y controles del SIG	- Riesgos del SIG - Controles de seguridad de la información - Controles de procesos del SIG Calidad													
Fase VIII. Identificación de Clientes y partes interesadas	- Matriz de partes interesadas													
Fase IX. Desarrollo del manual del SIG	- Manual del SIG y sus plantillas necesarias para registros													
IV. Etapa de implantación del SIG														
Fase X. Capacitación de la implantación	- Programa de capacitación - Capacitación en el SIG													
Fase XI. Prueba piloto	- Programa de prueba piloto - Informe de prueba piloto - Planes de acción de prueba piloto													
Fase XII. Apoyo en la implantación del SIG	- Resoluciones a consultas													
V. Etapa de evaluación del SIG														
Fase XIII. Evaluación del SIG (Auditoría)	- Programa de capacitación en auditoría													

Continúa Tabla 45 en la siguiente página →

Descripción del hito	Entregable	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Mes 13
	del SIG - Capacitación en auditoría del SIG - Plan de auditoría - Informe de auditoría del SIG													
Fase XIV. Apoyo en la gestión de hallazgos	- Planes de acción de hallazgos													
Fase XV. Re-evaluación del nivel de madurez de la organización	- Nivel de madurez de la organización post implementación del SIG													
VI. Etapa de mantenimiento y mejora del SIG														
Fase XVI. Empoderamiento en mejora continua	- Programa de capacitación en mejora continua - Capacitación en mejora continua - Capacitación en resolución de problemas - Formación de círculos de calidad													
Fase XVI. Revisión por la dirección	- Acta revisión por la dirección - Planes de acción de mejora continua													
VII. Etapa certificación del SIG														
Fase XVII. Acompañamiento en la certificación	- Tramitación del proceso de certificación con ente acreditado - Resolución y asesoría en proceso de acreditación													

Fuente: elaboración propia

4.5 Presupuesto de la implementación

Este presupuesto detalla los costos estimados para la implementación de las normativas ISO 9001:2015 e ISO/IEC 27001:2022 en Aseguradora ABANK. Se incluyen categorías como consultoría, capacitación, documentación, software y herramientas, infraestructura tecnológica, certificación y contingencias. Estos costos son estimativos y pueden variar según el contexto de la realidad nacional en el momento que se pretenda realizar el presente proyecto organizacional.

Tabla 46. Presupuesto de la implementación del SIG

Elementos	Descripción	Costo $ USD
Consultoría	Contratación de consultores externos para asesoramiento en la implementación de ISO 9001:2015 y ISO/IEC 27001:2022.	$15,000 - $25,000
Capacitación	Capacitación del personal en ambas normativas, incluyendo cursos de sensibilización y formación para el equipo de implementación.	$5,000 - $10,000
Documentación	Desarrollo de documentación necesaria, incluyendo manuales de calidad, políticas de seguridad de la información, procedimientos operativos estándar, etc.	$7,000 - $12,000
Software y Herramientas	Adquisición de software de gestión de calidad y seguridad de la información para facilitar el cumplimiento y la gestión de los sistemas. -Wireshark -Office 365 Dependiendo del número de usuarios y módulos requeridos, los costos pueden variar entre $2,000-$5,000 -Soporte y Mantenimiento Anual: Aproximadamente el 20% del costo de la licencia, estimado en $2,000 a $3,000 al año. -Capacitación en Uso de Software: Programas de formación para el personal clave, estimados en $2,000 a $3,000.	$10,000 - $15,000

Infraestructura Tecnológica	Mejoras en la infraestructura tecnológica para garantizar la seguridad de la información, como firewalls, sistemas de detección de intrusiones, etc. -Actualización o Adquisición de Firewalls de Última Generación: Como Palo Alto Networks o Fortinet, con un costo estimado entre $5,000 y $10,000 dependiendo del modelo y funcionalidades. -Soluciones de Encriptación de Datos en Reposo y en Tránsito: Productos como Symantec Data Loss Prevention o Vormetric, con un costo entre $3,000 y $5,000. Seguridad en la Nube: -Implementación de Seguridad para Servicios en la Nube: Integración de soluciones como AWS Shield o Microsoft Azure Security Center, con un costo estimado entre $5,000 y $8,000. -Servicios de Monitoreo Continuo de Seguridad: Servicios gestionados para la vigilancia continua de la infraestructura, con costos entre $2,000 y $5,000 anuales.	$20,000 - $30,000
Certificación	Costos asociados con la certificación por parte de un organismo de certificación acreditado.	$8,000 - $15,000
Contingencias	Fondos reservados para imprevistos y ajustes durante el proceso de implementación.	$5,000 - $7,000
	TOTAL	$70,000 – $114,000

Fuente: Elaboración propia

4.6 Resultados de la implementación

La implementación del Sistema Integrado de Gestión combina los estándares de la ISO 9001:2015 y la ISO/IEC 27001:2022 para abordar tanto la calidad como la seguridad de la información. Esto permitirá a la Aseguradora ABANK mejorar la eficiencia operativa, la satisfacción del cliente y la protección de datos, al tiempo que cumplen con regulaciones y fortalecen la confianza del cliente. La integración de ambos sistemas promueve una cultura organizacional cohesiva, centrada en la mejora continua y la seguridad integral.

Con respecto a calidad

- Mejora en la satisfacción del cliente: Al enfocarse en la mejora continua y la satisfacción del cliente, las empresas pueden identificar y abordar las necesidades y expectativas de los clientes de manera más efectiva, lo que conduce a una mayor retención de clientes y lealtad a la marca.
- Mejora de la eficiencia operativa: La ISO 9001 fomenta la estandarización de procesos y procedimientos dentro de una organización, lo que puede aumentar la eficiencia y reducir el desperdicio.
- Cumplimiento regulatorio: La implementación de un SG conforme a la norma ISO 9001 es un apoyo fundamental para la aseguradora en cumplir con los requisitos regulatorios y legales aplicables a sus operaciones.
- Mejora de la gestión de riesgos: La norma ISO 9001 promueve la identificación y gestión proactiva de los riesgos en los procesos de la organización, lo que ayuda a prevenir problemas y aumentar la capacidad de adaptación a cambios inesperados.

Con respecto a seguridad de la información

- Mejora de la confianza del cliente: La normativa ISO/IEC 27001 aumenta la confianza de los clientes, socios comerciales y otras partes interesadas al demostrar el compromiso de la organización con la seguridad de la información y la protección de los datos confidenciales.
- Protección de la información: La norma ISO/IEC 27001 es de apoyo para identificar y proteger la información sensible y crítica, como datos de clientes, propiedad intelectual y datos financieros, mitigando así el riesgo de pérdida, robo o acceso no autorizado.
- Cumplimiento legal y regulatorio: Al establecer un marco de control de seguridad de la información, la ISO/IEC 27001 ayuda a cumplir con las leyes y regulaciones relacionadas con la protección de datos, la privacidad y la seguridad de la información.
- Gestión de riesgos: La norma promueve la identificación y evaluación de riesgos de seguridad de la información, así como la implementación de controles para mitigar estos riesgos, lo que ayuda a proteger los activos de información de la organización contra posibles amenazas y vulnerabilidades.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

Después de realizar la investigación de campo y llevar a cabo un análisis sobre la propuesta de diseño de un sistema de gestión integrado basado en las normas ISO 9001:2015 para la Gestión de la Calidad e ISO/IEC 27001:2022 para la Seguridad de la Información en la empresa aseguradora ABANK, se presentan las siguientes conclusiones y recomendaciones:

5.1 Conclusiones

1. **Desafío en el enfoque a Calidad:** A pesar de algunos avances en la implementación de ISO 9001:2015, especialmente en los capítulos 4, 7, y 8, ABANK enfrenta dificultades importantes en áreas clave como el liderazgo y la mejora continua. La consistencia en los resultados obtenidos sugiere que los instrumentos utilizados para evaluar estos avances son fiables, pero se requiere una acción decisiva para abordar las deficiencias identificadas.
2. **Brechas en la Seguridad de la Información:** El cumplimiento parcial de ISO/IEC 27001:2022 muestra fortalezas en la operación, pero deficiencias graves en la implementación integral de elementos de control que garanticen la seguridad de la información. Los resultados reflejan una correlación media entre la implementación de medidas de seguridad y la operación eficiente, lo que destaca la urgencia de reforzar las prácticas en áreas críticas para proteger la información sensible de los asegurados y demás partes interesadas.
3. **Satisfacción del Cliente como Indicador Clave:** La encuesta de satisfacción revela un nivel considerable de satisfacción entre los clientes, aunque también pone de manifiesto áreas que requieren mejora. La variabilidad observada en las opiniones de los encuestados se mantiene dentro de los rangos esperados, lo que valida la fiabilidad de los datos y sugiere la necesidad de enfocar esfuerzos en los aspectos que generan insatisfacción o dudas.
4. **Enfoque estratégico del negocio:** Implementar un Sistema Integrado de Gestión de Calidad y Seguridad de la Información no solo es necesario para optimizar operaciones y mejorar la satisfacción del cliente, sino también para garantizar la protección de la información y reforzar la competitividad de ABANK. Los resultados obtenidos proporcionan evidencia de que los métodos de recolección de datos son fiables y válidos, apoyando la decisión de considerar esta implementación como una prioridad estratégica.

5.2 Recomendaciones

1. **Mejorar el Cumplimiento de ISO 9001:2015:** Aseguradora ABANK debe realizar una auditoría integral que identifique las deficiencias específicas en los capítulos 5, 6, 9, y 10 de la norma, enfocándose en áreas como liderazgo y mejora continua. Posteriormente, debe desarrollar un plan de acción que contemple la optimización de procesos críticos y la implementación de mecanismos de monitoreo adaptados a su contexto operativo. La capacitación debe centrarse en habilidades específicas que mejoren la gestión de calidad, y la adopción de herramientas tecnológicas debe alinearse con las necesidades particulares de ABANK, considerando una consultoría externa solo para aspectos donde la organización carece de experiencia interna.
2. **Fortalecer la Seguridad de la Información según ISO/IEC 27001:2022:** ABANK debe priorizar la mejora continua y la seguridad de la información, comenzando con una evaluación de riesgo específica que identifique vulnerabilidades en los controles actuales. Esto debe complementarse con una actualización de políticas y procedimientos, enfocada en áreas críticas identificadas en la evaluación, como la gestión de incidentes y la seguridad en las operaciones. Además, se deben diseñar programas de concienciación que aborden directamente las brechas en el conocimiento de seguridad del personal, y establecer auditorías internas dirigidas a monitorear la implementación efectiva de estas mejoras.
3. **Elevar la Satisfacción del Cliente:** Con base en los resultados de la encuesta de satisfacción, ABANK debe diseñar un plan de acción que aborde específicamente las preocupaciones de los clientes que se muestran indecisos o insatisfechos, enfocándose en mejorar la comunicación y la calidad del servicio en los puntos de contacto clave. Implementar un sistema de retroalimentación continua permitirá identificar y responder rápidamente a problemas emergentes, lo cual es crucial para aumentar la tasa de recomendación y la lealtad del cliente.
4. **Avanzar en la Implementación del Sistema Integrado de Gestión:** La implementación del Sistema Integrado de Gestión debe enfocarse en áreas estratégicas donde ABANK puede obtener los mayores beneficios competitivos, como la optimización de procesos críticos y la gestión de riesgos. La organización debe establecer un calendario de auditorías internas que priorice las áreas de mayor impacto y vincular las metas de formación del personal con las competencias necesarias para mantener y mejorar este sistema, asegurando que todas las iniciativas estén alineadas con los objetivos estratégicos de la empresa.

REFERENCIA BIBLIOGRÁFICA

Alvarado de Duran, J. I., Parras Velasco, M. C., & Zamora Zabaleta, G. A. (2017). *Sistema de Gestión de Calidad basado en riesgos para las pequeñas y mediana empresas corredoras de seguros del área metropolitana de San Salvador.* San Salvador: Universidad de El Salvador.

Ardila Navarrete, J. A. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva compañía de seguros S.A* . Bogotá: Universidad Nacional Abierta y a Distancia.

Asociación Española de Normalización [AENOR]. (2005). *Guía para la integración de sistemas de gestión.* (UNE 66177:2005).

Aseguradora ABANK. (2020). *Memoria Anual de Gobierno Corporativo*. Antiguo Cuscatlán: Aseguradora ABANK.

Aseguradora ABANK. (2022). Aseguradora ABANK. Recuperado de https://www.aseguradoraabank.com/mision-vision-valores

Baena Paz, Guillermina. (2014). *Metodología de la investigación.* Ciudad de México. Grupo Editorial Práctica.

British Standards Institution [BSI]. (2012). *Especificación de los requisitos comunes del sistema de gestión como marco para la integración*. (PAS 99).

Código de Comercio. Decreto N° 671. Diario Oficial N° 140. Tomo N° 228.

Der Wens, C. V. (2020). *Implementing and auditing an Information Security Management System in small and medium-sized Bussinesses.* Netherlands: Brave New Books.

Estruga, N. (23 de noviembre de 2021). EALDE Business School. Recuperado de https://www.ealde.es/insurtech/

García Remache, J. A. (2020). *Diseño de un Sistema Integrado de Gestión basado en las normas ISO 9001:2015 e ISO 27001:2013, para la emisión de documentos de identificación militar en la matriz de la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas*. Quito: Universidad Andina Simón Bolívar.

Hernández Hernández. N., Garnica González (2015). *Árbol de problemas del análisis al diseño y desarrollo de productos*. México. Instituto tecnológico de Aguas calientes.

Guízar Montufar, R. (2013). *Desarrollo organizacional-principios y aplicaciones*. México: McGraw-Hill/Interamericana Editores, S.A. de C. V.

Ley Especial Contra Actos de Terrorismo. Decreto N° 108. Diario Oficial N° 193. Tomo N° 373. San Salvador. 17 de octubre de 2006.

Ley de Protección al Consumidor. Decreto N° 776. Diario Oficial N°58. Tomo N° 330. San Salvador. 16 de julio 2021.

López Lemos, P. (2015). *Cómo documentar un Sistema de Gestión de Calidad según ISO 9001:2015*. Madrid: Fundación Confemetal.

Méndez Álvarez, C. (2020). Metodología de la investigación: diseño y desarrollo del proceso de investigación en ciencias empresariales. Colombia. Alpha editoriales

Najarro Alfaro, C. A., Urrutia López, E., & Ibarra de Martínez, L. J. (2015). *Metodología para implantar seguridad de la información en una empresa financiera en El Salvador.* Antiguo Cuscatlán: Universidad Don Bosco.

NCM-03 Normas Técnicas para la transparencia y divulgación de la información de las sociedades de seguros. (07 de enero de 2019) San Salvador: Superintendencia del Sistema Financiero. Recuperado de https://ssf.gob.sv/descargas/Normas/Normas_Prudenciales/Seguros/NCM-03.pdf

NRP-24 Normas Técnicas para la Gestión de la Continuidad del Negocio. (01 de julio de 2020). San Salvador: Banco Central de Reserva. Recuperado de https://www.transparencia.gob.sv/system/documents/documents/000/357/090/original/Normas_T%C3%A9cnicas_para_el_sistema_de_gesti%C3%B3n_del_negocio.pdf?1601575648

NRP-20 Normas Técnicas para la Gestión Integral de Riesgos de las Entidades Financieras. (1 de abril de 2020). San Salvador: Banco Central de Reserva. Recuperado de https://www.bcr.gob.sv/regulaciones/upload/NRP-20.pdf

NPR-23. Norma Técnica para la Gestión de la Seguridad de la Información. (14 de abril de 2020). San Salvador: Superintendencia del Sistema Financiero. Recuperado de https://www.bcr.gob.sv/regulaciones/upload/NRP-23.docx?v=1588193386

Ñaupas H., Valdivia M.R., Palacios J.J., Romero H.E. (2014). *Metodología de la investigación cuantitativa – cualitativa y redacción de tesis*. Bogotá Colombia. Ediciones de la U.

Organización Internacional de Normalización [ISO]. (2015). *Sistemas de gestión de la calidad — Fundamentos y vocabulario* (ISO 9000:2015, Traducción oficial).

Organización Internacional de Normalización [ISO]. (2015). *Sistemas de gestión de la calidad — Requisitos* (ISO 9001:2015, Traducción oficial).

Organización Internacional de Normalización [ISO]. (2018). *Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario* (ISO/IEC 27000:2018).

Organización Internacional de Normalización [ISO]. (2021). *Sistemas de gestión de la calidad — Orientación para la información documentada.* (ISO 10013:2021, Traducción oficial).

Organización Internacional de Normalización [ISO]. (2022). *Sistemas de gestión de la seguridad de la información— Requisitos* (ISO/IEC 27001:2022).

Pineda Capador, I. N. (2021). *Propuesta de implementación de la norma NTC ISO 9001:2015 en la organización integral de Seguros LTDA*. Bogotá: Fundación Universidad de América.

Reglamento de Protección al Consumidor. Decreto N° 52. Diario Oficial N° 88. Tomo N° 371. San Salvador. San Salvador. 1 de junio de 2021.

Rojas Soriano, R. (2013). *Guía para realizar investigaciones sociales. 38*ª Edición. México D.F. México: Editorial Plaza y Valdés, S.A. de C.V.

Sampieri, R. (2018). *Metodología de la Investigación: Las rutas cuantitativas, cualitativas y mixtas.* Ciudad de México: McGraw Hill.

Viteri Zambrano, R. X. (2016). *Diseño de un Sistema de Gestión de calidad para el proceso de indemnizaciones de vehículos en Aseguradora del Sur, período 2016*. Quito: Universidad Tecnológica Equinoccial.

Wrobel, M. (10 de Mayo de 2023). Cómo desarrollar un Inventario de Activos para ISO 27001. Obtenido de Invgate: https://blog.invgate.com/es/inventario-activos-iso-27001

BIBLIOGRAFÍA

Álvarez, J., Álvarez, I., & Bullón, J. (2006). Introducción a la Calidad. Aproximación a los sistemas de gestión y herramientas de calidad. Vigo, España. Editorial Ideas propias.

Calso Morales, Natalia, Pardo Álvarez, José Manuel. (2018). Guía práctica para la integración de sistemas de gestión. Madrid: AENOR EDICIONES.

Cantú Delgado, H. (2011). Desarrollo de una cultura de calidad. México D.F.: McGraw HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos, ciberseguridad e insurtech. Madrid: DYKINSON, S. L .

Ley de Sociedades de Seguros. Decreto N° 844. Diario Oficial N° 207. Tomo N° 333. San Salvador. 4 de noviembre de 1996.

Publicaciones Vértice SL. (2008). Aspectos prácticos de la calidad en el servicio. España: Vértice.

APÉNDICE 1. MATRIZ DIAGNÓSTICA PARA PLANTEAR EL PROBLEMA DE INVESTIGACIÓN

DIAGNÓSTICO (PRELIMINAR)	**SÍNTOMAS Y SIGNOS**	**CAUSAS**	**CONSECUENCIAS CRÍTICAS**	**FORMULACIÓN**	**SISTEMATIZACIÓN**
Descripción o antecedentes de la situación problemática. **Qué es lo que está ocurriendo (problema principal)**	*Hechos o situaciones que se observan al analizar el sujeto de investigación.*	*Hechos o situaciones que se producen por la existencia de los síntomas identificados.* **Por qué está ocurriendo**	*Situaciones que pueden presentarse si se siguen generando síntomas y causas.* **Que es lo que está ocasionando (efectos o consecuencias)**	*Redactar el problema como una pregunta o de forma enunciativa (cómo, cuál, dónde, qué) o aseveración, sobre lo que se busca resolver y que está estrechamente relacionada con el tema específico a investigar*	*Definir preguntas secundarias, las que serán útiles al redactar conclusiones*
	Variables				
	Dependientes	***Independientes***			
Aseguradora ABANK no cuenta con un modelo de gestión organizacional adecuado para la entrega eficaz de servicios de calidad y garantizar la seguridad de la información de sus clientes y partes interesadas.	-Reprocesos e incumplimiento de tiempos de servicio -Insatisfacción de clientes -Uso de documentación obsoleta -Vulnerabilidad de los sistemas de información	-Deficiente situación actual de los procesos -Falta de enfoque en los requisitos de los clientes -Estructuración documental desactualizada -Controles deficientes en seguridad de la información	- Aumento de costos para corregir errores - Pérdidas de negocios con clientes - Pérdida de la eficacia operativa - Procesos burocráticos y no estandarizados - Robo/daños/secuestro a la información de la organización - Incumplimiento de normativas	¿De qué manera se puede llevar a cabo la sistematización de los procesos para mejorar aspectos de calidad y seguridad de la información en Aseguradora ABANK?	1. ¿En qué estado se encuentran los procesos de Aseguradora ABANK en relación con la calidad de sus servicios? 2. ¿De qué manera se identifican las necesidades y expectativas de los clientes de la organización? 3. ¿Cuál es la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización? 4. ¿Cuáles son las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información?

Fuente: Adaptado de Méndez Álvarez, C. (2006). *Metodología: Diseño y desarrollo del proceso de investigación con énfasis en Ciencias Empresariales. 4ª. Ed. Editorial LIMUSA, S.A: de C.V. Grupo Noriega Editores. México. pág. 170.*

APÉNDICE 2. MATRIZ DE CONSISTENCIA MARCO REFERENCIAL

DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD NTS ISO 9001:2015 Y DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022 APLICABLE EN ASEGURADORA ABANK, S. A., SEGUROS DE PERSONAS					
DIAGNÓSTICO (PRELIMINAR)	**FORMULACIÓN Y SISTEMATIZACIÓN**	**OBJETIVO GENERAL Y ESPECÍFICOS**	**HIPÓTESIS GENERAL Y ESPECÍFICAS**	**OPERACIONALIZACIÓN DE VARIABLES**	
				VARIABLES	**MEDICIÓN (INDICADORES)**
Descripción o antecedentes de la situación problemática. Qué es lo que está ocurriendo (problema principal)	*¿De qué manera se puede llevar a cabo la sistematización de los procesos para mejorar aspectos de calidad y seguridad de la información en Aseguradora ABANK?*	*Diseñar un Sistema Integrado de Gestión de la Calidad ISO 9001:2015, y Seguridad de la Información ISO/IEC 27001:2022; aplicable en Aseguradora ABANK, S. A. Seguros de Personas.*	*El diseño e implementación de un Sistema Integrado de Gestión de la Calidad y Seguridad de la Información, basado en las normas ISO 9001:2015 e ISO/IEC 27001:2022, permitirá a Aseguradora ABANK mejorar la comunicación y el trabajo en equipo, aumentar el compromiso y liderazgo de gerentes y directores, optimizar las operaciones y servicios al cliente, y fortalecer la seguridad de la información, resultando en una mayor eficiencia operativa y mitigación de riesgos relacionados con la gestión de datos confidenciales.*	*Atributos que se miden o se argumentan, se utilizan para designar cualquier característica o cualidad de la unidad de observación*	*La operacionalización es un proceso de traslado de un nivel abstracto a un nivel empírico, observable, medible (cuantitativa o cualitativamente)*
Aseguradora ABANK no cuenta con un modelo de gestión organizacional adecuado para la entrega eficaz de servicios de Calidad y garantizar la seguridad de la información de sus clientes y partes interesadas.	*¿En qué estado se encuentran los procesos de Aseguradora ABANK en relación con la calidad de sus servicios?*	*Evaluar las condiciones actuales de Aseguradora ABANK en relación con aspectos de calidad, según ISO 9001:2015.*	*Las condiciones actuales de Aseguradora ABANK en aspectos de calidad, según ISO 9001:2015, están por debajo del 50% debido a problemas en la gestión de procesos, control de la información documentada, errores operacionales y deficiencias en liderazgo y compromiso.*	*Grado de conformidad con respecto a requisitos de Calidad*	*- Identificación del cumplimiento de la organización ante los requisitos de normativa ISO 9001:2015 (cualitativo)* *-(Requisitos cumplidos ante ISO 9001:2015/ Total de requisitos requeridos por ISO 9001:2015) *100 (cuantitativo)*
	¿De qué manera se identifican las necesidades y expectativas de los clientes de la organización?	*Identificar las necesidades y expectativas de los clientes de la organización conforme a ISO 9001:2015 e ISO IEC 27001:2022.*	*Las necesidades y expectativas de los clientes de Aseguradora ABANK no se identifican y no se consideran en las estrategias de la organización, por lo cual se genera insatisfacción de estos.*	*Satisfacción de las necesidades y expectativas de los clientes*	*-Identificación de necesidades y expectativas de Clientes (cualitativo)* *-(Número de clientes (asegurados) satisfechos/Total de encuestados) *100*
	¿Cuál es la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización?	*Identificar la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización.*	*El nivel de cumplimiento de información documentada de la organización, con relación a los requisitos ISO 9001:2015 e ISO/IEC 27001:2022 es inferior a 40%.*	*Información documental existente*	*-Identificación de información documentada de la organización (cualitativo)* *-(Información documentada de la organización/ información documentada requerida por ISO 9001:2015 e ISO/IEC 27001:2022) * 100 (cuantitativo)*
	¿Cuáles son las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información?	*Analizar las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información, según ISO/IEC 27001:2022.*	*Las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información, según ISO/IEC 27001:2022 es inferior a 40%.*	*Grado de conformidad con respecto a requisitos de Seguridad de la información*	*- Identificación del cumplimiento de la organización ante los requisitos de normativa ISO/IEC 27001:2022 (Mixto)* *-Identificación de los activos de información (cualitativo)* *-Identificación de controles de seguridad de la información (cualitativo)* *-(Controles de seguridad de seguridad de la información cumplidos/ Total de controles de seguridad de la información según ISO/IEC 27001:2022) *100 (cuantitativo)*

Fuente: Adaptado de Méndez Álvarez, C. (2006). *Metodología: Diseño y desarrollo del proceso de investigación con énfasis en Ciencias Empresariales.* 4ª. Ed. Editorial LIMUSA, S.A: de C.V. Grupo Noriega Editores. México. pág. 170.

APÉNDICE 3.VIABILIDAD TÉCNICA

Jueves 13 de enero de 2023

Maestría de Sistemas Integrados de Gestión de Calidad
Facultad de Ciencias Económicas
Universidad de El Salvador

A quien corresponda,

Nosotros, **Nora Nathaly Muñoz Sosa** con Carné **MS21032** y **Gustavo Manuel Rodas Laínez** con Carné **RL2102,** egresados de la Maestría de Sistemas Integrados de Gestión de Calidad de la Facultad de Ciencias Económicas de la Universidad de El Salvador quienes desarrollamos el trabajo de graduación titulado: **"DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE CALIDAD NTS ISO 9001:2015 Y DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022 APLICABLE EN ASEGURADORA ABANK, S. A., SEGUROS DE PERSONAS, LA LIBERTAD, EL SALVADOR"** manifestamos que contamos con la competencia técnica para desarrollar la investigación anteriormente expuesta y nos comprometemos a cumplir con los objetivos del proyecto de acuerdo a los requisitos exigidos por la Universidad.

Agradeciéndole su atención, atentamente:

Nora Nathaly Muñoz Sosa
MS21032
ms21032@ues.edu.sv

Gustavo Manuel Rodas Laínez
RL21027
rl21027@ues.edu.sv

Aseguradora ABANK
Aseguradora ABANK, S.A.
Seguros de personas

Recibido
Carlos Rivera
Gerente de TI

COORDINACION MASIG
MAESTRIA EN SISTEMAS INTEGRADOS DE GESTION DE CALIDAD FCE/UES

Maestro Julio César Valle Valdez
M. en Administración de Empresas y Consultoría Empresarial
M. en Gestión Ambiental

RECIBIDO 28 FEB 2023

APÉNDICE 4. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN SEGÚN ISO IEC 27001:2022

#	Tipo de control	Nro.	Control	Descripción
1	Control organizacional	A.5.1	Políticas de seguridad de la información	Las políticas de seguridad de la información de la organización especifican los principios que deben seguir los miembros y las partes interesadas, como los proveedores. Estas políticas deben revisarse periódicamente y actualizarse según sea necesario.
2	Control organizacional	A.5.2	Roles y responsabilidades de seguridad de la información	Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
3	Control organizacional	A.5.3	Segregación de deberes	Al delegar subtareas a diferentes personas, este principio crea un sistema de controles y equilibrios que puede reducir la probabilidad de que ocurran errores y fraudes. El control está diseñado para evitar que una sola persona pueda cometer, ocultar y justificar acciones indebidas, reduciendo así el riesgo de fraude y error. También evita que una sola persona anule los controles de seguridad de la información.
4	Control organizacional	A.5.4	Responsabilidades de gestión	La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
5	Control organizacional	A.5.5	Contacto con autoridades	La organización deberá establecer y mantener contacto con las autoridades pertinentes.
6	Control organizacional	A.5.6	Contacto con grupos de interés especial	La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
7	Control organizacional	A.5.7	Inteligencia de amenazas	Este control está diseñado para ayudar a las organizaciones a comprender su entorno de amenazas. Esto es para que puedan determinar las acciones adecuadas para mantener la seguridad de la información en función de las amenazas que identifiquen.

#	Tipo de control	Nro.	Control	Descripción
8	Control organizacional	A.5.8	Seguridad de la información en la gestión de proyectos.	El control A.5.8 tiene como objetivo garantizar que los riesgos de seguridad de la información relacionados con los proyectos y los entregables se gestionen de manera efectiva durante la ejecución del proyecto
9	Control organizacional	A.5.9	Inventario de información y otros activos asociados	Requiere que las organizaciones identifiquen y documenten los activos importantes para sus operaciones y los riesgos asociados, y tomen medidas para protegerlos.
10	Control organizacional	A.5.10	Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
11	Control organizacional	A.5.11	Devolución de activos	El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización en su posesión al momento del cambio o terminación de su empleo, contrato o acuerdo.
12	Control organizacional	A.5.12	Clasificación de la información	La información se clasificará de acuerdo con la seguridad de la información. Necesidades de la organización basadas en la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
13	Control organizacional	A.5.13	Etiquetado de información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación adoptado por la organización.
14	Control organizacional	A.5.14	Transferencia de información	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y con otras partes.
15	Control organizacional	A.5.15	Control de acceso	Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros activos asociados en función de los requisitos de seguridad empresarial.

#	Tipo de control	Nro.	Control	Descripción
16	Control organizacional	A.5.16	Gestión de identidad	El propósito del Anexo A 5.16 es describir cómo una organización puede identificar quién (usuarios, grupos de usuarios) o qué (aplicaciones, sistemas y dispositivos) está accediendo a datos o activos de TI en un momento dado, y cómo se les otorga acceso a esas identidades.
17	Control organizacional	A.5.17	Información de autenticación	La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autorización.
18	Control organizacional	A.5.18	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.
19	Control organizacional	A.5.19	Seguridad de la información en las relaciones con los proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.
20	Control organizacional	A.5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con estos.
21	Control organizacional	A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Se deben definir e implementar procesos y procedimientos para gestionarlos riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
22	Control organizacional	A.5.22	Supervisión, revisión y cambio de gestión de servicios de proveedores	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
23	Control organizacional	A.5.23	Seguridad de la información para el uso de servicios en la nube	Este control debe implementarse para la adquisición, el uso, la gestión y la salida de los servicios en la nube, en relación con los requisitos únicos de seguridad de la información de la organización.

Continúa Tabla 5 en la siguiente página

#	Tipo de control	Nro.	Control	Descripción
24	Control organizacional	A.5.24	Incidente de seguridad de la información planificación y preparación de la gestión racionar	La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando la información, procesos, roles y responsabilidades de gestión de incidentes de seguridad.
25	Control organizacional	A.5.25	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes.
26	Control organizacional	A.5.26	Respuesta a la seguridad de la información incidentes	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
27	Control organizacional	A.5.27	Aprender de los incidentes de seguridad de la información	El conocimiento obtenido de los incidentes se utilizará para fortalecer y mejorar los controles de seguridad de la información.
28	Control organizacional	A.5.28	Recolección de evidencia	La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
29	Control organizacional	A.5.29	Seguridad de la información durante la interrupción	La organización debe planificar cómo mantener la seguridad de la información a un nivel apropiado durante la interrupción.
30	Control organizacional	A.5.30	Preparación de las TIC para la continuidad del negocio	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio.
31	Control organizacional	A.5.31	Requisitos legales, estatutarias, reglamentarias y contractuales	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.
32	Control organizacional	A.5.32	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
33	Control organizacional	A.5.33	Protección de registros	Los registros se protegerán contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.

#	Tipo de control	Nro.	Control	Descripción
34	Control organizacional	A.5.34	Privacidad y protección de Información Identificable de una Persona (PII)	PII es cualquier dato que se pueda utilizar para identificar a una persona, por ejemplo: licencia de conducir, información financiera, registros médicos, entre otro.
35	Control organizacional	A.5.35	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
36	Control organizacional	A.5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	El cumplimiento de la política de seguridad de la información de la organización, las reglas y los estándares específicos del tema se revisará periódicamente.
37	Control organizacional	A.5.37	Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.
38	Control de personas	A.6.1	Poner en pantalla	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
39	Control de personas	A.6.2	Términos y condiciones de empleo	Los acuerdos contractuales de trabajo deberán expresar el personal y responsabilidades de la organización para la seguridad de la información.
40	Control de personas	A.6.3	Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes recibirán concientización, educación y capacitación apropiadas sobre la seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral.

#	Tipo de control	Nro.	Control	Descripción
41	Control de personas	A.6.4	Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
42	Control de personas	A.6.5	Responsabilidades después de la terminación o cambio de empleo	Responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la finalización o el cambio de empleo se definirán, ejecutarán y comunicarán al personal pertinente y otras partes interesadas.
43	Control de personas	A.6.6	Confidencialidad o no divulgación de acuerdos	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deberán ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.
44	Control de personas	A.6.7	Trabajo remoto	Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
45	Control de personas	A.6.8	Reporte de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de canales de manera oportuna.
46	Control físico	A.7.1	Perímetros físicos de seguridad	Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.
47	Control físico	A.7.2	Entrada física	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.
48	Control físico	A.7.3	Protección de oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.
49	Control físico	A.7.4	Monitoreo de seguridad física	Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.
50	Control físico	A.7.5	Protección contra amenazas físicas y ambientales.	Protección contra amenazas físicas y ambientales, tales como desastres y otras amenazas físicas intencionales o no intencionales a la infraestructura.

#	Tipo de control	Nro.	Control	Descripción
51	Control físico	A.7.6	Trabajar en áreas seguras	Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.
52	Control físico	A.7.7	Escritorio y pantalla despejados	Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.
53	Control físico	A.7.8	Emplazamiento y protección de equipos	El equipo se colocará de forma segura y protegida.
54	Control físico	A.7.9	Seguridad de los activos fuera de las instalaciones	Se protegerán los activos fuera del sitio.
55	Control físico	A.7.10	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
56	Control físico	A.7.11	Utilidades de apoyo	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
57	Control físico	A.7.12	Seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.
58	Control físico	A.7.13	Mantenimiento de equipo	El equipo se mantendrá correctamente para garantizar la disponibilidad, la integridad confidencialidad de la información.
59	Control físico	A.7.14	Eliminación segura o reutilización de equipos	Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
60	Controles tecnológicos	A.8.1	Dispositivos de punto final de usuario	Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.
61	Controles tecnológicos	A.8.2	Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.
62	Controles tecnológicos	A.8.3	Restricción de acceso a la información	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.

#	Tipo de control	Nro.	Control	Descripción
63	Controles tecnológicos	A.8.4	Acceso al código fuente	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.
64	Controles tecnológicos	A.8.5	Autenticación segura	Se implementarán tecnologías y procedimientos de autenticación seguros basado en las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
65	Controles tecnológicos	A.8.6	Gestión de capacidad	El uso de los recursos se controlará y ajustará de acuerdo con las normas vigentes y requisitos de capacidad esperados.
66	Controles tecnológicos	A.8.7	Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.
67	Controles tecnológicos	A.8.8	Gestión de vulnerabilidades técnicas	Ninguna red informática, sistema, pieza de software o dispositivo es completamente seguro. La ejecución de una LAN o WAN moderna implica vulnerabilidades como parte del proceso, por lo que es esencial que las organizaciones acepten su presencia y se esfuercen por reducir los riesgos.
68	Controles tecnológicos	A.8.9	Gestión de la configuración	Las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, supervisado y revisado.
69	Controles tecnológicos	A.8.10	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.
70	Controles tecnológicos	A.8.11	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
71	Controles tecnológicos	A.8.12	Prevención de fuga de datos	Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
72	Controles tecnológicos	A.8.13	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán regularmente de acuerdo con la política específica del tema acordada en copia de seguridad.

ontinúa Tabla 5 en la siguiente página →

#	Tipo de control	Nro.	Control	Descripción
73	Controles tecnológicos	A.8.14	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se implementarán con redundancia suficiente para cumplir con los requisitos de disponibilidad.
74	Controles tecnológicos	A.8.15	Inicio sesión	Se producirán, almacenarán, protegerán y analizarán bitácoras que registren actividades, excepciones, fallas y otros eventos relevantes.
75	Controles tecnológicos	A.8.16	Actividades de seguimiento	Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se tomarán las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.
76	Controles tecnológicos	A.8.17	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización se sincronizarán con las fuentes de tiempo aprobadas.
77	Controles tecnológicos	A.8.18	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.
78	Controles tecnológicos	A.8.19	Instalación de software en sistemas operativos	Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
79	Controles tecnológicos	A.8.20	Seguridad en redes	Los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.
80	Controles tecnológicos	A.8.21	Seguridad de los servicios de red.	Mecanismos de seguridad, niveles de servicio deben ser identificados, implementados y monitoreados.
81	Controles tecnológicos	A.8.22	Segregación de redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
82	Controles tecnológicos	A.8.23	Filtrado web	El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.
83	Controles tecnológicos	A.8.24	Uso de criptografía	Reglas para el uso efectivo de la criptografía, incluida la clave criptográfica gestión, debe ser definida e implementada.
84	Controles tecnológicos	A.8.25	Ciclo de vida de desarrollo seguro	Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.
85	Controles tecnológicos	A.8.26	Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

#	Tipo de control	Nro.	Control	Descripción
86	Controles tecnológicos	A.8.27	Arquitectura segura del sistema y principios de ingeniería	Se deben establecer principios para la ingeniería de sistemas seguros, documentación, y debe ser mantenido y aplicado a cualquier desarrollo de sistema de información actividades.
87	Controles tecnológicos	A.8.28	Codificación segura	Los principios de codificación segura se aplicarán al desarrollo de software.
88	Controles tecnológicos	A.8.29	Pruebas de seguridad en desarrollo y aceptación	Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.
89	Controles tecnológicos	A.8.30	Desarrollo subcontratado	La organización debe dirigir, monitorear y revisar las actividades relacionadas al desarrollo de sistemas subcontratados.
90	Controles tecnológicos	A.8.31	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
91	Controles tecnológicos	A.8.32	Gestión del cambio	Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.
92	Controles tecnológicos	A.8.33	Información de prueba	La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.
93	Controles tecnológicos	A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de sistemas operativos se planificarán y acordarán entre la persona que ejecuta la prueba y la dirección correspondiente.

APÉNDICE 5. MATRIZ INTEGRAL METODOLÓGICA DE VARIABLES, TÉCNICAS E INSTRUMENTOS

Unidad de análisis **Segmentos de población**	**Muestra**	**Variables** ***(Qué se investiga)***	**Método** ***(Cómo)***	**Técnica** ***(A través de qué)***	**Instrumentos** ***(Con qué)***
Fuente de información primaria					
Unidad de análisis 1: personal interno de Aseguradora ABANK Total de personas: 39	**Total de muestra por personas de cada gerencia/dirección: 37** Dirección comercial (6) Dirección técnica (6) Dirección financiera administrativa (9) Gerencia de servicios post venta (6) Auditoría (1) Unidad de riesgos (1) Gerencia de cumplimiento (1) Gerencia de tecnología (4) Recursos humanos (1) Gerencia de proyectos estratégicos (1) Presidencia (1)	Grado de conformidad con respecto a requisitos de Calidad	Deductivo, análisis, síntesis, observación	Entrevista estructurada Observación	Lista de verificación
		Información documental existente	Deductivo, análisis, síntesis, observación	Revisión documental	Lista de verificación
	Total de muestra por personas de cada gerencia/dirección: 2 Seguridad de la información y continuidad del negocio (1) Gerencia de tecnología (1)	Grado de conformidad con respecto a requisitos de Seguridad de la información	Deductivo, análisis, síntesis	Entrevista estructurada Observación	Lista de verificación Guía de entrevista
Unidad de análisis 2: clientes o asegurados de la organización	**Total de muestra: 381 Asegurados**	Satisfacción de las necesidades y expectativas de los clientes	Deductivo, análisis, síntesis	Encuesta	Cuestionario
Fuentes de información secundaria					
N/A	N/A	*Aplica para todas las variables debido que la búsqueda y utilización de información bibliográfica es general para toda la investigación.	Análisis, Síntesis	Sistematización bibliográfica	Ficha de referencia bibliográfica

Fuente: Elaboración propia, a partir de Rojas Soriano, R. (2013). *Guía para realizar investigaciones sociales. 38*ª Edición. México D.F. México: Ed. Plaza y Valdés, S.A. p.202-203.

