**UNIVERSIDAD DE EL SALVADOR**

**FACULTAD DE CIENCIAS ECONÓMICAS**

TRABAJO DE ESPECIALIZACIÓN EN: AUDITORIA INTERNA

# "IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS AL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN, PARA UNA ENTIDAD DEDICADA A LA PRESTACIÓN DE SERVICIOS DE GESTIÓN EMPRESARIAL"

**PRESENTADO POR:**


| | |
|---|---|
| MEJÍA SOLA JENNY CLARIBEL | L10802 |
| MIGUEL HERNÁNDEZ WEDER JOSUÉ | L10802 |
| SOSA UMAÑA MARCOS ALEXANDER | L10802 |


PARA OPTAR AL GRADO DE: LICENCIATURA EN CONTADURÍA PÚBLICA

NOVIEMBRE 2023

CIUDAD UNIVERSITARIA DR. FABIO CASTILLO FIGUEROA

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

**AUTORIDADES CENTRALES**

| | |
|---|---|
| Rector | : Ing. Juan Rosa Quintanilla |
| Vicerrectora Académica | : Dra. Evelyn Beatriz Farfán Mata |
| Secretario General | : Lic. Pedro Rosalío Escobar Castaneda |

**AUTORIDADES DE LA FACULTAD**

| | |
|---|---|
| Decana de la Facultad de Ciencias económicas | : Licda. Celina Amaya de Calderón |
| Secretario de la Facultad de Ciencias Económicas | : Lic. Pedro Javier Rivas Mejía |
| Director de la Escuela de Contaduría Pública | : Msc. Mauricio Ernesto Magaña Menéndez |
| Coordinador General del Proceso de Grado | : Maf. Ronald Edgardo Gálvez Rivera |
| Coordinador de Proceso de Grado de la Escuela de Contaduría Pública | : Lic. Daniel Nehemías Reyes López |
| Docente asesor | : MAFI. Jhony Alexander Argueta Amaya |
| Jurado Examinador | : MAFI. Jhony Alexander Argueta Amaya |
| | : Lic. Marco Antonio Orellana Orellana |
| | : Msc. Martha Eugenia Ávalos de Altamirano |

NOVIEMBRE 2023

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

## AGRADECIMIENTOS

Agradezco y doy gracias a Dios por haberme permitido culminar mi carrera universitaria, a pesar de las dificultades en todo el proceso siempre vi su respaldo en mí, fueron tantas pruebas a lo largo del camino momentos llenos de tristezas, frustraciones, cansancio que me hicieron dudar de llegar al final; gracias a mi familia que fueron un pilar fundamental en este logro, a mis amigos que siempre estuvieron motivándome a seguir adelante y vencer toda dificultad y limitante que pudiese tener.

**Jenny Claribel Mejía Sola**

En primer lugar le doy gracias a Dios por permitirme llegar hasta esta etapa tan importante en mi vida, ya que sin el esto no sería posible, así como también le doy gracias a mis padres que han sido un pilar fundamental en mi vida, ya que ellos me han brindado su apoyo incondicional en todo momento y me han animado a seguir cuando creí ya no poder, le doy gracias a mi hermana la cual ha sido una de mis más grandes inspiraciones para seguir en este proceso y a todos aquellos que han creído en mí y me han brindado su apoyo en todo momento, le doy gracias a todos aquellos docentes con los cuales tuve la oportunidad de recibir clases, así como también gracias al Licenciado Marco Orellana, el cual nos ha estado apoyando en todo momento en este proceso y nos ha guiado para poder culminar con éxito esta etapa.

**Weder Josué Miguel Hernández**

Agradezco a Dios por permitirme culminar esta etapa de mi vida, en la cual ha habido barreras y luchas, pero siempre su amor y misericordia no me ha dejado.

Gracias, madre, por cada esfuerzo, por cada palabra de apoyo y porque siempre has estado ahí para darme ánimos.

**Marcos Alexander Sosa Umaña**

**INDICE**

# ÌNDICE DE TABLAS

# ÌNDICE DE FIGURAS

# RESUMEN EJECUTIVO

La auditoría interna juega un rol fundamental debido a que agrega valor a la entidad a través de la realización de un examen de evidencia objetiva y desarrollo de aseguramiento basado en riesgos.

En el proceso de desarrollo de este trabajo, se ha procedido a seleccionar a una entidad dedicada a la prestación de servicios de gestión empresarial, ofreciendo herramientas informáticas a sus clientes. Es importante resaltar que, en la actualidad, esta entidad carece de un departamento de auditoría interna.