APÉNDICE 6. MATRIZ METODOLÓGICA DE CONSISTENCIA DE LA INVESTIGACIÓN

DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD NTS ISO 9001:2015 Y DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022 APLICABLE EN ASEGURADORA ABANK, S. A., SEGUROS DE PERSONAS					
FORMULACIÓN (PROBLEMA) SISTEMATIZACIÓN	**OBJETIVO GENERAL Y ESPECÍFICOS**	**HIPÓTESIS (SUPUESTOS)**	**OPERACIONALIZACIÓN DE VARIABLES**		**DISEÑO METODOLOGICO**
			VARIABLES	**MEDICIÓN (INDICADORES)**	
GENERAL			*Atributos que se miden o se argumentan, se utilizan para designar cualquier característica o cualidad de la unidad de observación.*	*Su operacionalización es un proceso de traslado de un nivel abstracto a un nivel empírico, observable, medible (cuantitativa o cualitativamente)*	*El diseño de investigación es el mapa operativo. Representa el punto donde se conectan las fases conceptuales del proceso con la recolección y el análisis de los datos.*
¿De qué manera se puede llevar a cabo la sistematización de los procesos para mejorar aspectos de calidad y seguridad de la información en Aseguradora ABANK?	*Diseñar un Sistema Integrado de Gestión de la Calidad ISO 9001:2015, y Seguridad de la Información ISO/IEC 27001:2022; aplicable en Aseguradora ABANK, S. A. Seguros de Personas.*	*El diseño e implementación de un Sistema Integrado de Gestión de la Calidad y Seguridad de la Información, basado en las normas ISO 9001:2015 e ISO/IEC 27001:2022, permitirá a Aseguradora ABANK mejorar la comunicación y el trabajo en equipo, aumentar el compromiso y liderazgo de gerentes y directores, optimizar las operaciones y servicios al cliente, y fortalecer la seguridad de la información, resultando en una mayor eficiencia operativa y mitigación de riesgos relacionados con la gestión de datos confidenciales.*			
Específicos					
¿En qué estado se encuentran los procesos de Aseguradora ABANK en relación con la calidad de sus servicios?	*Evaluar las condiciones actuales de Aseguradora ABANK en relación con aspectos de calidad, según ISO 9001:2015.*	*Las condiciones actuales de Aseguradora ABANK en aspectos de calidad, según ISO 9001:2015, están por debajo del 50% debido a problemas en la gestión de procesos, control de la información documentada, errores operacionales y deficiencias en liderazgo y compromiso.*	*Grado de conformidad con respecto a requisitos de Calidad*	*-Identificación del cumplimiento de la organización ante los requisitos de normativa ISO 9001:2015 (cualitativo)* *-(Requisitos cumplidos ante ISO 9001:2015/ Total de requisitos requeridos por ISO 9001:2015) *100 (cuantitativo)* *-Identificación de riesgos de la organización (cualitativo)*	• ***Tipo de investigación**: Aplicada* • ***Enfoque o ruta de la investigación:** Mixta* • ***Alcance o tipo de estudio:** Exploratorio y Descriptivo* • ***El método de investigación:** Observación/deductivo/análisis y síntesis* • ***Diseño metodológico:** no experimental* • ***Unidad de análisis y población:*** - *Unidad de análisis 1: personal de la empresa, 39 personas* - *Unidad de análisis 2: clientes o asegurados, 381 personas* • ***Determinación de población y muestra:*** - *Unidad de análisis 1: muestreo no probabilístico o dirigido* - *Unidad de análisis 2: muestreo probabilístico* • ***Fuentes de Información:** primarias y secundarias* • ***Técnicas de recolección de datos:** entrevista estructurada, observación, revisión documental, encuesta, sistematización bibliográfica.* • ***Instrumentos de recolección de datos:** Lista de verificación, guía de entrevista, cuestionario, ficha de referencia bibliográfica.* • ***Tabulación de datos y análisis:** tabulación, ordenamiento, procesamiento de información y análisis de resultados.*
¿De qué manera se identifican las necesidades y expectativas de los clientes de la organización?	*Identificar las necesidades y expectativas de los clientes de la organización conforme a ISO 9001:2015 e ISO IEC 27001:2022*	*Las necesidades y expectativas de los clientes de Aseguradora ABANK no se identifican y no se consideran en las estrategias de la organización, por lo cual se genera insatisfacción de estos.*	*Satisfacción de las necesidades y expectativas de los clientes*	*-Identificación de necesidades y expectativas de Clientes y partes interesadas (cualitativo)* *-(Número de clientes (asegurados) Muy satisfechos y satisfechos/Total de encuestados) *100 (cuantitativo)*	
¿Cuál es la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización?	*Identificar la gestión documental actualmente utilizada por Aseguradora ABANK para la gestión de sus documentos y registros, considerando las necesidades y requisitos específicos de la organización.*	*El nivel de cumplimiento de información documentada de la organización, con relación a los requisitos ISO 9001:2015 e ISO/IEC 27001:2022 es inferior a 40%.*	*Información documental existente*	*-Identificación de información documentada de la organización (cualitativo)* *-(Información documentada de la organización/ información documentada requerida por el SIG) * 100 (cuantitativo)* *-Identificación de los activos de información (cualitativo)*	
¿Cuáles son las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información?	*Analizar las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información, según ISO/IEC 27001:2022.*	*Las condiciones actuales de Aseguradora ABANK en relación con aspectos de seguridad de la información, según ISO/IEC 27001:2022 es inferior a 40%.*	*Grado de conformidad con respecto a requisitos de Seguridad de la información*	*-Identificación del cumplimiento de la organización ante los requisitos de normativa ISO/IEC 27001:2022 (Mixto)* *-Identificación de los activos de información (cualitativo)* *-Identificación de controles de seguridad de la información (cualitativo)* *-(Controles de seguridad de seguridad de la información cumplidos/ Total de controles de seguridad de la información según ISO/IEC 27001:2022) *100 (cuantitativo)*	

Fuente: Adaptado de Méndez Álvarez, C. (2006). *Metodología: Diseño y desarrollo del proceso de investigación con énfasis en Ciencias Empresariales.* 4ª. Ed. Editorial LIMUSA, S.A: de C.V. Grupo Noriega Editores. México. pág. 1

APÉNDICE 7. ANÁLISIS PESTEL

ANÁLISIS PESTEL			
CRITERIO	**FACTOR**	**DESARROLLO**	**TIPO**
Político	Polarización política	Genera incertidumbre política, por lo tanto, menos inversión para el país	Amenaza
	Creación de políticas que no favorecen al negocio	Menos margen de estrategias de negocio que beneficien a la aseguradora	Amenaza
Económico	Impacto del cambio de moneda (bitcoin)	El cambio de moneda de dólar a Bitcoin podría provocar un impacto negativo en la aseguradora pues esta moneda tiene variaciones de valor en el tiempo	Amenaza
	Variaciones en contribuciones tributarias	Si se llegase a tener cambios en el IVA, PIB, u otros aspectos en contribuciones tributarias va existir un impacto en la aseguradora.	Amenaza
Social	Delincuencia	Mayor cantidad de personas contratando seguros de vida, tanto clientes individuales como organizaciones	Oportunidad
	Responsabilidad social corporativa	Tendencias de responsabilidad social para destacar como empresas comprometidas con la sociedad	Oportunidad
Tecnológico	Nuevas tecnologías en el mercado	Nuevas ofertas de software para aplicación a seguros	Oportunidad
	Competencia compitiendo por desarrollo de nuevas tecnologías	Todas las aseguradoras en el país están compitiendo por llegar al Cliente por medio de software más sofisticado	Amenaza
	Riesgos de seguridad de la información	Incremento en casos de ataques cibernéticos a instituciones en el mercado financiero.	Amenaza
Ambiental	Leyes y reglamentos para cuido de medio ambiente	Mayor auge al cumplimiento de normativas ambientales. En el caso de la aseguradora relacionado a la papelería, entre otros.	Oportunidad
	Tendencias de reciclaje	Nuevas tendencias para reciclar materiales	Oportunidad
Legal	Cambios en la ley de seguros	Leyes de seguros son vitales para la estructuración de contratos de pólizas, cambios en ellas podrían afectar negativamente.	Amenaza
	Regulación estricta por parte del gobierno de entes reguladores de seguros	Sería una amenaza para el desarrollo del negocio, dado que afectaría estrategias de negocio en contratos de pólizas	Amenaza

Fuente: elaboración propia

APÉNDICE 8. MATRIZ DE PARTES INTERESADAS

MATRIZ DE PARTES INTERESADAS									
No.	**PARTES INTERESADAS**		**REQUISITOS**		**IMPACTO O INFLUENCIA (CAPACIDAD DE AFECTAR A LA INSTITUCIÓN)**				**Mecanismo de Seguimiento y Revisión de necesidades y expectativas**
	GRUPOS	**SUB GRUPOS**	**NECESIDAD**	**EXPECTATIVA**	**ESTRATEGICO**	**SERVICIO**	**REGULACIÓN**	**PROCESO ORGANIZACIONAL**	
1	Clientes	Persona natural	-Obtener un seguro de vida y/o gastos médicos.	-Un seguro innovador con procesos eficientes. -Servicio al cliente adecuado -Seguridad de la información.	X	X		X	-Encuesta de satisfacción al cliente.
		Persona jurídica (consumidor)	-Obtener un seguro de vida y/o gastos médicos.	-Un seguro innovador con procesos eficientes. -Servicio al cliente adecuado -Seguimiento posventa -Seguridad de la información.	X	X		X	-Encuesta de satisfacción al cliente.
2	Proveedores	Servicio de utilería	-Requerimiento de utilería.	-Recepción de pagos a tiempo y de acuerdo con lo estipulado.		X		X	-Evaluación de proveedores
		Servicios de tecnología (servidores, hardware, software)	-Venta de servicios	-Recepción de pagos a tiempo y de acuerdo con lo estipulado.		X			-Evaluación de proveedores

MATRIZ DE PARTES INTERESADAS									
No.	PARTES INTERESADAS		REQUISITOS		IMPACTO O INFLUENCIA (CAPACIDAD DE AFECTAR A LA INSTITUCIÓN)				Mecanismo de Seguimiento y Revisión de necesidades y expectativas
	GRUPOS	SUB GRUPOS	NECESIDAD	EXPECTATIVA	ESTRATEGICO	SERVICIO	REGULACIÓN	PROCESO ORGANIZACIONAL	
		Intermediarios	-Colocación de seguros.	-Recepción de pagos a tiempo y de acuerdo a lo estipulado. -Servicio al cliente adecuado -Seguimiento posventa		X		X	-Evaluación de proveedores
		Servicio de limpieza	-Requerimiento de mantener un ambiente limpio y ordenado.	-Recepción de pagos a tiempo y de acuerdo a lo estipulado.		X		X	-Evaluación de proveedores
3	Trabajadores	Operativos	-Colocación de seguros	-Buenos productos para ofertar -Sistemas informáticos adecuados para atención de las partes interesadas.		X		X	-Encuesta de satisfacción al cliente. -Clima organizacional.
		Administrativos	-Apoyar a todas las áreas funcionales del negocio.	-Que todas las áreas funcionales cumplan con los parámetros de la empresa.		X		X	-Clima organizacional.
4	Alta dirección	Gerencia general	-Rentabilidad operativa y financiera	-Cumplimiento de objetivos estratégicos para lograr la rentabilidad	X				Revisión periódica de indicador
		Presidencia	- Rentabilidad	-Cumplimiento de objetivos estratégicos para lograr la rentabilidad	X				Revisión periódica de indicador

MATRIZ DE PARTES INTERESADAS									
No.	**PARTES INTERESADAS**		**REQUISITOS**		**IMPACTO O INFLUENCIA (CAPACIDAD DE AFECTAR A LA INSTITUCIÓN)**				**Mecanismo de Seguimiento y Revisión de necesidades y expectativas**
	GRUPOS	**SUB GRUPOS**	**NECESIDAD**	**EXPECTATIVA**	**ESTRATEGICO**	**SERVICIO**	**REGULACIÓN**	**PROCESO ORGANIZACIONAL**	
5	Entidades de gobierno	Superintendencia de sistema financiero	-Cumplimiento con requisitos de lavado de dinero y financiamiento al terrorismo. -Cumplimiento a requerimientos legales.	- Acceso a la información. - Transparencia. -Disponibilidad de tiempo.			X		Inspección
		Ministerio de trabajo	-Verificación de la situación actual del trabajador	-Cumplimiento con los derechos del trabajador			X		Inspección

Fuente: elaboración propia

APÉNDICE 9. MATRIZ DE RIESGOS

					Riesgo Inicial						Riesgo Residual				
Ubicación del Riesgo		Estrategia	Riesgo	Tipo (O= Oportunidad A= Amenaza)	Probabilidad	Consecuencia/ Impacto	Riesgo (Cuantificado)	Evaluación del Riesgo C1 (Otros aspectos de Calidad)		Controles	Probabilidad	Consecuencia/ Impacto	Riesgo (Cuantificado)	Evaluación del Riesgo C1 (Otros aspectos de Calidad)	
Tipo de contexto	Factor					C1	C1	Oportunidad	Amenaza			C1	C1	Oportunidad	Amenaza
Amenaza	Alta competencia en el mercado de seguros	Desarrollar venta de seguros por medio del canal de bancaseguros, con el objetivo de aprovechar al máximo los recursos del banco	No entendimiento de estrategias de negocio entre banco y aseguradora	A	0.3	0.8	0.24	N/A	Alto	Programa de reuniones entre la alta dirección de ambas entidades financieras	0.1	0.4	0.04	N/A	Bajo
Fortaleza	Conglomerado financiero		Falta de apoyo en proyecto por parte de alguna parte interesadas involucrada	A	0.5	0.8	0.4	N/A	Alto	Identificación de involucrados comprometidos en proyecto y rendición de cuentas	0.3	0.4	0.12	N/A	Medio
Oportunidad	Nuevas tecnologías en el mercado	Desarrollar tecnologías de software que fortalezcan los servicios de cara a los Clientes	Gran oferta de nuevas tecnologias orientadas a seguros	O	0.9	0.2	0.18	Alto	N/A	Implementar nuevas tecnologías	0.5	0.1	0.05	Medio	N/A
Fortaleza	Inversión en desarrollo nacional		Incumplimiento en tiempos de desarrollo estipulados en proyecto	A	0.5	0.4	0.2	N/A	Alto	Selección de integrantes PM (proyect managers), para controlar y monitorer desarrollo de proyecto	0.1	0.2	0.02	N/A	Bajo
Amenaza	Alta competencia en el mercado de seguros	Crear procedimientos para la estandarización de procesos que permitan brindar servicios de Calidad y generen ventaja competitiva en el mercado	No comprensión del objetivo del proyecto de estandarización de procesos	A	0.5	0.4	0.2	N/A	Alto	Plan de concientización de proyecto y su respectivo seguimiento	0.1	0.2	0.02	N/A	Bajo
Debilidad	Falta de estandarización de procesos y documentación		Definición del alcance del proyecto no adecuada	A	0.5	0.4	0.2	N/A	Alto	Definición de proyecto en conjunto con la alta dirección	0.3	0.2	0.06	N/A	Medio
Debilidad	Entrega de productos de seguro a los clientes de forma tardía o con inconsistencias	Estandarización de procesos y aplicación de controles de calidad	Insatisfacción del cliente	A	0.5	0.4	0.2	N/A	Alto	Proyecto de estandarización de procesos en la cadena de valor del negocio	0.3	0.4	0.12	N/A	Medio

					Riesgo Inicial						Riesgo Residual				
Ubicación del Riesgo		Estrategia	Riesgo	Tipo (O= Oportunidad A= Amenaza)	Probabilidad	Consecuencia/ Impacto	Riesgo (Cuantificado)	Evaluación del Riesgo C1 (Otros aspectos de Calidad)		Controles	Probabilidad	Consecuencia/ Impacto	Riesgo (Cuantificado)	Evaluación del Riesgo C1 (Otros aspectos de Calidad)	
Tipo de contexto	Factor					C1	C1	Oportunidad	Amenaza			C1	C1	Oportunidad	Amenaza
Oportunidad	Nuevas tecnologías en el mercado	Incrementar la cantidad de productos para diferentes ramos de seguros a ofertar a los Clientes	Dificultado para que personal de Aseguradora se adapte a nuevos productos de seguros	O	0.7	0.4	0.28	Alto	N/A	Plan de concientización de proyecto y su respectivo seguimiento	0.3	0.2	0.06	Medio	N/A
Debilidad	Poca variedad de seguros		No aprobación de nuevos productos por parte de la SSF	A	0.5	0.4	0.2	N/A	Alto	Involucramiento de profesionales con experiencia en desarrollo de proyectos para nuevos productos con la SSF	0.1	0.2	0.02	N/A	Bajo
Debilidad	No conocimiento de las necesidades y expectativas de las partes interesadas	Estrategias de acercamiento y entendimiento de las necesidades y expectativas de las partes interesadas	Insatisfacción del cliente	A	0.5	0.8	0.4	N/A	Alto	Encuesta de satisfacción de cliente	0.3	0.4	0.12	N/A	Medio
Amenaza	Debilidades en aspectos de seguridad de la información	Aplicar controles de seguridad de la información	Robo, secuestro, daño a los activos de información de la aseguradora y sus partes interesadas	A	0.5	0.4	0.2	N/A	Alto	Controles de seguridad de ISO/IEC 27001:2022, Anexo A	0.3	0.2	0.06	N/A	Medio

Fuente: elaboración propia

APÉNDICE 10. MANUAL DE PROCEDIMIENTOS

MANUAL DE PROCEDIMIENTOS

Septiembre 2024

Presentado por:

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

MUÑOZ SOSA, NORA NATHALY

RODAS LAÍNEZ, GUSTAVO MANUEL

Para:

Aseguradora ABANK

5. INTRODUCCIÓN

En un mundo donde la seguridad de la información y la calidad del servicio son elementos fundamentales para el éxito de cualquier organización, Aseguradora ABANK se enorgullece de presentar este Manual de Procedimientos que abarca dos pilares cruciales en nuestra operación: el Sistema de Gestión de Calidad conforme a la norma ISO 9001:2015 y el Sistema de Gestión de Seguridad de la Información conforme a la norma ISO 27001:2022.

En Aseguradora ABANK, nuestro compromiso con la excelencia y la protección de los activos de nuestros clientes y colaboradores es primordial. La implementación y certificación de estos sistemas de gestión son un testimonio de nuestra determinación para garantizar la calidad de nuestros servicios y salvar la confidencialidad, integridad y disponibilidad de la información que manejamos.

Este manual constituye una guía esencial para todos los miembros de nuestra organización, estableciendo los procedimientos y directrices que aseguran que nuestras operaciones cumplan con los estándares internacionales más exigentes en términos de calidad y seguridad de la información. Además, refleja nuestro compromiso constante con la mejora continua, la innovación y la satisfacción de nuestros clientes.

6. OBJETIVO

El objetivo principal de este manual es proporcionar una guía integral y detallada para todos los miembros de Aseguradora ABANK, con el fin de:

- Facilitar la comprensión y la implementación efectiva de los procedimientos y directrices establecidos en el marco de los sistemas de gestión ISO 9001:2015 e ISO 27001:2022.
- Garantizar la consistencia en la prestación de servicios de alta calidad y la protección de la información en todas las áreas de nuestra organización.
- Impulsar la mejora continua de nuestros procesos y la satisfacción del cliente, asegurando la eficiencia y la eficacia en todas las operaciones.
- Reforzar el compromiso de Aseguradora ABANK con la excelencia en la gestión de calidad y la seguridad de la información, cumpliendo con los estándares internacionales más rigurosos.
- Promover la conciencia y la responsabilidad de todos los colaboradores en lo que respetan la calidad y la seguridad de la información, fomentando una cultura organizativa de compromiso y mejora constante.

7. ALCANCE DEL MANUAL

El manual de procedimientos aplica para la sede central de Aseguradora ABANK, ubicada en: Boulevard Merliot, Urbanización Jardines de la Hacienda, Lote 5 y 6, Zona Comercial Z.C 5, Antiguo Cuscatlán. La Libertad, El Salvador, C.A. Aplica para los procedimientos que se detallan a continuación:

Código	Descripción
SIG-6-02-PRO	Procedimiento de tratamiento de riesgos de calidad
SIG-6-03 PRO	Procedimiento de tratamiento de riesgos de seguridad de la información
SIG-7-01-PRO	Procedimiento de reclutamiento y selección
SIG-7-02-PRO	Procedimiento para la gestión del desarrollo del trabajador
SIG-7-03-PRO	Procedimiento de información documentada

Código	Descripción
SIG-8-04-PRO	Procedimiento de quejas/ canales de comunicación
SIG-8-05-PRO	Procedimiento de diseño y desarrollo de productos/servicios
SIG-8-06-PRO	Procedimiento para la evaluación de proveedores
SIG-8-07-PRO	Procedimientos de servicios post venta
SIG-9-08-PRO	Procedimiento de control y monitoreo de indicadores de desempeño del SIG
SIG-9-09-PRO	Procedimiento para evaluación de la satisfacción del Cliente
SIG-9-10-PRO	Procedimiento de auditoría interna
SIG-9-11-PRO	Procedimiento de la revisión por la dirección
SIG-10-12-PRO	Procedimiento de NC y acciones correctivas
SIG-10-13-PRO	Procedimiento para gestión de controles de seguridad de la información
SIG-1-1-PRO	Comercialización de seguros
SIG-1-2-PRO	Suscripción y emisión de pólizas de seguro
SIG-1-3-PRO	Atención de reclamos de seguros
SIG-1-4-PRO	Gestión de la cobranza de seguros *
SIG-1-5-PRO	Atención de beneficios de seguros *
SIG-1-6-PRO	Gestión contable *
SIG-1-7-PRO	Gestión del reaseguro *
SIG-1-8-PRO	Gestión del talento humano *
SIG-1-9-PRO	Gestión administrativa *
SIG-1-10-PRO	Control interno de las operaciones *
SIG-1-11-PRO	Administración de la atención al cliente *
SIG-1-12-PRO	Gestión tecnológica y soporte técnico *
SIG-1-13-PRO	Riesgos y seguridad de la información *
SIG-1-14-PRO	Tratamiento de la continuidad del negocio *
SIG-1-15-PRO	Gestión estratégica y planificación *
***Documentos no incluidos en manual debido a investigación se orienta en específico a los procedimientos sugeridos por las normativas ISO en cuestión; sin embargo se han adicionado algunos procedimientos clave del negocio.**	

Aseguradora ABANK	**PROCEDIMIENTO DE TRATAMIENTO DE RIESGOS DE CALIDAD**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	17/10/2023	
		CÓDIGO:	**SIG-6-02-PRO**	

PROCESO:	Gestión de Calidad
LÍDER DEL PROCESO:	Coordinador de Gestión de Calidad
OBJETIVO:	El objetivo de este procedimiento es establecer un proceso estructurado para la identificación, evaluación, tratamiento y seguimiento de los riesgos de calidad en los procesos de la organización.
ALCANCE:	Aplica para el análisis de riesgos y la correspondiente gestión de evaluación de la continuidad del negocio en caso de que un riesgo se active, a partir de la metodología BIA (Business Impact Analysis).
DOCUMENTO SOPORTE RELACIONADO:	Matriz de riesgos (SIG-6-01-MA)

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
1	*Evaluación inicial de riesgos*	Realizar una revisión exhaustiva de todos los productos y procesos relacionados con seguros, identificando posibles riesgos de calidad, desde la emisión de pólizas hasta la atención al cliente.	Coordinador de Gestión de Calidad
2	*Clasificación de Riesgos*	Clasificar los riesgos según su probabilidad de ocurrencia, impacto, nivel de riesgo	Coordinador de Gestión de Calidad
3	*Tratamiento de Riesgos*	Definir estrategias específicas para el tratamiento de cada riesgo identificado. Estas estrategias pueden incluir medidas de prevención, mitigación, transferencia o aceptación.	Coordinador de Gestión de Calidad

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
4	*Desarrollo de Planes de Acción*	Elaborar planes de acción detallados para abordar los riesgos priorizados, que incluyan asignación de responsabilidades, plazos de ejecución, recursos necesarios y métricas de seguimiento.	Coordinador de Gestión de Calidad
5	*Ejecución de Acciones*	Poner en marcha las acciones definidas en los planos de acción, asegurando que se apliquen de manera efectiva en los procesos y productos de seguros.	Coordinador de Gestión de Calidad
6	*Monitoreo Continuo*	Realizar un seguimiento continuo de los riesgos tratados, revisando los indicadores y métricas establecidas en los planos de acción. Evaluar la efectividad de las medidas implementadas.	Coordinador de Gestión de Calidad
	Fin del Procedimiento		

Proporcionó información:	Gerardo Ramos (Coordinador de Gestión de Calidad)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-6-03 PRO**	

PROCESO:	Unidad de riesgos, seguridad de la información y continuidad del negocio
LÍDER DEL PROCESO:	Coordinador de la Seguridad de la información y continuidad del negocio
OBJETIVO:	Garantizar la integridad, confidencialidad y disponibilidad de los datos médicos y financieros de los asegurados, reduciendo riesgos y asegurando la continuidad de los servicios médicos.
ALCANCE:	Incluye la gestión de riesgos de seguridad de la información para datos de clientes, procesos de facturación y sistemas informáticos, y la promoción de la cultura de seguridad en toda la organización.
DOCUMENTO SOPORTE RELACIONADO:	Matriz de riesgos (SIG-6-01-MA)

No.	ACTIVIDAD	CÓMO SE HACE	QUIÉN LO HACE
1	*Identificación de Activos y Evaluación de Riesgos*	Realizar un inventario completo de todos los activos de información, incluyendo datos de pacientes, sistemas de gestión de seguros médicos, servidores, registros financieros y sistemas de información.	Coordinador de la Seguridad de la información y continuidad del negocio
2	*Clasificación de Activo*	Clasificar los activos en función de su importancia y sensibilidad, asignando etiquetas de confidencialidad, integridad y disponibilidad.	Coordinador de la Seguridad de la información y continuidad del negocio
3	*Evaluación de Amenazas*	Identificar y evaluar amenazas, como ataques cibernéticos, errores humanos, desastres naturales y pérdida de datos.	Coordinador de la Seguridad de la información y continuidad del negocio

No.	ACTIVIDAD	CÓMO SE HACE	QUIÉN LO HACE
4	*Evaluación de Vulnerabilidades*	Realizar evaluaciones de seguridad en sistemas y procesos para identificar vulnerabilidades, como falta de parches, contraseñas débiles o configuraciones inseguras	Coordinador de la Seguridad de la información y continuidad del negocio
5	*Evaluación de Impacto*	Evaluar el impacto potencial de un incidente de seguridad en términos de pérdida de datos, interrupción de servicios y daño a la reputación.	Coordinador de la Seguridad de la información y continuidad del negocio
6	*Evaluación de Riesgos*	Calcular el riesgo para cada activo mediante una fórmula que combina probabilidad e impacto.	Coordinador de la Seguridad de la información y continuidad del negocio
7	*Selección de Medidas de Tratamiento*	Desarrollar un plan de tratamiento de riesgos que incluye medidas como la implementación de sistemas de seguridad, adquisición de seguros y la definición de políticas de seguridad.	Coordinador de la Seguridad de la información y continuidad del negocio
8	*Planificación e Implementación*	Desarrollar un plan detallado para la implementación de las medidas de tratamiento de riesgos, asignar responsabilidades y recursos.	Coordinador de la Seguridad de la información y continuidad del negocio
	Fin del Procedimiento		

Proporcionó información:	Ricardo Ramos (Encargado de seguridad de la información y continuidad del negocio)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE RECLUTAMIENTO Y SELECCIÓN**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-7-01-PRO**	

PROCESO:	Recursos Humanos
LÍDER DEL PROCESO:	Coordinador de Recursos Humanos
OBJETIVO:	Contratar candidatos calificados para cubrir vacantes en la aseguradora, alineando sus habilidades y valores con las necesidades de la organización.
ALCANCE:	Desde la planificación inicial hasta la integración, a incluir la selección y contratación de empleados aptos y su orientación en la cultura y procesos de la empresa.
DOCUMENTO SOPORTE RELACIONADO:	Plan de reclutamiento y selección, perfil de puestos, CV de candidatos.

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Planificación del proceso*	Identificar las necesidades de personal y las vacantes a cubrir.	Coordinador de Recursos Humanos
2	*Desarrollo de Descripciones de Puestos y Perfiles*	Crear descripciones de puestos y perfiles de candidatos que detallen las habilidades, competencias y requisitos necesarios.	Coordinador de Recursos Humanos
3	*Publicación de Ofertas de Trabajo*	Publicar las ofertas de trabajo en plataformas de reclutamiento, sitio web de la empresa y otros canales relevantes.	Coordinador de Recursos Humanos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
4	*Recepción de Solicitudes y Currículums*	Recopilar las solicitudes y currículums de los candidatos.	Coordinador de Recursos Humanos
5	*Revisión de Solicitudes y Preselección*	Evaluar las solicitudes y currículums para preseleccionar a los candidatos que cumplen con los requisitos iniciales.	Coordinador de Recursos Humanos
6	*Entrevistas, evaluación y pruebas*	Realizar entrevistas iniciales para evaluar las habilidades y competencias de los candidatos. Aplicar pruebas o evaluaciones específicas según las necesidades del puesto	Coordinador de Recursos Humanos Encargado o líder del proceso
7	*Oferta de empleo y negociación*	Seleccionar al candidato más adecuado para la vacante. Realizar la oferta de empleo y negociar términos y condiciones con el candidato seleccionado.	Coordinador de Recursos Humanos
	Fin del Procedimiento		

Proporcionó información:	Rosalia Pérez (Coordinadora de Recursos Humanos)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO PARA LA GESTIÓN DEL DESARROLLO DEL TRABAJADOR**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-7-02-PRO**	

PROCESO:	Recursos Humanos
LÍDER DEL PROCESO:	Coordinador de Recursos Humanos
OBJETIVO:	El objetivo es mejorar el desempeño y el crecimiento de los empleados al alinear sus habilidades con los objetivos estratégicos, fomentando un ambiente de trabajo motivador y productivo.
ALCANCE:	Incluye la identificación de necesidades de desarrollo, planes personalizados, programas de formación, seguimiento del progreso y promoción de una cultura de aprendizaje en toda la organización. Se integra como parte central de la gestión de recursos humanos.
DOCUMENTO SOPORTE RELACIONADO:	Plan de desarrollo del personal

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Evaluación de Necesidades de Desarrollo*	Identificar las necesidades de desarrollo de los empleados, ya sea mediante evaluaciones de desempeño, retroalimentación o identificación de brechas de habilidades.	Coordinador de Recursos Humanos
2	*Establecimiento de Objetivos de Desarrollo*	Definir objetivos de desarrollo individuales y planes de acción para los empleados.	Coordinador de Recursos Humanos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
3	*Identificación de Recursos de Desarrollo*	Determinar los recursos necesarios, como cursos, mentoría, formación en el trabajo, conferencias, para lograr los objetivos de desarrollo.	Coordinador de Recursos Humanos
4	*Implementación de Programas de Desarrollo*	Facilitar la participación de los empleados en programas de desarrollo, proporcionando acceso a recursos y oportunidades de formación.	Coordinador de Recursos Humanos
5	*Seguimiento y Evaluación del Progreso*	Realizar seguimiento continuo del progreso de desarrollo de los empleados, revisar planos y ajustarlos según sea necesario.	Coordinador de Recursos Humanos
6	*Promoción de una Cultura de Aprendizaje*	Fomentar una cultura de aprendizaje continuo en toda la organización mediante la promoción de oportunidades de desarrollo y el reconocimiento de los logros de desarrollo.	Coordinador de Recursos Humanos
7	*Evaluación del Impacto*	Evaluar el impacto de las actividades de desarrollo en el desempeño y la satisfacción de los empleados	Coordinador de Recursos Humanos
	Fin del Procedimiento		

Proporcionó información:	Rosalia Pérez (Coordinadora de Recursos Humanos)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	PROCEDIMIENTO DE INFORMACIÓN DOCUMENTADA	VERSIÓN	FECHA	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	SIG-7-03-PRO	

PROCESO:	Sistema integrado de gestión
LÍDER DEL PROCESO:	Gerente del SIG
OBJETIVO:	Establecer el procedimiento a seguir para el control de la información documentada con su respectiva evidencia de conformidad en base a los requisitos de la norma ISO 9001:2015 e ISO 27001:2022
ALCANCE:	Este procedimiento aplica para toda la información que deba documentarse en el Sistema Integrado Calidad y de Seguridad de la Información
DOCUMENTO SOPORTE RELACIONADO:	Repositorio de información (Sharepoint, archivo central)

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Elaborar información documentada*	Los líderes de procesos toman la iniciativa para la actualización, creación o eliminación de información documentada. A partir de plantillas de procesos, registros, políticas y demás tipos de información documentada según los principios de la Gestión por procesos	Coordinador del Sistema Integrado de Gestión
2	*Analizar información documentada*	Las coordinaciones del área correspondiente (seguridad ocupacional), recibe, analiza y verifica que la información documentada cumpla con los requisitos aplicables de los documentos de referencia y la normatividad vigente.	Coordinador del Sistema Integrado de Gestión
3	*Aprobar información documentada*	Los líderes de proceso y el coordinador del Sistema Integrado validan información documentada ¿Aprueban? SI: Continuar con actividad 4 NO: Regresar a la actividad 2	Coordinador del Sistema Integrado de Gestión

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
4	*Codificar información documentada*	Se procede a codificar información para registrar en inventario de información documentada del Sistema Integrado de Gestión	Coordinador del Sistema Integrado de Gestión
5	*Almacenar información documentada*	La información documentada se debe almacenar y preservar en condiciones adecuadas que garanticen su integridad, legibilidad, pérdida de confidencialidad o uso inadecuado. Por tal razón toda información documentada se almacena en un servidor en la nube (onedrive), para el cual se debe acceder por medio de usuario y contraseña.	Coordinador del Sistema Integrado de Gestión
6	*Difundir temática de información documentada*	El coordinador del Sistema Integrado de Gestión compartirá los documentos a las áreas o a las personas pertinentes relacionadas con la existencia y/o uso del documento.	Coordinador del Sistema Integrado de Gestión
	Fin del Procedimiento		

Proporcionó información:	Juan Ramírez (Coordinadora del Sistema Integrado de Gestión)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE QUEJAS/ CANALES DE COMUNICACIÓN**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-8-04-PRO**	

PROCESO:	Servicio Post Venta
LÍDER DEL PROCESO:	Gerente de Servicio Post Venta
OBJETIVO:	Realizar las gestiones de atención, análisis y resolución a quejas de Clientes y demás partes interesadas vinculadas a la comercialización de seguros por parte de Aseguradora ABANK.
ALCANCE:	Aplica para la gestión de quejas por parte de Clientes y las diferentes partes interesadas que se vinculan a la comercialización de seguros en Aseguradora ABANK.
DOCUMENTO SOPORTE RELACIONADO:	Matriz de quejas y reclamos, reporte mensual de queja y reclamos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Notificar queja a la aseguradora*	Los Clientes y demás partes interesadas (proveedores, intermediarios, entre otros) envían sus quejas a través de diferentes mecanismos con los que cuenta la aseguradora, por ejemplo: - Número telefónico de atención al Cliente - Correo electrónico de atención al Cliente - Redes sociales - Página WEB* - Personalmente en las instalaciones de la sede central de ABANK o sus comercializadores - A través de empleados (Gerentes comerciales, Oficial de reclamos, entro otros.) ¿Queja se comunicó por medio de Servicio al Cliente? SI: Continuar con actividad 3 (Atención al Cliente SAC) NO: Continuar con actividad 2 (Redes sociales, página WEB, teléfono, Gerentes comerciales, entre otros) *Nota: en la página WEB se encuentra alojado el enlace para presentar quejas o inconformidades, se encuentra en la sección "Atención al Cliente e Inconformidades"	Cliente

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
2	*Recibir queja y solicitar completar formulario online*	El personal de la dirección comercial u otra área funcional de Aseguradora ABANK que reciba una queja por parte de un Cliente o parte interesada, escucha dicha queja y recomienda amablemente el llenar un formulario de quejas, por lo cual se brinda un enlace o muestra un código QR para vincularse al formulario electrónico "formulario de quejas". El formulario de quejas posee los siguientes datos: - Origen de queja: Asegurado (o miembros de póliza), Intermediario, proveedor, contratista, otro. - Agencia o sucursal, medio donde se interpuso denuncia - Tipo de persona (natural o jurídica) - Número de póliza de seguro (aplica para asegurados) - Sexo de la persona (cuando es persona natural) - Nacionalidad (cuando es persona natural) - Descripción de la queja. - Correo electrónico (usuario que emitió queja) - Número telefónico (usuario que emitió queja) Nota: en los casos que el Cliente no tenga las facultades o le es complejo llenar el formulario, se le apoya para completar dicho registro, se puede citar a las instalaciones de Aseguradora ABANK o guiarle telefónicamente para apoyarle a completar dicha información; en los casos de Clientes (asegurados) un colaborador de la Dirección comercial, podría visitar al Asegurado.	Personal
3	*Recibir quejas, monitorear base de datos y analizar caso*	El oficial de Servicio al Cliente SAC, debe estar monitoreando el sistema de quejas en la cual se van alojando todas las quejas de Clientes y partes interesadas, de forma automática, para ello debe monitorear durante el día todas aquellas alertas de quejas nuevas registradas que recibe al Correo electrónico de SAC, cada vez que algún usuario ingresa una queja. De igual forma debe ingresar a la plataforma al menos tres veces al día (mañana, medio día y al finalizar la tarde). A partir de esta sección se visualiza una matriz de todas las quejas impuestas por Clientes y las diferentes Partes interesadas de la aseguradora. Para iniciar el análisis da clic en el icono en forma de calendario por cada queja, y se dirige a la pantalla "Seguimiento de inconformidades", en la cual se debe analizar el caso y colocar la siguiente información (como Oficial de Servicio al Cliente SAC): - Área vinculada a cada caso - Motivo (Según clasificaciones de la aseguradora y para casos de Asegurados usar las categorías que exige la normativa (NCM-03 Normas de transparencia y divulgación en Seguros) - Estado: por default el sistema muestra el estado "Recibido", - Nivel de riesgo: Alto*, Moderado Para finalizar análisis clic en botón "Guardar".	Oficial de Servicio al Cliente SAC

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		*Nota, se considera alto cuando existe una posible desvinculación del Cliente o parte interesada con la aseguradora, o existe el riesgo de sanciones por incumplimiento a normativas, leyes u otro requisito legal.	
4	*Remitir casos al área funcional implicada*	Posteriormente, luego de haber analizado el caso, se debe notificar a la persona y área que deben resolver caso. Por lo que cambia el estado de la columna "En proceso", luego coloca el nombre de la persona responsable de solventar caso. Para notificar a la persona y área correspondiente se debe enviar un correo electrónico solicitando apoyo para solventar caso. En el correo se adjunta lo que el usuario presentó en su queja, es decir lo que plasmo en formulario correspondiente y que en la aseguradora se registró, de forma automática y se le asignó un código de identificación, en la base de datos del Sistema de Quejas. Nota: es importante copiar al líder del proceso vinculado a cada caso. ¿Existen dudas sobre la queja? SI: Continuar con actividad 6 NO: Continuar con actividad 7	Oficial de Servicio al Cliente SAC
5	*Contactar a Cliente o parte interesada para solventar duda*	Cuando sea necesaria información adicional, el Oficial de Servicio al Cliente SAC, se contacta con el Cliente o parte interesada para aclarar dudas. Regresar a la actividad 5	Oficial de Servicio al Cliente SAC
6	*Dar solución a queja de Cliente (acción correctiva)*	El área vinculada al caso debe resolver la queja del Cliente o parte interesadas. Luego de haber realizado una acción correctiva, debe contactar al Oficial de Servicio al Cliente, comunicando que caso ya fue resuelto, dicha comunicación se realiza por medio de correo electrónico, tomando como base el primer correo que recibió por parte de SAC. En el correo se debe exponer: - Código de queja - Acción correctiva implementada	Responsable de proceso
7	*Recibir correo y contactar al Cliente o parte interesada para seguimiento*	El Oficial de Servicio al Cliente SAC se pone en contacto con el Cliente o Parte interesada e indaga, amablemente, en la resolución del caso que exponía. Cada seguimiento que se da se debe registrar en el Sistema de quejas, en la pestaña "Seguimiento" ¿Cliente satisfecho?	Oficial de Servicio al Cliente SAC

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		SI: Continuar con actividad 10 NO: Continuar con actividad 9	
8	*Contactar al líder del área para preparación de plan de acción*	En los casos que no se haya logrado solventar problemática por parte de las áreas responsables se les comunica nuevamente que caso no ha sido cerrado y que es importante darle seguimiento al tema para cerrarlo definitivamente. En este correo ya no solo irá dirigido al responsable de proceso o persona que ejecuta actividades en el área relacionada a cada caso, sino que también se le enviará al líder de proceso de dicha área (ya no solo se copiará como la primera vez), se debe copiar al área de Gestión de Calidad y si tiene relación con asegurados a la Dirección comercial. Regresar a la actividad 7	Oficial de Servicio al Cliente SAC
9	*Actualizar seguimiento en sistema de quejas*	En los casos que ya se haya resuelto la queja de los Clientes y/o Partes interesadas, el Oficial de Servicio al Cliente SAC debe regresar al Sistema de quejas y en la pestaña "Cierre" debe colocar el estado de resolución: - Favorable - Desfavorable - Desistido por el Cliente Al dar clic en botón "Guardar", cambia el estado del caso a "Cerrado". Se coloca el nombre de la persona que resolvió y se agrega los comentarios de cierre en los que se basó para darle como finalizado (por ejemplos los comentarios que compartió el área involucrada en la resolución del caso).	Líder de proceso
10	*Generar reporte mensual de quejas (No conformidades)*	Los primeros 5 días de cada mes, se envía un reporte a las Superintendencia del Sistema Financiero (SSF) el cual es generado en el sistema de quejas. En la estructuración del reporte mensual dos documentos, uno para el envío al ente regulador (SSF) y otro de análisis interno en la aseguradora. Diferencia entre ambos: 1. Reporte para SSF: Contiene solo casos de quejas de Clientes (asegurados) 2. Reporte interno (COMPLETO): Contiene todos los casos tanto de Cliente como de las diferentes partes interesadas	Oficial de Servicio al Cliente SAC

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
11	*Enviar informe mensual entidades reguladores y al SGC y Dirección comercial*	Posteriormente, el Encargado de Atención al Cliente SAC a través del portal oficial de la SSF VARE, envía el reporte mensual de quejas de Clientes, esto con el fin de cumplir la normativa de transparencia solicitado por esta entidad reguladora. El reporte para la SSF debe contener como mínimo: - Número de casos - Tipo y motivo de denuncias - Casos resueltos y casos pendientes Además, se comparte reporte mensual COMPLETO al área de Gestión de Calidad y la Dirección comercial.	Gerente de Servicios Post venta/ Oficial de Servicio al Cliente SAC
12	*Preparar y reporte de quejas trimestral para página WEB*	Trimestralmente el Oficial de Servicio al Cliente SAC, envía el reporte trimestral al área de Mercadeo y Comunicaciones debido a que se debe cargar en la página WEB de Aseguradora ABANK. La información se aloja en la página WEB teniendo en cuenta los siguientes parámetros: - Motivos a los que aplica la queja (NCM-03 Normas de transparencia y divulgación en Seguros) - Número de casos - Casos resueltos y casos pendientes de resolución - Estado de resolución de caso (Favorable, Desfavorable, Cliente desistió) - Gráficos para visualizar datos y tablas resumen - Tiempos de respuesta (fecha de inicio de reclamo y fecha de resolución	Oficial de Servicio al Cliente SAC
13	*Cargar reporte de quejas trimestral en página WEB*	La encargada de Mercadeo y Comunicaciones recibe el reporte trimestral de quejas con el objetivo que este sea cargado cada trimestre en la página WEB de Aseguradora ABANK.	Oficial de Servicio al Cliente SAC
	Fin del Procedimiento		

Proporcionó información:	Alejandra Merlos (Gerente de Servicio Post Venta)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE DISEÑO Y DESARROLLO DE PRODUCTOS/SERVICIOS**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-6-05-PRO**	

PROCESO:	Gestión estratégica
LÍDER DEL PROCESO:	Gerente de portafolio de productos
OBJETIVO:	Establecer las actividades y su secuencia para que a partir de una idea se pueda crear, formalizar, autorizar y depositar productos de seguros ante la Superintendencia del Sistema Financiero.
ALCANCE:	Aplica para la creación de nuevos productos de seguros
DOCUMENTO SOPORTE RELACIONADO:	- Póliza de seguro, nota técnica y sus anexos (modelo de negocio, certificaciones auditoría, interna, riesgos, investigación de mercado, procedimientos, entre otros.). - Bitácora de diseño y desarrollo de producto

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Identificar necesidad e idea para desarrollar nuevo producto de seguros.*	Todos los Colaboradores de la Aseguradora pueden realizar propuestas, consensuarlas con su jefe o encargado inmediato superior, para el adecuado entendimiento de las iniciativas se debe realizar las siguientes actividades: - Propuesta considerando la necesidad e idea para desarrollar el producto de seguros. - Presentar propuesta a Equipo de Productos. El equipo de productos está constituido por los siguientes cargos: - Directores (Técnico y comercial) - Gerente de proyectos estratégicos - Administrador de portafolio	Colaboradores

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
2	*Conocer la necesidad e idea, establecer objetivo, alcance, alternativas de solución y canal.*	El Equipo de Productos, con los Directores y/o Gerentes necesarios para la concretización y desarrollo del producto, considerando la necesidad e idea identificadas, define lo siguiente: • El proyecto es compatible con los objetivos corporativos. • Existe la necesidad en el mercado objetivo identificado. • El mercado potencial para el producto es lo suficiente para lograr las metas comerciales y financieras esperadas. • Desarrollo de la justificación del producto de seguros. • Objetivo del desarrollo del producto de seguros. • Alternativas de solución tomando en cuenta: desarrollar un producto nuevo, modificar un producto existente, incluir asistencia o red de servicio de proveedores. • Valorar implicaciones en contratos de reaseguro. • Definir el canal de distribución. • Cualquier otro aspecto relevante y necesario para concretar el producto a desarrollar.	Equipo de Productos
3	*Establecer proyecto de desarrollo de producto.*	Tomando en cuenta lo establecido en la actividad anterior, se designan a miembros del equipo para: • Documentar, formalizar y definir la funcionalidad del proyecto. • Determinar con la información que se cuenta o si deberá hacerse algún levantamiento de información de mercado. • Viabilidad del producto y desarrollo del mismo. A partir de la presente actividad se debe comenzar a completar la carpeta del producto, la cual contiene todos los documentos que componen el diseño y desarrollo del mismo. Además se inicia el llenado de una bitácora en Excel en la cual se expone cada una de las etapas en las que se encuentra el desarrollo, los datos más relevantes que contiene dicho archivo son: - Etapa en la que se encuentra: las etapas son las actividades del presente procedimiento. - Fecha de inicio y fin de cada etapa - Resultado obtenido de cada etapa - Responsable de cada etapa - Vínculo a evidencia documental de cada etapa - Check list de elementos de calidad que debe cumplirse previo a su puesta en el mercado - Observaciones generales: es decir si se han realizado cambios en el diseño, entre otros... ¿Proyecto viable? SI: continuar con actividad 5. NO: continuar con actividad siguiente.	Equipo del Productos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
4	*Archivar proyecto de desarrollo de producto.*	Se archiva el proyecto de desarrollo de producto estableciendo las razones de su inviabilidad. Esto con el objetivo que una vez se puedan superar las razones detalladas, el proyecto pueda ser retomado, si fuere el caso. Fin del procedimiento.	Director Técnico
5	*Realizar estudio de mercado para el proyecto de desarrollo de producto.*	Analizar necesidades del cliente o mercado objetivo, considerando lo siguiente: - Definir la naturaleza y tamaño del mercado objetivo. - Identificar los productos o servicios que son similares al proyecto y realizar el estudio de mercado. - Analizar los resultados del estudio de mercado y se define el atractivo del producto para el cliente. Siendo esto el insumo para determinar si el proyecto va encaminado a solucionar la necesidad que había sido definida y si todos los atributos del producto realmente generan valor para el cliente. - Estimar el potencial de ventas, persistencia y fidelización esperada de los clientes hacia el producto. Todos los resultados del estudio de mercado son plasmados por escrito en un documento que será un anexo al proyecto de desarrollo de producto.	Director Comercial/Coordinadora de Mercadeo
6	*Analizar resultados de estudio de mercado*	Los resultados obtenidos en las actividades anteriores y que han sido plasmadas en el proyecto de desarrollo de producto, se presentan al Equipo del Producto por parte del Director Comercial para analizar la factibilidad del proyecto. ¿Proyecto factible? SI: continuar con actividad 6 NO: continuar con la siguiente actividad	Equipo del Productos
7	*Archivar proyecto de desarrollo de producto.*	Se archiva el proyecto de desarrollo de producto estableciendo las razones de su inviabilidad. Esto con el objetivo que una vez se puedan superar las razones detalladas, el proyecto pueda ser retomado, si fuere el caso. Fin del procedimiento.	Director Técnico
8	*Definir requerimiento y gestión de desarrollo del producto con el Actuario.*	Con los resultados del proyecto de desarrollo de producto, se define el requerimiento del desarrollo del producto considerando condicionados, anexos y nota técnica.	Director Técnico/Proyectos Estratégicos
9	*Realizar producto según especificaciones.*	De acuerdo al requerimiento, se desarrolla el condicionado del producto, anexos y nota técnica, considerando las leyes y normativas aplicables.	Actuario/Proyectos Estratégicos
10	*Presentar el modelo de póliza de seguro y nota técnica.*	Presenta al Equipo del Productos, el modelo de póliza de seguro y su nota técnica de acuerdo al requerimiento efectuado y explica las variaciones que pudiera tener con sus justificantes.	Actuario/Equipo de Productos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
11	*Validar modelo de póliza y nota técnica.*	El Equipo del Productos valida el modelo de póliza y la nota técnica desarrollada por el Actuario, revisando que cuente con los factores que se solicitaron y el desarrollo del mismo. ¿Todo bien? SI: Continuar con actividad 13 NO: Continuar con actividad siguiente	Equipo de Productos
12	*Aplica mejoras y entrega del modelo de póliza y nota técnica.*	En caso de ser necesario, aplicar las mejoras o solicitudes que realiza el Equipo del Productos para posteriormente hacer entrega del modelo de póliza y nota técnica. Regresar a la actividad 9	Actuario/Proyectos Estratégicos
13	*Establecer las reglas de negocio del modelo de póliza a comercializar*	Con el producto desarrollado, se establecen las reglas de negocio, parametrizaciones, configuraciones de los medios a utilizar para comercializar el producto considerando, entre otros, lo siguiente: • Métodos de pago. • Lineamientos de emisión. • Beneficios. • Precio. • Comisiones. • Gastos. • Reclamos: definición de la política para la presentación de reclamos. • Operaciones: definir la documentación necesaria para la emisión de pólizas, cancelaciones, inclusiones, exclusiones, devoluciones de prima, etc. • Definición de los canales de distribución. • Subcontratación de servicios: contratos de tercerización de servicios, asistencia, redes médicas, farmacias, hospitales (en caso apliquen). • Elaboración de representación visual del producto. • Otros aspectos a considerar como aplicaciones de reaseguro. La Descripción del modelo de negocio del producto en creación puede ser un anexo al documento del proyecto.	Equipo del Productos/Gerentes O Personal necesarios para la concretización y desarrollo del producto
14	*Analizar el producto de seguros considerando riesgos, cumplimiento legal y regulatorio.*	El Equipo de Productos, remite el producto de seguros desarrollado incluyendo las reglas de negocio establecidas para que sea analizada por las áreas de riesgos, cumplimiento legal y prevención de lavado de dinero y auditoría interna, para su análisis, validación de cumplimiento regulatorio, emisión de informes o certificación. ¿Se determinaron riesgos, observaciones o presuntos incumplimientos? SI: Continuar con actividad siguiente NO: continuar con actividad 16	Gerente de Riesgos, Gerente de cumplimiento, Legal, Auditoria Interna.

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
15	*Identificar las medidas mitigantes para subsanar los riesgos o presuntos incumplimientos legales del producto de seguros.*	Proceder a realizar las correcciones pertinentes a fin de subsanar lo observado o superar el presunto incumplimiento, el cual una vez establecido el plan de acción para su corrección, se remite nuevamente para que sea validado por el área que determinó el incumplimiento y procede a emitir su opinión.	Equipo de Productos
16	*Recopilar los documentos que componen el producto de seguros*	Con los resultados de los informes y/o certificaciones de riesgos y cumplimientos, se procede a recopilar los documentos que componen la póliza de seguros, anexos y nota técnica, con el objeto de consolidar el proyecto de desarrollo de producto, que deberá ser resguardado por el Director Técnico, con copia al Director Comercial para su monitoreo y consulta.	Equipo de Productos
17	*Analizar implicaciones fiscales y económicas, las que se agregan proyecto de desarrollo del producto.*	El Equipo de Productos, remite el documento a la Dirección de Finanzas y Administración para: • Analizar las implicaciones y consideraciones fiscales que podría conllevar el producto y detallar las opciones de actuación, si las hubiere. • Analizar juntamente con la Dirección Comercial las consideraciones económicas y puesta en marcha del producto; entre las cuales está el planteamiento de un presupuesto de ventas y flujos de efectivo, entre otros. • El resultado del análisis generará una opinión que se coloca como anexo al mismo. • Entrega el documento al Director Técnico.	Director Financiero/ Director Comercial
18	*Organizar y realizar Focus Group.*	• El Equipo de Productos solicita al Director Comercial que realice el análisis para desarrollar reunión con un grupo focalizado y de ser necesario, defina las actividades que debe efectuar para llevar a cabo dicha reunión, presentando las necesidades, la solución con sus cualidades más destacadas obtenidas en el ejercicio del estudio de mercado. • Los resultados de la reunión con el grupo focalizado se detallan en un informe que será anexo al proyecto de desarrollo de producto y lo presenta al Director Comercial y Director Técnico. El producto debe cumplir con un estándar de calidad previo de su entrega al Cliente, por lo que se debe considerar un check list de control de Calidad previo a continuar con actividades con la SSF y/o comercialización del mismo. Algunos de los elementos que se debe dar cumplimiento son (se deben expresar en la bitácora de Diseño y desarrollo de producto): - Cumple con las expectativas y necesidades de los Clientes - Los tiempos de atención al Cliente son mejores o iguales a la competencia - Es un producto rentable para la organización - Cumple con las disposiciones establecidas desde el inicio del diseño del producto - Cumple con el marco legal ¿Mejoras? SI: Continuar con actividad siguiente	Equipo del Productos/Personal interno relacionado al proyecto/ Personal externo, Intermediarios de seguros

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		NO: Continuar con actividad 20/21 (paralelas)	
19	*Modificar, aclarar o redefinir el proyecto de desarrollo de producto.*	De acuerdo a los resultados de la reunión con el grupo focalizado, se modifica, aclara o redefinen aspectos del proyecto de desarrollo de producto. Entre los aspectos revisados y redefinidos, de acuerdo a lo establecido por el Equipo del Productos, son: • Características básicas del producto. • Beneficios/coberturas especiales. • Límites de suma asegurada, edades. Regresara a la actividad 9	Director Comercial, Director Técnico, Coordinadora de Mercadeo/Gerentes necesarios.
Inicio de actividades paralelas			
20	*Definir estrategia de mercadeo*	Con los insumos que se cuentan, se define la primer versión de la estrategia de mercadeo y se establece en el proyecto de desarrollo de producto, colocando como anexo al mismo, considerando lo siguiente: • Revisar la estrategia de mercadeo existente y tomarla de base para aplicar ajustes. • Inteligencia de mercado sobre la Competencia sobre el producto y el mercado. • Cobertura básica. • Beneficios y características diferenciadoras. • Nivel competitivo de precio contra productos similares y planes existentes. • Estructura de comisión. • Entrenamiento y soporte requerido. • Canal de distribución a ser utilizado. • Publicidad, plan de comunicaciones y relaciones públicas, entre otros.	Equipo del Productos y Coordinadora de Mercadeo
21	*Validar requerimientos para el sistema*	Se de realizar una validación de los requerimientos para adaptar el sistema al producto desarrollado, en las reuniones con el área de tecnología se debe analizar: • Si fuere necesario efectuar cambios en la parametrización de los sistemas actuales. • Efectuar las pruebas de las parametrizaciones efectuadas. • De resultar exitoso el proceso de pruebas, se pasa al proceso de producción para la comercialización del producto.	Equipo del Productos/Gerente de tecnología
Fin de actividades paralelas			

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
22	*Solicitar depósito de producto en la Superintendencia del Sistema Financiero.*	Miembros del Equipo de Productos, desarrollan lo siguiente: • Prepara la documentación requerida por la Superintendencia del Sistema Financiero (SSF). • Solicitar de ser posible, una reunión con la SSF para presentar las características del producto de seguros, tomando en cuenta las observaciones y/o recomendaciones propuestas. • Solicitar el depósito del producto de seguros desarrollado, esperando la autorización para su comercialización. • Una vez recibidos los documentos con sello del depósito, notificar al Equipo del Productos para continuar con las actividades de comercialización.	Director Técnico/ Proyectos Estratégicos
23	*Implementa, monitorea ventas y revisa resultados*	La implementación del producto conlleva la revisión de la estrategia de marketing para confirmar la primer versión desarrollada para posteriormente ejecutar. Una vez finalizado este procedimiento, el producto de seguros se vuelve parte de la cartera por lo que se monitorea en ventas, gastos, presupuesto, revisión de canales de distribución, utilidad, entre otros. Para determinar según los resultados, si el producto se sigue comercializando, se modifica o se elimina.	Coordinadora de Mercadeo, Director Comercial y Director Técnico
	Fin del Procedimiento		

Proporcionó información:	Pedro Ramírez (Gerente de portafolio de productos)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	PROCEDIMIENTO PARA LA EVALUACIÓN DE PROVEEDORES	VERSIÓN	FECHA	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	SIG-8-06-PRO	

PROCESO:	Control interno
LÍDER DEL PROCESO:	Director financiero administrativo/Gerente de tecnología.
OBJETIVO:	Determinar los criterios para seleccionar, evaluar y evaluar a los contratistas y proveedores en función de su capacidad para suministrar bienes y/o servicios, ya sean estos administrativos o tecnológicos.
ALCANCE:	El tipo y alcance del control aplicado a los contratistas y proveedores, se determina con base en los productos y/o servicios adquiridos considerados de impacto para la ejecución de actividades que pueden afectar de manera directa o indirecta la calidad de los servicios que recibe, por parte de la aseguradora, los asegurados y otras partes interesadas del negocio, así como garantizar la seguridad de la información organizacional.
DOCUMENTO SOPORTE RELACIONADO:	Check list de evaluación de proveedores

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Planificar inspección y/o evaluación de contratistas*	Se realizan la planificación anual de las inspecciones a realizar a los diferentes contratistas de la organización Se debe completar el programa anual y gestionar los recursos necesarios para dicho objetivo	Gerente de tecnología.
2	*Realizar inspección de contratistas*	Se realizan inspecciones in situ o por medio de entrevista virtual a los proveedores con la finalidad de identificar todos aquellos riesgos, y el cumplimiento a los principios del SIG de Aseguradora ABANK. Para el registro de los hallazgos se deben plasmar en la plantilla “check list de evaluación contratistas”, en el cual se detalla: -Tipo de hallazgo (Peligros, No conformidades, Observaciones, Conformidades, Puntos de mejora) -Descripción del hallazgo -Evidencia	Director financiero administrativo/Gerente de tecnología.

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
3	*Analizar registros de inspección*	Posteriormente se consolida la información recabada en la inspección	Director financiero administrativo/Gerente de tecnología.
4	*Generar informe de inspección y matriz de riesgos*	Se genera el informe de inspección en el cual se enlistan todos los hallazgos y se ordenan según el impacto de los mismos. Además, se incorporan las consideraciones y experiencias del evaluador conforme a los servicios prestados por el contratista.	Director financiero administrativo/Gerente de tecnología.
5	*Informar al contratista y/o proveedor los resultados de inspección*	El informe se comparte con la alta dirección y con el mismo proveedor/contratista con el objetivo que lo lea y verifique los hallazgos que deben tratarse para mitigar riesgos de SIG.	Director financiero administrativo/Gerente de tecnología.
6	*Ejecutar planes de acción*	El Contratista debe ejecutar planes de acción según lo descrito en el informe de evaluación emitido por Aseguradora ABANK. En el planteamiento de los planes de acción, el contratista debe considerar: - Análisis causa-raíz - Actividades a ejecutar - Responsable - Evidencia Estos planes de acción deben enviarse a Fulltac, antes de las primeras 72 horas. Regresar a la actividad 2	Director financiero administrativo/Gerente de tecnología.
7	*Evaluar desempeño anual de contratistas*	Anualmente se realiza un análisis del desempeño de los contratistas, entre los parámetros que se analizan son los relacionados a la SIG. La evaluación se realiza basada en criterios específicos de cumplimento los cuales se encuentran descritos en la matriz “Requisitos para contratistas y proveedores”. Dichos criterios se consolidan en 4 grandes grupos, los cuales son: 1. Cumplimiento a la política del SIG de Aseguradora ABANK. 2. Evaluación y seguimiento de Peligros y riesgos 3. Implementación como contratistas de mecanismos de SIG 4. Cumplimiento al marco legal nacional Cada criterio dentro de estos grupos se pondera y se obtienen resultados que se establecen en los siguientes niveles de cumplimiento: 0 a 25: incumplimiento extremo 25 a 50: incumplimiento medio	Director financiero administrativo/Gerente de tecnología.

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		50 a 75: en cumplimiento 75 a 100: excelente cumplimiento A partir de la comparativa entre contratistas y estos factores se decide si se continúa o no con un contratista ¿Se continúa trabajando con proveedor? SI: Continuar con actividad 9 NO: Continuar con actividad 8	
8	*Desvincular contratista de organización*	Se le comunica al contratista de manera formal que Aseguradora ABANK se desvinculará de la organización y se dará por finalizado el contrato de trabajo. Fin de procedimiento	Director financiero administrativo/Gerente de tecnología.
9	*Dar seguimiento riesgos identificados con contratistas*	A los contratistas que se encuentren vinculados a la organización se les brinda seguimiento de riesgos a través de la matriz de riesgos. Aseguradora ABANK garantiza una comunicación permanente y propositiva para que las actividades entre la compañía y contratista sean seguras para todas las personas. Para ello se brindan capacitaciones, campañas, entre otros.	Director financiero administrativo/Gerente de tecnología.
	Fin del Procedimiento		

Proporcionó información:	Pedro Laínez (Director financiero administrativo), Carlos Rivera (Gerente de tecnología)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	PROCEDIMIENTOS DE SERVICIOS POST VENTA	VERSIÓN	FECHA	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	SIG-8-07-PRO	

PROCESO:	Servicio post venta
LÍDER DEL PROCESO:	Gerente de servicios post venta
OBJETIVO:	Realizar las gestiones de atención y seguimiento de solicitudes de información y soporte requerido por los asegurados de la compañia
ALCANCE:	Aplica para la gestión de solicitudes y seguimiento por parte de Clientes y las diferentes partes interesadas que se vinculan a la comercialización de seguros en Aseguradora ABANK
DOCUMENTO SOPORTE RELACIONADO:	- Informe mensual y trimestral de quejas - ISO 9001:2015 (8.7 "Control de salidas No conformes", 9.1.2 "Satisfacción del Cliente") - NCM-03 Normas de transparencia y divulgación en Seguros (Art.10 en adelante)

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Recepción de la solicitud de servicio postventa*	Cuando un cliente contacta a la aseguradora con una solicitud de servicio postventa, ya sea por teléfono, correo electrónico, chat en vivo o a través de la plataforma en línea, el proceso comienza con la recepción de la solicitud.	Oficial de atención al cliente
2	*Identificación y registro del cliente*	El agente o representante de servicio al cliente debe identificar al cliente y verificar su información. Esto puede incluir el número de póliza, nombre, número de teléfono y dirección.	Oficial de atención al cliente
3	*Escucha activa y comprensión de la solicitud*	El agente debe escuchar atentamente al cliente para comprender completamente su solicitud o inquietud. Esto puede incluir cambios en la póliza, actualizaciones de datos personales, preguntas o asesoramiento sobre la cobertura, entre otros.	Oficial de atención al cliente
4	*Análisis de la solicitud*	Una vez que la solicitud se ha entendido, el agente debe analizarla para determinar la mejor manera de abordarla. Puede ser necesario consultar la póliza y las políticas internas para tomar decisiones informadas.	Oficial de atención al cliente

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
5	*Resolución de la solicitud*	El agente debe tomar las medidas necesarias para resolver la solicitud del cliente. Esto puede incluir realizar cambios en la póliza, responder preguntas o proporcionar asesoramiento. Es importante que la resolución sea oportuna y eficiente.	Oficial de atención al cliente
6	*Comunicación con el cliente*	Mantener una comunicación constante con el cliente es esencial. El agente debe mantener al cliente informado sobre el progreso de la solicitud y proporcionar una estimación de cuánto tiempo tomará resolverla.	Oficial de atención al cliente
7	*Documentación y registro*	Cada interacción con el cliente y todas las acciones tomadas deben registrarse en el sistema de la aseguradora. Esto asegura un seguimiento adecuado y proporciona un historial detallado de la interacción con el cliente.	Oficial de atención al cliente
8	*Seguimiento de calidad*	La aseguradora debe realizar un seguimiento de calidad para garantizar que los agentes de servicio al cliente cumplan con los estándares de servicio establecidos. Esto puede incluir escuchas de llamadas, revisiones de casos y retroalimentación.	Oficial de atención al cliente
9	*Retroalimentación del cliente*	Después de que se resuelve la solicitud del cliente, es importante solicitar retroalimentación. Esto ayuda a evaluar la satisfacción del cliente y a identificar áreas de mejora.	Oficial de atención al cliente
10	*Seguimiento a largo plazo*	La atención al cliente no termina con la resolución de una solicitud. Las aseguradora debe mantener un seguimiento a largo plazo para garantizar que los clientes estén satisfechos con su póliza y para ofrecer asesoramiento adicional a medida que cambian las circunstancias del cliente.	Oficial de atención al cliente
	Fin del Procedimiento		

Proporcionó información:	Alejandra Merlos (Gerente de Servicio Post Venta)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**CONTROL Y MONITOREO DE INDICADORES DE DESEMPEÑO DEL SIG**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-9-08-PRO**	

PROCESO:	Gestión de calidad
LÍDER DEL PROCESO:	Analista de proceso
OBJETIVO:	Desarrollar actividades de monitoreo del desempeño de todos los indicadores de proceso de Aseguradora ABANK, con el fin de aplicar controles específicos para mejorar o mantener el rendimiento del Sistema de Gestión de la compañía.
ALCANCE:	Aplica para todos los indicadores de desempeño de procesos declarados para el Sistema de Gestión de Aseguradora ABANK
DOCUMENTO SOPORTE RELACIONADO:	- Consolidado de indicadores de desempeño ISO - Informe mensual de indicadores de desempeño ISO - Plantilla para registro de indicadores de desempeño

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Recibir resultados de indicadores de desempeño de forma mensual*	Periódicamente (mensualmente, trimestralmente, anualmente, según se haya establecido en la ficha del proceso) se reciben, por medio de correo electrónico (gestiondecalidad@aseguradoraabank.com), los resultados de los indicadores de desempeño de procesos los cuales son enviados por los diferentes Responsables de proceso con copia del líder de proceso correspondiente. Los resultados de indicadores se comparten a través de un plantilla específica, la cual se titula "Plantilla para registro de indicadores de desempeño", la cual se encuentra alojada en la intranet en SharePoint de Gestión de Calidad (https://segurosvivirsv.sharepoint.com/sites/GestionDeCalidad)/ en la sección: - Formatos/Plantillas: como lo dice su titulo plantillas que se utilizan en la operación diaria (ejemplo: ficha integral, formulario PEP, entre otros.) Dicho registro de resultados debe ir acompañado de evidencia que demuestre de donde se han obtenido dichos resultados, esta evidencia objetiva puede ser archivos de Excel completados de forma manual o que provengan de Sistemas informáticos, entre otro tipo de evidencias. Los resultados de indicadores de desempeño se reciben a más tardar 13 días hábiles posteriores a la finalización del mes que se reporta.	Analista de procesos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
2	*Analizar resultados de indicadores*	Al recibir los resultados de desempeño de procesos se procede a revisar cada indicador, según su meta, tolerancia y resultado mismo. ¿Faltan datos? SI: Continuar con actividad 4 NO: Continuar con actividad 3	Analista de procesos
3	*Realizar cuadre con datos de sistemas*	Para garantizar la fiabilidad de los resultados mensuales, el Analista de Procesos debe realizar las descargas necesarias en Sistema para cuadrar los datos recibidos, cuando sea factible. Algunos de los sistemas o aplicativos para realizar cuadraturas y la disposición del Analista de procesos son: - Sistema SISE 3G - Canal Digital - Red médica - Módulo de quejas - Bancaseguros - Entre otros... ¿Incumplimiento de metas? SI: Ver procedimiento "Tratamiento de No conformidades" NO: ¿Datos cuadran? SI: Continuar con actividad 5 NO: Continuar con actividad 4	Analista de procesos
4	*Solventar caso con área involucrada*	El Analista de Procesos debe establecer contacto con área involucrada (en especial con el líder de proceso) y comentar las inconsistencias identificadas para obtener aclaraciones o corrección o aplicación de mejora al indicador. Regresar a la actividad 1	Analista de procesos
5	*Consolidar indicadores en una sola matriz*	Los resultados de indicadores se consolidan en la matriz "Consolidado de indicadores de desempeño ISO", en el cual se encuentra todos los indicadores de desempeño por procesos de todo el Sistema de Gestión. Dicho consolidado se resguarda carpeta en OneDrive del área de Procesos. El contenido del consolidado registra de forma mensual cada uno de los resultados de los indicadores y los compara con las metas y tolerancias correspondientes, este registro es el mayor consolidado de resultados de los procesos de la organización	Analista de procesos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
6	*Elaborar informe mensual de indicadores de desempeño de procesos*	Posterior a la realización de consolidado en matriz correspondiente, el Analista de Procesos genera un "Informe mensual de indicadores de desempeño ISO" el cual se define en formato PDF y se comparte a la Alta Dirección cada mes. El contenido principal del informe es: 1. Resultados generales del mapa de procesos 2. Resultados por procesos 3. Resultados negativos, incumplimientos 4. Resumen y recomendaciones de Procesos Dicho informe se resguarda carpeta en OneDrive del área de Procesos	Analista de procesos
7	*Cargar informe en Sitio de Gestión de Calidad*	El Analista de Procesos debe cargar en la intranet de SharePoint el informe, mes a mes. Para realiza dicha carga se debe ingresar a la intranet en SharePoint https://segurosvivirsv.sharepoint.com/sites/GestionDeCalidad y se ingresa al administrador del sitio para visualizar las páginas de información en la cual se debe alojar informe, en este caso, página "Indicadores de desempeño (procesos)" del año correspondiente.	Analista de procesos
8	*Divulgar resultados de indicadores a la compañía*	Los resultados de indicadores mensuales se comparten a toda la aseguradora, por medio del correo electrónico "gestiondecalidad@aseguradoraabank.com". Los datos que se exponen son generales por cada proceso y se brinda un vínculo al sitio de la Gestión de Calidad para revisar informe detalle	Analista de procesos
	Fin del Procedimiento		

Proporcionó información:	Victor Mendizabal (Gerente de servicios post venta)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO PARA EVALUACIÓN DE LA SATISFACCIÓN DEL CLIENTE**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-9-09-PRO**	

PROCESO:	Servicios post venta
LÍDER DEL PROCESO:	Gerente de servicios post venta
OBJETIVO:	Evaluar la satisfacción de los asegurados de Aseguradora ABANK.
ALCANCE:	Evaluación de la satisfacción de los asegurados, tanto naturales como jurídicos, de Aseguradora ABANK.
DOCUMENTO SOPORTE RELACIONADO:	Encuesta de evaluación del cliente, plan de evaluación de la satisfacción.

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Definir el objetivo y alcance de la encuesta*	Identificar los objetivos específicos de la evaluación de satisfacción, como mejorar la retención de clientes o la calidad del servicio. Delimitar el alcance de la evaluación, especificando qué líneas de negocio, productos o servicios se incluirán en la evaluación.	Oficial de atención al cliente/ Gerente de servicio post venta
2	*Seleccionar métricas de la encuesta y diseño de instrumento de evaluación*	Elegir las métricas clave que se utilizarán para medir la satisfacción, como puntajes de satisfacción, tasas de retención de clientes, tasas de quejas, etc. Crear cuestionarios de satisfacción adaptados a cada segmento de clientes. Desarrollar indicadores específicos para evaluar la calidad de los productos o servicios.	Oficial de atención al cliente/ Gerente de servicio post venta
3	*Desarrollar encuesta*	Seleccionar los métodos de encuesta adecuados, que pueden incluir encuestas por correo, encuestas telefónicas, encuestas en línea o entrevistas en persona. Programar las encuestas en función de la estrategia definida en la planificación.	Oficial de atención al cliente/ Gerente de servicio post venta
4	*Procesamiento de resultados*	Tabular y analizar las respuestas de las encuestas. Calcular estadísticas de resumen, como promedios, desviaciones estándar y tasas de respuesta.	Oficial de atención al cliente/ Gerente de servicio post venta

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
5	*Analizar quejas y sugerencias e identificación de áreas de mejora*	Investigar a fondo las quejas y sugerencias de los clientes para identificar patrones y tendencias. Clasificar las quejas en categorías, como servicio al cliente, procesamiento de reclamaciones, facturación, etc. Utilizar los resultados del análisis para identificar áreas específicas donde la satisfacción del cliente sea baja o donde se detecten problemas recurrentes.	Oficial de atención al cliente/ Gerente de servicio post venta
6	*Comunicar resultados*	Informar a los equipos y a la dirección de la aseguradora sobre los hallazgos y los resultados de la evaluación de satisfacción del cliente.	Oficial de atención al cliente/ Gerente de servicio post venta
7	*Creación de planes de acción*	Crear un plan que incluya acciones específicas para abordar las áreas identificadas como problemáticas. Definir los recursos y plazos necesarios para la implementación.	Oficial de atención al cliente/ Gerente de servicio post venta
8	*Desarrollo y seguimiento*	Llevar a cabo las acciones correctivas de acuerdo con el plan desarrollado. Proporcionar capacitación y apoyo al personal, si es necesario. Realizar un seguimiento constante para asegurarse de que las mejoras se implementen de manera efectiva y consistente.	Personal involucrado de la aseguradora/ Oficial de atención al cliente
9	*Aplicar mejora continua*	Realizar evaluaciones regulares de la satisfacción del cliente para evaluar el impacto de las mejoras y ajustar el enfoque según sea necesario. Hacer ajustes en el proceso de evaluación y en las estrategias de mejora según sea necesario para mantener la satisfacción del cliente a lo largo del tiempo.	Oficial de atención al cliente/ Gerente de servicio post venta
	Fin del Procedimiento		

Proporcionó información:	Victor Mendizabal (Gerente de servicios post venta)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE AUDITORÍA INTERNA**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-9-10-PRO**	

PROCESO:	Control interno
LÍDER DEL PROCESO:	Auditor interno
OBJETIVO:	Establecer la metodología para la planificación, desarrollo y evaluación de las Auditorías Internas.
ALCANCE:	Desde la elaboración de los programas de auditoría interna hasta la elaboración y presentación de Informes de Cierre.
DOCUMENTO SOPORTE RELACIONADO:	Plan de auditoría, programa de auditía, check list de auditoría, informe de auditoría

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	*Planificación de Auditoría:*	Al inicio de cada año, el cual indica el periodo en que se realizará cada auditoría, así como el alcance de cada una. Esta programación se realizará tomando en cuenta los siguientes criterios: Auditorías previas realizadas, alcance y objetivo de la auditoría, Disponibilidad de tiempo, Disponibilidad de recursos, Estado e importancia de los procesos. De acuerdo con el programa de auditorías, el auditor interno elabora el Plan de Auditoría utilizando el El auditor designado a cada proceso y su equipo auditor, cuando aplique, prepara la auditoría tomando en consideración lo siguiente: 1. Revisar los documentos del área a auditar 2. Revisar resultados de auditorías previas (internas, externas, de clientes) 3. Preparar Lista de Verificación según 4. Informar al dueño del proceso el Plan de Auditoría, confirmando la fecha y hora definida. 5. Definir y coordinar aspectos logísticos.	Coordinador del Sistema Integrado de Gestión

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
2	*Ejecución de la auditoria*	los auditores ejecutan el trabajo de campo de acuerdo al Plan de Auditoría, realizando las siguientes actividades: 1. Entrevistar al personal de la dependencia auditada utilizando como apoyo la Lista de Verificación 2. Verificar la información, tanto documental como la proporcionada durante la entrevista, con la ejecución de la actividad 3. Hacer muestreo y seguimiento 4. Recolectar evidencias que permitan verificar la funcionalidad y eficacia de las actividades. Revisa que los documentos y registros referenciados sean consistentes, que cumpla con los requisitos de las normativas.	Coordinador del Sistema Integrado de Gestión
3	*Analizar resultados de la auditoría y cierre de la auditoria*	Analizar resultados de la auditoría (consolidación de hallazgos). Reunión de cierre de auditoría Nota: en esta actividad se reciben objeciones de hallazgos	Coordinador del Sistema Integrado de Gestión
4	*Informe de la auditoria*	El Equipo de Auditoría Interna registra y redacta los hallazgos encontrados durante la ejecución de las auditorías internas.	Coordinador del Sistema Integrado de Gestión
	Fin del Procedimiento		

Proporcionó información:	Juan Ramírez (Coordinadora del Sistema Integrado de Gestión)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE LA REVISIÓN POR LA DIRECCIÓN**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-9-11-PRO**	

PROCESO:	Gestión estratégica
LÍDER DEL PROCESO:	Gerente de tecnología
OBJETIVO:	Estandarizar las actividades de reunión de la alta dirección para la revisión del desempeño del Sistema de Gestión de Aseguradora ABANK.
ALCANCE:	Aplica para la revisión de los resultados periódicos del Sistema de Gestión por parte de la Alta dirección.
DOCUMENTO SOPORTE RELACIONADO:	- Cronograma de reuniones SG de revisión por la Dirección - Acta de reunión de revisión por la Dirección SG - Informe de revisión por la Dirección SG - Planes de acción de mejora

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
	Planificar reuniones para revisión del SG	Anualmente el Gerente de tecnología planea las revisiones por la Dirección del Sistema de Gestión (SG) de Aseguradora ABANK, las reuniones se realizan cada 2 meses y en ella se revisa el rendimiento y resultados del SG de la organización. La planificación se realiza por medio de un "Programa de reuniones SG de revisión por la Dirección" el cual es un documento que contiene: - Objetivos de las reuniones - Alcance (puntos a tratar*) - Fecha de reuniones - Involucrados	Gerente de tecnología

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		Este documento se envía a la Alta dirección de la compañía, es decir al STAFF (conformado por Gerentes, directores, auditoría y otros líderes de proceso de la organización), con el objetivo que sea aprobado. Este envío se realiza por medio de correo electrónico. El documento es resguardado en carpeta compartida en OneDrive de la Gerencia de tecnología-procesos *Nota: si hay planes de acción o temas pendientes desde la última revisión por la dirección se deben plasmar en el programa.	
	Revisar planificación	El personal de la organización que compone el STAFF se reúne cada semana en reuniones específicas para ver temas de negocio, el Gerente de tecnología aprovecha dicha ocasión para requerir el visto bueno del programa de revisiones por la dirección. ¿Se aprueba? SI: Continuar con actividad 3 NO: Regresara a la actividad 1	Alta dirección - STAFF
	Enviar agendas de reunión	Posterior a la aprobación por parte de la Alta dirección se envían las agendas de reunión para cada periodo que se haya plasmado en programa de Revisiones por la Dirección, a través de Outlook.	Analista de procesos
	Consolidar la información pertinente para la revisión	Previamente a la reunión por la dirección, el Analista de procesos y el Gerente deben tener toda la información que la normativa requiere, debidamente ordenada y plasmada en una presentación en PowerPoint.	Analista de procesos/ Gerente de tecnología
	Realizar apertura de reunión y comunicar agenda	El Gerente de tecnología da apertura a la reunión periódica y establece la agenda de reunión, la cual debe contener: a) el estado de las acciones de las revisiones por la dirección previas b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la calidad b) la información sobre el desempeño y la eficacia del sistema de gestión de la calidad, incluidas las tendencias relativas a: 1) la satisfacción del cliente y la retroalimentación de las partes interesadas pertinentes; 2) el grado en que se han logrado los objetivos de la calidad; 3) el desempeño de los procesos y conformidad de los productos y servicios; 4) las no conformidades y acciones correctivas; 5) los resultados de seguimiento y medición; 6) los resultados de las auditorías; 7) el desempeño de los proveedores externos; d) la adecuación de los recursos;	Gerente de tecnología

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		e) la eficacia de las acciones tomadas para abordar los riesgos y las oportunidades (véase 6.1); f) las oportunidades de mejora. A partir de esta actividad debe completarse el registro del "Acta de reunión de revisión por la Dirección SG", en el cual se establece: - Título de reunión - Fecha de reunión - Objetivo y alcance - Participantes requeridos - Acuerdos establecidos	
	Analizar estado actual del Sistema de Gestión	Los participantes en la reunión deben poner atención en el resumen de resultados periódicos del rendimiento del Sistema de Gestión, esto con el objetivo que cada uno de los participantes se empodere de la responsabilidad del éxito del Sistema de Gestión, por ende de la aseguradora.	Alta dirección - STAFF/ Gerente de tecnología
	Concretar acciones a seguir	Las acciones que se definan deben plasmarse en el "Acta de reunión de revisión por la Dirección SG", registro el cual debe contener en la sección "Acuerdos establecidos": - Oportunidades de mejora - Cualquier necesidad de cambio en el Sistema de Gestión - Necesidades de recursos Es importante que por cada punto acordado se solicite el responsable y las fechas tentativas para ejecución de actividades. Posteriormente se realizará un Plan de Acción de mejoras para definir el detalle.	Alta dirección - STAFF/ Gerente de tecnología/ Analista de procesos
	Realizar cierre de reunión y lectura final del acta de reunión	El Gerente de tecnología da la pauta para la lectura del acta de reunión y el Analista de procesos procede a leer los acuerdos establecidos en "Acta de reunión de revisión por la Dirección" para que se establezca un acuerdo final consensuado por cada punto registrado en dicho formato. Si no hay acuerdo en ciertos acuerdos, se realiza dialogó y aprobación por mayoría para establecer acuerdo final.	Analista de procesos/ Gerente de tecnología
	Generación de informe de la revisión por la Dirección y enviar a los participantes	El analista de procesos resguarda el acta de reunión en carpeta compartida de OneDrive de la Gerencia de tecnología-procesos. Y procede a generar el informe final de la reunión sostenida. El informe final se titula "Informe de revisión por la Dirección SG" y se envía a todos los participantes de la reunión. El contenido del informe está constituido principalmente por: - Título de la reunión - Fecha y hora - Check list de puntos revisados	Analista de procesos

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		- Acuerdos establecidos ¿Se requieren Planes de acción de Mejora? SI: Continuar con actividad 8 NO: Continuar con actividad 7	
	Comunicar y reunir a los involucrados en planes de acción	El Gerente de tecnología cita a los Líderes de proceso involucrados en los Planes de acción de mejora para reunirse y establecer conjuntamente los planes de acción correspondientes. Esta comunicación para establecer reunión se realiza por medio de correo electrónico.	Gerente de tecnología - Procesos/ Analista de procesos/ Líderes de proceso
	Crear planes de acción de mejora	Se desarrollan los planes de acción, en esta actividad puede mediar tanto el Gerente tecnología como el Analista de procesos, este último redacta el Plan de acción, si es necesario. La estructura de los Planes de acción de Mejora es: - Objetivo y alcance - Involucrados en plan de acción - Actividades a desarrollar - Fechas de actividades a desarrollar - Recursos - Riesgos del plan	Gerente de tecnología - Procesos/ Analista de procesos/ Líderes de proceso
	Ejecutar plan de acción	El personal de la organización involucrado en Plan de acción de Mejora realiza las actividades plasmadas y envía los resultados de las evidencias de cumplimientos a Procesos, por medio del correo electrónico gestióndecalidad@aseguradoraabank.com. Es muy importante que se adjunte evidencia objetiva que garantice que se ha cumplido con actividad plasmada en plan.	Gerente de tecnología - Procesos/ Analista de procesos/ Líderes de proceso
	Evaluar la eficacia del plan de acción de mejora	El Analista de proceso en conjunto con el Gerente de tecnología proceden a revisar que la evidencia objetiva sea acorde a las actividades planteadas en Plan de acción. En los casos que no, se procede a comunicar a los involucrados y establecer nuevamente una mesa de trabajo para solventar inconsistencias. ¿Todo bien? SI: Continuar con actividad 13 NO: Regresar a la actividad 10	Analista de procesos/ Gerente de tecnología
	Dar seguimiento a los planes de acción de mejora de la organización	Una semana antes de cada Revisión por la Dirección, el Gerente de tecnología en conjunto con el Analista de procesos deben revisar que las actividades plasmadas en los planes de acción de Mejora que han sido ya cerrados, se encuentren realmente cerradas.	Analista de procesos/ Gerente de tecnología

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
		¿Riesgos vigentes aún? SI: Regresar a la actividad 11 NO: Fin de procedimiento	
	Fin del Procedimiento		

Proporcionó información:	Juan Ramírez (Coordinadora del Sistema Integrado de Gestión)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO DE NC Y ACCIONES CORRECTIVAS**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	18/10/2023	
		CÓDIGO:	**SIG-10-12-PRO**	

PROCESO:	Gestión de Calidad
LÍDER DEL PROCESO:	Coordinador del Sistema Integrado de Gestión
OBJETIVO:	Establecer la metodología para la detección, documentación, análisis y evaluación de las No Conformidades y Acciones Correctivas.
ALCANCE:	Desde las actividades para el análisis y determinación de las causas hasta el seguimiento y cierre de las acciones determinadas.
DOCUMENTO SOPORTE RELACIONADO:	Bitácora de NC y Acciones correctivas, planes de acción.