En vista de esta carencia, se ha emprendido una consultoría que tiene como finalidad principal identificar y evaluar los riesgos que están intrínsecamente asociados al ámbito de la tecnología de la información (TI). Dado que la TI constituye el núcleo esencial de las operaciones de la entidad, siendo así y con la necesidad crítica en el área de TI ya que se han confirmado muchos problemas a los que la entidad se encuentra expuestas desde la parte de servicios proveídos por terceros, la infraestructura tecnológica, el acceso a la red lógica.

El proceso comenzó con una entrevista exhaustiva al encargado del área de TI, durante la cual se formularon consultas específicas acerca de los riesgos identificados y de los posibles controles existentes para su mitigación con base en la información recopilada se diagnosticaron muchas observaciones, las cuales representan riesgos a los que la entidad se encuentra expuesta, por lo cual se trabajaron en las vulnerabilidades de la entidad a través de los procesos brindados por la entidad en esta etapa, luego se procedió a la

elaboración de una matriz de riesgos detallada que documenta minuciosamente los riesgos identificados y su potencial impacto en el funcionamiento de la entidad.

El propósito primordial de este ejercicio es proporcionar a la entidad un análisis exhaustivo que permita la identificación de los riesgos relacionados con el área de TI. Además, se llevará a cabo una evaluación para determinar cuáles de estos riesgos tienen una mayor incidencia y un impacto más significativo en los objetivos de la entidad. Esto posibilitará que la entidad pueda implementar controles más efectivos y definir los procesos en los cuales se requiere una mitigación de riesgos más robusta. En última instancia, esta iniciativa está diseñada para contribuir al crecimiento y desarrollo continuo de la entidad.

En el marco de este trabajo, se han formulado recomendaciones específicas que tienen como objetivo principal brindar apoyo en la identificación de riesgos y en la mejora de la gestión de estos riesgos. Estas recomendaciones están diseñadas para ser un recurso valioso para la entidad, ayudándola a fortalecer su posición en cuanto a la seguridad y la eficiencia de sus operaciones.

# INTRODUCCIÓN

En el dinámico entorno empresarial de El Salvador, la Tecnología de la Información (TI) juega un papel fundamental en el éxito y la eficiencia de las empresas. Sin embargo, la falta de procesos adecuados en el área de TI puede representar un riesgo significativo para estas entidades.

En los últimos años, El Salvador ha experimentado un rápido avance en la adopción de tecnologías de la información, lo que ha permitido a las organizaciones optimizar sus operaciones, mejorar la comunicación y acceder a nuevas oportunidades de mercado. No obstante, esta rápida adopción también ha dado lugar a desafíos en la gestión de la TI, especialmente en la falta de procesos claros y bien definidos.

En la investigación se evalúa que la carencia de procesos en el área de TI puede conllevar una serie de riesgos potenciales para la entidad objeta de estudio. Entre los riesgos presentados se incluye la pérdida de datos críticos, interrupción de servicios, falta de seguridad en la información, retrasos en la toma de decisiones y falta de alineación entre los objetivos empresariales y las soluciones tecnológicas implementadas.

A continuación, se describe el contenido de cada capítulo que forma parte de este trabajo de investigación:

En el primer capítulo de la presente investigación se aborda todo lo relacionado al planteamiento del problema que contiene antecedentes, caracterización, objetivos, seguido del marco teórico y por último la base técnica y legal.

En el segundo capítulo, se describe la estructura metodológica que contiene el tipo de estudio, unidad de análisis, técnicas e instrumentos a realizar, procesamiento de

la información, determinación y operacionalización de variables de la investigación, y por último punto se elaboró un cronograma de actividades y el diagnóstico final.

En el tercer capítulo de esta investigación, se presenta un componente fundamental de la misma, consistente en la creación de una herramienta de análisis específicamente diseñada para evaluar el riesgo inherente en el área de Tecnologías de la Información (TI). Esta herramienta se desarrolló con el propósito de construir una matriz de riesgo que permitiera abordar de manera sistemática y precisa los desafíos relacionados con la gestión de riesgos en empresas dedicadas a la prestación de servicios de gestión empresarial.

Por último, se incluyen las conclusiones, recomendaciones, bibliografía y anexos como resultado de la investigación realizada.

# CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA, MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL.

## 1.1 Planteamiento del problema

El inicio de operaciones de una empresa en un país es esencial, ya que de ello depende su funcionamiento futuro. Implementar procesos eficientes desde el principio es clave para utilizar los recursos de manera adecuada y alcanzar los objetivos para los cuales se ha creado. Esto es especialmente relevante para las empresas que ofrecen servicios de gestión empresarial, ya que su principal objetivo es brindar apoyo a otras entidades mediante una variedad de servicios que contribuyen al buen funcionamiento de estas últimas.

En la actualidad, la adopción de nuevas tecnologías es imprescindible, ya que las empresas buscan agilizar sus operaciones y reducir costos. Estas tecnologías permiten realizar actividades de manera más eficiente y en menos tiempo, lo que aumenta la productividad y reduce los gastos operativos, siendo esencial para la competitividad en el mercado actual.

La gestión empresarial desempeña un papel crucial en todas las organizaciones, independientemente de su tamaño o sector. Su objetivo es planificar, organizar, integrar y controlar los recursos de manera eficiente para alcanzar los objetivos y metas establecidos. Por esta razón, existen empresas dedicadas a complementar estos procesos mediante una amplia gama de servicios que han evolucionado con el tiempo.

Dentro de la gestión empresarial, la auditoría interna desempeña un papel fundamental. Es una herramienta clave para identificar posibles fallas en los procesos y prevenir problemas que podrían afectar el logro de los objetivos. Sin embargo, su

importancia va más allá de la detección de fallas; también contribuye al fortalecimiento del control interno, promueve la transparencia y la confianza, y establece un marco para la mejora continua.

La actividad de auditoría interna se define como "Un departamento, división, equipo de consultores, u otro/s practicante/s que proporciona/n servicios independientes y objetivos de aseguramiento y consulta, concebidos para agregar valor y mejorar las operaciones de una organización" *(The Institute of Internal Auditors , 2017*).

Para ello es necesario tener conocimiento sobre el Marco Internacional para la Práctica Profesional de la Auditoría Interna (MIPP), ya que este engloba distintos aspectos relevantes para lograr una auditoria eficaz, este se divide en tres componentes los cuales son: la misión de auditoría interna, guías obligatorias y guías recomendadas, dentro las guías obligatorias se puede encontrar la definición de auditoría interna, los principios básicos, el código de ética y las NIEPAI (Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna) las cuales proporcionan diferentes herramientas que facilitan y brindan lineamientos para poder ejecutar la auditoría interna de manera eficaz y dentro de las guías recomendadas se dividen en guías de implementación y guías complementarias.

La entidad de estudio se fundó en 2015 con dos socios y un equipo de diez empleados. Con el tiempo, el crecimiento del personal se ha debido a la necesidad de satisfacer las demandas de los clientes. Inicialmente, no se estableció un departamento de auditoría interna, lo que resultó en que no se le diera la debida importancia.

Esta carencia ha llevado a la falta de un área encargada de proporcionar un aseguramiento continúo basado en riesgos. Este enfoque busca identificar aspectos de mejora y deficiencias en los diversos controles internos mediante una evaluación de riesgos adecuada. El objetivo es que la entidad fortalezca sus procesos y controles mediante un análisis y seguimiento apropiado, generando valor y facilitando el cumplimiento de objetivos.

La ausencia de un marco formal para el control interno y el gobierno ha dificultado la capacidad de tomar decisiones informadas, rendir cuentas y supervisar de manera efectiva las operaciones relacionadas con el área de Tecnologías de la Información (TI).

La entidad de estudio inició actividades con muchas carencias en todas las áreas siendo una de estas el área de TI ya que no se cuenta con manuales ni procesos establecidos, siendo este un problema para incorporar nuevos profesionales al área, y esto afecto todas las áreas de la empresa poniendo en riesgo la integridad de la información, tenían una estructura organizativa sencilla que se limitó en los controles implementados:

- Descriptores de puestos sencillos y solo de los puestos claves de la empresa sin incluir las demás áreas que conforman la empresa.
- Anotaciones de asistencia en libros generales.

La entidad objeto de estudio ha experimentado un notable crecimiento en el mercado, por la demanda que ha ido surgiendo en relación con tecnología y digitalización. Cuenta con una sólida infraestructura tecnológica y ha sido clave para satisfacer la creciente demanda de digitalización y brindar apoyo a otras organizaciones en su transición hacia

entornos digitales. Como resultado, la empresa ha logrado expandirse y aumentar su cartera de clientes.

Además, la organización ha demostrado una atención continua hacia el bienestar de su personal, garantizando un entorno propicio para el desarrollo y la eficiencia laboral. Esto ha contribuido a mantener una fuerza laboral comprometida y motivada, lo que ha permitido un crecimiento en el número de personal de manera efectiva; este crecimiento ha causado la necesidad de identificar y evaluar riesgos que pueden ocasionar la materialización de eventos que no permitan alcanzar el cumplimiento de objetivos deseados debido a la falta de controles internos efectivos, y una gestión de riesgos no desarrollada, por lo que se sugiere realizar una consultoría.