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
1	Recopilar acción correctiva	Se recibe acción correctiva por parte del Coordinador de Sistema Integrado de Gestión y se procede a revisar su grado de impacto al negocio. Las No conformidades detectadas se ingresan al Sistema para delegar al responsable de la No Conformidad y darle seguimiento al plan de acción, desde su inicio a su fin. De igual se codifica un identificador de la acción correctiva, por ejemplo: AC_SGC_001"	Coordinador del Sistema Integrado de Gestión
2	Delegar a lider de proceso responsable en sistema	Se procede a delegar al líder de proceso responsable de la No conformidad, a través del sistema. Se parametrizan los siguientes aspectos: 1. Líder responsable 2. Fecha de inicio 3. Fecha límite para presentar plan de acción para acción correctiva (8 días a partir de ingresada no conformidad en sistema) 4. Fecha en la que Gestión de Calidad realizará una evaluación de eficacia de la acción correctiva ejecutada.) (2 días después de cargado plan de acción).	Coordinador del Sistema Integrado de Gestión

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
3	Recibir y revisar acción correctiva delegada	El líder de proceso, del área funcional correspondiente, procede a revisar la notificación que recibió en correo y e ingresa al sistema para revisar No conformidad.	Coordinador del Sistema Integrado de Gestión Líder del proceso
5	Analizar causa raíz y crear plan de acción	Se revisar la no conformidad y se realiza un análisis de causa raíz para darle un tratamiento adecuado al hallazgo, para ello en el plan de acción se dispone de técnicas como: Ishikawa, pareto, 5W+2H, lluvia de ideas. Posteriormente se crea el plan de acción y se colocan los siguientes parámetros: - Resumen de análisis de la no conformidad - Acción correctiva que se ejecutará - Fecha de inicio y fin de aplicación de acción correctiva - Evidencia de iniciación - Responsable Los demás campos como código de no conformidad, área, responsable de no conformidad, el sistema los completa automáticamente.	Coordinador del Sistema Integrado de Gestión
6	Ejecutar acción correctiva planificada	El líder de proceso inicia a ejecutar las acciones correctivas planificadas y posterior a ello carga la evidencia de su realización en la plataforma Certool. Algunos documentos de evidencia pueden ser: - Registros (listas de asistencia, check list, correos, agendas de reunión, entre otros.) - Documentos (Cambios en documentos internos, políticas, entre otros.) - Fotografías - Capturas de pantalla - Entre otros	Coordinador del Sistema Integrado de Gestión
7	Evaluar eficacia de plan de acción correctiva cargada en sistema	El Coordinador de Gestión de Calidad revisa en sistema el plan de acción de acciones correctivas y su respectiva evidencia. ¿Todo bien? SI: Continuar con actividad 8 NO: Continuar con actividad 7	Coordinador del Sistema Integrado de Gestión
8	Devolver acción correctiva	A través del sistema, el Coordinador de Sistema Integrado de Gestión devuelve plan de acción con las observaciones correspondientes para ser resueltas. El tiempo límite a partir del envío de las correcciones es de 3 días, para que el líder de proceso realice las gestiones correspondientes y vuelva a cargar plan y/o evidencia. Regresar a actividad 4	Coordinador del Sistema Integrado de Gestión

No.	ACTIVIDAD	CÓMO SE HACE	RESPONSABLE
9	Cerrar no conformidad y evaluar como eficaz	Se evalúa como eficaz la acción correctiva y se cierra en sistema el plan de acción. Cada 6 meses, después de cerrada una no conformidad, el sistema abre un nuevo proceso de seguimiento para que el Coordinador evalue el estado de la no conformidad. Luego de 2 seguimientos se cierra completamente y desaparece de sistema. Se resguarda en un respaldo especial. ¿Dar seguimiento a no conformidad? SI: Continuar con actividad 9 NO: Fin de procedimiento	Coordinador del Sistema Integrado de Gestión
10	Dar seguimiento a no conformidad	Se revisa que la acción correctiva haya sido efectiva al pasar el tiempo. ¿Todo bien? SI: Regresar a actividad 8 NO: Regresar a actividad 7	Coordinador del Sistema Integrado de Gestión
	Fin del Procedimiento		

Proporcionó información:	Juan Ramírez (Coordinadora del Sistema Integrado de Gestión)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**PROCEDIMIENTO PARA GESTIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	17/10/2023	
		CÓDIGO:	**SIG-10-13-PRO**	

PROCESO:	Gestión de Seguridad de la Información
LÍDER DEL PROCESO:	Coordinador de Seguridad de la Información
OBJETIVO:	Establecer un proceso estructurado para la implementación y seguimiento efectivo de los controles de seguridad de la información del Anexo A de la ISO/IEC 27001:2022.
ALCANCE:	Este procedimiento es aplicable a todos los procesos, activos, sistemas y personal involucrados en la gestión de la seguridad de la información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) en Aseguradora ABANK.
DOCUMENTO SOPORTE RELACIONADO:	Matriz de Controles (SIG-6-03-MA) Declaración de Aplicabilidad (SIG-6-04-DOA) Matriz de Riesgos de Seguridad (SIG-6-05-MA)

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
1	Identificación de riesgos relacionados con la seguridad de la información	Se realizará una revisión exhaustiva de todos los procesos críticos de la organización para identificar riesgos relacionados con la seguridad de la información, basados en los controles del anexo A.	Coordinador de seguridad de la información
2	Clasificación de riesgos	Los riesgos identificados se clasificarán de acuerdo con su probabilidad de ocurrencia, su impacto en la organización, y su nivel de riesgo (alto, medio, bajo).	Coordinador de seguridad de la información
3	Selección de controles del Anexo A	Se seleccionarán los controles del Anexo A que sean aplicables a los riesgos identificados. Estoscontroles incluyen medidas de control físico, lógico, y organizativo para mitigar los riesgos.	Coordinador de seguridad de la información

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
4	Tratamiento de riesgos	Se definirán estrategias de tratamiento para cada riesgo, considerando medidas de prevención, mitigación, transferencia o aceptación, conforme a los controles del Anexo A seleccionados.	Coordinador de seguridad de la información
5	Desarrollo de planes de acción	Se elaborarán planes de acción para implementar los controles del Anexo A, con asignación de responsables, plazos, recursos necesarios y métricas para el seguimiento de la implementación.	Coordinador de seguridad de la información
6	Ejecución de controles	Se llevará a cabo la implementación de los controles definidos en los planes de acción, garantizando que se integren de manera efectiva en los procesos de la organización.	Coordinador de seguridad de la información
7	Monitoreo continuo y auditoría interna	Se realizará un monitoreo continuo de los riesgos tratados y de la efectividad de los controles implementados. Se establecerán auditorías internas periódicas para evaluar la conformidad.	Coordinador de seguridad de la información
8	Revisión y actualización del tratamiento de riesgos	Se evaluarán periódicamente los controles implementados y su efectividad, y se actualizarán los planes de acción y controles en función de los cambios en el entorno de la organización.	Coordinador de seguridad de la información
	Fin del Procedimiento		

Proporcionó información:	Ricardo Ramos (Encargado de seguridad de la información y continuidad del negocio)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	COMERCIALIZACIÓN DE SEGUROS	VERSIÓN	FECHA	
			Elaboración	Actualización
		V1.0	17/10/2023	
		CÓDIGO:	SIG-1-1-PRO	

PROCESO:	Comercialización
LÍDER DEL PROCESO:	Gerente comercial
OBJETIVO:	Realizar la comercialización de seguros a través de intermediarios de seguros, y con el apoyo de las diferentes Gerencias comerciales de Aseguradora Abank.
ALCANCE:	Aplica para las etapas de prospección, cotización e implementación inicial de la comercialización a través de intermediarios independientes vinculados Aseguradora Abank.
DOCUMENTO SOPORTE RELACIONADO:	- Pipeline comercial - Bitácora de llamadas - Bitácora de visitas - Manual de niveles de suscripción

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
1	*Recibir propuesta de comercialización de seguros*	El intermediario contacta a la Dirección Comercial para negociar la venta de un seguro, ya sea individual o colectivo. Este contacto puede realizarse por teléfono, correo o presencialmente. Si el intermediario contacta, se sigue al paso 3; de lo contrario, se busca intermediarios en la cartera.	Gerente comercial
2	*Revisar cartera y bases de datos*	El Gerente Comercial revisa bases de datos y carteras para identificar intermediarios potenciales. Se propone a los intermediarios nuevos negocios y se les explica brevemente los beneficios de trabajar con la aseguradora. Si el intermediario está interesado, se continúa; si no, se busca un nuevo intermediario.	Gerente comercial
3	*Reunión inicial con el intermediario*	Se realiza una reunión (virtual o presencial) entre el Gerente Comercial y el intermediario, donde se discuten las necesidades del Cliente y los requisitos generales que buscan en una aseguradora. Se entrega material informativo sobre los productos de la aseguradora.	Gerente comercial

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
		Se registra la visita o llamada en el sistema.	
4	*Solicitar requisitos para cotización*	El Gerente Comercial solicita al intermediario toda la información necesaria para generar una oferta, según el tipo de seguro (individual o colectivo). Se requieren datos como nombre del Cliente, edad, contactos, listado de personas a asegurar, montos, etc.	Gerente comercial
5	Recibir y revisar TDR	El Gerente Comercial recibe el TDR del intermediario y revisa los requisitos, apoyándose en un checklist. Se actualiza el registro de la negociación en un control de negocios ("pipeline"). Si el caso puede ser manejado por Comercial, se analiza internamente; si no, se envía a Suscripción.	Gerente comercial
6	*Realizar análisis de términos*	El Gerente Comercial realiza un análisis detallado de los términos del TDR. Si aplica, se apoya en el área de Suscripción o en los niveles de suscripción autorizados. Si se requiere un análisis más profundo, se envía a Suscripción.	Gerente comercial
7	*Elaboración y envío de oferta*	Tras el análisis, se elabora la oferta de seguro en la plantilla correspondiente. Para seguros individuales, se usa un cotizador web, mientras que para colectivos se utilizan plantillas específicas. La oferta se envía al intermediario por correo electrónico o cualquier medio acordado.	Gerente comercial
8	*Reunión con el Cliente*	El intermediario presenta la oferta al Cliente. Se agenda una reunión presencial o virtual, donde se explican detalles como coberturas, beneficios y condiciones. Se registra el resultado de la reunión y se actualiza el estado en el sistema "pipeline".	Gerente comercial
9	*Negociación y aceptación del Cliente*	El Cliente revisa la oferta y acepta o solicita renegociación. Si la oferta es aceptada, se continúa con la firma de la documentación. Si no, se negocia nuevamente o se da seguimiento para futuras oportunidades.	Intermediario y Gerente Comercial
10	*Firmar documentación y oferta*	Una vez que el Cliente acepta la oferta, se procede a la firma de los documentos legales requeridos (ficha integral, declaración jurada, etc.). El estado de la negociación se actualiza en el sistema "pipeline".	Gerente comercial
11	*Enviar información para suscripción*	Se envía toda la documentación recolectada al área de Suscripción para que se realice el análisis de la póliza. Se asegura que toda la información necesaria esté completa y se adjunta a la solicitud de emisión.	Gerente comercial
12	*Evaluación de satisfacción*	Al finalizar el proceso, se contacta al Cliente para conocer su nivel de satisfacción con respecto a la gestión del seguro. Se envía una encuesta digital o se realiza una llamada telefónica. Los resultados se analizan mensualmente para identificar oportunidades de mejora.	Gerente comercial
	Fin del Procedimiento		

Proporcionó información:	Pedro Antonio (Gerente comercial)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	SUSCRIPCIÓN Y EMISIÓN DE PÓLIZAS DE SEGUROS	VERSIÓN	FECHA	
			Elaboración	Actualización
		V1.0	17/10/2023	
		CÓDIGO:	SIG-1-2-PRO	

PROCESO:	Suscripción de pólizas; Emisión de pólizas
LÍDER DEL PROCESO:	Director técnico
OBJETIVO:	Establecer un proceso claro y efectivo para la suscripción y emisión de pólizas, garantizando la correcta evaluación de riesgos, la transparencia en la comunicación y el cumplimiento de las normativas vigentes, con el fin de proporcionar un servicio de calidad al Cliente.
ALCANCE:	Este procedimiento se aplica a todas las pólizas emitidas por la aseguradora, abarcando desde la recepción de la solicitud hasta el seguimiento post-emisión. Incluye todas las áreas involucradas en el proceso de suscripción y emisión.
DOCUMENTO SOPORTE RELACIONADO:	TDR (Términos de Referencia) Política de Suscripción Normativa de Reaseguro Plantillas de Póliza Manual de Procedimientos de Emisión de Pólizas

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
1	*Recepción de solicitud de póliza*	El área de Suscripción recibe la documentación completa enviada por el Gerente Comercial, que incluye el TDR, información del Cliente y cualquier otro documento requerido. Se verifica que toda la información esté completa.	Suscriptor
2	*Revisión de requisitos*	Se revisan los requisitos establecidos en el TDR. Si hay información faltante, se comunica con el Gerente Comercial para solicitarla. Se registra el estado de la solicitud en el sistema.	Suscriptor
3	*Evaluación de riesgos*	Se realiza un análisis detallado de los riesgos asociados al Cliente y a la cobertura solicitada. Esto incluye la evaluación de datos demográficos, historial de reclamaciones y cualquier factor relevante.	Suscriptor

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
4	*Consulta a reaseguro (si aplica)*	Si el riesgo supera los límites establecidos por la aseguradora, se consulta con el reasegurador para obtener la aprobación. Se prepara un informe con los detalles del riesgo para el reaseguro.	Suscriptor
5	*Elaboración de condiciones y tarifas*	Basándose en la evaluación de riesgos y las políticas internas, se definen las condiciones de la póliza y las tarifas correspondientes. Se utiliza una plantilla estándar para asegurar la coherencia.	Suscriptor
6	*Generación de la póliza*	Se elabora el borrador de la póliza utilizando la información aprobada. Se verifica que todos los detalles, incluidos coberturas, exclusiones y condiciones, estén correctamente reflejados.	Emisor
7	*Revisión interna de la póliza*	El borrador de la póliza se somete a una revisión interna por parte de otros miembros del equipo de Suscripción. Se revisan todos los aspectos para garantizar la precisión y el cumplimiento de las normativas.	Emisor
8	*Aprobación de la póliza*	Una vez revisada, la póliza es presentada a un supervisor o gerente para su aprobación final. Se registra la decisión en el sistema. Si la póliza no es aprobada, se comunican los motivos al equipo de Suscripción.	Director técnico
9	*Emisión de la póliza*	Tras la aprobación, se procede a la emisión oficial de la póliza. Se envía la póliza al Gerente Comercial o directamente al intermediario, junto con cualquier documento adicional necesario.	Emisor
10	*Facturación*	Se genera la factura correspondiente al Cliente, basándose en las tarifas definidas en la póliza. Se envía la factura al Gerente Comercial o al intermediario para su entrega al Cliente.	Emisor
11	*Registro en sistema*	Se registra toda la información relacionada con la póliza emitida en el sistema de gestión de pólizas, incluyendo detalles del Cliente, condiciones, fechas y tarifas.	Emisor
12	*Seguimiento de la póliza*	Se establece un plan de seguimiento para asegurar que el Cliente reciba el servicio adecuado y se mantenga la satisfacción. Se realiza un contacto posterior a la emisión para resolver dudas o consultas.	Emisor
	Fin del Procedimiento		

Proporcionó información:	Juan Carlos Torres (Director técnico)
Procesó información:	Felicia Torres (Analista de procesos)

Aseguradora ABANK	**ATENCIÓN DE RECLAMOS DE SEGUROS**	**VERSIÓN**	**FECHA**	
			Elaboración	Actualización
		V1.0	17/10/2023	
		CÓDIGO:	**SIG-1-2-PRO**	

PROCESO:	Suscripción de pólizas; Emisión de pólizas
LÍDER DEL PROCESO:	Director técnico
OBJETIVO:	Establecer un proceso claro y efectivo para la atención de reclamos de seguros, garantizando una respuesta rápida y adecuada a las necesidades de los asegurados, así como el cumplimiento de las normativas y políticas internas.
ALCANCE:	Este procedimiento aplica a todos los reclamos presentados por los asegurados de la compañía de seguros, desde la recepción inicial hasta la liquidación y cierre del reclamo.
DOCUMENTO SOPORTE RELACIONADO:	Políticas de Atención al Cliente Normativa Interna de Reclamos Formatos de Reclamos Manual de Procedimientos para Ajustadores Plantillas de Notificación

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
1	*Recepción del reclamo*	El área de Atención al Cliente recibe el reclamo del asegurado, ya sea por teléfono, correo electrónico o en persona. Se registran los datos del reclamante y se crea un expediente de reclamo.	Atención al Cliente
2	*Verificación de cobertura*	Se verifica que la póliza esté activa y que el tipo de reclamo esté cubierto por la misma. Se consultan los términos y condiciones de la póliza.	Atención al Cliente

No.	ACTIVIDAD	CÓMO SE HACE	Responsable
3	*Recolección de documentación*	Se solicita al reclamante la documentación necesaria para procesar el reclamo, como informes médicos, fotografías, denuncias policiales, etc. Se especifica un plazo para la entrega de la documentación.	Atención al Cliente
4	*Análisis del reclamo*	Se revisa toda la documentación recibida y se analiza la naturaleza del reclamo. Se evalúa si hay suficiente información para proceder.	Ajustador de Reclamos
5	Investigación del caso	En caso de que se necesite más información, se realiza una investigación adicional. Esto puede incluir entrevistas con testigos, inspecciones del lugar de los hechos y análisis de daños.	Ajustador de Reclamos
6	*Elaboración de informe de reclamo*	Se elabora un informe que resume el análisis realizado y las conclusiones obtenidas. Este informe incluye la recomendación sobre la aprobación o rechazo del reclamo.	Ajustador de Reclamos
7	*Revisión del informe*	El informe de reclamo se somete a revisión por parte del supervisor o gerente del área. Se evalúa la recomendación y se toma una decisión final.	Supervisor de Reclamos
8	*Notificación al asegurado*	Se comunica al asegurado la decisión sobre el reclamo. Si es aprobado, se indican los pasos a seguir para la liquidación del mismo. Si es rechazado, se explican las razones.	Atención al Cliente
9	*Liquidación del reclamo*	En caso de que el reclamo sea aprobado, se procede a la liquidación del mismo. Esto incluye el cálculo del monto a indemnizar y la preparación de los pagos necesarios.	Ajustador de Reclamos
10	*Cierre del reclamo*	Se cierra el expediente del reclamo en el sistema, asegurando que toda la documentación esté completa y que se hayan registrado todos los detalles del proceso.	Ajustador de Reclamos
11	*Seguimiento y feedback*	Se realiza un seguimiento con el asegurado para verificar su satisfacción con el proceso de reclamo y se solicitan comentarios sobre la atención recibida.	Ajustador de Reclamos
	Fin del Procedimiento		

Proporcionó información:	Adonay Petro (Supervisor de reclamos)
Procesó información:	Felicia Torres (Analista de procesos)

APÉNDICE 11. MANUAL DE INTERPRETACIÓN Y APLICACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

MANUAL DE INTERPRETACIÓN Y APLICACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Septiembre 2024

Presentado por:

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

MUÑOZ SOSA, NORA NATHALY

RODAS LAÍNEZ, GUSTAVO MANUEL

Para:

Aseguradora ABANK

INTRODUCCIÓN

En un mundo cada vez más digitalizado y conectado, la información se ha convertido en uno de los activos más valiosos para organizaciones de todos los tamaños y sectores. La confidencialidad, integridad y disponibilidad de los datos son cruciales para garantizar la continuidad de las operaciones, la confianza de los clientes y la competitividad en un mercado globalizado. En este contexto, la norma internacional ISO/IEC 27001:2022 se erige como un faro en el horizonte de la seguridad de la información.

La norma ISO/IEC 27001 es un estándar ampliamente reconocido y adoptado a nivel global para la gestión de la seguridad de la información. Su propósito fundamental es proporcionar un marco sólido y flexible que permita a las organizaciones establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) eficaz. La publicación de la versión 2022 de esta norma representa un paso adelante en la adaptación a las crecientes amenazas cibernéticas y la evolución tecnológica, brindando a las organizaciones las herramientas necesarias para abordar los desafíos del entorno digital actual.

OBJETIVO

Este manual tiene como objetivo servir como una guía completa y de fácil comprensión para la interpretación y aplicación de los controles de seguridad de la información establecidos en la norma ISO/IEC 27001:2022. A través de una exposición detallada y accesible, pretendemos facilitar la comprensión y ejecución de las medidas necesarias para salvaguardar la información crítica de su organización.

ALCANCE

El manual aplica para la interpretación y aplicación genérica de los controles de seguridad de la información según Anexo A de ISO/IEC 27001:2022, en función de Aseguradora ABANK.

#	Tipo de control	Nro.	Control	Descripción
1	Control organizacional	A.5.1	Políticas de seguridad de la información	Las políticas de seguridad de la información de la organización especifican los principios que deben seguir los miembros y las partes interesadas, como los proveedores. Estas políticas deben revisarse periódicamente y actualizarse según sea necesario.

Aplicación: Aseguradora ABANK deberá implementar políticas documentadas obligatorias del estándar, incluidas, por ejemplo, la Política de seguridad de la información, la Política de uso aceptable, la Política de trabajo remoto y la Política de control de acceso, así como varias otras políticas documentadas. registros.

A continuación, se presenta la política de seguridad de la información:

Aseguradora ABANK

1. Propósito

La Política de Seguridad de la Información de Aseguradora ABANK tiene como propósito establecer las directrices y principios fundamentales para proteger la confidencialidad, integridad y disponibilidad de la información en toda la organización. Esta política tiene el objetivo de asegurar que la gestión de la seguridad de la información se lleve a cabo de manera sistemática y coherente en todas las operaciones y niveles de la organización, en conformidad con la norma ISO/IEC 27001:2022.

2. Alcance

Esta política se aplica a todos los empleados, contratistas, y terceros que interactúan con la información de Aseguradora ABANK. Cubre todos los activos de información, incluidos los sistemas de información, documentos en papel, equipos informáticos, redes, y datos alojados en la nube, sin importar su formato o ubicación.

3. Compromiso de la Dirección

La alta dirección de Aseguradora ABANK se compromete a liderar y apoyar activamente la implementación de esta política para garantizar que los objetivos de seguridad de la información se alineen con las metas estratégicas de la organización. La dirección se compromete a proporcionar los recursos necesarios para la implementación, mantenimiento, y mejora continua de la seguridad de la información

4. Principios de Seguridad de la Información

Aseguradora ABANK se compromete a:

- Confidencialidad: Proteger la información contra accesos no autorizados para garantizar que solo las personas debidamente autorizadas tengan acceso a los datos.
- Integridad: Mantener la exactitud y completitud de la información y los métodos de procesamiento.
- Disponibilidad: Asegurar que la información y los servicios asociados estén disponibles cuando se necesiten.

5. Directrices Generales

- Cumplimiento Legal y Normativo: Aseguradora ABANK cumplirá con todas las leyes, regulaciones y normativas aplicables relacionadas con la seguridad de la información.
- Gestión de Riesgos: Se establecerá un proceso continuo para identificar, evaluar y gestionar los riesgos de seguridad de la información, asegurando que estos sean mitigados o gestionados de manera adecuada.
- Política de Acceso: Los accesos a la información y sistemas estarán basados en el principio de "mínimo privilegio" y serán revisados regularmente para mantener la seguridad.
- Protección contra Amenazas: Se implementarán controles técnicos, organizativos y físicos para proteger la información contra amenazas internas y externas.
- Concienciación y Capacitación: Todos los empleados recibirán formación regular sobre seguridad de la información para garantizar que comprendan sus responsabilidades y las prácticas adecuadas.

#	Tipo de control	Nro.	Control	Descripción
6. Comunicación y Concienciación Esta política será comunicada a todos los empleados, contratistas y partes interesadas relevantes. La dirección se asegurará de que todos comprendan la importancia de la seguridad de la información y su papel en la protección de los activos de información de la organización. **7. Revisión y Mejora Continua** La Política de Seguridad de la Información será revisada al menos anualmente o cuando se produzcan cambios significativos en el entorno de negocio, la tecnología o las regulaciones. La revisión garantizará que la política sigue siendo adecuada, efectiva y alineada con los objetivos estratégicos de la organización. **8. Cumplimiento y Sanciones** El incumplimiento de esta política puede resultar en medidas disciplinarias, que incluyen, pero no se limitan a, la suspensión, el despido o acciones legales, dependiendo de la gravedad de la violación. **9. Aprobación** Esta política ha sido aprobada por la alta dirección de Aseguradora ABANK y está en vigor desde agosto 2024 Esta política se revisa anualmente o cuando sea necesario para garantizar que siga siendo adecuada y efectiva para nuestra organización.  Jaime García-Prieto Director Presidente				
2	Control organizacional	A.5.2	Roles y responsabilidades de seguridad de la información	Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
Aplicación: Es importante que Aseguradora ABANK defina y comunique claramente las funciones y responsabilidades de todos los individuos y grupos involucrados en el mantenimiento de la seguridad de sus activos de información. Esto ayuda a garantizar que exista una cadena de responsabilidad clara y que todos comprendan su papel en la protección de la información confidencial. Algunas funciones y responsabilidades comunes en materia de seguridad de la información incluyen: • Director de seguridad de la información: es responsable de la estrategia general de seguridad de la información, la política y la gestión diaria del programa de seguridad de la información de la organización. • Equipo de seguridad de la información: este equipo es responsable de implementar y mantener los controles de seguridad de la información de la organización, como firewalls, sistemas de detección de intrusos y controles de acceso. • Administradores de sistemas: estas personas son responsables de mantener la seguridad de los sistemas y redes de la organización, incluida la aplicación de parches y la actualización de sistemas y aplicaciones. • Administradores de red: estas personas son responsables de administrar la infraestructura de red de la organización, incluidos enrutadores, conmutadores y otros equipos de red. • Usuarios finales: todos los empleados dentro de una organización son responsables de cumplir con las políticas y prácticas de seguridad de la información de la organización y de informar cualquier incidente o inquietud de seguridad al personal apropiado.				

#	Tipo de control	Nro.	Control	Descripción
3	Control organizacional	A.5.3	Segregación de deberes	Al delegar subtareas a diferentes personas, este principio crea un sistema de controles y equilibrios que puede reducir la probabilidad de que ocurran errores y fraudes. El control está diseñado para evitar que una sola persona pueda cometer, ocultar y justificar acciones indebidas, reduciendo así el riesgo de fraude y error. También evita que una sola persona anule los controles de seguridad de la información.
Aplicación: Aseguradora ABANK puede requerir que diferentes individuos o grupos sean responsables de diferentes aspectos del proceso de seguridad, como configurar cuentas de usuario, otorgar acceso a recursos y monitorear registros de actividad. Separar estas responsabilidades hace que sea más difícil para un solo individuo comprometer la seguridad del sistema. La segregación de funciones es un principio importante en la seguridad de la información que ayuda a reducir el riesgo de errores y fraude y a garantizar la integridad y seguridad de los activos de información de una organización.				
4	Control organizacional	A.5.4	Responsabilidades de gestión	La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
Aplicación: En el contexto de la seguridad de la información, las responsabilidades de gestión se refieren a las tareas y deberes específicos de los que es responsable el personal de gestión dentro de Aseguradora ABANK para garantizar la seguridad y protección de los activos de información. Estas responsabilidades pueden variar dependiendo del tamaño y la estructura de la organización, así como de las necesidades y requisitos de seguridad específicos de la organización.				
5	Control organizacional	A.5.5	Contacto con autoridades	La organización deberá establecer y mantener contacto con las autoridades pertinentes.
Aplicación: Las fuerzas del orden, los organismos reguladores y las autoridades supervisoras desempeñan un papel enorme a la hora de ayudar a Aseguradora ABANK a prevenir incidentes cibernéticos. Además, ayudan a recuperarse de incidentes cibernéticos en caso de que una organización se vea afectada por uno. Por lo tanto, las organizaciones deben establecer y mantener contacto con estas entidades.				
6	Control organizacional	A.5.6	Contacto con grupos de interés especial	La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
Aplicación: Suscribirse a revistas o boletines semanales, mensuales o trimestrales sobre seguridad de la información es una buena práctica. Fuentes como los boletines informativos de SANS Information Security, Knowbe4, Security Weekly, Infosecurity Magazine, etc., son excelentes fuentes a considerar.				

#	Tipo de control	Nro.	Control	Descripción
7	Control organizacional	A.5.7	Inteligencia de amenazas	Este control está diseñado para ayudar a las organizaciones a comprender su entorno de amenazas. Esto es para que puedan determinar las acciones adecuadas para mantener la seguridad de la información en función de las amenazas que identifiquen.
Aplicación: La inteligencia sobre amenazas podría ser una experiencia intimidante para Aseguradora ABANK. Lógicamente no es sencillo y requiere tanto de recursos humanos como de equipamiento y de un esfuerzo continuo. Sin embargo, una vez que la organización establece su escenario, resulta ser una de las prácticas más beneficiosas y de apoyo. Se recomienda dividir la inteligencia sobre amenazas en tres capas: estratégica, operativa y táctica. La inteligencia estratégica sobre amenazas se centra en comprender áreas como tipos de atacantes, tipos de ataques, etc. La inteligencia operativa debe centrarse principalmente en los detalles relacionados con el ataque específico, incluidos indicadores técnicos, fuentes importantes de ataque, etc. Finalmente, el enfoque de la inteligencia táctica debe ser contemplar los métodos de ataque, herramientas y tecnologías involucradas.				
8	Control organizacional	A.5.8	Seguridad de la información en la gestión de proyectos.	El control A.5.8 tiene como objetivo garantizar que los riesgos de seguridad de la información relacionados con los proyectos y los entregables se gestionen de manera efectiva durante la ejecución del proyecto
Aplicación: Las medidas de seguridad difieren de un proyecto a otro dependiendo de la naturaleza del mismo. No obstante, la idoneidad de las consideraciones y actividades de seguridad de la información debe ser evaluada en etapas predefinidas por una persona u organismo rector apropiado, como el Comité Directivo del Proyecto. Además, se deben definir responsabilidades y autoridades para la seguridad de la información relevante para el proyecto.				
9	Control organizacional	A.5.9	Inventario de información y otros activos asociados	Requiere que las organizaciones identifiquen y documenten los activos importantes para sus operaciones y los riesgos asociados, y tomen medidas para protegerlos.
Aplicación: Aseguradora ABANK debe identificar todos los activos tangibles y no tangibles dentro de la organización. Los métodos y procedimientos de gestión de activos difieren de una empresa a otra; la organización debe adoptar un enfoque adecuado para sí misma. Si bien algunas organizaciones prefieren crear un registro de activos utilizando aplicaciones de oficina básicas como Excel, otras empresas pueden optar por utilizar un software de gestión de activos más dedicado y detallado. Independientemente del método que adopte, una organización debe asegurarse de que los activos se registren con los detalles adecuados, se determine el propietario del activo y el registro de activos se actualice periódicamente. Además, es crucial para una organización que el inventario de soporte no contenga datos duplicados y que los datos estén clasificados.				
10	Control organizacional	A.5.10	Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
Aplicación: Estas reglas y pautas generalmente se describen en una política de uso aceptable (PUA), que es un documento que especifica los tipos de actividades que están permitidas y prohibidas cuando se utilizan los recursos de información de la organización. Una política de uso aceptable puede incluir una variedad de disposiciones, tales como como: • Prohibiciones sobre el uso de los activos de información de la organización con fines ilegales o poco éticos. • Reglas para proteger la seguridad y confidencialidad de la información sensible.				

#	Tipo de control	Nro.	Control	Descripción
• Restricciones al uso de los activos de información de la organización para fines personales. • Requisitos para reportar incidentes o inquietudes de seguridad. • Directrices para el uso del correo electrónico, internet y otros sistemas de comunicación de la organización. Las políticas de uso aceptable son una parte importante del programa de seguridad de la información de una organización, ya que ayudan a garantizar que los activos de información de la organización se utilicen de manera responsable y ética, y que se mantengan la seguridad y confidencialidad de esos activos. al establecer y hacer cumplir pautas claras de uso aceptable, las organizaciones pueden ayudar a proteger sus activos de información y mantener la confianza de los clientes, socios y otras partes interesadas.				
11	Control organizacional	A.5.11	Devolución de activos	El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización en su posesión al momento del cambio o terminación de su empleo, contrato o acuerdo.
Aplicación: Lo mejor para Aseguradora ABANK es tener un proceso formal para poder retener y proteger los activos relacionados con la empresa cuando un empleado deja su puesto. En la mayoría de los casos, es más fácil rastrear y retener dispositivos como terminales de usuario, almacenamiento portátil, claves token, tarjetas inteligentes, etc. Sin embargo, algunas organizaciones luchan por garantizar que los activos digitales de la empresa se hayan conservado tras la terminación del empleo, especialmente cuando los empleados utilizan sus propios dispositivos para acceder a los activos digitales de la empresa. Este control sugiere que las organizaciones deberían tener formalmente un proceso para evitar que los empleados accedan a los activos relacionados con la empresa tras su despido.				
12	Control organizacional	A.5.12	Clasificación de la información	La información se clasificará de acuerdo con la seguridad de la información. Necesidades de la organización basadas en la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
Aplicación: La clasificación de la información puede ser una práctica desalentadora. La mayoría de las organizaciones luchan por comprender el nivel requerido de acceso a los empleados dentro de la organización, así como a otras partes interesadas fuera de la organización. Mantener el equilibrio adecuado es un aspecto crítico de la clasificación de la información. Demasiado secreto viola las reglas de disponibilidad, mientras que una apertura innecesaria o excesiva podría comprometer la confidencialidad y la integridad de la información. Por lo tanto, la organización necesita gestionar la clasificación de la información mediante un buen proceso. Es beneficioso para la organización redactar una política de control de acceso que defina los niveles de clasificación, las personas responsables de manejar la información confidencial, etc.				
13	Control organizacional	A.5.13	Etiquetado de información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación adoptado por la organización.
Aplicación: Para implementar mejor este control, Aseguradora ABANK deberá pensar en formas de reconocer fácilmente la información etiquetándola. La organización debe adoptar un método para manejar su información. Por ejemplo, utiliza técnicas de etiquetado como etiquetas físicas, encabezados, pies de página, marcas de agua, etc.				

#	Tipo de control	Nro.	Control	Descripción
14	Control organizacional	A.5.14	Transferencia de información	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y con otras partes.
Aplicación: El control de transferencia de información sugiere que Aseguradora ABANK debe contar con controles para garantizar que se eviten incidentes como la interceptación, el acceso no autorizado, el desvío, la modificación y la destrucción. Es importante que se cuente con reglas, procedimientos y acuerdos adecuados al transferir cualquier tipo de información tanto en forma física como digital. Este control considera tres tipos de transferencia de información: Física, Electrónica y Verbal. Además, proporciona detalles sobre cómo se debe manejar cada uno de estos métodos y los pasos necesarios a seguir.				
15	Control organizacional	A.5.15	Control de acceso	Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros activos asociados en función de los requisitos de seguridad empresarial.
Aplicación: • Acceso físico a personas en el local, • Determinar el nivel de acceso a recursos tanto físicos como digitales. esto podría lograrse considerando los principios de autorización, necesidad de uso y necesidad de conocer, • Segregación de deberes, • Gestión de derechos de acceso y logging.				
16	Control organizacional	A.5.16	Gestión de identidad	El propósito del Anexo A 5.16 es describir cómo una organización puede identificar quién (usuarios, grupos de usuarios) o qué (aplicaciones, sistemas y dispositivos) está accediendo a datos o activos de TI en un momento dado, y cómo se les otorga acceso a esas identidades.
Aplicación: La gestión de la identidad es una práctica crucial. Requiere registrar, monitorear y revisar los derechos de acceso de individuos y sistemas a los activos y recursos asociados de Aseguradora ABANK. La gestión de identidad incluye tanto a humanos como a otros sistemas digitales que interactúan con los recursos de la organización. Si bien la interacción humana es un concepto sencillo de entender, otras interacciones del sistema podrían ser difíciles de contemplar. La interacción del sistema puede incluir casos como aplicaciones de terceros que acceden a los recursos de la empresa para proporcionar o facilitar un servicio. Por ejemplo, un sistema de terceros podría necesitar acceso a documentos cruciales para realizar copias de seguridad diarias, semanales o mensuales. Es una práctica recomendada para una organización mapear los derechos de acceso de las interacciones, ya sean humanos u otros sistemas.				
17	Control organizacional	A.5.17	Información de autenticación	La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autorización.

<table>
<tr><th>#</th><th>Tipo de control</th><th>Nro.</th><th>Control</th><th>Descripción</th></tr>
<tr><td colspan="5">Aplicación: La gestión de la autenticación es una práctica importante para Aseguradora ABANK. Uno de los métodos más eficaces contra las violaciones de la seguridad de la información es eludir el proceso de autenticación. Por lo tanto, es crucial que la organización considere aspectos como:

• Contraseñas y números de identificación personal (pin) únicos e imposibles de adivinar generados automáticamente.
• Procedimientos para identificar y verificar los métodos de autenticación temporal y permanente.
• La información de autenticación se transfiere a una ubicación segura de forma segura.
• Dispositivos y métodos de autenticación dudosos que se eliminarán del sistema

Es beneficioso para la organización registrar los detalles de los métodos de autenticación en un documento bien estructurado. Identificar las responsabilidades de los usuarios y todos los métodos de autenticación relevantes.</td></tr>
<tr><td>18</td><td>Control organizacional</td><td>A.5.18</td><td>Derechos de acceso</td><td>Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.</td></tr>
<tr><td colspan="5">Aplicación: Si bien el otorgamiento de derechos de acceso a información crítica parece ser la primera vez que un usuario ingresa al sistema, se recomienda revisar, modificar y, si es necesario, eliminar el derecho de acceso del usuario a largo plazo. Este es un error común de las organizaciones que no olvidan o no revisan y modifican los derechos de acceso de los usuarios, lo que facilita el terreno para que ocurran numerosos incidentes de seguridad de la información. Por ejemplo, los empleados descontentos que se degradan de un puesto superior a un puesto inferior en Aseguradora ABANK podrían causar daños a la información crítica a la que tienen acceso utilizando sus derechos de acceso escalados. De manera similar, un atacante podría apuntar a información confidencial de la organización utilizando una persona con una posición inferior, pero con derechos de acceso escalados dentro de la organización. Por lo tanto, el aprovisionamiento, revisión, modificación y eliminación de derechos de acceso dentro de la política de control de acceso es un aspecto considerable de la organización.</td></tr>
<tr><td>19</td><td>Control organizacional</td><td>A.5.19</td><td>Seguridad de la información en las relaciones con los proveedores</td><td>Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.</td></tr>
<tr><td colspan="5">Aplicación: En una relación con un proveedor, es importante que Aseguradora ABANK se asegure de que su información esté protegida contra riesgos como violaciones de datos, acceso no autorizado o pérdida de confidencialidad. Esto se puede lograr mediante una combinación de medidas técnicas y organizativas y mediante el establecimiento de políticas y procedimientos claros para el manejo y protección de la información. Algunas medidas específicas que las organizaciones pueden tomar para mejorar la seguridad de la información en las relaciones con los proveedores incluyen:

• Realizar la debida diligencia con los proveedores para garantizar que cuentan con las medidas de seguridad adecuadas para proteger la información de la organización.
• Establecer políticas y procedimientos claros para el manejo y protección de la información sensible o confidencial de la organización.
• Implementar medidas técnicas como cifrado y controles de acceso para proteger la información de la organización.
• Revisar y actualizar periódicamente las medidas de seguridad de la información para garantizar que son efectivas y satisfacen las necesidades de la organización.
• Brindar capacitación y educación a empleados y proveedores sobre las mejores prácticas de seguridad de la información.</td></tr>
</table>

#	Tipo de control	Nro.	Control	Descripción
20	Control organizacional	A.5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con estos.

Aplicación: Al abordar la seguridad de la información en los acuerdos con proveedores, es importante que Aseguradora ABANK defina claramente sus expectativas y requisitos para proteger la información sensible o confidencial. Esto se puede hacer mediante la inclusión de cláusulas específicas en el acuerdo que describan las responsabilidades de ambas partes en relación con la seguridad de la información. Algunas cláusulas específicas que las organizaciones pueden considerar incluir en los acuerdos con proveedores para abordar la seguridad de la información son:

- Cláusula de protección y confidencialidad de datos: esta cláusula describe las responsabilidades del proveedor en relación con la protección de la información sensible o confidencial de la organización. puede incluir requisitos para que el proveedor implemente medidas técnicas y organizativas apropiadas para proteger la información y garantizar que todos los empleados o contratistas que tengan acceso a la información estén sujetos a acuerdos de confidencialidad.
- Cláusula de notificación de violación de datos: esta cláusula describe los procedimientos que debe seguir el proveedor en caso de violación de datos o acceso no autorizado a la información de la organización. esto puede incluir requisitos para que el proveedor notifique rápidamente a la organización sobre dichos incidentes y coopere con cualquier investigación o esfuerzo de remediación.
- Cláusula de eliminación de datos: esta cláusula describe los procedimientos que debe seguir el proveedor a la hora de deshacerse de cualquier soporte físico o electrónico que contenga información sensible o confidencial de la organización. esto puede incluir requisitos para que el proveedor borre o destruya de forma segura la información de una manera que cumpla con los estándares de la industria.