Las consultorías son actividades de asesoramiento y servicios relacionados, proporcionadas a los clientes, cuya naturaleza y alcance están acordados con los mismos y estén dirigidos a añadir valor y a mejorar los procesos de gobierno, gestión de riesgos y control de una organización. Por lo general existen dos partes en los servicios de consultoría: (1) la persona o grupo que ofrece el consejo, es decir el auditor interno, y (2) la persona o grupo que busca y recibe el consejo, es decir el cliente del trabajo *(The Institute of Internal Auditors , 2017).*

En El Salvador son pocas las empresas que cuentan con un departamento de auditoría interna, esto depende de varios factores que incluyen:

**1.Tamaño de la Empresa:** Las empresas más pequeñas pueden no tener los recursos financieros o humanos para mantener un departamento de auditoría interna a tiempo completo.

**2- Enfoque Externo:** Algunas empresas optan por contratar auditores externos en lugar de mantener un departamento interno.

**3- Cultura Organizacional:** En algunas empresas, la cultura organizacional puede no enfatizar la importancia de la auditoría interna o puede haber una falta de comprensión sobre cómo puede beneficiar a la empresa.

**4- Desconocimiento de Beneficios:** Algunas empresas pueden no estar al tanto de los beneficios que una auditoría interna bien gestionada puede aportar, como la mejora en los controles internos, la identificación de riesgos y la eficiencia operativa.

Aun con estos factores la auditoría interna se está fomentando, tanto que es imprescindible para lograr los objetivos de la entidad ya que la función de un profesional en el área no es solo la evaluación del riesgo y detección de errores, sino contribuir aportando valor a la entidad a través de un plan estratégico dentro de las organizaciones por medio de la supervisión todo esto para enfrentarse a nuevos riesgos.

La Tecnología de la Información (TI) desempeña un papel fundamental en las entidades dedicadas a la prestación de servicios de gestión empresarial. Sin embargo, la falta de una adecuada identificación y evaluación de riesgos en el área de TI puede representar una amenaza significativa para la seguridad, la eficiencia operativa y la continuidad del negocio de estas entidades.

La empresa de estudio está enfocada en prestación de servicios de gestión empresarial dando énfasis a los métodos analíticos y herramientas informáticas, generando empleo a nivel nacional e internacional, a través de los años ha ido en constante crecimiento en la parte operativa, pero desde sus inicios no ha contado con un

departamento de auditoría interna debido a los costos que esto genera acarreando el riesgo de confiar en la gerencia que puede no estar en la mejor posición para ofrecer opiniones objetivas y competentes ya que el gerente financiero es el encargado de controlar los procedimientos de forma empírica que tienen; en la actualidad la empresa cuenta con un sistema de control interno deficiente por la falta de procesos claros y estandarizados y esto obstaculiza su efectividad en las diferentes áreas. Hoy en día es clave tener personal capacitado que nos brinde una evaluación objetiva del control interno y nos aporte valor a la empresa proporcionando consultorías, aseguramiento y análisis en base a riesgos.

En el contexto salvadoreño, se han observado situaciones en las que las entidades dedicadas a la prestación de servicios de gestión empresarial carecen de una adecuada identificación y evaluación de riesgos en el ámbito tecnológico. Esta falta de enfoque sistemático y proactivo hacia la gestión de riesgos en este ámbito puede exponer a las organizaciones a diversas amenazas, como ataques cibernéticos, pérdida de datos críticos, interrupción de servicios y falta de cumplimiento de regulaciones y leyes relacionadas con la seguridad de la información.

Una de las áreas con mayor riesgo es la siguiente:

- **Área de tecnología de la Información (TI)**

**Soporte**

- **Obsolescencia de activo:** La presencia de activos tecnológicos significativamente antiguos, como servidores y computadoras, plantea inquietudes en el entorno. Estos dispositivos a menudo carecen de licencias de antivirus actualizadas, lo que resulta en una vulnerabilidad de seguridad. Además, la obtención de actualizaciones para mejorar

su estado suele implicar costos elevados. En consecuencia, mantener estos activos tecnológicos se convierte en un motivo de preocupación, ya que su mantenimiento es más oneroso y requiere una supervisión y seguimiento más rigurosos para gestionarlos de manera efectiva.