21	Control organizacional	A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Se deben definir e implementar procesos y procedimientos para gestionarlos riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.

Aplicación: La cadena de suministro de TIC incluye todas las entidades involucradas en la producción, distribución y mantenimiento de productos y servicios de TIC. Esto puede incluir fabricantes, distribuidores, revendedores, proveedores de servicios y cualquier subcontratista o subproveedor que puedan utilizar. Para gestionar la seguridad de la información en la cadena de suministro de TIC, Aseguradora ABANK debe considerar los riesgos asociados con el trabajo con proveedores de TIC e implementar medidas apropiadas para mitigar esos riesgos. Esto puede incluir realizar la debida diligencia con los proveedores para garantizar que cuenten con las medidas de seguridad adecuadas, establecer políticas y procedimientos claros para manejar y proteger información sensible o confidencial e implementar medidas técnicas como cifrado y controles de acceso. Las organizaciones también deben revisar y actualizar sus medidas de seguridad de la información para garantizar que siguen siendo efectivas y satisfacen las necesidades de la organización. Además, deben brindar capacitación y educación a los empleados y proveedores sobre las mejores prácticas de seguridad de la información para ayudar a garantizar que todas las partes involucradas en la cadena de suministro de TIC comprendan sus responsabilidades y sean capaces de proteger la información de la organización de manera efectiva.

22	Control organizacional	A.5.22	Supervisión, revisión y cambio de gestión de servicios de proveedores	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: Estas actividades ayudan a las organizaciones a garantizar que sus proveedores cumplan con sus expectativas y requisitos y que cualquier problema o inquietud se identifique y aborde de manera oportuna. Para monitorear, revisar y gestionar de manera efectiva los cambios en los servicios de los proveedores, Aseguradora ABANK puede tomar los siguientes pasos: • Defina métricas de desempeño claras: establezca métricas de desempeño claras que se utilizarán para evaluar el desempeño del proveedor y comunicar estas métricas al proveedor. esto puede ayudar a garantizar que el proveedor cumpla con las expectativas y requisitos de la organización. • Revisar periódicamente el desempeño de los proveedores: programe revisiones periódicas del desempeño del proveedor utilizando las métricas establecidas. esto se puede hacer a través de reuniones, informes u otros medios de comunicación. • Identifique y aborde cualquier problema o inquietud: durante el proceso de revisión, identifique cualquier problema o inquietud que pueda surgir y trabaje con el proveedor para abordarlo. esto puede implicar la implementación de cambios en los servicios o procesos del proveedor. • Comunicar cambios: comunicar claramente cualquier cambio que se realice en los servicios o procesos del proveedor y garantizar que el proveedor comprenda el impacto de estos cambios en su desempeño y las necesidades de la organización.				
23	Control organizacional	A.5.23	Seguridad de la información para el uso de servicios en la nube	Este control describe los procesos que se requieren para la adquisición, el uso, la gestión y la salida de los servicios en la nube, en relación con los requisitos únicos de seguridad de la información de la organización.
Aplicación: La seguridad de la información para el uso de servicios en la nube debería ser una política específica de alto nivel. Es posible que algunas organizaciones prefieran fusionar esta política como parte de su política de infraestructura o mantenerla separada. Cualquiera de los métodos es aceptable si definen y comunican específicamente el uso de los servicios en la nube. Una organización debe especificar y expresar claramente su intención con respecto al uso de los servicios en la nube. Si los servicios en la nube construirían la red de la organización total o parcialmente. La política de uso de servicios en la nube puede incluir, entre otros, los aspectos que se mencionan a continuación: • Requisitos relevantes de seguridad de la información asociados con el uso de servicios en la nube, • Especificar y comprender los controles de seguridad de la información gestionados por el proveedor de servicios en la nube. • Obtención de garantía del control de seguridad de la información implementado por un proveedor de servicios en la nube. • Planificar, diseñar y gestionar interfaces y cambios en los servicios cuando una organización utiliza múltiples proveedores de servicios. • Se manejaría una definición clara de los incidentes en la nube. • Especificar el cambio y detener los servicios en la nube, incluida una estrategia de salida.				
24	Control organizacional	A.5.24	Incidente de seguridad de la información planificación y preparación de la gestión racionar	La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando la información, procesos, roles y responsabilidades de gestión de incidentes de seguridad.
Aplicación: Un procedimiento de gestión de incidentes es uno de los aspectos más críticos de un Sistema de Gestión de Seguridad de la Información. Sin un plan adecuado de gestión de incidentes, una organización enfrentaría graves desafíos si ocurriera un incidente. Razonablemente, cuando una organización tiene una definición clara de un incidente, si ocurre el mismo incidente o uno similar, las personas responsables de la organización deben saber qué hacer a continuación. Por lo tanto, una organización debe contar con un documento de gestión de incidentes adecuado y bien estructurado. Además, no				

#	Tipo de control	Nro.	Control	Descripción
se trata sólo de tener un documento de gestión de incidentes, sino que es fundamental practicar y garantizar que el documento sea probado en el campo de batalla.				
25	Control organizacional	A.5.25	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes.
Aplicación: Razonablemente, considerar todo como un incidente significa que Aseguradora ABANK necesita diseñar e implementar contramedidas de seguridad para todos aquellos incidentes registrados en la lista. Puede parecer una buena práctica, pero a largo plazo, la organización ha estado pagando por numerosos roles dentro de la empresa y gastado grandes sumas de dinero para protegerse contra un incidente que tal vez nunca suceda. Por otro lado, muchas organizaciones son víctimas de incidentes de seguridad de la información debido a que subestiman el ataque genuino que aborda la naturaleza de su negocio.				
26	Control organizacional	A.5.26	Respuesta a la seguridad de la información incidentes	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
Aplicación: La implementación de una respuesta a incidentes de seguridad de la información normalmente implica varios pasos: • Desarrollar un plan de respuesta a incidentes: Aseguradora ABANK debe contar con un plan formal de respuesta a incidentes que describa los procedimientos y roles para responder a diferentes tipos de incidentes. este plan debe revisarse y probarse para garantizar que esté actualizado y sea eficaz. • Capacitar al personal: todos los empleados deben recibir capacitación sobre el plan de respuesta a incidentes y sus funciones en la respuesta a incidentes. la capacitación y los simulacros periódicos pueden ayudar al personal a prepararse para responder de manera rápida y efectiva. • Establecer equipos de respuesta a incidentes: Aseguradora ABANK debe contar con equipos de respuesta a incidentes dedicados, formados por personas con las habilidades técnicas y organizativas necesarias para responder a los incidentes. • Identificar y priorizar activos: las organizaciones deben identificar y priorizar los activos que son más críticos para sus operaciones para que puedan protegerse mejor y restaurarse rápidamente en caso de un incidente. • Implementar monitoreo y detección: las organizaciones deben implementar mecanismos de monitoreo y detección, como sistemas de detección de intrusiones, para detectar posibles incidentes lo más rápido posible. • Establecer procedimientos de respuesta a incidentes: las organizaciones deben establecer procedimientos para responder a diferentes tipos de incidentes, como violaciones de datos, intrusiones en la red y ataques de denegación de servicio. • Comunicarse con las partes interesadas: Aseguradora ABANK deben establecer procedimientos de comunicación claros con las partes interesadas, como clientes y socios, para mantenerlos informados sobre los incidentes y las acciones que se están tomando para abordarlos. • Revisar y mejorar: finalmente, las organizaciones deben revisar y mejorar periódicamente sus procesos de respuesta a incidentes, utilizando las lecciones aprendidas de incidentes pasados para mejorar su postura general de seguridad.				
27	Control organizacional	A.5.27	Aprender de los incidentes de seguridad de la información	El conocimiento obtenido de los incidentes se utilizará para fortalecer y mejorar los controles de seguridad de la información.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: Una organización no necesita esperar y ser víctima de un ataque para comprender la naturaleza del desastre. Mantener una lista de posibles ataques y aprender de los errores de los demás es una práctica vital. Al final, más vale prevenir que curar. Por lo tanto, es crucial establecer y mantener una lista de ataques pasados que aún son efectivos en el ámbito de la seguridad de la información. Sin embargo, la lista no debería ser exhaustiva, ya que algunos ataques contra la última tecnología podrían quedar obsoletos.				
28	Control organizacional	A.5.28	Recolección de evidencia	La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
Aplicación: La recopilación de pruebas es un ámbito muy amplio en el espectro de la ciberseguridad. Más específicamente, la ciencia forense es el campo que resume el proceso de recopilación de pruebas. La recopilación de pruebas puede diferir de una empresa a otra, según el tamaño y la naturaleza. No obstante, cada empresa debe contar con un procedimiento de recopilación de pruebas para los peores escenarios. El documento de recopilación de evidencia es un documento más operativo y técnico que requiere aportes de especialistas en seguridad de la información. Especialmente los especialistas del campo de la ciencia forense digital tendrían mejores conocimientos sobre el tema.				
29	Control organizacional	A.5.29	Seguridad de la información durante la interrupción	La organización debe planificar cómo mantener la seguridad de la información a un nivel apropiado durante la interrupción.
Aplicación: Este control debe estar incluido en su Plan de Continuidad del Negocio (BCP). La falta de documentos BCP es una no conformidad importante. Aseguradora ABANK debe considerar un plan alternativo a niveles estratégico, operativo y táctico. Un BCP bien establecido permite una organización resiliente; la falta de un plan alternativo da como resultado graves interrupciones que dañan la confidencialidad, la integridad y la disponibilidad de la seguridad de la información en todos los niveles. Se recomienda encarecidamente que una empresa pruebe la eficacia del BCP.				
30	Control organizacional	A.5.30	Preparación de las TIC para la continuidad del negocio	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio.
Aplicación: El análisis de impacto empresarial debe utilizarse para evaluar e identificar tipos de impacto y criterios para evaluar los impactos a lo largo del tiempo resultantes de la interrupción de las actividades comerciales que entregan productos y servicios. Es beneficioso para una organización establecer e implementar un documento de análisis de impacto empresarial que determine los objetivos de tiempo de recuperación y los recursos necesarios para mitigar un ataque. Una vez que este completado, los objetivos finalizados deben incluirse brevemente en la Política de Continuidad del Negocio para reflejar mejor una La posición estratégica, operativa y táctica de la organización durante un ataque. La organización debe garantizar que: • Hay recursos adecuados disponibles • Las personas a cargo si ocurre un ataque están bien determinadas. además, los pasos a seguir como curso de acción se identifican y comunican claramente.				
31	Control organizacional	A.5.31	Requisitos legales, estatutarias, reglamentarias y contractuales	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.
Aplicación: Los requisitos legales para la seguridad de la información están establecidos por leyes nacionales e internacionales que definen cómo las organizaciones deben manejar y proteger la información confidencial. Los requisitos legales son leyes o regulaciones establecidas por gobiernos nacionales o locales. Estos requisitos pueden variar ampliamente según la jurisdicción y pueden incluir requisitos específicos para la protección de ciertos tipos de información, como datos				

#	Tipo de control	Nro.	Control	Descripción
financieros o personales. Los requisitos regulatorios para la seguridad de la información los establecen agencias reguladoras específicas de la industria. Estos requisitos pueden ser obligatorios o voluntarios, y pueden establecerse para garantizar que las organizaciones cumplan con estándares específicos de la industria para la protección de información confidencial.				
32	Control organizacional	A.5.32	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
Aplicación: La propiedad intelectual (PI) se refiere a creaciones de la mente, como invenciones, obras literarias y artísticas, símbolos, nombres e imágenes utilizadas en el comercio. Los derechos de propiedad intelectual son derechos legales otorgados a individuos u organizaciones para proteger sus creaciones y evitar que otros las utilicen sin permiso. A continuación, se detallan algunos pasos que las organizaciones pueden tomar para implementar pautas de propiedad intelectual (PI) en sus prácticas de seguridad de la información: • Identificar y evaluar los activos de propiedad intelectual: el primer paso para proteger la propiedad intelectual es identificar qué activos de propiedad intelectual tiene la organización, incluidas patentes, marcas comerciales, derechos de autor y secretos comerciales. es importante evaluar el valor y la importancia de estos activos y determinar el nivel de protección que requieren. • Desarrollar e implementar controles apropiados: con base en la evaluación de los activos de propiedad intelectual, la organización debe desarrollar e implementar controles apropiados para proteger estos activos. esto puede incluir medidas como cifrado, controles de acceso y almacenamiento y transmisión seguros de información confidencial. • Establecer políticas y procedimientos: desarrollar e implementar políticas y procedimientos relacionados con la protección de la propiedad intelectual puede ayudar a garantizar que todos los empleados y partes interesadas comprendan sus responsabilidades y obligaciones con respecto a la propiedad intelectual. esto puede incluir pautas para el manejo y uso de información confidencial, así como procedimientos para responder a posibles violaciones de propiedad intelectual. • Proporcionar formación y concienciación: garantizar que todos los empleados y partes interesadas conozcan las directrices de propiedad intelectual de la organización es crucial para su implementación efectiva. proporcionar capacitación y esfuerzos continuos de concientización puede ayudar a garantizar que todos comprendan la importancia de la protección de la propiedad intelectual y su papel en el mantenimiento de la seguridad de la información confidencial. • Monitorear y revisar los controles: es importante monitorear y revisar periódicamente la efectividad de los controles de protección de la propiedad intelectual para garantizar que sigan siendo apropiados y efectivos. esto puede incluir la realización de evaluaciones de riesgos periódicas y la implementación de controles adicionales según sea necesario.				
33	Control organizacional	A.5.33	Protección de registros	Los registros se protegerán contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
Aplicación: Si bien el establecimiento y desarrollo de registros es una parte vital del negocio, la protección de los datos contra el acceso, modificación o eliminación no autorizados desempeña el mismo nivel de importancia, así como la atención de los niveles operativos, tácticos y de alta dirección dentro de una organización.				
34	Control organizacional	A.5.34	Privacidad y protección de Información Identificable de una Persona (PII)	PII es cualquier dato que se pueda utilizar para identificar a una persona, por ejemplo: licencia de conducir, información financiera, registros médicos, entre otro.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: La implementación de las siguientes medidas puede ayudar a proteger la PII y mantenerla segura dentro de su organización. • Implemente controles de acceso para limitar el acceso a la PPI solo a aquellos que la necesitan para realizar sus tareas laborales. • Cifre la PPI cuando se almacene o transmita para evitar el acceso no autorizado. • Utilice servidores y redes seguros para almacenar y transmitir PPI. • Actualice periódicamente el software y las aplicaciones de seguridad para protegerse contra las últimas amenazas. • Implemente políticas sólidas de contraseñas para evitar el acceso no autorizado a la PPI. • Capacite a los empleados sobre cómo manejar y proteger la PPI. • Implementar auditorías y monitoreo periódicos para detectar y prevenir el acceso no autorizado a la PPI. • Tenga un plan implementado para responder a filtraciones de datos e incidentes relacionados con PPI. • Considere implementar autenticación de dos factores para acceder a sistemas y redes que contienen PPI.				
35	Control organizacional	A.5.35	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
Aplicación: Aseguradora ABANK debería llevar a cabo esto de forma regular. Las revisiones generalmente se inician anualmente. Los puntos a revisar incluyen, entre otros: • Leyes y regulaciones que afectan el cambio organizacional. • Se producen incidentes importantes • La organización implementa un cambio importante en el negocio actual o agrega un nuevo negocio en el alcance. • Organización que utiliza o produce nuevos productos o servicios. • Cambios importantes en las políticas y procedimientos de la organización. • También se requiere que la organización establezca un programa de auditoría que tenga en cuenta las auditorías internas y externas.				
36	Control organizacional	A.5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	El cumplimiento de la política de seguridad de la información de la organización, las reglas y los estándares específicos del tema se revisará periódicamente.
Aplicación: Hay varios pasos que puede seguir para revisar los requisitos de seguridad de la información definidos en una política de seguridad de la información: • Familiarícese con la política: comience leyendo la política detenidamente y asegurándose de comprender todos los requisitos descritos. • Identifique cualquier brecha: busque áreas donde la política no proporciona suficiente orientación o puede que no esté claro cómo cumplir con los requisitos. • Consulte con las partes interesadas relevantes: hable con otros miembros de la organización, como personal de ti, asesores legales y líderes empresariales, para obtener sus opiniones sobre la política y cualquier brecha o inquietud que tengan. • Revise las mejores prácticas de la industria: consulte otras pautas o estándares de la industria para ver si tienen				

#	Tipo de control	Nro.	Control	Descripción
recomendaciones o requisitos que no estén cubiertos en la política. • Realizar una evaluación de riesgos: utilice un proceso de evaluación de riesgos para identificar posibles vulnerabilidades o riesgos que no se abordan en la política. • Haga recomendaciones de mejora: basándose en su revisión, haga recomendaciones para cualquier cambio o adición a la política que pueda ser necesaria para garantizar el cumplimiento y proteger los activos de información de la organización.				
37	Control organizacional	A.5.37	Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.
Aplicación: Se deben preparar procedimientos documentados para las actividades operativas de la organización asociadas con la seguridad de la información, por ejemplo: • Todos los empleados deben utilizar la misma forma para realizar una actividad común. • Se deben tener en cuenta las tareas que podrían introducir nuevos riesgos. • Las funciones y responsabilidades de la persona que asuma un nuevo puesto o actividad deberán estar bien definidas y establecidas.				
38	Control de personas	A.6.1	Poner en pantalla	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
Aplicación: Se pueden utilizar varios métodos para realizar controles de personal en seguridad de la información: • Verificación de antecedentes: esto implica verificar el empleo anterior, la educación y el historial personal de una persona para evaluar su confiabilidad e idoneidad para acceder a información confidencial. • Procesos de autorización de seguridad: para puestos que requieren acceso a información clasificada, es posible que los empleados deban pasar por un proceso de autorización de seguridad, que puede incluir una verificación exhaustiva de antecedentes, una prueba de polígrafo y otras medidas de seguridad. • Verificaciones de referencias: pedir referencias de empleadores anteriores, colegas u otras personas que hayan trabajado con la persona puede brindar información sobre su carácter y hábitos de trabajo. • Evaluaciones psicológicas: en algunos casos, una organización puede exigir que los empleados se sometan a una evaluación psicológica para evaluar su estabilidad emocional y su capacidad para manejar información confidencial. • Pruebas de drogas: algunas organizaciones pueden exigir que los empleados se sometan a pruebas de drogas para garantizar que no estén bajo la influencia de sustancias que puedan comprometer su juicio o su capacidad para manejar información confidencial. • Capacitación y educación: brindar a los empleados capacitación y educación sobre protocolos y mejores prácticas de seguridad de la información puede ayudar a garantizar que sean conscientes de la importancia de proteger datos confidenciales y los riesgos asociados con su manejo inadecuado.				
39	Control de personas	A.6.2	Términos y condiciones de empleo	Los acuerdos contractuales de trabajo deberán expresar el personal y responsabilidades de la organización para la seguridad de la información.

<table>
<tr><th>#</th><th>Tipo de control</th><th>Nro.</th><th>Control</th><th>Descripción</th></tr>
<tr><td colspan="5">Aplicación: Algunos consejos, entre otros, para implementar los mejores términos y condiciones de empleo en seguridad de la información:

• Describa claramente las expectativas y responsabilidades de los empleados con respecto a la seguridad de la información. esto debe incluir información sobre el manejo de datos confidenciales, el uso de contraseñas seguras y la notificación de posibles amenazas o violaciones de seguridad.
• Incluir consecuencias por violar protocolos o políticas de seguridad de la información, como medidas disciplinarias o despido.
• Revisar y actualizar periódicamente los términos y condiciones de empleo para garantizar que estén actualizados y en línea con las mejores prácticas actuales.
• Proporcionar a los empleados capacitación y educación sobre protocolos y mejores prácticas de seguridad de la información.
• Asegúrese de que todos los empleados reconozcan y firmen los términos y condiciones de empleo, indicando que los comprenden y aceptan.
• Contar con un sistema para monitorear y hacer cumplir periódicamente los términos y condiciones de empleo para garantizar su cumplimiento.</td></tr>
<tr><td>40</td><td>Control de personas</td><td>A.6.3</td><td>Concientización, educación y capacitación en seguridad de la información</td><td>El personal de la organización y las partes interesadas relevantes recibirán concientización, educación y capacitación apropiadas sobre la seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral.</td></tr>
<tr><td colspan="5">Aplicación: Se pueden utilizar varios métodos para brindar concientización, educación y capacitación sobre seguridad de la información, que incluyen:

• Capacitación presencial: implica brindar a los empleados capacitación presencial sobre temas de seguridad de la información a través de conferencias grupales o instrucción individualizada.
• Capacitación en línea: esto se puede realizar a través de seminarios web, cursos en línea u otras formas de aprendizaje electrónico. esto permite a los empleados acceder a materiales de capacitación a su propio ritmo y puede ser una opción conveniente para organizaciones con una fuerza laboral dispersa.
• Campañas de concientización sobre la seguridad: son campañas continuas que brindan a los empleados información sobre las amenazas a la seguridad de la información y las mejores prácticas a través de una variedad de canales, como correos electrónicos, carteles o redes sociales.
• Los ejercicios de simulación implican simular una violación de seguridad u otro incidente de seguridad para enseñar a los empleados cómo responder adecuadamente.
• Capacitación en el trabajo: esto implica brindar a los empleados capacitación y orientación mientras realizan sus tareas laborales, permitiéndoles aprender sobre seguridad de la información en un entorno práctico.
• No existe un enfoque único para brindar concientización, educación y capacitación sobre seguridad de la información, y el mejor método dependerá de las necesidades y recursos de la organización. a menudo resulta beneficioso utilizar una combinación de estos métodos para garantizar que los empleados reciban una educación completa sobre seguridad de la información.</td></tr>
<tr><td>41</td><td>Control de personas</td><td>A.6.4</td><td>Proceso Disciplinario</td><td>Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.</td></tr>
</table>

#	Tipo de control	Nro.	Control	Descripción
Aplicación: Implementar un proceso disciplinario en seguridad de la información implica varios pasos: • Desarrollar y comunicar claramente políticas de seguridad de la información: las organizaciones deben tener políticas bien definidas que describan lo que se espera de los empleados en términos de seguridad de la información. estas políticas deben ser fácilmente accesibles y comunicadas a todos los empleados. • Proporcionar formación y educación: los empleados deben recibir formación sobre las políticas de seguridad de la información de la organización y las posibles consecuencias de violarlas. esto puede incluir programas regulares de capacitación y concientización. • Cree un plan de respuesta a incidentes: las organizaciones deben contar con un plan sobre cómo responder e investigar incidentes de seguridad de la información. esto debe incluir funciones y responsabilidades claras para los diferentes miembros de la organización. • Investigar incidentes: cuando ocurre un incidente, se debe investigar de inmediato para determinar la causa y quién es el responsable. • Tomar medidas disciplinarias: con base en los hallazgos de la investigación, se deben tomar medidas disciplinarias apropiadas contra aquellos que violen las políticas de seguridad de la información de la organización. esto podría incluir una advertencia, suspensión o terminación del empleo. • Revisar y actualizar políticas: las organizaciones deben revisar y actualizar periódicamente sus políticas de seguridad de la información para garantizar que estén actualizadas y sean efectivas. Es importante señalar que los procesos disciplinarios deben implementarse de manera justa y consistente y deben estar alineados con los estándares legales y éticos de la empresa.				
42	Control de personas	A.6.5	Responsabilidades después de la terminación o cambio de empleo	Responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la finalización o el cambio de empleo se definirán, ejecutarán y comunicarán al personal pertinente y otras partes interesadas.
Aplicación: Cuando un empleado es despedido o su empleo cambia, existen varias responsabilidades que la organización debe tener en cuenta para garantizar la protección continua de la seguridad de su información: • Revocar el acceso: la organización debe revocar inmediatamente el acceso del empleado a todos los sistemas, redes y datos de la empresa para evitar el acceso no autorizado. esto incluye deshabilitar cuentas de usuario, acceso al correo electrónico y aplicaciones y servicios en la nube de la empresa. • Recopilación de propiedad de la empresa: la organización debe recopilar del empleado todos los dispositivos propiedad de la empresa, como computadoras portátiles, teléfonos inteligentes y tokens de seguridad, para evitar cualquier uso indebido de la información de la empresa. • Realización de entrevistas de salida: las organizaciones deben realizar entrevistas de salida con el empleado saliente para discutir cualquier problema o inquietud relacionada con el acceso del empleado a la información de la empresa y para garantizar que el empleado comprenda sus obligaciones según las políticas de seguridad de la información de la empresa. • Revisión de registros de auditoría: las organizaciones deben revisar los registros de auditoría para detectar cualquier actividad sospechosa o violación de datos que pueda haber ocurrido durante el mandato del empleado. • Cambio de contraseñas y claves: las organizaciones deben cambiar todas las contraseñas y claves de cifrado que se compartieron con el empleado para evitar el acceso no autorizado a la información de la empresa. • Revisión del acceso de terceros: las organizaciones también deben revisar y revocar cualquier acceso de terceros a la información de la empresa que se haya otorgado a través de la cuenta del ex empleado, como redes sociales, almacenamiento en la nube y otras plataformas. • Obligación legal: las organizaciones deben ser conscientes de sus obligaciones legales con respecto a la protección de datos personales y deben considerar consultar con un asesor legal con respecto a la retención y destrucción de los datos de los empleados después de la terminación o cambio de empleo.				

#	Tipo de control	Nro.	Control	Descripción
43	Control de personas	A.6.6	Confidencialidad o no divulgación de acuerdos	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deberán ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

Aplicación: La implementación de acuerdos de confidencialidad o no divulgación (NDA) en seguridad de la información implica varios pasos:

- Identifique la información que se debe proteger: el primer paso para implementar una NDA es determinar qué información debe protegerse. esto puede incluir secretos comerciales, datos personales, propiedad intelectual y otra información confidencial.
- Desarrolle una plantilla de NDA estándar: cree una plantilla estándar para NDA que pueda usarse con diferentes partes. la plantilla debe incluir los tipos de información protegida, las responsabilidades de las partes involucradas y las consecuencias por violar el acuerdo.
- Comunicar la NDA a las partes relevantes: una vez desarrollada la NDA, se debe comunicar a todas las partes relevantes, como empleados, contratistas y socios comerciales. debe quedar claro que la NDA es un documento legalmente vinculante y que las partes deben cumplir con sus términos.
- Obtenga firmas: obtenga copias firmadas de la NDA de todas las partes relevantes para asegurarse de que conocen y han aceptado los términos del acuerdo.
- Capacite y eduque a los empleados: brinde capacitación y educación a los empleados sobre la importancia de proteger la información confidencial y el papel que desempeñan las NDA en el mantenimiento de la confidencialidad de esta información.
- Supervisar y hacer cumplir el cumplimiento: las organizaciones deben supervisar el cumplimiento de los NDA y tomar las medidas adecuadas si se produce una infracción. esto puede incluir revocar el acceso a información confidencial, rescindir contratos y emprender acciones legales si es necesario.
- Revisar y actualizar: revise y actualice la plantilla y las políticas de NDA periódicamente para garantizar que cumpla con las leyes y regulaciones de la jurisdicción en la que se utiliza y que proteja de manera efectiva la información que se supone que debe proteger.

44	Control de personas	A.6.7	Trabajo remoto	Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.

Aplicación: Implementar el trabajo remoto en seguridad de la información implica varios pasos:

- Desarrollar y comunicar una política de trabajo remoto: Aseguradora ABANK deben desarrollar y comunicar una política que describa las expectativas y pautas para el trabajo remoto, incluido el acceso a los sistemas y datos de la empresa, y el uso de dispositivos personales.
- Acceso remoto seguro: se debe garantizar que el acceso remoto a los sistemas y datos de la empresa sea seguro mediante la implementación de medidas como redes privadas virtuales (VPN), autenticación de dos factores y cifrado.
- Proporcionar dispositivos y software seguros: deben proporcionar a los empleados dispositivos seguros, como computadoras portátiles con software de cifrado y soluciones de infraestructura de escritorio virtual (VDI), y garantizar que todo el software y las aplicaciones utilizadas por los empleados estén actualizados y sean seguros.
- Monitorear y proteger los datos de la empresa: deben monitorear y proteger los datos de la empresa implementando soluciones de prevención de pérdida de datos (DLP) y verificando periódicamente si hay actividades sospechosas o violaciones de datos.
- Capacitar y educar a los empleados: deben brindar capacitación y educación periódicas a los empleados sobre la importancia de la seguridad de la información y cómo mantener la seguridad mientras trabajan de forma remota.
- Establecer un plan de respuesta a incidentes: se deben contar con un plan sobre cómo responder e investigar

#	Tipo de control	Nro.	Control	Descripción
incidentes de seguridad de la información y garantizar que los empleados conozcan el plan y su papel en él. • Revisar y actualizar políticas: Se debe revisar y actualizar periódicamente sus políticas y procedimientos de trabajo remoto para garantizar que estén actualizados y sean eficaces para proteger la seguridad de la información de la empresa. Es importante señalar que las políticas de trabajo remoto deben implementarse de manera flexible y adaptable a las necesidades de los empleados y deben estar alineadas con los estándares legales y éticos de la empresa.				
45	Control de personas	A.6.8	Reporte de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de canales de manera oportuna.
Aplicación: Los informes de eventos de seguridad de la información normalmente incluyen los siguientes pasos: • Identificación: identificar y detectar incidentes o eventos de seguridad, como accesos no autorizados, violaciones de datos o fallas del sistema. • Documentación: documentar los detalles del incidente o evento, incluida la fecha, hora y gravedad del incidente, así como cualquier información relevante sobre la causa y el impacto del incidente. • Análisis: analizar el incidente o evento para determinar la causa y el impacto, e identificar cualquier vulnerabilidad o debilidad que pueda haber contribuido al incidente. • Notificación: notificar a las personas o grupos apropiados dentro de la organización, como el equipo de respuesta a incidentes, la administración y el personal de ti, sobre el incidente o evento. • Respuesta: implementar una respuesta al incidente o evento, como contener el incidente, erradicar la amenaza y restaurar sistemas y datos. • Informes: informar del incidente o evento a las partes apropiadas, como organismos reguladores o autoridades policiales, de conformidad con los requisitos legales. • Revisión: revisar el incidente o evento e implementar los cambios necesarios en el plan, las políticas y los procedimientos de respuesta a incidentes de la organización para prevenir incidentes similares en el futuro. Los informes de eventos de seguridad de la información ayudan a las organizaciones a responder rápidamente y mitigar los incidentes de seguridad, minimizar el impacto de las violaciones de seguridad y mantener el cumplimiento de los requisitos reglamentarios.				
46	Control físico	A.7.1	Perímetros físicos de seguridad	Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.
Aplicación: La mayoría de las organizaciones ignoran la seguridad física porque dependen de la seguridad general mantenida por las fuerzas del orden. Sin embargo, para una organización es importante conocer su posición en el espectro general de amenazas. Esto significa que dependiendo de la naturaleza, tamaño y tipo de industria; toda empresa tiene un adversario de algún tipo. De hecho, las fuerzas del orden son responsables de proteger el entorno físico de un país, ciudad, pueblo y espacio empresarial. Sin embargo, es un mito percibir que las organizaciones encargadas de hacer cumplir la ley tienen sus ojos las 24 horas del día, los 7 días de la semana, digamos, en un edificio de oficinas compartido. Por lo tanto, es necesario que la organización considere redactar una política de seguridad física y procedimientos relacionados si es necesario. Algunas organizaciones incluyen políticas de seguridad física dentro de la política de seguridad de la información. Esta es una elección subjetiva. Dependiendo de la naturaleza y el tamaño del negocio, esto podría lograrse. Para una organización más grande con mayor espacio de oficina y área de cobertura, se recomienda preparar un conjunto separado de documentos de seguridad física para incluir las políticas, procedimientos y pautas. El documento de seguridad física podrá contener: • Perímetros de un edificio o sitio • Especificación de las instalaciones de procesamiento de información. • Medidas de seguridad requeridas en cerraduras, techos, ventanas, escritorios, áreas de entrega, etc.				

#	Tipo de control	Nro.	Control	Descripción
• Pruebas y monitoreo de sistemas de alarma.				
47	Control físico	A.7.2	Entrada física	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.
Aplicación: Los detalles de la Entrada Física podrían ser parte del documento de seguridad física o de seguridad de la información. Los detalles deben incluir: • Restringir el acceso a sitios y edificios al personal autorizado. el proceso para la gestión del acceso a considerar • Mantener un libro de registro o un registro de auditoría electrónico de todos los accesos y proteger todos los registros. • Configurar el área de recepción asegurándose de que no quede desatendida. • Establecer e implementar mecanismos técnicos para la gestión del acceso a lugares de información sensible. esto se puede lograr introduciendo el uso de tarjetas inteligentes, cerraduras con pin y puertas de doble seguridad. • Garantizar que los empleados y visitantes tengan identificaciones/insignias distintas y visibles. lo más importante es desarrollar una cultura de pedir a personas desconocidas que deambulen por las instalaciones. • Separar físicamente los paquetes y correos entrantes y salientes.				
48	Control físico	A.7.3	Protección de oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.
Aplicación: Cuando se trata de proteger oficinas, habitaciones e instalaciones, existen varias pautas que se deben considerar. Éstas incluyen: • Implementar políticas y procedimientos estrictos de control de acceso, como exigir a los empleados que utilicen tarjetas de acceso o contraseñas para acceder a determinadas áreas. • Instalar cerraduras en puertas y ventanas y revisarlas y mantenerlas periódicamente para garantizar que sean seguras. • Usar cámaras de seguridad y otros sistemas de vigilancia para monitorear las instalaciones e identificar posibles violaciones de seguridad. • Contratar guardias de seguridad capacitados para patrullar las instalaciones y responder a cualquier incidente de seguridad. • Usar barreras físicas como portones, cercas y bolardos para evitar que vehículos no autorizados ingresen a las instalaciones. • Realizar periódicamente auditorías y revisiones de seguridad para identificar posibles vulnerabilidades y tomar medidas para abordarlas. • Proporcionar a los empleados formación sobre protocolos y procedimientos de seguridad y recordarles periódicamente la importancia de seguir estas directrices. • Establecer planes y procedimientos de respuesta de emergencia en caso de una violación de la seguridad u otra emergencia. en general, la clave para proteger las oficinas, salas e instalaciones es contar con un plan de seguridad integral y revisarlo y actualizarlo periódicamente para garantizar que sea efectivo.				
49	Control físico	A.7.4	Monitoreo de seguridad física	Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: Para monitorear y vigilar las instalaciones físicas, puede utilizar una combinación de cámaras de seguridad, alarmas y otros equipos de vigilancia. Se pueden colocar cámaras de seguridad en todas las instalaciones para proporcionar un monitoreo visual del área en tiempo real. Estas cámaras se pueden conectar a una red y monitorear de forma remota, lo que le permite vigilar las instalaciones incluso cuando no esté en el sitio. Las alarmas también se pueden usar para monitorear las instalaciones y alertarlo sobre posibles violaciones de seguridad. Estas alarmas pueden activarse mediante sensores de movimiento, sensores de puertas o ventanas u otros tipos de sensores y pueden alertarlo sobre posibles amenazas para que pueda tomar las medidas adecuadas. Además de las cámaras y alarmas de seguridad, también puede utilizar otros tipos de vigilancia. equipos, tales como sistemas de control de acceso, para monitorear y controlar el acceso a las instalaciones. Esto puede ayudar a evitar que personas no autorizadas ingresen a las instalaciones y potencialmente comprometan la seguridad. En general, el monitoreo y la vigilancia de las instalaciones físicas implican el uso de una combinación de diferentes tecnologías y sistemas de seguridad para proporcionar monitoreo y protección en tiempo real contra amenazas potenciales.				
50	Control físico	A.7.5	Protección contra amenazas físicas y ambientales.	Protección contra amenazas físicas y ambientales, tales como desastres y otras amenazas físicas intencionales o no intencionales a la infraestructura.
Aplicación: La protección contra amenazas físicas y ambientales, como los desastres naturales, es un aspecto importante de la preparación para emergencias. Algunas estrategias para protegerse contra este tipo de amenazas incluyen: • Construir o modernizar estructuras para que sean más resistentes a desastres naturales, como terremotos o inundaciones. esto puede incluir reforzar cimientos y paredes, instalar ventanas resistentes a roturas y utilizar otras medidas estructurales para hacer que los edificios sean más resistentes a los daños. una buena práctica es comprobar la evaluación gubernamental de la zona utilizando sitios como gov.uk. • Desarrollar e implementar planes de evacuación para que las personas sepan adónde ir y qué hacer en caso de un desastre natural. esto puede incluir identificar rutas de evacuación seguras, establecer refugios de emergencia y coordinar con las autoridades locales para proporcionar transporte y otro tipo de asistencia a los evacuados. • Abastecerse de suministros esenciales, como alimentos, agua y medicamentos, en caso de una emergencia. esto puede ayudar a las personas a sobrevivir durante unos días o más sin acceso a recursos externos. • Educar a las personas sobre los riesgos de los desastres naturales y cómo prepararse para ellos. esto puede incluir proporcionar información sobre los tipos de desastres que son comunes en un área en particular y enseñar a las personas cómo identificar las señales de advertencia de un desastre inminente. • En general, la protección contra amenazas físicas y ambientales requiere una combinación de medidas físicas, como códigos de construcción y planes de evacuación, y preparación individual, como tener un kit de emergencia abastecido.				
51	Control físico	A.7.6	Trabajar en áreas seguras	Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.
Aplicación: Trabajar en un área de oficina segura es importante para proteger la información confidencial y mantener la seguridad de los empleados de Aseguradora ABANK. Algunas estrategias para crear un área de oficina segura incluyen: • Instalar cámaras de seguridad y otros sistemas de monitoreo para realizar un seguimiento de quién entra y sale de la oficina. esto puede ayudar a identificar posibles violaciones de seguridad y proporcionar un registro de las actividades en la oficina. • Usar cerraduras seguras y sistemas de control de acceso para restringir el acceso a áreas sensibles de la oficina. esto puede incluir el uso de tarjetas de acceso o escáneres biométricos para permitir que solo el personal autorizado ingrese a ciertas partes de la oficina. • Implementar protocolos de seguridad, como exigir a los empleados que usen tarjetas de identificación o se sometan a controles de seguridad al ingresar a la oficina. esto puede ayudar a evitar que personas no autorizadas accedan a la oficina. • Capacitar periódicamente a los empleados sobre procedimientos y protocolos de seguridad para que sepan cómo identificar y responder a posibles amenazas a la seguridad. esto puede incluir capacitación sobre cómo detectar posibles violaciones de seguridad, cómo informar actividades sospechosas y cómo evacuar la oficina en caso de				

#	Tipo de control	Nro.	Control	Descripción
una emergencia. En general, crear un área de oficina segura requiere una combinación de medidas de seguridad física y capacitación y concientización de los empleados. al implementar estas estrategias, las empresas pueden ayudar a proteger su información confidencial y garantizar la seguridad de sus empleados.				
52	Control físico	A.7.7	Escritorio y pantalla despejados	Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.
Aplicación: Un "escritorio despejado" significa eliminar cualquier desorden o elemento innecesario de su escritorio para crear un espacio de trabajo limpio y organizado. Esto podría incluir papel, bolígrafos, tazas de café o cualquier otro elemento que no sea esencial para su trabajo actual. "Borrar pantalla" generalmente se refiere a borrar la pantalla de una computadora u otro dispositivo electrónico. Esto podría implicar cerrar todos los programas y ventanas abiertos o simplemente regresar a la pantalla de inicio o al escritorio. Limpiar la pantalla puede ayudar a ordenar su espacio de trabajo y hacer que sea más fácil concentrarse en la tarea. Para practicar más estos conceptos, puede intentar incorporarlos a su rutina diaria. Por ejemplo, podrías acostumbrarte a comenzar cada día con un escritorio y una pantalla despejados, o podrías tomar descansos regulares a lo largo del día para ordenar tu espacio de trabajo y reenfocar tu atención. Además, puedes intentar experimentar con diferentes estrategias y técnicas para Encontrar lo que funciona mejor para usted.				
53	Control físico	A.7.8	Emplazamiento y protección de equipos	El equipo se colocará de forma segura y protegida.
• Aplicación: A continuación, se presentan algunos puntos a considerar al proteger la tecnología y otros dispositivos físicos en la seguridad de la información: • Implementar medidas de seguridad física: esto puede incluir cosas como cerraduras, sistemas de control de acceso y cámaras de vigilancia para evitar el acceso no autorizado a la tecnología y los dispositivos. • Utilice controles ambientales: esto puede incluir controles de temperatura y humedad para proteger la tecnología y los dispositivos contra daños debidos a temperaturas extremas u otras condiciones ambientales. • Implementar mantenimiento y monitoreo regulares: esto puede ayudar a garantizar que la tecnología y los dispositivos funcionen correctamente y que cualquier problema potencial se identifique y solucione antes de que cause algún daño. • Utilice fuentes de energía seguras: esto puede ayudar a proteger contra sobretensiones y otros problemas relacionados con la energía que podrían dañar la tecnología y los dispositivos. • Implementar procedimientos de eliminación seguros: esto puede ayudar a evitar que personas no autorizadas accedan a información confidencial cuando la tecnología y los dispositivos ya no estén en uso. • Implementar protocolos de seguridad para el uso de la tecnología y los dispositivos: esto puede incluir cosas como exigir contraseñas seguras e implementar controles de acceso para evitar el acceso no autorizado a la tecnología y los dispositivos.				
54	Control físico	A.7.9	Seguridad de los activos fuera de las instalaciones	Se protegerán los activos fuera del sitio.
Aplicación: Hay varias medidas que las organizaciones pueden tomar para proteger los dispositivos que almacenan o procesan información fuera de las instalaciones de la organización: • Cifre los datos en los dispositivos: esto puede ayudar a proteger los datos contra el acceso de personas no autorizadas, incluso si el dispositivo se pierde o es robado. • Utilice contraseñas y métodos de autenticación seguros: esto puede ayudar a evitar el acceso no autorizado a los dispositivos y a los datos que contienen. • Utilice redes seguras al acceder a los dispositivos de forma remota: esto puede ayudar a evitar que personas no				

#	Tipo de control	Nro.	Control	Descripción
autorizadas intercepten los datos que se transmiten a través de la red. • Implemente controles de acceso estrictos: esto puede ayudar a garantizar que solo las personas autorizadas tengan acceso a los dispositivos y a los datos que contienen. • Haga una copia de seguridad periódica de los datos de los dispositivos: esto puede ayudar a proteger contra la pérdida de datos en caso de una falla del dispositivo u otro problema. • Supervise los dispositivos en busca de signos de violaciones de seguridad: esto puede ayudar a identificar posibles problemas de seguridad y tomar medidas para abordarlos antes de que causen algún daño.				
55	Control físico	A.7.10	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
Aplicación: A continuación, se detallan algunos pasos que las organizaciones pueden seguir para administrar medios de almacenamiento extraíbles en seguridad de la información. • Desarrollar e implementar políticas y procedimientos para el uso de medios de almacenamiento extraíbles. estos deben especificar quién está autorizado a utilizar los medios, cómo deben usarse y cómo deben almacenarse y manipularse. • Cifre los datos en los medios de almacenamiento extraíbles. esto puede ayudar a proteger los datos contra el acceso de personas no autorizadas, incluso si los medios se pierden o son robados. • Utilice contraseñas seguras y métodos de autenticación para acceder a los datos en los medios de almacenamiento extraíbles. esto puede ayudar a evitar el acceso no autorizado a los datos. • Actualice periódicamente el software de seguridad en los medios de almacenamiento extraíbles. esto puede ayudar a proteger contra las últimas amenazas a la seguridad. • Supervise el uso de medios de almacenamiento extraíbles y realice un seguimiento de quién los utiliza. esto puede ayudar a identificar posibles problemas de seguridad y tomar medidas para solucionarlos antes de que causen algún daño. • Haga una copia de seguridad periódica de los datos en los medios de almacenamiento extraíbles. esto puede ayudar a proteger contra la pérdida de datos en caso de falla del dispositivo u otro problema. • Implemente estrictos controles de acceso a los medios de almacenamiento extraíbles. esto puede ayudar a garantizar que sólo las personas autorizadas tengan acceso a los datos de los medios.				
56	Control físico	A.7.11	Utilidades de apoyo	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
Aplicación: Para organizar servicios públicos que respalden las instalaciones de procesamiento de información, Aseguradora ABANK puede seguir los siguientes pasos: • Identificar las utilidades específicas que se necesitan para soportar las instalaciones de procesamiento de información. esto puede incluir electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado. • Desarrollar un plan sobre cómo se proporcionará cada una de estas utilidades a las instalaciones de procesamiento de información. esto puede implicar trabajar con empresas de servicios públicos para garantizar que exista la infraestructura necesaria y que las instalaciones tengan acceso a los servicios públicos que necesitan. • Implemente el plan, asegurándose de seguir todas las leyes y regulaciones relevantes. esto puede implicar la instalación de la infraestructura necesaria, como líneas eléctricas y equipos de telecomunicaciones, y la celebración de contratos con proveedores de servicios públicos.				

#	Tipo de control	Nro.	Control	Descripción
• Supervisar los servicios públicos para garantizar que estén funcionando correctamente y que las instalaciones de procesamiento de información tengan acceso a los servicios públicos que necesitan. esto puede implicar comprobar periódicamente la infraestructura y los equipos y supervisar el uso y el consumo. • Tome medidas correctivas si se identifica algún problema. esto puede implicar reparar o reemplazar equipos, ajustar contratos con proveedores de servicios públicos o implementar nuevas políticas y procedimientos para garantizar que las instalaciones de procesamiento de información tengan acceso a los servicios públicos necesarios.				
57	Control físico	A.7.12	Seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.
Aplicación: Hay varias pautas a considerar al implementar la seguridad del cableado en un sistema de seguridad de la información. Algunas de estas pautas incluyen: • Seguridad física: implica proteger los cables y otros componentes físicos de la red para evitar el acceso no autorizado. esto puede incluir medidas como el uso de candados para cables, encerrar cables en conductos protectores y asegurar físicamente los puntos de acceso a la red. • Cifrado: el uso de cables cifrados puede ayudar a prevenir la interceptación de datos y proteger la confidencialidad de la información transmitida a través de la red. • Inspecciones y mantenimiento periódicos: la inspección y el mantenimiento periódicos de los cables pueden ayudar a garantizar que estén en buen estado de funcionamiento y pueden ayudar a identificar posibles vulnerabilidades de seguridad. • Controles de acceso: la implementación de controles de acceso puede ayudar a prevenir el acceso no autorizado a la red y proteger los datos transmitidos a través de los cables. esto puede incluir medidas como exigir autenticación para acceder a la red y usar listas de control de acceso para restringir el acceso a usuarios o grupos específicos. • Protección contra incendios: la implementación de medidas de protección contra incendios puede ayudar a prevenir daños a los cables y otros componentes físicos de la red. esto puede incluir medidas como el uso de materiales ignífugos y la instalación de sistemas de extinción de incendios. • Recuperación ante desastres: contar con un plan de recuperación ante desastres puede ayudar a garantizar que la red permanezca operativa incluso en caso de un desastre. esto puede incluir medidas como realizar copias de seguridad de los datos periódicamente y contar con sistemas redundantes para proporcionar conectividad de respaldo en caso de una interrupción.				
58	Control físico	A.7.13	Mantenimiento de equipo	El equipo se mantendrá correctamente para garantizar la disponibilidad, la integridad confidencialidad de la información.
Aplicación: Existen varias pautas recomendadas para el mantenimiento de equipos en seguridad de la información. Algunas de estas pautas incluyen: • Políticas y procedimientos de seguridad: tener políticas y procedimientos de seguridad claros y bien definidos puede ayudar a garantizar que la red permanezca segura y que todos los empleados sean conscientes de sus responsabilidades cuando se trata de mantener la seguridad de la red. es importante revisar y actualizar periódicamente estas políticas y procedimientos para garantizar que sigan siendo relevantes y eficaces. • Inspecciones y limpieza periódicas: inspeccionar y limpiar periódicamente los componentes de hardware de la red puede ayudar a garantizar que estén en buen estado de funcionamiento y ayudar a prevenir vulnerabilidades de seguridad. esto puede incluir tareas como limpiar el polvo y los residuos del hardware, verificar si hay signos de daño físico y probar la funcionalidad del equipo. • Pruebas y monitoreo: probar y monitorear periódicamente la red puede ayudar a identificar posibles vulnerabilidades de seguridad y garantizar que la red esté funcionando correctamente. esto puede incluir tareas como realizar pruebas de penetración periódicas, monitorear el tráfico de la red en busca de signos de actividad sospechosa y usar herramientas como sistemas de detección de intrusiones para monitorear posibles amenazas a				

#	Tipo de control	Nro.	Control	Descripción
la seguridad. • Copias de seguridad de datos: realizar copias de seguridad de los datos con regularidad puede ayudar a garantizar que no se pierdan en caso de un desastre u otro evento imprevisto. es importante contar con un sólido plan de respaldo y recuperación ante desastres para proteger los datos en la red.				
59	Control físico	A.7.14	Eliminación segura o reutilización de equipos	Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
Aplicación: Existen varias pautas estándar para la eliminación segura o la reutilización de equipos en seguridad de la información. Algunas de estas pautas incluyen: • Documentación: es importante mantener registros de la eliminación o reutilización del equipo, incluidos detalles como la fecha y el método de eliminación, la persona responsable de la eliminación y cualquier otra información relevante. esta documentación se puede utilizar para demostrar el cumplimiento de las políticas y regulaciones de seguridad y puede ayudar a garantizar que la eliminación o reutilización del equipo se realice de manera segura y responsable. • Borrado de datos: antes de desechar o reutilizar el equipo, es importante borrar de forma segura los datos almacenados en el equipo. esto se puede hacer utilizando herramientas de software especializadas que sobrescriben los datos del equipo varias veces, haciendo imposible recuperarlos. • Destrucción física: en algunos casos, puede ser necesario destruir físicamente el equipo para evitar que pueda ser reutilizado. esto puede incluir tareas como destruir discos duros, triturar discos y destruir otros componentes de hardware. • Eliminación adecuada: es importante eliminar adecuadamente el equipo para evitar daños al medio ambiente. esto puede incluir reciclar o donar el equipo, si es posible, o eliminarlo de acuerdo con las leyes y regulaciones locales.				
60	Controles tecnológicos	A.8.1	Dispositivos de punto final de usuario	Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.
Aplicación: La implementación de dispositivos terminales de usuario en la seguridad de la información se puede realizar de varias maneras, entre ellas: • Gestión de dispositivos: establecer políticas y procedimientos para la gestión de dispositivos terminales de usuario, incluida la gestión de inventario, actualizaciones de software y configuraciones de seguridad. • Control de acceso: implementar controles de acceso para garantizar que solo los usuarios autorizados puedan acceder a la red y a los datos confidenciales. esto puede incluir el uso de métodos de autenticación como contraseñas, datos biométricos y autenticación multifactor. • Cifrado: cifrado de datos almacenados en los dispositivos finales del usuario para protegerlos del acceso no autorizado en caso de pérdida o robo del dispositivo. • Antivirus y antimalware: instalar y mantener software antivirus y antimalware actualizado para proteger los dispositivos terminales de los usuarios contra malware y otro software malicioso. • Capacitación en seguridad: brinde capacitación sobre concientización sobre seguridad a los usuarios para educarlos sobre la importancia de la seguridad y cómo proteger sus dispositivos y datos. • Segmentación de red: segmentar la red para restringir el acceso y el movimiento de dispositivos terminales y evitar el movimiento lateral de amenazas dentro de la red.				

#	Tipo de control	Nro.	Control	Descripción
• Monitoreo regular: monitorear periódicamente los dispositivos terminales para detectar y responder a incidentes de seguridad. Es importante señalar que la implementación de estos controles requiere una combinación de medidas técnicas y administrativas y requerirá mantenimiento y monitoreo continuos.				
61	Controles tecnológicos	A.8.2	Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.
Aplicación: Estos usuarios o sistemas privilegiados tienen más acceso y control que los usuarios normales y, como tales, sus acciones y acceso deben ser monitoreados y controlados de cerca para minimizar el riesgo de acceso no autorizado o uso indebido. Ejemplos de derechos de acceso privilegiados incluyen: • Cuentas de administrador en una computadora o red. • Acceso root en un sistema unix o linux, windows y plataformas en la nube. • Acceso a datos sensibles como información financiera o información personal. • La capacidad de instalar software, realizar cambios de configuración o acceder a archivos confidenciales del sistema. Es importante limitar la cantidad de personas que tienen derechos de acceso privilegiados y revisar y revocar el acceso periódicamente según sea necesario. además, es importante implementar controles de acceso y autenticación sólidos para garantizar que solo las personas autorizadas puedan acceder a los recursos privilegiados y que todos los intentos de acceso privilegiado se registren y auditen. la implementación de soluciones de gestión de acceso privilegiado también es una buena práctica para monitorear y controlar acceso privilegiado, incluye características como autenticación multifactor, monitoreo en tiempo real, administración de sesiones y aprovisionamiento de acceso automatizado.				
62	Controles tecnológicos	A.8.3	Restricción de acceso a la información	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.
Aplicación: El objetivo es garantizar que solo personas o sistemas autorizados puedan acceder a la información y que la información permanezca segura y confidencial. Esto se puede lograr implementando una variedad de controles de seguridad, tales como: • Controles de acceso: implementar mecanismos de autenticación y autorización, como id de usuario y contraseñas, para garantizar que solo las personas autorizadas puedan acceder a la información. • Cifrado de datos: cifrar la información para protegerla del acceso no autorizado en caso de que sea robada o interceptada. • Clasificación de datos: clasificar la información en función de su sensibilidad e implementar diferentes niveles de protección en consecuencia. • Prevención de fuga de datos (DLP): implementación de soluciones DLP para monitorear y controlar el flujo de datos confidenciales, tanto dentro como fuera de la organización. Es importante señalar que la restricción del acceso a la información es un proceso continuo y requiere revisión y mantenimiento periódicos para garantizar que los controles sigan siendo efectivos. además, es importante implementar en Aseguradora ABANK principio de privilegio mínimo, que garantice que las personas solo tengan acceso a la información y los recursos necesarios para realizar su trabajo. esto ayuda a reducir el riesgo de uso indebido accidental o intencional de la información.				

#	Tipo de control	Nro.	Control	Descripción
63	Controles tecnológicos	A.8.4	Acceso al código fuente	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.

Aplicación: El acceso al código fuente también plantea una serie de riesgos de seguridad, como:

- El acceso no autorizado o la modificación del código, que podría dar lugar a la introducción de vulnerabilidades de seguridad o funcionalidades maliciosas.
- Distribución del código sin la licencia o el permiso adecuados, lo que podría generar problemas legales o pérdida de ingresos.
- Para mitigar estos riesgos, las organizaciones pueden implementar varios controles, tales como:
- Controles de acceso: implementar mecanismos de autenticación y autorización para garantizar que solo las personas autorizadas puedan acceder al código fuente.
- Firma de código: firmar el código con una firma digital para garantizar que el código no haya sido modificado y proporcionar un medio para identificar al autor o editor.
- Revisión del código: hacer que un equipo de expertos en seguridad revise el código en busca de posibles vulnerabilidades de seguridad y haga recomendaciones para abordarlas.

También es importante que las organizaciones establezcan políticas y procedimientos para la gestión y distribución del código fuente, incluidas pautas de acceso y uso, así como para informar cualquier posible problema de seguridad.

64	Controles tecnológicos	A.8.5	Autenticación segura	Se implementarán tecnologías y procedimientos de autenticación seguros basado en las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.

Aplicación: El objetivo es garantizar que solo las personas o sistemas autorizados puedan acceder a una red, sistema o aplicación, y que sean quienes dicen ser. Los factores de autenticación generalmente se clasifican en tres tipos:

- Algo que el usuario sepa, como una contraseña o pin.
- Algo que tenga el usuario, como un token de seguridad o una tarjeta inteligente.
- Algo que es el usuario, como una huella dactilar o un reconocimiento facial.

Es importante tener en cuenta que ningún método de autenticación es completamente infalible, por lo que Aseguradora ABANK debe revisar y actualizar periódicamente sus métodos de autenticación para garantizar que sean seguros y eficaces. además, las organizaciones deben implementar políticas de contraseñas seguras para protegerse contra ataques de fuerza bruta y monitorear la red en busca de actividades sospechosas.

65	Controles tecnológicos	A.8.6	Gestión de capacidad	El uso de los recursos se controlará y ajustará de acuerdo con las normas vigentes y requisitos de capacidad esperados.

Aplicación: Algunos métodos comunes utilizados para la protección contra malware incluyen, entre otros:

- Políticas y procedimientos antivirus y antimalware: es beneficioso para la organización tener una política separada que aborde los antivirus y antimalware. sin embargo, para algunas organizaciones esto podría no resultar práctico. por lo tanto, algunas organizaciones prefieren agregar detalles relacionados con antivirus o antimalware en la política de seguridad de la información.
- Software antivirus: el software antivirus utiliza una base de datos de firmas de malware conocidas para detectar y eliminar malware de una computadora o red.
- Cortafuegos: los cortafuegos se utilizan para bloquear el tráfico de red malicioso y evitar que el malware se comunique con los servidores de comando y control.

#	Tipo de control	Nro.	Control	Descripción
Es importante que la organización conserve evidencia de los puntos mencionados anteriormente. poder presentar pruebas cuando se le solicite.				
66	Controles tecnológicos	A.8.7	Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.
Aplicación: Algunos métodos comunes utilizados para la protección contra malware incluyen, entre otros: • Políticas y procedimientos antivirus y antimalware: es beneficioso para la organización tener una política separada que aborde los antivirus y antimalware. sin embargo, para algunas organizaciones esto podría no resultar práctico. por lo tanto, algunas organizaciones prefieren agregar detalles relacionados con antivirus o antimalware en la política de seguridad de la información. • Software antivirus: el software antivirus utiliza una base de datos de firmas de malware conocidas para detectar y eliminar malware de una computadora o red. • Cortafuegos: los cortafuegos se utilizan para bloquear el tráfico de red malicioso y evitar que el malware se comunique con los servidores de comando y control. Es importante que la organización conserve evidencia de los puntos mencionados anteriormente. poder presentar pruebas cuando se le solicite.				
67	Controles tecnológicos	A.8.8	Gestión de vulnerabilidades técnicas	Ninguna red informática, sistema, pieza de software o dispositivo es completamente seguro. La ejecución de una LAN o WAN moderna implica vulnerabilidades como parte del proceso, por lo que es esencial que las organizaciones acepten su presencia y se esfuercen por reducir los riesgos.
Aplicación: El proceso de gestión de vulnerabilidades técnicas normalmente incluye los siguientes pasos: • Escaneo de vulnerabilidades: uso de herramientas automatizadas para escanear sistemas y redes en busca de vulnerabilidades conocidas. • Evaluación de vulnerabilidades: evaluar el impacto potencial de las vulnerabilidades identificadas y priorizarlas en función de su gravedad. • Gestión de vulnerabilidades: desarrollar e implementar un plan para abordar las vulnerabilidades identificadas, que puede incluir la aplicación de parches de seguridad o actualizaciones de software, la reconfiguración de sistemas o redes o la implementación de controles de seguridad adicionales. Es importante tener un plan de gestión de vulnerabilidades y revisarlo y actualizarlo periódicamente para garantizar que siga siendo eficaz a la hora de abordar vulnerabilidades nuevas y emergentes. esto puede incluir escaneos de vulnerabilidades regulares, evaluación de vulnerabilidades y gestión de vulnerabilidades. además, las organizaciones también deben tener un plan de respuesta a incidentes para abordar cualquier incidente de seguridad que pueda ocurrir debido a una vulnerabilidad. también es importante contar con un plan de gestión de riesgos para identificar, evaluar y priorizar las vulnerabilidades que podrían tener un impacto en la organización. esto puede ayudar a la organización a centrarse en las vulnerabilidades que tienen una mayor probabilidad de ser explotadas y que causarían consecuencias más graves.				
68	Controles tecnológicos	A.8.9	Gestión de la configuración	Las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, supervisado y revisado.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: El objetivo de la gestión de la configuración es garantizar que los sistemas de TI sean seguros, compatibles y funcionen de manera óptima manteniendo un inventario preciso de todos los elementos de configuración, controlando y monitoreando los cambios en ellos y restaurando los sistemas a un estado seguro conocido en caso de un problema de seguridad. incidente. El proceso de gestión de la configuración normalmente incluye los siguientes pasos: • Identificar y documentar los elementos de configuración: esto incluye la creación de un inventario de todo el hardware, software y dispositivos de red, y sus configuraciones. • Establecer un proceso para controlar los cambios: esto incluye la creación de un proceso para solicitar, aprobar e implementar cambios en los elementos de configuración, y para documentar y rastrear esos cambios. • Implementación del proceso de gestión de cambios: esto incluye implementar un proceso para probar, aprobar e implementar cambios en los elementos de configuración. • Monitoreo e informes: esto incluye monitorear los elementos de configuración para detectar problemas de cumplimiento y seguridad e informar cualquier problema que se encuentre. • Copia de seguridad y restauración: esto incluye la creación y el mantenimiento de copias de seguridad de los elementos de configuración y la implementación de un proceso para restaurar los sistemas a un estado conocido y seguro en caso de un incidente de seguridad. Es importante contar con un plan de gestión de la configuración y revisarlo y actualizarlo periódicamente para garantizar que siga siendo eficaz a la hora de abordar vulnerabilidades nuevas y emergentes. además, es importante contar con un plan de respuesta a incidentes para abordar cualquier incidente de seguridad, que incluya restaurar los sistemas a un estado seguro conocido.				
69	Controles tecnológicos	A.8.10	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.
Aplicación: Se pueden utilizar varios métodos de eliminación de información, tales como: • Eliminación segura de archivos: implica el uso de software o utilidades especializadas que sobrescriben los datos varias veces, lo que hace imposible su recuperación mediante técnicas de recuperación de datos estándar. • Limpieza del disco duro: implica el uso de software o hardware especializado para borrar completamente todos los datos de un disco duro o dispositivo de almacenamiento, incluido el sistema operativo y todos los archivos. este método se utiliza normalmente cuando un dispositivo se retira o se vende. • Destrucción física: esto implica destruir físicamente el dispositivo de almacenamiento, como triturarlo o fundirlo; este método se usa generalmente para dispositivos que contienen datos extremadamente confidenciales. Es importante contar con un plan de eliminación de datos y revisarlo y actualizarlo periódicamente para garantizar que siga siendo eficaz a la hora de abordar vulnerabilidades nuevas y emergentes. además, es importante contar con un plan de respuesta a incidentes para abordar cualquier incidente de seguridad, que incluya la eliminación segura de datos.				
70	Controles tecnológicos	A.8.11	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
Aplicación: Hay varias formas de implementar el enmascaramiento de datos en la seguridad de la información, según las necesidades y requisitos específicos de Aseguradora ABANK. Aquí están algunos ejemplos: • Sustitución aleatoria: este método implica reemplazar datos confidenciales con caracteres, números o símbolos aleatorios. esto se puede hacer utilizando un algoritmo predefinido o un generador de números aleatorios. • Cifrado que preserva el formato: este método utiliza cifrado para proteger los datos confidenciales y al mismo tiempo preservar el formato de los datos originales. esto es útil para datos que deben usarse en sistemas o				

#	Tipo de control	Nro.	Control	Descripción
aplicaciones que tienen requisitos de formato específicos, como números de tarjetas de crédito o números de seguridad social. • Tokenización: este método reemplaza los datos confidenciales con un token o marcador de posición único. los datos originales se pueden recuperar utilizando un servidor de tokenización o una base de datos, pero los datos no están en texto sin formato. • Enmascaramiento: este método implica reemplazar datos confidenciales con datos ficticios pero realistas, como reemplazar un nombre real por un nombre ficticio. esto se puede hacer utilizando algoritmos predefinidos o scripts personalizados. • Redacción: este método elimina físicamente los datos confidenciales del documento o tacha la información confidencial del documento. Es importante señalar que estos métodos se pueden utilizar juntos o en combinación con otras medidas de seguridad, como controles de acceso y monitoreo, para proporcionar un enfoque integral de la protección de datos.				
71	Controles tecnológicos	A.8.12	Prevención de fuga de datos	Las medidas de prevención de fuga de datos (dlp) se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
Aplicación: Las soluciones DLP suelen utilizar una combinación de técnicas para detectar y prevenir la fuga de datos, como: • Inspección de contenido: pueden escanear datos a medida que se transmiten o almacenan para detectar información confidencial, como números de tarjetas de crédito, números de seguro social o información comercial confidencial. • Cifrado: pueden cifrar automáticamente datos confidenciales para evitar el acceso no autorizado o la filtración. • Controles de acceso: se pueden configurar para aplicar controles de acceso y permisos para evitar que usuarios no autorizados accedan a datos confidenciales. • Política de prevención de pérdida de datos: pueden configurar para hacer cumplir políticas de prevención de pérdida de datos en toda la organización, como prohibir el intercambio de datos confidenciales por correo electrónico o mensajería instantánea. • Monitoreo y alertas: pueden monitorear las transmisiones y el almacenamiento de datos en busca de actividades sospechosas y alertar al personal de seguridad cuando se detecta una posible fuga de datos. Es importante tener en cuenta que dlp no es una solución única, sino más bien un proceso continuo que requiere revisión, actualización y pruebas periódicas para garantizar que protege eficazmente los datos confidenciales de la organización.				
72	Controles tecnológicos	A.8.13	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán regularmente de acuerdo con la política específica del tema acordada en copia de seguridad.
Aplicación: Existen varios tipos de respaldo de información, que incluyen: • Copia de seguridad completa: una copia de seguridad completa crea una copia completa de todos los datos de los que se realiza la copia de seguridad. • Copia de seguridad incremental: una copia de seguridad incremental solo copia los datos que han cambiado desde la última copia de seguridad. • Copia de seguridad diferencial: una copia de seguridad diferencial copia todos los datos que han cambiado desde la última copia de seguridad completa. • Copia de seguridad externa: la copia de seguridad externa es un método para almacenar una copia de datos en una ubicación segura que está geográficamente separada de los datos originales. a menudo, esto se hace para proteger contra desastres naturales u otras amenazas físicas a la ubicación de los datos primarios. • Copia de seguridad en la nube: la copia de seguridad en la nube es un método para almacenar datos de copia de				

#	Tipo de control	Nro.	Control	Descripción
seguridad en servidores remotos, generalmente operados por un proveedor externo. La frecuencia de las copias de seguridad y el tipo de copia de seguridad utilizada dependerán de las necesidades específicas de la organización y de la importancia de los datos de los que se realiza la copia de seguridad. es importante contar con un plan de respaldo bien definido y probar las copias de seguridad periódicamente para garantizar que se puedan restaurar exitosamente en caso de una emergencia.				
73	Controles tecnológicos	A.8.14	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se implementarán con redundancia suficiente para cumplir con los requisitos de disponibilidad.
Aplicación: Se pueden implementar varios tipos de redundancia en un sistema de seguridad de la información en Aseguradora ABANK, que incluyen: • Redundancia de hardware: esto implica tener múltiples componentes de hardware independientes que puedan asumir las funciones de procesamiento en caso de falla. por ejemplo, tener múltiples servidores con diferentes configuraciones, usar almacenamiento raid y tener múltiples fuentes de alimentación. • Redundancia de software: esto implica tener múltiples componentes de software independientes que puedan asumir las funciones de procesamiento en caso de falla. por ejemplo, tener múltiples sistemas operativos, aplicaciones o bases de datos que puedan usarse para procesar datos en caso de falla. • Redundancia de ubicación: implica tener múltiples instalaciones de procesamiento de información independientes ubicadas en diferentes ubicaciones geográficas. esto garantiza que el sistema pueda seguir funcionando incluso si una ubicación no está disponible debido a un desastre u otra interrupción. Es importante señalar que la redundancia por sí sola no es suficiente para garantizar la seguridad y disponibilidad de los datos; debe combinarse con otras medidas de seguridad, como controles de acceso, monitoreo y respuesta a incidentes.				
74	Controles tecnológicos	A.8.15	Inicio sesión	Se producirán, almacenarán, protegerán y analizarán bitácoras que registren actividades, excepciones, fallas y otros eventos relevantes.
Aplicación: El objetivo principal del inicio de sesión en seguridad de la información es proporcionar un registro de actividad en Aseguradora ABANK que pueda usarse para: • Auditoría: los registros se pueden utilizar para rastrear y revisar las acciones del usuario, eventos del sistema y otras actividades para garantizar que cumplan con las políticas y regulaciones de la organización. • Respuesta a incidentes: los registros se pueden utilizar para identificar e investigar incidentes de seguridad, como accesos no autorizados, violaciones de datos e intrusiones en la red. • Análisis forense: los registros se pueden utilizar para reconstruir eventos pasados e identificar la causa de un incidente. • Monitoreo: los registros se pueden utilizar para monitorear el estado y el rendimiento de sistemas, redes y aplicaciones. Es importante contar con una política de registro bien definida, que describa los tipos de registros que deben recopilarse, cómo deben almacenarse y quién tiene acceso a ellos. los registros deben almacenarse en un lugar seguro y deben revisarse periódicamente para garantizar que estén completos, sean precisos y que no haya signos de manipulación.				
75	Controles tecnológicos	A.8.16	Actividades de seguimiento	Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se tomarán las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: Las actividades de seguimiento pueden incluir el uso de diversas herramientas y técnicas, tales como: • Escaneo de vulnerabilidades y pruebas de penetración: estas actividades implican el uso de herramientas automatizadas o técnicas manuales para identificar y evaluar vulnerabilidades de sistemas, redes y aplicaciones. • Análisis de comportamiento: este enfoque monitorea el comportamiento de los usuarios, los sistemas y el tráfico de la red para detectar cualquier actividad anormal o maliciosa. • Monitoreo de redes y sistemas: implica monitorear el rendimiento y la disponibilidad de sistemas, redes y aplicaciones para garantizar que estén funcionando correctamente y detectar cualquier problema que pueda afectar la seguridad. • Cámaras de seguridad y controles de acceso físico: se trata de monitorear el acceso físico a los edificios y centros de datos, para detectar cualquier acceso no autorizado, y también registrar las actividades a utilizar en caso de incidente. El objetivo de las actividades de monitoreo es detectar y responder a incidentes de seguridad lo más rápido posible para minimizar el impacto del incidente y mejorar la postura general de seguridad de la organización. es importante contar con un plan de seguimiento bien definido y garantizar que las herramientas y procesos de seguimiento sean eficaces, eficientes y cumplan con los requisitos reglamentarios.				
76	Controles tecnológicos	A.8.17	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización se sincronizarán con las fuentes de tiempo aprobadas.
Aplicación: Esto es importante por varias razones y se deben considerar los siguientes puntos: • Correlación de registros: cuando se recopilan registros de múltiples sistemas y dispositivos, es esencial que las marcas de tiempo en los registros sean precisas y consistentes para poder correlacionar eventos e identificar posibles incidentes de seguridad. • Controles de acceso basados en el tiempo: muchos sistemas y aplicaciones utilizan controles de acceso basados en el tiempo, como restricciones de tiempo de inicio de sesión o vencimiento de certificados digitales, por lo que es necesaria una sincronización horaria precisa para garantizar que estos controles se apliquen correctamente. • Análisis forense: en caso de un incidente de seguridad, la sincronización horaria precisa es esencial para la respuesta a incidentes y las investigaciones forenses, para comprender la cronología de los eventos e identificar la causa del incidente.				
77	Controles tecnológicos	A.8.18	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.
Aplicación: Ejemplos de programas de utilidad privilegiados incluyen: • Herramientas de administración del sistema: estas herramientas se utilizan para administrar y configurar varios aspectos de un sistema, como usuarios, grupos y servicios. • Herramientas de administración de red: estas herramientas se utilizan para administrar y configurar dispositivos de red, como enrutadores, conmutadores y firewalls. • Utilidades de copia de seguridad y recuperación: estas herramientas se utilizan para crear y administrar copias de seguridad de datos y para restaurar datos en caso de falla o desastre. • Herramientas de seguridad: estas herramientas se utilizan para realizar tareas relacionadas con la seguridad, como escaneo de vulnerabilidades, detección de intrusiones y análisis de registros. • Herramientas de respuesta a incidentes: estas herramientas se utilizan para recopilar datos forenses y realizar actividades de respuesta a incidentes en caso de un incidente de seguridad. El uso de programas de utilidad privilegiados es importante porque permiten a los administradores de sistemas y al personal de seguridad realizar tareas críticas que son necesarias para mantener la seguridad y disponibilidad de un sistema				

#	Tipo de control	Nro.	Control	Descripción
o red. sin embargo, es importante utilizar estas herramientas con precaución y garantizar que se utilicen de acuerdo con las políticas y mejores prácticas de la organización, ya que el uso indebido de programas de utilidad privilegiados puede introducir vulnerabilidades de seguridad y aumentar el riesgo de un incidente de seguridad.				
78	Controles tecnológicos	A.8.19	Instalación de software en sistemas operativos	Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
Aplicación: Este proceso es importante por varias razones: • Mantener los sistemas actualizados: instalar actualizaciones y parches de software es importante para abordar vulnerabilidades conocidas y corregir errores que podrían afectar la seguridad y estabilidad de un sistema. • Agregar nuevas funciones: la instalación de nuevo software puede agregar nuevas características y capacidades a un sistema, lo que puede mejorar la productividad y la eficiencia. • Cumplimiento: la instalación de actualizaciones y parches de software puede ayudar a garantizar que los sistemas cumplan con los requisitos reglamentarios y los estándares de la industria. • Gestión de licencias de software: la instalación de software también puede garantizar que la organización cumpla con los acuerdos de licencia de software y tenga la cantidad adecuada de licencias para el software que se utiliza. Sin embargo, es importante tener cuidado al instalar software en sistemas operativos en Aseguradora ABANK, ya que puede introducir nuevas vulnerabilidades, causar problemas de compatibilidad con otro software o provocar un mal funcionamiento del sistema. es importante contar con un plan de instalación de software bien definido y garantizar que el software que se está instalando provenga de una fuente confiable y que haya sido probado y aprobado para su uso en la organización. además, es importante contar con un proceso para monitorear y administrar el software instalado, y realizar un seguimiento de las versiones, licencias, vulnerabilidades y parches del software.				
79	Controles tecnológicos	A.8.20	Seguridad en redes	Los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.
Aplicación: Esto puede incluir el uso de diversas herramientas y tecnologías como: • Cortafuegos: un cortafuegos es un sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente según reglas y políticas de seguridad predeterminadas. • Control de acceso: los mecanismos de control de acceso se utilizan para restringir el acceso a los recursos de la red en función de la identidad, el rol u otros atributos del usuario. • Cifrado: el cifrado consiste en convertir datos de texto sin formato a un formato ilegible para protegerlos del acceso o divulgación no autorizados. • Segmentación de red: la segmentación de red es una técnica que implica separar diferentes partes de una red en diferentes subredes, con el fin de limitar el alcance de un incidente de seguridad. • Monitoreo de red: el monitoreo de red es el proceso de monitorear la actividad y el rendimiento de la red, con el fin de detectar y responder a incidentes de seguridad y garantizar que la red esté funcionando correctamente. • Gestión de la seguridad de la red: la gestión de la seguridad de la red es el proceso de gestionar, monitorear y proteger una red y sus recursos. Es importante tener en cuenta que la seguridad de la red es un proceso continuo y las medidas de seguridad deben revisarse, actualizarse y probarse periódicamente para garantizar que protejan eficazmente la red y sus recursos.				
80	Controles tecnológicos	A.8.21	Seguridad de los servicios de red.	Mecanismos de seguridad, niveles de servicio deben ser identificados, implementados y monitoreados.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: La seguridad de los servicios de red se puede lograr mediante varios métodos, tales como: • Configuraciones seguras: garantizar que los servicios de red estén configurados de forma segura y que los servicios innecesarios estén deshabilitados. • Gestión de parches: mantener los servicios de red y los sistemas operativos subyacentes actualizados con los últimos parches de seguridad. • Controles de acceso: implementar controles de acceso para restringir el acceso a los servicios de red en función de la identidad, el rol u otros atributos del usuario. • Segmentación de red: segmentar la red para limitar el alcance de un incidente de seguridad y aislar los servicios de red de otras partes de la red. • Cifrado: uso de cifrado para proteger datos confidenciales que se transmiten a través de los servicios de red. • Sistemas de detección y prevención de intrusiones: monitorear la red en busca de actividades sospechosas y bloquear cualquier tráfico malicioso que pueda estar dirigido a los servicios de red. • Monitorización de seguridad y respuesta a incidentes: monitorización continua de los servicios de red y detección rápida de posibles incidentes de seguridad que puedan ocurrir. Es importante tener en cuenta que la seguridad de los servicios de red es un proceso continuo y las medidas de seguridad necesarias deben revisarse, actualizarse y probarse periódicamente para garantizar que protejan eficazmente los servicios de red y su infraestructura subyacente.				
81	Controles tecnológicos	A.8.22	Segregación de redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
Aplicación: Esto se puede lograr a través de varios métodos como: • Cortafuegos: los cortafuegos se pueden utilizar para segmentar una red controlando el acceso entre diferentes partes de la red. • VPN (red privada virtual): las VPN permiten a los usuarios remotos acceder a la red interna de forma segura, manteniendo la red interna separada de la internet pública.				
82	Controles tecnológicos	A.8.23	Filtrado web	El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.
Aplicación: Lo siguiente a considerar para el filtrado web: • Bloquear el acceso a sitios web maliciosos conocidos: esto se hace utilizando bases de datos de sitios web maliciosos conocidos e impidiendo el acceso a ellos. • Bloquear el acceso a determinadas categorías de sitios web: esto se hace mediante el uso de categorías preconfiguradas, como juegos de apuestas, redes sociales o contenido para adultos, e impidiendo el acceso a ellas. • Bloquear el acceso a ciertos tipos de contenido: esto se hace identificando y bloqueando ciertos tipos de archivos, como archivos ejecutables o scripts, que podrían ser potencialmente maliciosos. • Filtrado de url: esto se realiza controlando el acceso a URL o nombres de dominio específicos y evitando el acceso a ellos. • Prevención de pérdida de datos: esto se logra monitoreando el tráfico saliente y bloqueando la filtración de datos confidenciales. • Control de aplicaciones: esto se realiza controlando el acceso a aplicaciones específicas, como mensajería instantánea o intercambio de archivos de igual a igual. El filtrado web se puede implementar mediante soluciones de hardware o software y se puede aplicar a toda la organización o a grupos específicos de usuarios. el filtrado web puede ayudar a proteger la red de la organización y a los usuarios del				

#	Tipo de control	Nro.	Control	Descripción
malware y otras amenazas cibernéticas y también puede usarse para hacer cumplir las políticas organizacionales y cumplir con los requisitos reglamentarios. sin embargo, es importante tener en cuenta que el filtrado web por sí solo no es una solución de seguridad integral y debe usarse junto con otras medidas de seguridad como antivirus, detección de intrusiones y respuesta a incidentes.				
83	Controles tecnológicos	A.8.24	Uso de criptografía	Reglas para el uso efectivo de la criptografía, incluida la clave criptográfica gestión, debe ser definida e implementada.
Aplicación: Algunos ejemplos del uso de la criptografía en la seguridad de la información que pueden tomarse en cuenta en Aseguradora ABANK incluyen: • Cifrado: el cifrado es el proceso de convertir datos de texto sin formato a un formato ilegible, llamado texto cifrado, para protegerlos del acceso o divulgación no autorizados. se puede utilizar para proteger datos en reposo, como en un disco duro, o datos en tránsito, como a través de una red. • Firmas digitales: las firmas digitales son una forma de garantizar la autenticidad de los datos; utiliza una clave privada para cifrar el hash de los datos y una clave pública para descifrarlos, lo que permite al receptor estar seguro de que los datos provienen de una fuente confiable. El uso de la criptografía es una parte fundamental de la seguridad de la información moderna y se utiliza ampliamente para proteger datos confidenciales, asegurar las comunicaciones y autenticar usuarios y dispositivos. es importante tener en cuenta que el uso de criptografía por sí solo no es una solución de seguridad integral y debe usarse junto con otras medidas de seguridad como firewall, además, la organización debería considerar incluir el uso de criptografía a nivel de políticas e implementar los procedimientos necesarios.				
84	Controles tecnológicos	A.8.25	Ciclo de vida de desarrollo seguro	Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.
Aplicación: El SDLC normalmente incluye las siguientes fases: • Planificación: durante esta fase, la organización define el alcance del proyecto y describe los requisitos de seguridad que deben cumplirse. • Análisis: durante esta fase, la organización identifica posibles amenazas y vulnerabilidades de seguridad y evalúa los riesgos asociados con ellas. • Diseño: durante esta fase, la organización diseña el sistema, teniendo en cuenta los requisitos de seguridad y los riesgos identificados durante la fase de análisis. • Implementación: durante esta fase, la organización desarrolla y prueba el software e integra la seguridad en el sistema. • Pruebas: durante esta fase, la organización realiza una variedad de pruebas para garantizar que el sistema cumpla con los requisitos de seguridad y que esté libre de vulnerabilidades. • Implementación: durante esta fase, el sistema se implementa en el entorno de producción. • Mantenimiento: durante esta fase, la organización monitorea el sistema, lo actualiza con nuevos parches de seguridad y realiza los cambios necesarios para mantener la seguridad del sistema. • Retiro: durante esta fase, la organización desmantela el sistema y borra los datos de forma segura.				
85	Controles tecnológicos	A.8.26	Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

#	Tipo de control	Nro.	Control	Descripción
Aplicación: Ejemplos de requisitos de seguridad de aplicaciones incluyen: • Validación de entradas: las aplicaciones deben validar todas las entradas recibidas de fuentes externas para garantizar que sean seguras de usar y estén libres de códigos maliciosos. • Autenticación y control de acceso: las aplicaciones deben contar con mecanismos para autenticar y autorizar a los usuarios, y para controlar el acceso a datos y funciones confidenciales. • Cifrado de datos: las aplicaciones deben cifrar datos confidenciales, tanto en tránsito como en reposo, para protegerlos del acceso o divulgación no autorizados. • Manejo y registro de errores: las aplicaciones deben manejar los errores de manera segura y deben registrar todos los eventos relevantes para la seguridad para su posterior revisión. • Prácticas de codificación segura: las aplicaciones deben desarrollarse utilizando prácticas de codificación segura, como el uso de bibliotecas y marcos seguros, y siguiendo pautas para evitar vulnerabilidades comunes. • Pruebas de penetración: las aplicaciones deben probarse para detectar vulnerabilidades utilizando herramientas automatizadas y pruebas de penetración manuales. • Respuesta a incidentes: las aplicaciones deben tener un plan implementado para responder a incidentes de seguridad, incluida la detección de incidentes, la respuesta a incidentes y la recuperación de incidentes.				
86	Controles tecnológicos	A.8.27	Arquitectura segura del sistema y principios de ingeniería	Se deben establecer principios para la ingeniería de sistemas seguros, documentación, y debe ser mantenido y aplicado a cualquier desarrollo de sistema de información actividades.
Aplicación: Hay varias formas diferentes de implementar principios de ingeniería y arquitectura de sistemas seguros en la seguridad de la información. Algunos pasos clave incluyen: • Realizar un ejercicio de modelado de amenazas: esto implica identificar posibles amenazas y vulnerabilidades que un sistema puede enfrentar y determinar la probabilidad y el impacto de esas amenazas. • Implementación del principio de privilegio mínimo: este principio establece que un sistema solo debe tener el nivel mínimo de acceso y privilegios necesarios para realizar la función prevista. • Uso de la defensa en profundidad: esto implica implementar múltiples capas de controles de seguridad, como controles de acceso y cifrado, para proteger contra posibles amenazas y vulnerabilidades. • Realizar evaluaciones periódicas de vulnerabilidades: esto implica revisar periódicamente el sistema para identificar y abordar cualquier vulnerabilidad potencial. • Planificación de respuesta a incidentes: contar con un plan sobre cómo responder a incidentes de seguridad puede ayudar a minimizar el daño causado por un ataque y ayudar a que el sistema vuelva rápidamente a sus operaciones normales. • Monitorear y revisar periódicamente el sistema: monitorear continuamente el sistema para detectar cualquier actividad sospechosa y revisar y actualizar periódicamente los controles de seguridad para garantizar que sigan siendo efectivos.				
87	Controles tecnológicos	A.8.28	Codificación segura	Los principios de codificación segura se aplicarán al desarrollo de software.
Aplicación: A continuación, se muestran algunos pasos y prácticas generales que se pueden utilizar para implementar la codificación segura en la seguridad de la información en Aseguradora ABANK: • Comprenda y siga las pautas y estándares de codificación segura: familiarícese con las pautas estándar de la industria. • Utilice técnicas de codificación segura: utilice técnicas como validación de entradas, manejo de errores y consultas parametrizadas para evitar tipos comunes de vulnerabilidades como desbordamientos de búfer, inyección SQL y secuencias de comandos entre sitios. • Utilice bibliotecas y marcos de seguridad: utilice bibliotecas y marcos prediseñados que proporcionen funciones				

#	Tipo de control	Nro.	Control	Descripción
de codificación segura, como cifrado y autenticación. esto puede ayudarle a evitar tener que escribir código sensible a la seguridad desde cero. • Realice revisiones de código: utilice la revisión de código para identificar y solucionar cualquier problema de seguridad antes de implementar el código. esto se puede hacer realizando revisiones periódicas del código y utilizando herramientas automatizadas que puedan escanear el código en busca de vulnerabilidades. • Supervise continuamente el código: vigile el código después de que se haya implementado y supervise continuamente para detectar cualquier signo de problemas de seguridad. esto puede ayudarle a responder rápidamente a cualquier incidente de seguridad que pueda ocurrir. • Actualice y parchee el código periódicamente: mantenga el código actualizado con los últimos parches de seguridad y asegúrese de aplicarlos tan pronto como estén disponibles. • Capacite y eduque al equipo: asegúrese de que los miembros del equipo conozcan los riesgos de seguridad y las mejores prácticas y estén capacitados continuamente para implementar prácticas de codificación segura.				
88	Controles tecnológicos	A.8.29	Pruebas de seguridad en desarrollo y aceptación	Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.
Aplicación: Las pruebas de seguridad durante la fase de desarrollo incluyen una variedad de técnicas, como revisiones de código, pruebas de penetración. Estas técnicas ayudan a identificar y corregir vulnerabilidades de seguridad en el código antes de implementarlo. Las pruebas de aceptación son la etapa final de las pruebas antes de que el software se entregue al cliente. Verifica que el software cumpla con los criterios de aceptación especificados y que esté libre de vulnerabilidades de seguridad conocidas. Esto puede incluir pruebas funcionales, pruebas de rendimiento y pruebas de seguridad. El objetivo de las pruebas de seguridad durante el desarrollo y la aceptación es garantizar que el software esté libre de vulnerabilidades de seguridad conocidas y que cumpla con los requisitos de seguridad antes de su implementación.				
89	Controles tecnológicos	A.8.30	Desarrollo subcontratado	La organización debe dirigir, monitorear y revisar las actividades relacionadas al desarrollo de sistemas subcontratados.
Aplicación: El desarrollo de la subcontratación puede proporcionar una serie de beneficios a las organizaciones, incluido el ahorro de costos, el acceso a experiencia especializada y una mayor flexibilidad. Sin embargo, también presenta una serie de riesgos de seguridad que deben gestionarse. Al subcontratar el desarrollo, es importante asegurarse de que el desarrollador externo siga práctico de codificación seguras y que el software que está desarrollando esté libre de vulnerabilidades conocidas. Esto se puede hacer exigiendo al desarrollador que siga las pautas de seguridad y realizando pruebas de seguridad periódicas en el software. Además, es importante contar con un contrato sólido que describa las responsabilidades de seguridad de ambas partes, así como cualquier responsabilidad legal y implicaciones financieras en caso de una violación de la seguridad.				
90	Controles tecnológicos	A.8.31	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
Aplicación: El entorno de desarrollo es donde se crea y prueba inicialmente el software. Aquí es donde los desarrolladores escriben y prueban el código, y donde se agregan nuevas características y funcionalidades al software. El entorno de prueba es donde el software se prueba minuciosamente antes de implementarlo en producción. Este entorno se utiliza para identificar y solucionar cualquier problema con el software, incluidas las vulnerabilidades de seguridad. El entorno de producción es donde los usuarios finales utilizan realmente el software. Este es el entorno real donde los clientes implementan y utilizan el software. La separación de estos entornos es importante por razones de seguridad porque ayuda a evitar que cualquier problema que pueda ocurrir en los entornos de desarrollo o prueba afecte el entorno de producción. También ayuda para evitar cualquier acceso no autorizado, modificación o eliminación accidental de los datos de producción y la configuración. Al mantener entornos separados para el desarrollo, las pruebas y la producción, las organizaciones pueden gestionar mejor los riesgos de seguridad, garantizar que el software se pruebe exhaustivamente antes de implementarlo y minimizar el impacto potencial de cualquier problema que pueda ocurrir.				

#	Tipo de control	Nro.	Control	Descripción
91	Controles tecnológicos	A.8.32	Gestión del cambio	Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.

Aplicación: La gestión de cambios es un aspecto importante de la seguridad de la información porque ayuda a garantizar que los cambios en los sistemas y aplicaciones se planifiquen, prueben e implementen adecuadamente. Esto ayuda a minimizar el riesgo de incidentes de seguridad y garantiza que cualquier cambio realizado en los sistemas y aplicaciones no afecte negativamente a su seguridad o funcionalidad. El proceso de gestión de cambios normalmente incluye varios pasos, como:

- Identificación y evaluación del cambio: identificar la necesidad de un cambio y evaluar su impacto en el sistema o aplicación.
- Planificación y programación: planifique y programe el cambio, incluidas las pruebas y validaciones necesarias.
- Implementación: implementar el cambio, siguiendo los procedimientos y lineamientos establecidos.
- Prueba y validación: pruebe y valide el cambio para garantizar que no afecte negativamente la seguridad o la funcionalidad del sistema o la aplicación.
- Documentación y comunicación: documente y comunique el cambio a las partes relevantes, como administradores del sistema y otras partes interesadas.
- Monitoreo y revisión: monitoree el cambio para asegurarse de que esté funcionando según lo previsto y revíselo para identificar cualquier problema que pueda haberse pasado por alto durante las pruebas.

La gestión de cambios es un proceso continuo que ayuda a las organizaciones a mantener sus sistemas y aplicaciones actualizados, seguros y funcionando sin problemas. también ayuda a garantizar que cualquier cambio esté controlado y sea seguro y que la organización pueda revertir los cambios si es necesario.

92	Controles tecnológicos	A.8.33	Información de prueba	La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.

Aplicación: La información de prueba es importante para las pruebas de seguridad porque ayuda a garantizar que el sistema que se está probando se evalúe minuciosamente en busca de vulnerabilidades de seguridad. Al proporcionar un conjunto completo de casos de prueba y datos de prueba, los evaluadores de seguridad pueden identificar y corregir vulnerabilidades que pueden haberse pasado por alto durante el desarrollo. También ayuda a garantizar que el sistema que se está probando cumpla con los requisitos de seguridad y con los estándares y estándares de la industria. regulaciones. La información de prueba también se utiliza para documentar el proceso de prueba y para proporcionar evidencia de la seguridad del sistema con fines de cumplimiento, reglamentación y certificación.

93	Controles tecnológicos	A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de sistemas operativos se planificarán y acordarán entre la persona que ejecuta la prueba y la dirección correspondiente.

Aplicación: Las pruebas de auditoría son el proceso de evaluar los controles de seguridad de un sistema de información para determinar si funcionan según lo previsto y si cumplen con las políticas y estándares de seguridad de la organización. Para proteger el sistema durante las pruebas de auditoría, las organizaciones pueden implementar varias medidas:

- Uso de cuentas de prueba: utilice cuentas de prueba en lugar de cuentas reales para acceder al sistema durante la prueba. esto puede ayudar a evitar cambios accidentales o no autorizados en el sistema.
- Uso de datos de prueba: utilice datos de prueba en lugar de datos reales para realizar las pruebas. esto puede ayudar a proteger los datos sensibles o confidenciales para que no se vean comprometidos.
- Aislamiento del entorno de prueba: aísle el entorno de prueba del entorno de producción para evitar interrupciones

#	Tipo de control	Nro.	Control	Descripción
				o daños al entorno de producción. • Copia de seguridad de datos: realice una copia de seguridad del sistema antes de realizar la prueba en caso de que sea necesario restaurar el sistema en caso de un problema inesperado. • Monitoreo: monitoree el sistema durante las pruebas para detectar cualquier problema que pueda ocurrir. • Planes de prueba: tenga un plan de prueba detallado y comuníqueselo con las partes relevantes, como administradores del sistema y otras partes interesadas. Al implementar estas medidas, Aseguradora ABANK pueden ayudar a proteger sus sistemas de información durante las pruebas de auditoría, minimizar el impacto potencial de cualquier problema que pueda ocurrir y garantizar que el proceso de prueba se lleve a cabo de manera controlada y segura.

Fuente: adaptado de "Implementing and Auditing an Information Security Management System in Small and Medium-sized Businesses" por Cees Van Der Wens, julio de 2023.

APÉNDICE 12. OBJETIVOS DEL SIG Y SUS PLANES DE ACCIÓN

Objetivo del SIG Nro.1

ESTRATEGIA	OBJETIVO	INDICADORES VERIFICABLES Y METAS DEL OBJETIVO ESTRATÉGICO	
Excelencia en la Satisfacción del Cliente	Mejorar la satisfacción del cliente mediante la optimización de los procesos de atención y resolución de incidencias.	NOMBRE	META
		Índice de Satisfacción del Cliente	Incrementar el índice de satisfacción del cliente en un 15% en el próximo año.
		Tiempo Promedio de Resolución de Incidencias	Reducir el tiempo promedio de resolución de incidencias en un 20% en 12 meses.

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS

PROYECTOS	ACCIONES	Indicadores y metas del proyecto	RECURSO	Responsable	2025				2026			
					I	II	III	IV	I	II	III	IV
Implementación de un sistema de gestión de incidencias automatizado.	**Seleccionar y adquirir la plataforma de gestión de incidencias.** **Configurar y personalizar el sistema según las necesidades de ABANK.** **Capacitar al personal en el uso del nuevo sistema**	**Indicadores:** Tasa de Adopción del Sistema: Porcentaje de usuarios que utilizan activamente el sistema en un mes. Tiempo de Implementación: Duración en semanas desde el inicio hasta la completa implementación del sistema. **Metas:** Tasa de Adopción del Sistema: Alcanzar un 90% de adopción en los primeros 3 meses. Tiempo de Implementación: Completar la implementación en 16 semanas.	Software de gestión de incidencias. Consultores de TI para implementación. Materiales de formación	Gerente comercial								

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	II	III	IV	I	II	III	IV
Capacitación del personal en atención al cliente y resolución de problemas.	**Diseñar el programa de capacitación en atención al cliente.** **Realizar sesiones de formación para todo el personal de atención al cliente.** **Evaluar la eficacia de la capacitación mediante encuestas y pruebas.**	**Indicadores:** Número de Empleados Capacitados: Porcentaje de personal capacitado en los primeros 6 meses. Evaluación Post-Capacitación: Puntuación promedio obtenida en evaluaciones post-capacitación. **Metas:** Número de Empleados Capacitados: Capacitar al 100% del personal de atención al cliente en 6 meses. Evaluación Post-Capacitación: Lograr una puntuación promedio de al menos 85% en las evaluaciones.	Instructores de capacitación. Materiales didácticos. Espacios para la formación.	Gerente comercial								

Objetivo del SIG Nro.2

ESTRATEGIA	**OBJETIVO**	INDICADORES VERIFICABLES Y METAS DEL OBJETIVO ESTRATÉGICO	
Fortalecimiento de la Seguridad de la Información	Garantizar la protección de la información sensible mediante la mejora de las medidas de seguridad y	NOMBRE	META
		Índice de Incidencias de Seguridad	Reducir las incidencias de seguridad en un 25% en los próximos 12 meses.

	cumplimiento normativo.	Nivel de Cumplimiento con ISO/IEC 27001:2022	Alcanzar un 100% de cumplimiento en la auditoría anual de ISO/IEC 27001.

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS													
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026				
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
Actualización e implementación de políticas de seguridad de la información.	**Revisar y actualizar las políticas actuales de seguridad de la información.** **Comunicar y distribuir las nuevas políticas a todo el personal.** **Monitorear el cumplimiento de las políticas a través de auditorías internas.**	**Indicadores:** Número de Políticas Actualizadas: Cantidad de políticas de seguridad actualizadas y aprobadas. Cumplimiento en Auditorías: Porcentaje de cumplimiento en auditorías de seguridad tras la actualización de políticas. **Metas:** Número de Políticas Actualizadas: Actualizar y aprobar el 100% de las políticas de seguridad críticas en 4 meses. Cumplimiento en Auditorías: Alcanzar un 100% de cumplimiento en las auditorías posteriores a la actualización.	Especialistas en seguridad de la información. Herramientas de comunicación interna. Equipos de auditoría.	Gerente de tecnología									
Auditorías internas trimestrales de seguridad de la información.	**Planificar y calendarizar las auditorías internas.** **Realizar auditorías de acuerdo con las políticas y normativas**	**Indicadores:** Número de Auditorías Realizadas: Cantidad de auditorías internas realizadas por trimestre. Número de No Conformidades Detectadas: Número de no conformidades encontradas en cada auditoría. **Metas:**	Auditores internos especializados. Herramientas de auditoría. Documentación de políticas y procedimientos.	Gerente de tecnología									

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
	establecidas. **Implementar medidas correctivas basadas en los hallazgos de la auditoría.**	Número de Auditorías Realizadas: Realizar al menos 4 auditorías internas de seguridad por año. Número de No Conformidades Detectadas: Reducir las no conformidades en un 50% en un año.										
Implementación de un programa de concienciación en seguridad de la información	**- Diseñar un programa de capacitación en seguridad de la información para todos los empleados.** **- Realizar sesiones de capacitación trimestrales.** **- Evaluar la efectividad de la capacitación mediante encuestas y pruebas.**	**Indicadores:** - Participación en Capacitación: Porcentaje de empleados capacitados. - Evaluaciones Post-Capacitación: Promedio de calificación en evaluaciones de seguridad tras las capacitaciones. **Metas:**	Formadores en seguridad de la información. Materiales de capacitación.	Gerente de tecnología								
Implementación de controles de seguridad de la información (Anexo A de ISO/IEC 27001:2022	**- Realizar un análisis de brechas para identificar controles existentes.** **- Desarrollar e implementar**	**Indicadores:** - Número de Controles Implementados: Cantidad de controles del Anexo A implementados. - Eficiencia de Controles: Porcentaje de controles que cumplen con las normativas tras	Especialistas en seguridad de la información. Herramientas de gestión de seguridad.	Gerente de tecnología/ Coordinador de seguridad de la información								

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
	controles de seguridad específicos del Anexo A. **- Realizar revisiones periódicas para evaluar la eficacia de los controles implementados.**	revisiones. **Metas:** - Implementar el 100% de los controles en 12 meses. - Alcanzar un 90% de eficacia en la evaluación de controles.										
Desarrollo de un plan de respuesta a incidentes	**- Definir y documentar un plan de respuesta a incidentes de seguridad.** **- Realizar simulacros de respuesta a incidentes semestrales.** **- Establecer un canal de comunicación para reportar incidentes.**	**Indicadores:** - Plan Documentado: Existencia y actualización del plan de respuesta. - Simulacros Realizados: Número de simulacros realizados por año. **Metas:** - Tener un plan de respuesta documentado en 6 meses. - Realizar al menos 2 simulacros al año.	Consultores en gestión de incidentes. Herramientas de gestión de incidentes.	Gerente de tecnología/ Coordinador de seguridad de la información								

Objetivo del SIG Nro.3

ESTRATEGIA	OBJETIVO	INDICADORES VERIFICABLES Y METAS DEL OBJETIVO ESTRATÉGICO	
		NOMBRE	META
Optimización de Procesos Internos	Mejorar la eficiencia operativa mediante la optimización de los procesos internos clave.	Tiempo de Ciclo de Proceso	Reducir el tiempo de ciclo de los procesos clave en un 30% en el próximo año.
		Costos Operativos	Disminuir los costos operativos en un 10% en 12 meses.

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSOS**	**Responsable**	2025				2026			
					I	II	III	IV	I	II	III	IV
Implementación de tecnología RPA para automatización de procesos.	**Identificar los procesos clave que pueden ser automatizados.** **Desarrollar e implementar bots RPA para esos procesos.** **Monitorear y ajustar los bots para optimizar su rendimiento.**	**Indicadores:** Número de Procesos Automatizados: Cantidad de procesos clave automatizados con RPA. Reducción en el Tiempo de Ejecución: Porcentaje de reducción en el tiempo de ejecución de los procesos automatizados. **Metas:** Número de Procesos Automatizados: Automatizar al menos 5 procesos críticos en 6 meses. Reducción en el Tiempo de Ejecución: Reducir el tiempo de ejecución de los procesos automatizados en 40% en un año.	Software RPA. Desarrolladores RPA. Infraestructura TI para soporte.	Gerente de riesgos y procesos								

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSOS**	**Responsable**	2025				2026			
					I	II	III	IV	I	II	III	IV
Revisión y rediseño de los flujos de trabajo internos.	**Mapear los flujos de trabajo actuales y detectar ineficiencias.** **Rediseñar los flujos para mejorar la eficiencia.** **Implementar los nuevos flujos de trabajo y capacitar al personal.**	**Indicadores:** Número de Flujos Rediseñados: Cantidad de flujos de trabajo revisados y optimizados. Eficiencia Operativa Post-Rediseño: Porcentaje de mejora en la eficiencia operativa tras la optimización. **Metas:** Número de Flujos Rediseñados: Rediseñar al menos 3 flujos de trabajo clave en 6 meses. Eficiencia Operativa Post-Rediseño: Incrementar la eficiencia operativa en un 30% en los procesos revisados en un año.	Consultores de procesos. Herramientas de mapeo de procesos. Recursos para formación del personal.	Gerente de riesgos y procesos								

Objetivo del SIG Nro.4

ESTRATEGIA	OBJETIVO	INDICADORES VERIFICABLES Y METAS DEL OBJETIVO ESTRATÉGICO	
		NOMBRE	META
Innovación en Productos y Servicios	Desarrollar y lanzar nuevos productos y servicios que satisfagan las necesidades emergentes del mercado.	Número de Nuevos Productos/Servicios Lanzados	Introducir al menos 3 nuevos productos o servicios en el próximo año.
		Cuota de Mercado	Incrementar la cuota de mercado en un 5% en 12 meses.

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
Creación de un equipo de innovación y desarrollo de productos.	**Seleccionar miembros del equipo con habilidades clave.** **Definir y asignar roles dentro del equipo de innovación.** **Establecer un proceso de desarrollo de productos ágil.**	**Indicadores:** Número de Productos/Servicios Desarrollados: Cantidad de nuevos productos o servicios desarrollados. Tiempo de Desarrollo: Duración promedio del ciclo de desarrollo de nuevos productos o servicios. **Metas:** Número de Productos/Servicios Desarrollados: Desarrollar al menos 3 nuevos productos o servicios en un año. Tiempo de Desarrollo: Reducir el ciclo de desarrollo en un 25% en un año.	Talento humano especializado en innovación. Espacios de trabajo colaborativo. Herramientas de gestión de proyectos.	Gerente comercial								
Investigación de mercado para identificar necesidades emergentes de clientes.	**Diseñar y ejecutar encuestas y estudios de mercado.** **Analizar los datos obtenidos para identificar tendencias.** **Utilizar los hallazgos para desarrollar nuevos productos/serv**	**Indicadores:** Número de Estudios de Mercado Realizados: Cantidad de estudios de mercado llevados a cabo. Tasa de Adopción de Nuevos Productos: Porcentaje de adopción de nuevos productos o servicios basados en la investigación de mercado. **Metas:** Número de Estudios de Mercado Realizados: Realizar al menos 2 estudios de mercado en un año. Tasa de Adopción de Nuevos Productos: Lograr una tasa de adopción del 20% para nuevos productos en el primer año de su lanzamiento.	Software de análisis de mercado. Paneles de consumidores para encuestas. Analistas de mercado.	Gerente comercial								

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
	icios.											

Objetivo del SIG Nro.5

ESTRATEGIA	**OBJETIVO**	INDICADORES VERIFICABLES Y METAS DEL OBJETIVO ESTRATÉGICO	
		NOMBRE	META
Cultura Organizacional Orientada a la Calidad	Fomentar una cultura organizacional que priorice la calidad y la mejora continua.	Índice de Participación en Programas de Calidad	Lograr una participación del 90% del personal en programas de calidad y mejora continua en 12 meses.
		Índice de Satisfacción del Empleado	Incrementar el índice de satisfacción del empleado en un 20% en un año.

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
Implementación de un programa de formación continua en gestión de calidad.	**Desarrollar el contenido de los cursos de formación en calidad.** **Organizar sesiones de formación periódicas**	**Indicadores:** Número de Cursos Completados: Cantidad de cursos de formación continua completados por el personal. Índice de Participación: Porcentaje de empleados que participan activamente en los programas de	Instructores de calidad. Plataformas de e-learning. Materiales educativos.	Gerente de riesgos y procesos								

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
	para todo el personal. **Evaluar y mejorar continuamente el programa de formación.**	formación. **Metas:** Número de Cursos Completados: Lograr que el 80% del personal complete al menos 2 cursos de calidad en un año. Índice de Participación: Alcanzar una participación del 90% en los programas de formación en 24 meses.										
Desarrollo de un programa de incentivos para empleados que promuevan la calidad.	**Diseñar un esquema de incentivos alineado con los objetivos de calidad.** **Comunicar el programa a todos los empleados.** **Evaluar el desempeño y otorgar incentivos según criterios establecidos.**	**Indicadores:** Número de Incentivos Otorgados: Cantidad de incentivos entregados por cumplimiento de objetivos de calidad. Índice de Mejora en Calidad: Porcentaje de mejora en los indicadores de calidad tras la implementación del programa. **Metas:** Número de Incentivos Otorgados: Otorgar al menos 50 incentivos relacionados con la calidad en un año. Índice de Mejora en Calidad: Incrementar los indicadores de calidad en un 15% en un 2 años tras	Fondo de incentivos. Sistema de evaluación de desempeño. Herramientas de comunicación interna.	Gerente de riesgos y procesos								

PLAN DE ACCIÓN PARA CUMPLIMIENTO DE OBJETIVOS												
PROYECTOS	**ACCIONES**	**Indicadores y metas del proyecto**	**RECURSO**	**Responsable**	2025				2026			
					I	**II**	**III**	**IV**	**I**	**II**	**III**	**IV**
		la implementación del programa.										

APÉNDICE 13. MATRIZ DE COMUNICACIÓN DEL SIG

MATRIZ DE COMUNICACIONES DEL SIG						
N°	**QUE SE COMUNICA**	**PROCESO**	**CUANDO LO COMUNICA**	**A QUIEN LO COMUNICA**	**COMO LO COMUNICA**	**QUIEN LO COMUNICA**
1	Política, objetivos, indicadores y estrategias de la organización	Gestión estratégica	cada 3 meses o cada vez que presenten cambios	A todo el personal de la organización	Correo electrónico, reuniones, boletín, carteleras	Gerente general, coordinador de SGC
2	Desempeño gerencial. Informe de revisión por la dirección	Sistema Integrado de Gestión	Cada año	Socios, auditoría interna, departamento de SGC	Reuniones, correo electrónico	Alta dirección, coordinador de SGC
3	Planeación del Sistema de Gestión	Sistema Integrado de Gestión	Cada año o cada vez que se modifique	A todo el personal de la organización	Reuniones, correo electrónico, revisión gerencial	Gerente general, coordinador de SGC
4	Planeación estratégica	Sistema Integrado de Gestión	Cada año o cada vez que se modifique	A todo el personal de la organización, proveedores y accionistas	Reuniones, correo electrónico, revisión gerencial	Gerente general, coordinador de SGC
5	Necesidades y expectativas de las partes interesadas	Sistema Integrado de Gestión	Cada año o cada vez que se modifique	Gerente general, líderes de procesos	Correo electrónico, reuniones, boletín, carteleras	Gerente general, coordinador de SGC
6	Informe de desempeño de procesos	Sistema Integrado de Gestión	Mensual, anual o cada vez que se verifique un proceso	Gerente general, líderes de procesos	Informe de resultados de procesos, reuniones	Gerente general, líderes de proceso
7	Requisitos legales y reglamentos aplicables	Control interno	Cada vez que se emita un reglamento o nueva ley o cualquier modificación de estas	Líderes de proceso y todo personal que requiera de dicha información	Correo electrónico, reuniones, boletín, carteleras	Coordinador de SGC
8	Informe de auditorías	Auditoría	Cada vez que se presente una auditoría interna o externa	A todo el personal de la organización	Reuniones, correo electrónico, revisión gerencial	Coordinador de SGC

MATRIZ DE COMUNICACIONES DEL SIG						
N°	**QUE SE COMUNICA**	**PROCESO**	**CUANDO LO COMUNICA**	**A QUIEN LO COMUNICA**	**COMO LO COMUNICA**	**QUIEN LO COMUNICA**
9	Requisitos del cliente	Comercialización	Cada que se realice una venta o al presentar cambios	Líderes de proceso y todo personal que requiera de dicha información	Reuniones, correo electrónico, revisión gerencial	Gerente general, gerente comercial
10	Pólizas o contratos	Comercialización	Cada vez que se realice una venta	Gerente general, gerente comercial y todo personal que requiera dicha información	Contratos, reuniones, correo electrónico	Gerente comercial
11	Divulgación del procedimiento de comercialización	Comercialización	Cada año o cada vez que se modifique	A todo el personal involucrado en el proceso de comercialización y partes interesadas	Reuniones, correo electrónico, revisión gerencial	Gerente comercial
12	Divulgación del procedimiento de Suscripción	Suscripción	Cada año o cada vez que se modifique	A todo el personal involucrado en el proceso de suscripción y partes interesadas	Reuniones, correo electrónico, revisión gerencial	Gerente técnico
13	Divulgación del procedimiento de Emisión	Emisión	Cada año o cada vez que se modifique	A todo el personal involucrado en el proceso de emisión y partes interesadas	Reuniones, correo electrónico, revisión gerencial	Gerente Técnico
14	Divulgación del procedimiento de servicio post venta	Servicio post-venta	Cada año o cada vez que se modifique	A todo el personal involucrado en el proceso de servicio post venta y partes interesadas	Reuniones, correo electrónico, revisión gerencial	Gerente de servicio post venta
15	Divulgación de procedimiento de Control de información documentada	Administración	Cada año o cada vez que se modifique	Gerente general, líderes de procesos	Reuniones, correo electrónico, revisión gerencial	Coordinador de SGC

MATRIZ DE COMUNICACIONES DEL SIG						
N°	**QUE SE COMUNICA**	**PROCESO**	**CUANDO LO COMUNICA**	**A QUIEN LO COMUNICA**	**COMO LO COMUNICA**	**QUIEN LO COMUNICA**
16	Divulgación de procedimiento de Acciones correctivas	Sistema Integrado de Gestión	Cada año o cada vez que se modifique	Gerente general, líderes de procesos	Reuniones, correo electrónico, revisión gerencial	Coordinador de SGC
17	Necesidad de recursos	Todos los procesos	Cada año o cada vez que se requiera	Gerente general, gerente financiero	Reuniones, correo electrónico, revisión gerencial	Líderes de proceso
18	Informe de quejas y reclamos. No conformidades	Comercialización, suscripción, emisión y servicio post venta	Cada vez que se genera una queja, reclamo o no conformidad	Gerente general, líderes de procesos, todo personal relacionado	Reuniones, correo electrónico, revisión gerencial	Líderes de proceso
19	Responsabilidades y autoridades	Gestión del talento humano	Cada año, modificación de puestos, contratación de personal	A todo el personal	Reuniones, correo electrónico, revisión gerencial	RRHH, Gerente general, alta dirección
20	Evaluación de proveedores	Administración/ Tecnología	Cada año	Proveedores, contratistas, Gerencia general, gerencia financiera	Documento de evaluación de proveedores, Informe de revisión de alta dirección	Coordinador de SGC
21	Acciones correctivas, preventivas y de mejora	Sistema Integrado de Gestión	Cada vez que se genere un hallazgo	Líderes de procesos	Reuniones, correo electrónico, revisión gerencial	Alta dirección, gerente general y coordinador de SGC
22	Planificación y cronograma de capacitaciones	Gestión del talento humano	Cada año o cada vez que se modifique el cronograma	A todo el personal relacionado con las capacitaciones	Reuniones, correo electrónico, revisión gerencial	RRHH, Gerente general
23	Programación de auditorias	Auditoría	Cada año o cada vez que se modifique el cronograma	Líderes de proceso, gerencia general, auditores internos	Reuniones, correo electrónico, revisión gerencial	Coordinador de SGC

Fuente elaboración propia

APÉNDICE 14. INSTRUMENTOS UTILIZADOS POR VARIABLES

a) Variable 1: Grado de conformidad con respecto a requisitos de Calidad

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
4. Contexto de la Organización	4.1 Comprensión de la organización y de su contexto	¿La organización ha identificado y comprendido las cuestiones internas y externas que son relevantes para su propósito y su dirección estratégica?	En términos metodológicos, la identificación de factores internos y externos ha demostrado ser superficial y carente de un enfoque analítico adecuado. Además, los ejemplos documentales presentan carencias en la representación precisa de los elementos clave relacionados con la organización y su contexto. La aseguradora no posee una metodología o proceso específico para la realización periódica de dichas evaluaciones de su contexto. Recientemente la organización realizó un análisis FODA el cual no contempla todos los escenarios descritos en los párrafos anteriores.
4. Contexto de la Organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	¿La organización ha determinado y comprendido las necesidades y expectativas de las partes interesadas pertinentes para el sistema de gestión de la calidad?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
4. Contexto de la Organización	4.3 Determinación del alcance del sistema de gestión de la calidad	¿La organización ha definido claramente el alcance de su sistema de gestión de la calidad, identificando los límites y las aplicaciones dentro de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
4. Contexto de la Organización	**4.4 Sistema de gestión de la calidad y sus procesos**		
4. Contexto de la Organización	4.4.1	¿La organización ha identificado los procesos necesarios para el sistema de gestión de calidad y su aplicación a través de la organización?	Metodológicamente, la identificación y evaluación de los procesos es parcial y carece de una cobertura completa, lo que sugiere una falta de profundidad en el análisis. Las técnicas empleadas para esta determinación parecen ser insuficientes, reflejando debilidades en la selección de criterios y en la identificación precisa de los procesos clave. Los ejemplos documentales presentan limitaciones en la representación detallada de la estructura y la interrelación de los procesos identificados. Además, se posee pocos procesos documentados lo cual se ve reflejado en la falta de estandarización de procesos del negocio.
4. Contexto de la Organización	4.4.2	¿La planificación y el control de estos procesos están orientados a lograr los resultados deseados y mejorar la eficacia del sistema de gestión de calidad?	Se observa una falta de rigurosidad en la identificación y clasificación de la información relevante para la organización. Las acciones utilizadas para el mantenimiento y conservación de documentos parecen carecer de la sistematicidad necesaria, reflejando debilidades en la gestión de registros clave de la aseguradora. Además, los ejemplos documentales presentan limitaciones en la demostración clara de las prácticas y procedimientos utilizados para asegurar la integridad y disponibilidad de la información documentada.
5. Liderazgo	**5.1 Liderazgo y compromiso**		
5. Liderazgo	5.1.1 Generalidades	¿Existen evidencias de la participación activa de la alta dirección en la mejora continua del sistema?	Las técnicas empleadas para abordar este requisito son insuficientes, reflejando debilidades en la interpretación y aplicación de los mismos La alta dirección no refleja un compromiso suficiente para reflejar un liderazgo ante los principios de la normativa ISO 9001:2015.
5. Liderazgo	5.1.2 Enfoque al cliente	¿Hay evidencia de que los procesos de negocio incorporan los objetivos y requisitos de calidad?	Las acciones utilizadas para identificar y abordar las expectativas del cliente son insuficientes, evidenciando debilidades en la gestión de la relación con el cliente. Los ejemplos documentales presentan limitaciones en la demostración clara de cómo la organización ha incorporado y respondido a las demandas del cliente. No se posee un medio específico de retroalimentación de los clientes para el negocio lo cual repercute en la no ejecución de procesos que satisfagan a los asegurados en su totalidad.
5. Liderazgo	**5.2 Política**		

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
5. Liderazgo	5.2.1 Establecimiento de la política de la calidad	¿La política de calidad es coherente con los objetivos estratégicos de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
5. Liderazgo	5.2.2 Comunicación de la política de la calidad	¿Hay evidencia de que el personal es consciente de la política de calidad y de su relevancia para las actividades diarias?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
5. Liderazgo	5.3 Roles, responsabilidades y autoridades en la organización	¿Se han asignado roles y responsabilidades para el sistema de gestión de calidad?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
6. Planificación	**6.1 Acciones para abordar riesgos y oportunidades**		
6. Planificación	6.1.1	¿Se documenta el proceso de identificación de riesgos y oportunidades?	Metodológicamente, la planificación para lograr resultados previstos y aumentar defectos deseables parece ser superficial y carente de un enfoque detallado, esto se ve reflejado en que los riesgos y oportunidades no son acordes al contexto de la aseguradora y sus procesos.
6. Planificación	6.1.2	¿Se establecen medidas preventivas y correctivas adecuadas en respuesta a los riesgos y oportunidades identificados?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
6. Planificación	**6.2 Objetivos de la calidad y planificación para lograrlos**		
6. Planificación	6.2.1	¿Se documentan y comunican estos objetivos a través de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
6. Planificación	6.2.2	¿Se asignan responsabilidades y recursos para alcanzar los objetivos de calidad?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
6. Planificación	6.3 Planificación de los cambios	¿Se identifican los impactos potenciales de los cambios y se toman medidas adecuadas para garantizar la integridad del sistema?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
7. Apoyo	**7.1 Recursos**		
7. Apoyo	7.1.1 Generalidades	¿La organización ha determinado y proporciona los recursos necesarios para gestionar el sistema? (Capacidades y limitaciones internas, proveedores externos)	La aseguradora realiza gestiones para la planificación de los recursos de la organización, sin embargo, no se posee ningún registro sobre tal planificación, ni tampoco algún mecanismo que evidencie el seguimiento al mismo.
7. Apoyo	7.1.2 Personas	¿La organización ha determinado y cuenta con el personal suficiente y capaz para la implementación, operación y control del sistema de gestión y de sus procesos?	La comprensión de los requisitos en relación con el personal se aborda de manera parcial, mostrando una falta de profundidad en la evaluación y gestión de las competencias del personal. Los ejemplos documentales proporcionan evidencia de la implementación de procesos relacionados con el personal, pero presentan limitaciones en la representación detallada de cómo se gestionan las competencias y el desarrollo del personal de manera específica.
7. Apoyo	7.1.3 Infraestructura	¿La organización cuenta con la infraestructura y equipos necesarios para lograr la conformidad de sus productos y servicios?	Las técnicas empleadas, aunque indican cierto grado de efectividad, presentan áreas de mejora en la identificación y mantenimiento de la infraestructura clave. Los ejemplos documentales proporcionan evidencia de la implementación de procesos relacionados con la infraestructura, aunque presentan limitaciones en la representación detallada de cómo se gestionan y mantienen específicamente los recursos físicos y tecnológicos.

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
7. Apoyo	7.1.4 Ambiente para la operación de los procesos	¿Se analiza y mantiene el entorno ambiental para el buen funcionamiento de los procesos, productos y servicios?	La comprensión de los requisitos vinculados al ambiente operativo se aborda de manera parcial, mostrando una falta de profundidad en la evaluación y gestión de las condiciones necesarias para la eficaz ejecución de los procesos. No existe evidencia clara del seguimiento y desarrollo de un mecanismo que garantice el adecuado ambiente operacional para los trabajadores de la aseguradora, se presentan limitaciones en la representación detallada de cómo se gestionan y mantienen específicamente las condiciones para la operación efectiva.
7. Apoyo	**7.1.5 Recursos de seguimiento y medición**		
7. Apoyo	7.1.6 Conocimientos de la organización	¿Existe un plan de formación del personal, adaptado a las necesidades actuales y futuras de los procesos, productos y servicios de la organización?	Las acciones empleadas, aunque indican cierto grado de efectividad, presentan áreas de mejora en la identificación, adquisición y aplicación de conocimientos. Los ejemplos documentales proporcionan evidencia de la implementación de procesos relacionados con la gestión del conocimiento, aunque presentan limitaciones en la representación detallada de cómo se adquieren, comparten y aplican específicamente los conocimientos organizacionales.
7. Apoyo	7.2 Competencia	¿Se han determinado las competencias del personal requerido para el funcionamiento y operación del sistema de gestión y sus procesos?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
7. Apoyo	7.3 Toma de conciencia	¿El personal es consciente de la política de calidad, los objetivos, los beneficios del SGC y la mejora?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
7. Apoyo	7.4 Comunicación	¿Se han definido cuáles son las comunicaciones internas y externas relevantes para el sistema de gestión de la calidad?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
7. Apoyo	7.5.1 Generalidades	¿Se tienen definidos documentos aplicables al proceso? (Procedimientos, Instrucciones, Hojas Técnicas, Especificaciones de Producto, Matrices de Control, Formularios, etc.)	Se identifican áreas donde la documentación puede ser más completa y detallada, especialmente en lo que respecta a la determinación de la información documentada necesaria para la eficacia del Sistema de Gestión de la calidad.
7. Apoyo	7.5.2 Creación y actualización	¿Se actualiza y controla de manera eficaz la información documentada del SGC y se asegura su accesibilidad?	La evidencia recopilada refleja la existencia de procedimientos documentados, sin embargo, se identifican deficiencias en la actualización regular y la revisión de la documentación para asegurar su pertinencia y vigencia. No existen procesos documentados y comunicados entre el personal de la aseguradora para establecer una ruta clara de gestión de la documentación en la organización.
7. Apoyo	**7.5.3 Control de la información documentada**		
7. Apoyo	7.5.3.1	¿Puede la organización asegurar la trazabilidad de sus servicios a lo largo de los procesos?	La evidencia recopilada indica que, si bien existe documentación disponible, la accesibilidad y su idoneidad para su uso no están completamente garantizadas. Se observan deficiencias en los mecanismos de protección y en la disponibilidad oportuna de la documentación necesaria. No existe un sitio (por ejemplo intranet) para alojar documentos y que estos sean de accesibilidad para todo el personal de la aseguradora; actualmente cada área y colaborador de la organización resguarda la información en sus computadoras personales. A excepción documentos o registros operaciones resguardados en carpetas compartidas.
7. Apoyo	7.5.3.2	¿Existen medidas para evitar el uso no planificado, la pérdida o el deterioro de la propiedad proporcionada por el cliente?	La evidencia recopilada señala que los procedimientos documentados abordan parcialmente los aspectos relacionados con la distribución, acceso, recuperación y uso de la documentación del sistema de gestión de la calidad. Sin embargo, se identifican deficiencias en el control de cambios, almacenamiento, preservación y disposición de la documentación.
8.Operación	8.1 Planificación y control operacional	Se ha incomparado dentro de la planificación de los procesos las acciones para actuar ante los	La evidencia recopilada indica que si bien existen procedimientos documentados para la planificación y control operacional, se identifican áreas donde la planificación no se alinea completamente con los objetivos estratégicos de la organización. Además, se

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
		riesgos y oportunidades identificadas.	observa una falta de mecanismos efectivos de control operacional para asegurar la consistencia en la ejecución de procesos clave.
8.Operación	**8.2 Requisitos para los productos y servicios**		
8.Operación	8.2.1 Comunicación con el cliente	¿Existe un proceso de comunicación con el cliente para: proporcionar información del producto Consultas, cambios, etc.? ¿Captura de los requisitos del producto y cualquier acción de contingencia que se requiera?	La información recopilada indica que existen procedimientos documentados para la comunicación con el cliente, pero se identifican deficiencias en la claridad y la efectividad de dicha comunicación. Se observa una falta de establecimiento claro de requisitos del cliente y una comunicación proactiva sobre cambios relevantes.
8.Operación	8.2.2 Determinación de los requisitos para los productos y servicios	¿Existe un proceso para confirmar que se comprenden y pueden cumplirse los requisitos de los clientes?	La evidencia recopilada indica que, aunque se han establecido procesos documentados para la determinación de requisitos, se observan áreas donde la identificación y documentación de los requisitos del cliente no son exhaustivas. Se ha detectado una necesidad de mejora en la claridad y la comprensión de los requisitos específicos del cliente.
8.Operación	**8.2.3 Revisión de los requisitos para los productos y servicios**		
8.Operación	8.2.3.1	¿Se asegura la disponibilidad de información actualizada y completa antes de la revisión?	La información recopilada sugiere la existencia de procesos documentados para la revisión antes de comprometerse, pero se identifican deficiencias en la exhaustividad de dichas revisiones. Se observa una necesidad de mejora en la evaluación integral de requisitos del cliente, recursos necesarios y la capacidad de cumplir con los compromisos antes de su aceptación.
8.Operación	8.2.3.2	¿Se asegura la resolución de cualquier discrepancia entre los requisitos del contrato y la oferta?	La evidencia recopilada indica que, si bien se han establecido estrategias para la conservación de información sobre requisitos, se identifican lagunas en la exhaustividad y consistencia de esta conservación. Se observa la necesidad de mejorar, documentar e implementar el control de cambios para asegurar la integridad y accesibilidad de la información relacionada con los requisitos de productos y servicios.
8.Operación	8.2.4 Cambios en los requisitos para los productos y servicios	¿Se lleva a cabo una revisión adicional y se realiza la confirmación de la documentación pertinente antes de aceptar los cambios?	La evidencia recopilada indica que existen procedimientos documentados para gestionar cambios en los requisitos, y se observa un esfuerzo en la comunicación y evaluación de impacto. Sin embargo, se identifican áreas donde la trazabilidad y la revisión completa de los cambios podrían mejorarse.
8.Operación	**8.3 Diseño y desarrollo de los productos y servicios**		
8.Operación	8.3.1 Generalidades	¿Se han establecido y mantenido procedimientos documentados para el diseño y desarrollo?	La evidencia obtenida muestra que la organización ha establecido un proceso de diseño y desarrollo, reflejando un compromiso con la calidad y la entrega de productos y servicios. Se han implementado procedimientos documentados para el diseño y desarrollo, aunque se identifican áreas donde la adecuación y la efectividad del proceso podrían mejorarse.
8.Operación	8.3.2 Planificación del diseño y desarrollo	¿Existe un plan que identifique las responsabilidades, los recursos y los plazos para cada fase del diseño y desarrollo?	La información recopilada indica la existencia de un proceso documentado de planificación del diseño y desarrollo. Sin embargo, se observan áreas donde la planificación podría ser más detallada y abordar de manera más integral los riesgos y las oportunidades asociadas al diseño
8.Operación	8.3.3 Entradas para el diseño y desarrollo	¿Existe un proceso para asegurar que todas las necesidades y expectativas del cliente estén documentadas y consideradas?	La evidencia recopilada indica que la organización ha establecido procedimientos documentados para la identificación y revisión de las entradas del diseño y desarrollo. Sin embargo, se identifican áreas donde la claridad y exhaustividad de las entradas podrían mejorarse. Se sugiere una revisión más detallada de los criterios de diseño y requisitos, asegurando su completa definición y comprensión para orientar eficazmente el proceso de diseño y desarrollo.
8.Operación	8.3.4 Controles del diseño y desarrollo	¿Se lleva a cabo la revisión, verificación y validación en las etapas apropiadas del diseño y desarrollo?	La información recopilada señala que la organización ha establecido procedimientos documentados para los controles del diseño y desarrollo, aunque se identifican deficiencias en la implementación efectiva de medidas de verificación y validación. Se

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
			observa una necesidad de mejorar la revisión y la validación de los resultados del diseño, así como la gestión de los cambios en esta etapa.
8.Operación	8.3.5 Salidas del diseño y desarrollo	¿Se documentan y comunican claramente las especificaciones para la producción y la prestación del servicio?	La evidencia recopilada indica que, aunque la organización ha establecido procedimientos documentados para las salidas del diseño y desarrollo, se identifican áreas donde la claridad y la exhaustividad de dichas salidas podrían mejorarse. Se observa una necesidad de fortalecer la documentación de los resultados del diseño, asegurando una completa definición y comprensión de las especificaciones para orientar eficazmente las etapas posteriores del proceso.
8.Operación	8.3.6 Cambios del diseño y desarrollo	¿Se verifica la integridad del diseño y desarrollo después de cualquier cambio?	La evidencia recopilada indica que, a pesar de contar con procedimientos documentados para gestionar cambios en el diseño y desarrollo, se identifican deficiencias en la evaluación y comunicación efectiva de dichos cambios. Se observa una necesidad de mejorar la revisión y la aprobación de los cambios, así como la comunicación oportuna a todas las partes pertinentes.
8.Operación	**8.4 Control de los procesos, productos y servicios suministrados externamente**		
8.Operación	8.4.1 Generalidades	¿Se han establecido y mantenido procedimientos documentados para el control de la producción y la prestación del servicio?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
8.Operación	8.4.2 Tipo y alcance del control	¿Existen métodos para rastrear y registrar la trazabilidad de los productos y servicios?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
8.Operación	8.4.3 Información para los proveedores externos	¿Existe un proceso para identificar, verificar, proteger y gestionar adecuadamente los activos proporcionados por el cliente?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
8.Operación	**8.5 Producción y provisión del servicio**		
8.Operación	8.5.1 Control de la producción y de la provisión del servicio	¿Existen procedimientos documentados para la gestión y control de los equipos de seguimiento y medición?	La evidencia recopilada indica que, aunque la organización cuenta con procedimientos documentados para el control de la producción y la provisión de servicios, se identifican áreas donde la implementación y el monitoreo podrían ser más rigurosos. Se observa una necesidad de fortalecer la supervisión y verificación de los procesos, así como mejorar la trazabilidad y la documentación de la conformidad con los requisitos especificados.
8.Operación	8.5.2 Identificación y trazabilidad	¿Se mantiene registros de las actividades de verificación y calibración de estos equipos?	La evidencia recopilada indica que la organización cuenta con procedimientos documentados para la identificación y trazabilidad de productos y servicios, aunque se identifican áreas donde la implementación y la documentación podrían ser más robustas. Se ha identificado la necesidad de fortalecer la identificación única de productos y servicios, así como mejorar la trazabilidad a lo largo de las diferentes etapas del proceso.
8.Operación	8.5.4 Preservación	¿Se asegura la identificación, protección y estado de estos equipos?	La evidencia recopilada sugiere que, aunque la organización cuenta con procedimientos documentados para la preservación de productos y servicios, se identifican áreas donde la implementación y seguimiento podrían ser más sólidos. Existe la necesidad de fortalecer los controles de preservación para garantizar la integridad y la conformidad de los productos y servicios a lo largo del tiempo de almacenamiento y manipulación.
8.Operación	8.5.5 Actividades posteriores a la entrega	¿Existen condiciones ambientales específicas para el almacenamiento y manejo de estos equipos?	La evidencia recopilada indica que la organización posee procedimientos documentados para las actividades posteriores a la entrega de productos y servicios, aunque se identifican áreas donde la implementación y el monitoreo podrían ser más efectivos. Se observa la necesidad de fortalecer la supervisión y seguimiento de las actividades posteriores a la entrega, asegurando la conformidad continua con los requisitos y la satisfacción del cliente.
8.Operación	8.5.6 Control de los cambios	¿Se documentan y comunican las acciones correctivas y preventivas tomadas?	La información recopilada indica que, a pesar de contar con procedimientos documentados para el control de los cambios, se identifican áreas donde la gestión y documentación de los cambios podrían ser más robustas.

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
			Existe la necesidad de fortalecer la revisión y aprobación de los cambios, así como la comunicación efectiva a las partes pertinentes.
8.Operación	8.6 Liberación de los productos y servicios	¿Se lleva a cabo la revisión y aprobación necesaria antes de la liberación?	La información recopilada indica que, aunque la organización cuenta con procedimientos documentados para la liberación de productos y servicios, se identifican áreas donde la implementación y verificación de la liberación podrían ser más rigurosas. Se observa una necesidad de fortalecer los controles y la documentación para asegurar la conformidad con los criterios de liberación y la prevención de productos no conformes.
8.Operación	**8.7 Control de las salidas no conformes**		
8.Operación	8.7.1	¿Se asegura que las no conformidades detectadas sean documentadas, evaluadas y gestionadas de manera adecuada?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
8.Operación	8.7.2	¿Existe un proceso para la revisión y evaluación sistemática de las no conformidades y la implementación de acciones para abordarlas?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	**9, Evaluación del desempeño**		
9. Seguimiento y evaluación	**9.1 Seguimiento, medición, análisis y evaluación**		
9. Seguimiento y evaluación	9.1.1 Generalidades	¿Se documentan y mantienen registros de las actividades de seguimiento y medición realizadas?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	9.1.2 Satisfacción del Cliente	¿Existen procesos establecidos para abordar quejas y preocupaciones de los clientes de manera efectiva?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	9.1.3 Análisis y evaluación	¿Se incorpora la retroalimentación en procesos de mejora continua?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	**9.2 Auditoría interna**		
9. Seguimiento y evaluación	9.2.1	¿Se asegura de que las auditorías cubran áreas relevantes y se realicen de acuerdo con el programa establecido?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	9.2.2	¿Existe un proceso documentado para llevar a cabo a cabo las auditorías internas, incluida la preparación, la ejecución y la presentación de informes?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	**9,3 Revisión por la dirección**		
9. Seguimiento y evaluación	9.3.1	¿Se asegura de que estas revisiones incluyan la evaluación del desempeño del sistema de gestión de calidad y la idoneidad de la política y objetivos?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	9.3.2	¿Cómo se garantiza que la alta dirección tenga acceso a la información relevante para tomar decisiones informadas?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	9.3.3 Salidas de la revisión por la dirección	¿Existen procesos para la identificación y seguimiento de las acciones resultantes de estas revisión?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
10. Mejora	**10 Mejora**		
10. Mejora	10.1 Generalidades	¿Se promueve activamente la cultura de mejora continua en todos los niveles de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
10. Mejora	**10.2 No conformidades y acción correctiva**		
10. Mejora	10.2.1	¿Existe un proceso documentado para la gestión de no conformidades y la aplicación de acciones correctivas?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
10. Mejora	10.2.2	¿Se verifica la eficacia de las acciones correctivas implementadas?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
10. Mejora	10.3 Mejora continua	¿Existen procesos para identificar oportunidades de mejora y para implementar cambios que contribuyan al desarrollo sostenible de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.

b) Variable 4: Identificación del cumplimiento de la organización ante los requisitos de normativa ISO/IEC 27001:2022

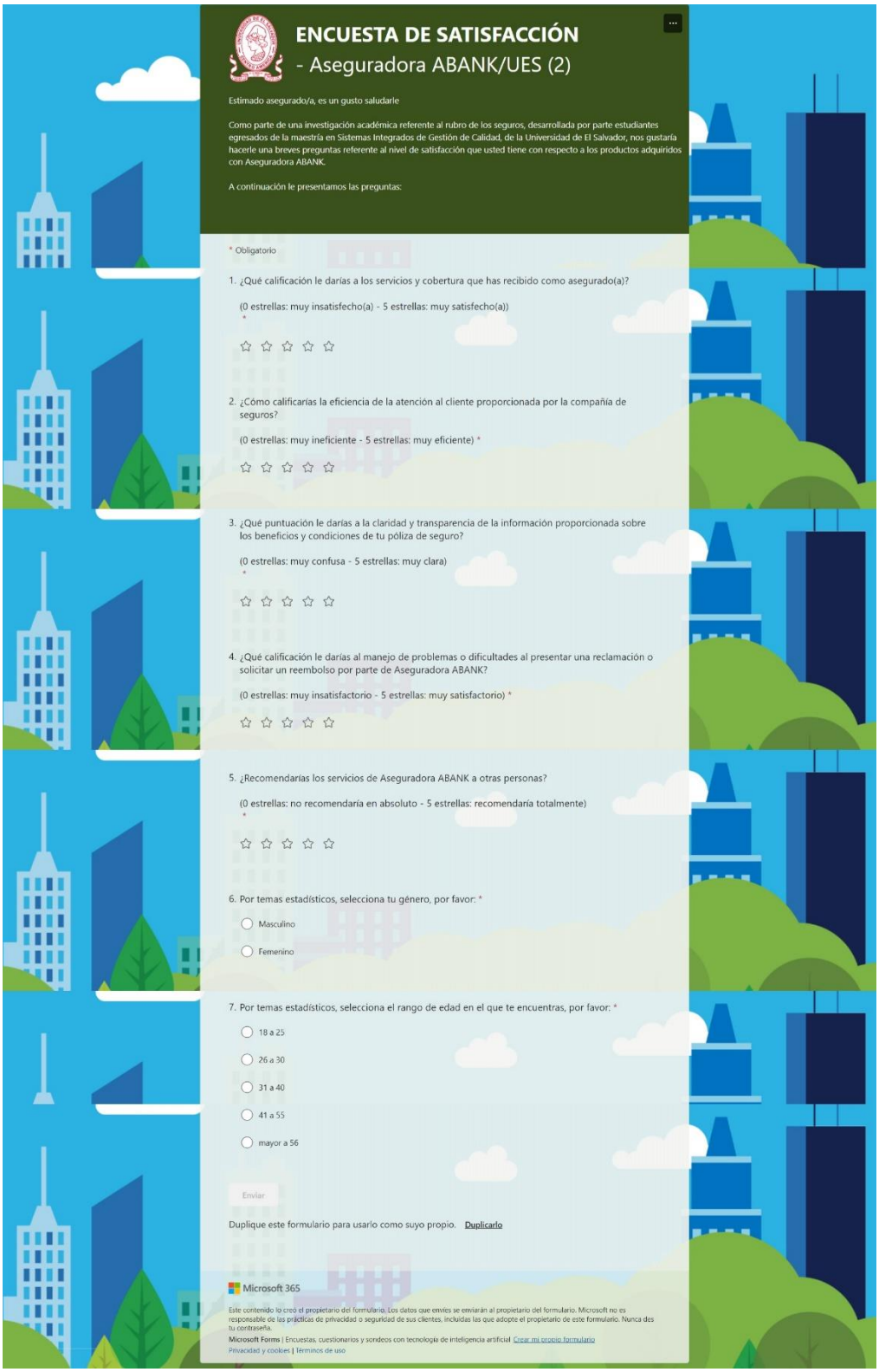
Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
4. Contexto de la organización	4.1 Comprensión de la organización y de su contexto	¿La organización ha identificado y comprendido las cuestiones internas y externas que son relevantes para su propósito y su dirección estratégica?	En términos metodológicos, la identificación de factores internos y externos ha demostrado ser superficial y carente de un enfoque analítico adecuado. Además, los ejemplos documentales presentan carencias en la representación precisa de los elementos clave relacionados con la organización y su contexto. La aseguradora no posee una metodología o proceso específico para la realización periódica de dichas evaluaciones de su contexto. Recientemente la organización realizó un análisis FODA el cual no contempla todos los escenarios descritos en los párrafos anteriores.
4. Contexto de la organización	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	¿La organización ha determinado y comprendido las necesidades y expectativas de las partes interesadas pertinentes para el sistema de gestión de seguridad de la información?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
4. Contexto de la organización	4.3 Determinación del alcance del sistema de gestión de la SI	¿La organización ha definido claramente el alcance de su sistema de gestión de la seguridad de la información, identificando los límites y las aplicaciones dentro de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
4. Contexto de la organización	4.4 Sistema de gestión de SI	¿La organización ha identificado los procesos necesarios para el sistema de gestión de seguridad de la información y su aplicación a través de la organización?	Se observa una falta de rigurosidad en la identificación y clasificación de la información relevante para la organización. Las acciones utilizadas para el mantenimiento y conservación de documentos parecen carecer de la sistematicidad necesaria, reflejando debilidades en la gestión de registros clave de la aseguradora. Además, los ejemplos documentales presentan limitaciones en la demostración clara de las prácticas y procedimientos utilizados para asegurar la integridad y disponibilidad de la información documentada.

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
5. Liderazgo	5.1 Liderazgo y compromiso	¿Existen evidencias de la participación de la alta dirección en la mejora continua del sistema?	Las técnicas empleadas para abordar este requisito son insuficientes, reflejando debilidades en la interpretación y aplicación de los mismos La alta dirección no refleja un compromiso suficiente para reflejar un liderazgo ante los principios de la normativa ISO/IEC 27001:2022.
5. Liderazgo	5.2 Política	¿Existe una política de seguridad de la información, coherente con los objetivos estratégicos de la organización?	En la organización ha establecido una política no documentada sobre seguridad de la información y continuidad del negocio, dicho documento no es oficial y no se ha comunicado ante la organización.
5. Liderazgo	5.3 Funciones, responsabilidades y autoridades de la organización	¿Se han asignado roles y responsabilidades para el sistema de gestión de seguridad de la información?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
6. Planificación	**6.1 Acciones para abordar riesgos y oportunidades**		
6. Planificación	6.1.1 Generalidades	¿Se han establecido acciones para abordar los riesgos y aprovechar las oportunidades identificadas?	Metodológicamente, la planificación para lograr resultados previstos y aumentar defectos deseables parece ser superficial y carente de un enfoque detallado, esto se ve reflejado en que los riesgos y oportunidades no son acordes al contexto de la aseguradora y sus procesos.
6. Planificación	6.1.2 Evaluación de riesgos de SI	¿Existe un enfoque coherente para asegurar que la seguridad de la información esté alineada con los objetivos y procesos de la organización?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
6. Planificación	6.1.3 Tratamiento de RI de SI	¿Se documentan y revisan periódicamente los resultados de la evaluación del riesgo?	La aseguradora realiza acciones para dar tratamiento de las actividades sospechosas y riesgos mapeados en la organización, sin embargo, este seguimiento es reactivo y no proactivo, por lo que no existe un procedimiento o metodología de seguimiento y desarrollo de dichos tratamientos.
6. Planificación	6.2 Objetivos de la SI y planificación para lograrlos	¿Se documentan y revisan periódicamente los resultados de la evaluación del riesgo?	Se han definido objetivos para la seguridad e la información, pero no se encuentran documentados ni existe un plan para que la aseguradora los alcance.
6. Planificación	6.3 Planificación de los cambios	¿Se monitorean y revisan regularmente las medidas de tratamiento de riesgos para evaluar su eficacia?	La aseguradora desarrolla de forma genérica iniciativas de gestión de cambios, sin embargo, no está documentado ni existe un procedimiento estandarizado que estandarice y guíe a la organización para lograr una efectiva gestión del cambio adecuadamente organizada.
7. Apoyo	7.1 Recursos	¿Se revisan regularmente las necesidades de recursos para asegurar su adecuación?	La aseguradora realiza gestiones para la planificación de los recursos de la organización, sin embargo, no se posee ningún registro sobre tal planificación, ni tampoco algún mecanismo que evidencie el seguimiento al mismo.
7. Apoyo	7.2 Competencia	¿Se proporciona formación y desarrollo continuo para garantizar que el personal tenga las habilidades y conocimientos necesarios?	En cuanto a competencia sobre el personal orientado a la seguridad de la información, la aseguradora procura garantizar la idoneidad de sus colaboradores; sin embargo, no se posee una metodología o mecanismo para desarrollar a dicho personal. De igual forma no se posee información documentada que lo evidencie.
7. Apoyo	7.3 Toma de conciencia	¿Existen programas de sensibilización y formación para fomentar la toma de conciencia sobre la seguridad de la información?	La aseguradora desarrolla campañas de concientización y conocimiento sobre seguridad de la información, sin embargo, esto se realiza sin establecer una calendarización o metodología que garantice el éxito del programa a largo plazo.
7. Apoyo	7.4 Comunicación	¿Se asegura de que la información sobre la seguridad de la información se comunica de manera efectiva a las partes interesadas pertinentes?	Se observa que existen comunicaciones sobre los acontecimientos sobre seguridad e la información de forma particular, debido a que la comunicación no es proactiva, sino reactiva y sin seguimiento a lo largo del tiempo. Actualmente la comunicación se realiza básicamente por medio de correo electrónico.
7. Apoyo	7.5.1 Generalidades	¿Se asegura de que la información documentada sea adecuada, esté actualizada y esté disponible cuando sea necesario?	Se identifican áreas donde la documentación puede ser más completa y detallada, especialmente en lo que respecta a la determinación de la información documentada necesaria para la eficacia del Sistema de Gestión de la Seguridad de la Información.

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
7. Apoyo	7.5.2 Creación y actualización	¿Se establecen revisiones regulares para garantizar que la información documentada esté al día?	La evidencia recopilada refleja la existencia de procedimientos documentados, sin embargo, se identifican deficiencias en la actualización regular y la revisión de la documentación para asegurar su pertinencia y vigencia. No existen procesos documentados y comunicados entre el personal de la aseguradora para establecer una ruta clara de gestión de la documentación en la organización.
7. Apoyo	7.5.3 Control de información documentada	¿Existe un proceso para identificar, proteger y asegurar la integridad de la información documentada?	La evidencia recopilada indica que, si bien existe documentación disponible, la accesibilidad y su idoneidad para su uso no están completamente garantizadas. Se observan deficiencias en los mecanismos de protección y en la disponibilidad oportuna de la documentación necesaria. No existe un sitio (por ejemplo, intranet) para alojar documentos y que estos sean de accesibilidad para todo el personal de la aseguradora; actualmente cada área y colaborador de la organización resguarda la información en sus computadoras personales. A excepción documentos o registros operaciones resguardados en carpetas compartidas
8. Operación	8.1 Planificación y control operacional	¿Se documentan y comunican los procedimientos y responsabilidades operativas pertinentes?	La evidencia recopilada indica que, si bien existen procedimientos documentados para la planificación y control operacional, se identifican áreas donde la planificación no se alinea completamente con los objetivos estratégicos de la organización. Además, se observa una falta de mecanismos efectivos de control operacional para asegurar la consistencia en la ejecución de procesos clave.
8. Operación	8.2 Evaluación de RI de SI	¿Existen medidas para proteger la confidencialidad, integridad y disponibilidad de los activos de información?	Existen en la aseguradora mecanismos para la evaluación de los riesgos según las normativas de los entes reguladores, sin embargo, no existen evidencia documental del seguimiento a lo largo del tiempo sobre dichas evaluaciones relacionadas a seguridad de la información.
8. Operación	8.3 Tratamiento de RI de SI	¿Se establecen requisitos de seguridad de la información en los acuerdos con proveedores y socios comerciales?	Se realizan acciones específicas para el tratamiento de riesgos relacionados con seguridad de la información, sin embargo, no se posee evidencia documental de seguimiento proactivo a dichos planes de acción.
9. Seguimiento y evaluación	**9. Evaluación del desempeño**		
9. Seguimiento y evaluación	9.1 Seguimiento, medición, análisis y evaluación	¿Se documentan y revisan periódicamente los resultados del seguimiento y la medición?	Para seguridad de la información se poseen indicadores de medición que ayudan a entender el contexto de la operación de cara a este aspecto, sin embargo, se ha observado que no se posee evidencia de seguimientos oportunos, además, no existe un mecanismo de acción a seguir para los incumplimientos y demás tipo de situaciones que evidencien alerta ante la seguridad de la información.
9. Seguimiento y evaluación	**9.2 Auditoría interna**		
9. Seguimiento y evaluación	9.2.1 Generalidades	¿Se asegura de que las auditorías se refieren a áreas relevantes y se realizan de acuerdo con el programa establecido?	Se considera en la organización la realización de auditorías para la seguridad de la información de forma reactiva; no existe un programa específico o un mecanismo que garantice la evaluación periódica y efectiva a este aspecto. De igual forma no existe documentación que respalde esta actividad.
9. Seguimiento y evaluación	9.2.2 Programa de auditoría interna	¿Existe un proceso documentado para llevar a cabo a cabo las auditorías internas, incluyendo la preparación, ejecución y presentación de informes?	Se ejecutan sesiones de revisión, con enfoque de auditoría, pero no poseen la rigidez e integridad de una auditoría formal, no se documenta adecuadamente ni se da el seguimiento oportuno.
9. Seguimiento y evaluación	**9.3 Revisión por la dirección**		
9. Seguimiento y evaluación	9.3.1 Generalidades	¿Se asegura de que estas revisiones incluyan la evaluación del desempeño de SGSI y la idoneidad de la política y los objetivos?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.

Capítulo de norma	Punto de norma	Preguntas	Resultado obtenido
9. Seguimiento y evaluación	9.3.2 Entradas de la revisión por la dirección	¿Se garantiza que la alta dirección tenga acceso a la información relevante para tomar decisiones informadas?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
9. Seguimiento y evaluación	9.3.3 Resultados de la revisión por la dirección	¿Existen procesos para la identificación y seguimiento de las acciones resultantes de estas revisión?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
	10 Mejora		
10. Mejora	10.1 Mejora continua	¿Se han establecido procesos para identificar y abordar oportunidades de mejora y no conformidades?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.
10. Mejora	10.2 No conformidades y acción correctiva	¿Se verifica la eficacia de las acciones correctivas implementadas para prevenir la recurrencia de no conformidades?	La aseguradora no posee ninguna evidencia que cumpla con este punto de norma.

APÉNDICE 15. PLANTILLA DE ENCUESTAS DE SATISFACCIÓN AL CLIENTE



ENCUESTA DE SATISFACCIÓN
- Aseguradora ABANK/UES (2)

Estimado asegurado/a, es un gusto saludarle

Como parte de una investigación académica referente al rubro de los seguros, desarrollada por parte estudiantes egresados de la maestría en Sistemas Integrados de Gestión de Calidad, de la Universidad de El Salvador, nos gustaría hacerle una breves preguntas referente al nivel de satisfacción que usted tiene con respecto a los productos adquiridos con Aseguradora ABANK.

A continuación le presentamos las preguntas:

* Obligatorio

1. ¿Qué calificación le darías a los servicios y cobertura que has recibido como asegurado(a)?

(0 estrellas: muy insatisfecho(a) - 5 estrellas: muy satisfecho(a)) *

☆ ☆ ☆ ☆ ☆

2. ¿Cómo calificarías la eficiencia de la atención al cliente proporcionada por la compañía de seguros?

(0 estrellas: muy ineficiente - 5 estrellas: muy eficiente) *

☆ ☆ ☆ ☆ ☆

3. ¿Qué puntuación le darías a la claridad y transparencia de la información proporcionada sobre los beneficios y condiciones de tu póliza de seguro?

(0 estrellas: muy confusa - 5 estrellas: muy clara) *

☆ ☆ ☆ ☆ ☆

4. ¿Qué calificación le darías al manejo de problemas o dificultades al presentar una reclamación o solicitar un reembolso por parte de Aseguradora ABANK?

(0 estrellas: muy insatisfactorio - 5 estrellas: muy satisfactorio) *

☆ ☆ ☆ ☆ ☆

5. ¿Recomendarías los servicios de Aseguradora ABANK a otras personas?

(0 estrellas: no recomendaría en absoluto - 5 estrellas: recomendaría totalmente) *

☆ ☆ ☆ ☆ ☆

6. Por temas estadísticos, selecciona tu género, por favor: *

- ◯ Masculino
- ◯ Femenino

7. Por temas estadísticos, selecciona el rango de edad en el que te encuentras, por favor: *

- ◯ 18 a 25
- ◯ 26 a 30
- ◯ 31 a 40
- ◯ 41 a 55
- ◯ mayor a 56

Enviar

Duplique este formulario para usarlo como suyo propio. **Duplicarlo**

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial Crear mi propio formulario

Privacidad y cookies | Términos de uso

Llenado de encuesta de satisfacción_ Aseguradora ABANK - Fines académicos - Mensaje (HTML)

Archivo | Mensaje | Insertar | Opciones | Formato de texto | Revisar | ¿Qué desea hacer?

Pegar | Cortar | Copiar | Copiar formato — Portapapeles

Segoe UI | 10.5 — Texto básico

Libreta de direcciones | Comprobar nombres — Nombres

Adjuntar archivo | Adjuntar elemento | Firma — Incluir

Seguimiento | Importancia alta | Importancia baja — Etiquetas

Ideas Viva

Ver plantillas — Mis plantillas

Enviar

Para... cristina.lopez@hotmail.com ricardo.martinez@hotmail.com luciago87_@hotmail.com andres.perez@hotmail.com mariana.diaz@hotmail.com julio.rodriguez@hotmail.com daniela.hernandez@hotmail.com carlos.sanchez@hotmail.com paula.gomez@hotmail.com javier.r78@hotmail.com estefania.fernandez@hotmail.com felipe.garcia@hotmail.com valeria.torres@hotmail.com matias.945@hotmail.com laura.estrada@hotmail.com juan.carvajal@hotmail.com sofia.mendoza@hotmail.com alejandro.34@hotmail.com camila.alvarez@hotmail.com diego.kilas@hotmail.com maria.rios@hotmail.com carolina.gutierrez@hotmail.com roberto.chavez@hotmail.com andrea.flores@hotmail.com manuel.vargas@hotmail.com ...

CC...

Asunto: Llenado de encuesta de satisfacción_ Aseguradora ABANK - Fines académicos

Estimado asegurado/a, es un gusto saludarle

Como parte de una investigación académica referente al rubro de los seguros, desarrollada por parte estudiantes egresados de la maestría en Sistemas Integrados de Gestión de Calidad, de la Universidad de El Salvador, nos gustaría hacerle una breves preguntas referente al nivel de satisfacción que usted tiene con respecto a los productos adquiridos con Aseguradora ABANK.

https://forms.office.com/r/8pGeHEmStK

o por medio de código QR:

ANEXO 1. CONSENTIMIENTO INFORMADO DE RESULTADOS INVESTIGATIVOS

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD

San Salvador El Salvador América Central
Teléfonos: (503) 2521-0170 / 2521-0173 Correo electrónico: masig.economia@ues.edu.sv

Ciudad Universitaria, 27 de enero de 2023

Estimado(a)(s)
Lic. / Ing. / Dr. Jaime Fernando García-Prieto Figueroa
Director Presidente
Aseguradora ABANK, S.A. Seguros de Personas
Presente

Reciba un cordial saludo de la Dirección de la Maestría en Sistemas Integrados de Gestión de la Calidad de la Facultad de Ciencias Económicas de la Universidad de El Salvador.

Por este medio respetuosamente solicito la atención del(la)(s) Lic.(a)/Ing.(a)/Dr.(a) **Muñoz Sosa, Nora Nathaly (MS21032)** y **Rodas Laínez, Gustavo Manuel (RL21027)**, estudiante(s) egresados(s) de la **MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD (MASIG)** de la Facultad de Ciencias Económicas de la Universidad de El Salvador, quién(es) se encuentra(n) en la **etapa de identificar su tema preliminar de trabajo de graduación y formular su respectivo anteproyecto**, el cual debe considerar las siguientes características:

a) Orientado a la realidad nacional.
b) Con utilidad social, es decir de preferencia beneficiar a un sector del país y no a una organización en particular.
c) Enfocado en investigación aplicada, con apego práctico.
d) Calidad y veracidad de la información reflejada en el documento final.
e) Con una redacción estructurada, lógica, sencilla y de fácil comprensión, según normas APA.
f) Aplicación de una metodología adecuada y coherente con un trabajo de investigación de nivel de maestría.
g) Libre de errores de ortografía y gramática.
h) Apegado a criterios éticos y de profesionalismo de un trabajo de esta naturaleza.

Dicho trabajo de graduación debe enfocarse en términos generales en los sistemas integrados de gestión (por ejemplo: calidad, ambiente, seguridad y salud en el trabajo, etc.) en base a normas internacionales y/o la reglamentación aplicable, como mínimo en dos ámbitos de gestión y se desarrollará en un período mínimo de 6 meses y un máximo de 12 meses. A partir de los resultados de la investigación del trabajo de graduación aplicado a la organización sujeto del estudio, el análisis e interpretación los resultados de la etapa de campo, los maestrantes procederán a la realización de una propuesta de sistema integrado de gestión aplicado a la organización sujeto del estudio con enfoque de consultoría empresarial.

Como tema de su trabajo de graduación el/la/los(as) maestrante(s) ha(n) identificado el siguiente como propuesta preliminar **"DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE CALIDAD NTS ISO 9001:2015 Y DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022 APLICABLE EN ASEGURADORA ABANK, S. A., SEGUROS DE PERSONAS, LA LIBERTAD, EL SALVADOR"**, para lo cual, **en los casos de aplicación a una organización determinada, se requiere carta formal de "consentimiento informado" declarando de forma explícita el conocimiento y aceptación de los siguientes términos, de preferencia por un nivel de dirección o gerencial de la organización sujeto del estudio**:

- La empresa u organización debe asegurar el trabajo de campo de los maestrantes para la recopilación de la información cualitativa y cuantitativa de la investigación / consultoría mediante la realización de entrevistas, encuestas, observación de procesos y actividades, revisión de documentos y registros, informes, entre otras metodologías y herramientas para tener acceso a fuentes documentales y no documentales, con la participación activa de personal clave de la

organización, mediante un plan de visitas debidamente organizado y consensuado para asegurar la viabilidad de la investigación en la etapa metodológica y de obtención de la información requerida del sujeto de estudio, acorde al anteproyecto formulado y aprobado al inicio del trabajo de graduación.

- El documento final del trabajo de graduación con sus diferentes apartados de marco referencial, marco teórico, marco metodológico y resultados de la investigación y la propuesta de diseño del sistema integrado de gestión, entre otros apartados de un documento académico aplicado a nivel de maestría, será de dominio público, a través de su publicación y las consultas en las bibliotecas de la Facultad de Ciencias Económicas y de la Universidad de El Salvador y en los diferentes repositorios institucionales u otras fuentes de la red de internet.

El(la)(los)(las) maestrante(s) se compromete(n) a entregar los diferentes productos resultantes del trabajo de graduación como documento final de tesis y/o entregables parciales del proyecto de trabajo de graduación a la empresa u organización sujeto del estudio, una vez sean aprobados por la Coordinación MASIG acorde al Proceso de Seminario de Trabajo de Graduación correspondiente.

No omito manifestar el agradecimiento por la atención a la presente.

Atentamente,

COORDINACION MASIG

Maestro Julio César Valle Valdez
M. en Administración de Empresas y Consultoría Empresarial
M. en Gestión Ambiental

Maestro Julio César Valle Valdez
Coordinador MASIG – FCE - UES
Teléfono 25210175 – Correo electrónico julio.valle@ues.edu.sv
Maestría en Sistemas Integrados de Gestión de Calidad (MASIG)
Facultad de Ciencias Económicas – Universidad de El Salvador

c.c.: Expediente(s) alumno(s)

Recibido

Aseguradora ABANK
Aseguradora ABANK, S.A.
Seguros de personas

COORDINACION MASIG FCE/UES

Maestro Julio César Valle Valdez
M. en Administración de Empresas y Consultoría Empresarial
M. en Gestión Ambiental

RECIBIDO 28 FEB 2023

ANEXO 2. VIABILIDAD DEL CONSENTIMIENTO INFORMADO DEL SUJETO DE ESTUDIO

Aseguradora ABANK

Lunes 06 de febrero de 2022

Maestría en Sistemas Integrados de Gestión de Calidad,
Facultad de Ciencias Económicas
Universidad Nacional de El Salvador
Presente

A quien corresponda:

Un gusto saludarlos/as, mi nombre es Jaime Fernando García-Prieto, con documento único de identificación (DUI): 01306685-3 y con el cargo de Director Presidente en Aseguradora Abank, S.A., Seguros de Personas; el motivo de la presente carta es comunicar el **consentimiento** por parte de Aseguradora Abank, para la realización del trabajo de graduación denominado **"DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE CALIDAD NTS ISO 9001:2015 Y DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022 APLICABLE EN ASEGURADORA ABANK, S. A., SEGUROS DE PERSONAS, LA LIBERTAD, EL SALVADOR."**, a realizar por parte de los profesionales Nora Nathaly Muñoz Sosa, con carnet de identificación estudiantil MS21032 y Gustavo Manuel Rodas Laínez, con carnet RL21027, estudiante(s) egresado(s) de la **MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD (MASIG)** de la Facultad de Ciencias Económicas de la Universidad de El Salvador.

Como Aseguradora Abank, se da el aval para que se realice dicho trabajo de graduación a partir de enero 2023 a julio 2023; considerando que el *alcance del trabajo de graduación abarca los macroprocesos de Comercialización, Suscripción, Gestión de la emisión, Cobranzas, Ciclo de siniestros, Servicios postventa y procesos de Seguridad de la Información* que intervengan en el diseño del Sistema Integrado de Gestión ISO 9001:2015 e ISO 27001:2022.

Por nuestra parte, y cumpliendo en todo momento las regulaciones fiscalizadoras, tributarias y de supervisión que nos rigen, garantizamos el proveer mecanismos que faciliten la recopilación de la información cualitativa y cuantitativa, realización de entrevistas, encuestas, observación de procesos y actividades, revisión de documentos y registros, informes, entre otras metodologías y herramientas para tener acceso a fuentes documentales y no documentales, con la participación activa de personal clave de la organización, mediante un plan de visitas debidamente organizado y consensuado. De igual forma se autoriza para que el documento final sea de dominio público.

Aseguradora Abank bajo acuerdo mutuo con los profesionales antes mencionados, acordaron el notificar a la aseguradora avances y entregables del trabajo de graduación y que el documento final también se entregará a la compañía.

Atentamente,

Aseguradora ABANK
Aseguradora ABANK, S.A.
Seguros de personas

Jaime Fernando García-Prieto
Director Presidente
Teléfono 2521-8300 – Correo electrónico: jgarciaprieto@aseguradoraabank.com
Aseguradora Abank, S.A, Seguros de Personas

Maestro Julio César Valle Valdez
M. en Administración de Empresas y Consultoría Empresarial
M. en Gestión Ambiental

MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD
COORDINACION MASIG
FCE/UES

RECIBIDO 28 FEB 2023

Aseguradora ABANK S.A. Seguros de Personas, antes Aseguradora Vivir

ANEXO 3. CARTA DE VIABILIDAD METODOLÓGICA

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
MAESTRÍA EN SISTEMAS INTEGRADOS DE GESTIÓN DE CALIDAD
San Salvador El Salvador América Central
Teléfonos: (503) 2521-0170 / 2521-0173 Correo electrónico: masig.economia@ues.edu.sv

Ciudad Universitaria, San Salvador, junio de 2023

ANTEPROYECTO DE TRABAJO DE GRADUACIÓN – MASIG 6ª GENERACIÓN

"DICTAMEN DE APROBACIÓN CON OBSERVACIONES"

En el marco del desarrollo del Anteproyecto de Trabajo de Graduación correspondiente a la 6ª Generación de la Maestría en Sistemas Integrados de Gestión de Calidad (M10811 – 2016) cumpliendo el documento de referencia de "Metodología del Proceso de Trabajo de Graduación de la MASIG 6a Promoción – Ciclo I / 2023" con Acuerdo No. 1,080 de Junta Directiva Período 2021/2023 de la Facultad de Ciencias Económicas de la Universidad de El Salvador, de sesión ordinaria No. 39-2023 de fecha 15 de marzo de 2023 y la correspondiente "Programación del Seminario de Trabajo de Graduación" durante el Ciclo I del Año Académico 2023, en referencia al tema **"DISEÑO DE UN SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD ISO 9001:2015, Y SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022; APLICABLE EN ASEGURADORA ABANK, S. A. SEGUROS DE PERSONAS"** inscrito/presentado por el(la)(los)(las) maestrante(s):

- **Ing. MUÑOZ SOSA, NORA NATHALY (MS21032)**
- **Ing. RODAS LAÍNEZ, GUSTAVO MANUEL (RL21027)**

Posterior a la **revisión del Anteproyecto de Trabajo de Graduación** por la "Coordinación MASIG" y la respectiva exposición y defensa por los maestrantes en fecha 10 de junio de 2023 ante el Coordinador de la MASIG y el "Asesor" asignado, se presenta el siguiente **"DICTAMEN DE ANTEPROYECTO DE TRABAJO DE GRADUACIÓN (ATG)":**

- **Ing. MUÑOZ SOSA, NORA NATHALY (MS21032)**
- **Ing. RODAS LAÍNEZ, GUSTAVO MANUEL (RL21027)**

Posterior a la **revisión del Anteproyecto de Trabajo de Graduación** por la "Coordinación MASIG" y la respectiva exposición y defensa por los maestrantes en fecha 10 de junio de 2023 ante el Coordinador de la MASIG y el "Asesor" asignado, se presenta el siguiente **"DICTAMEN DE ANTEPROYECTO DE TRABAJO DE GRADUACIÓN (ATG)":**

☐ APROBADO ☒ **APROBADO CON OBSERVACIONES**

En base a lo anterior, la Coordinación de la MASIG emite el respectivo dictamen de "APROBACIÓN DE ATG" con los efectos consiguientes.

Maestro Julio César Valle Valdez
Coordinador MASIG – FCCEE - UES
Teléfono 25210175 – Correo electrónico julio.valle@ues.edu.sv
Maestría en Sistemas Integrados de Gestión de Calidad (MASIG)
Facultad de Ciencias Económicas – Universidad de El Salvador

Con conocimiento: **Maestra Ing. Mónica Romero de Ulloa (Asesora).**

c.c.: Expediente(s) alumno(s) MASIG.

BREVE HOJA DE VIDA DE MAESTRANTES EGRESADOS MASIG

El equipo de maestrantes egresados MASIG, autores del Anteproyecto de Trabajo de Graduación; presenta sus correspondientes hojas de vida, evidenciando en ellas; las competencias y pericias viables para la efectiva realización del trabajo de graduación.

Nora Nathaly Muñoz Sosa

Maestrante egresada MASIG No. Carné: MS21032

- Nombre del proyecto servicio social MASIG: "Capacitaciones en Medio Ambiente y Seguridad y Salud en el Trabajo en la Academia Nacional de Seguridad Pública (ANSP)"
- Nivel académico y nombre de Titulo: Ingeniera Química. Universidad Centroamericana "José Simeón Cañas"-Antiguo Cuscatlán, El Salvador, 2019
- Experiencia profesional y/o laboral: Coordinadora de Control de Calidad, Fulltac Adhesive & Coatings
- Formación adicional: Yellow Belt Lean Six Sigma,
- Habilidades, destrezas, logros e intereses: Facilidad para trabajar en equipo, persistencia y constancia para obtener los resultados deseados.
- Teléfono Móvil: 7967-5625
- E-mail: ms21032@ues.edu.sv

Gustavo Manuel Rodas Laínez

Maestrante egresado MASIG No. Carné: RL21027

- Nombre del proyecto servicio social MASIG: "Capacitaciones en Medio Ambiente y Seguridad y Salud en el trabajo en la Academia Nacional de Seguridad Pública (ANSP)"
- Nivel académico y nombre de Titulo: Ingeniero Industrial. Universidad Francisco Gavidia El Salvador –San Salvador, El Salvador, 2020
- Experiencia profesional: Coordinador de procesos y RPA, Aseguradora ASSA.
- Formación adicional: Yellow Belt Lean Six Sigma.
- Habilidades, destrezas, logros e intereses: conocimiento sobre tecnologías de la información y las comunicaciones, filosofía lean para mejora continua, proactivo y constante.
- Teléfono Móvil: 7096-6078
- E-mail**:** rl21027@ues.edu.sv