- **Adquisición de activos inadecuados:** En el proceso de solicitud de equipos para las diferentes áreas, se ha observado que la falta de controles relacionados con la adquisición de equipo informático basado en análisis de requisitos mínimos y la falta de un apropiado proceso para autorización oportuna de la compra de equipos dificulta la adquisición de equipo acorde a las necesidades de cada departamento, esto debido a que se toma en consideración el factor precio en lugar de priorizar la calidad y que cumpla con los requisitos mínimos solicitados, para tomar las decisiones de compra.
- **Dificultad en el proceso de pago a proveedores:** Este desafío conlleva consecuencias significativas, ya que los proveedores encargados de servicios críticos para la entidad muestran una renuencia en proporcionar actualizaciones o responder a consultas. Esta situación, en ocasiones, ha resultado en la interrupción de los servicios que brindan, lo que impacta negativamente en la operatividad de la organización.
- **Uso de equipos informáticos personales:** Algunos empleados optan por utilizar sus propios dispositivos en lugar de los proporcionados por la empresa, lo que aumenta la vulnerabilidad. Esto se debe a que, en algunos casos, se les otorgan ciertos privilegios, como el acceso a la VPN y otros recursos, lo que potencialmente facilita la exposición a riesgos de seguridad, incluido el riesgo de robo de información confidencial alojada en la red de la organización.

- **Equipos corporativos para fines personales por parte de los empleados:** Esta situación representa un riesgo recurrente, dado que no existen políticas de restricción o bloqueo de acceso a la red para las máquinas de la empresa. Los empleados utilizan los dispositivos de la compañía para llevar a cabo actividades de índole personal, lo que plantea un riesgo para la seguridad de la información empresarial. Existe la posibilidad de extracción de datos confidenciales o el acceso a sitios web no autorizados, lo que incrementa la vulnerabilidad de la organización.

**Internet**

- **Ciberataques por *Phishing*:** Existe una alta probabilidad de que se produzcan ataques mediante correos electrónicos fraudulentos, dado que la comunicación de la información se realiza principalmente a través de correos electrónicos. Esta situación puede propiciar que las personas proporcionen sus datos personales en sitios web no confiables, lo que podría resultar en fraudes, estafas y otras actividades maliciosas.
- **Amenaza por software malicioso:** La falta de restricciones en la navegación por páginas web conlleva el riesgo de descargar documentos o archivos potencialmente infectados con virus. Esto representa un riesgo significativo, ya que la organización maneja información de clientes que podría verse comprometida como resultado de estas descargas.

**Infraestructura**

- **Deficiente control de accesos:** La falta de actualización y mantenimiento regular de los usuarios, tanto activos como inactivos, en el sistema puede dar lugar a situaciones en las que los empleados que ya no están vinculados a la entidad conserven sus accesos

activos durante un período prolongado. Esta situación conlleva un riesgo significativo, ya que podría posibilitar la extracción de información por parte de personas no autorizadas con intenciones maliciosas.

- **Condiciones no adecuadas para el buen funcionamiento de los equipos:** No se cuenta con una infraestructura adecuada para la debida protección del hardware, ya que no cumple con una adecuada seguridad física, ya que, al no contar con aires acondicionados adecuados, puede ocasionar un sobre calentamiento de los servidores y pueden dañarse y perder información.
- **Poco control con los respaldos de las bases de datos:** La infraestructura actual carece de las condiciones necesarias para garantizar una protección adecuada del hardware, ya que no cumple con los estándares de seguridad física requeridos. La falta de sistemas de aire acondicionado adecuados puede resultar en un sobrecalentamiento de los servidores, lo que, a su vez, podría provocar daños y la pérdida de información crítica.
- **Problemas con equipos de red:** Se han identificado algunas deficiencias en lo que respecta a la actualización de datos en el sistema. Además, el personal de distintas áreas ha manifestado su insatisfacción debido a la lentitud de la red, lo cual dificulta su desempeño óptimo en sus labores.
- **Falta de capacitación al personal de la empresa:** La falta de capacitación en el personal respecto a la gestión de redes. En la actualidad, la responsabilidad de administrar los servidores recae en una única persona, y este conocimiento no ha sido compartido con los demás miembros del equipo. Esto plantea una falta de

diversificación en habilidades y una dependencia significativa en una única persona para tareas críticas de TI.

- **Libre acceso a la nube:** No se mantiene un registro de las personas que cuentan con autorización para acceder a la nube, incluyendo la capacidad de editar, agregar o eliminar archivos. Esta falta de control plantea un riesgo significativo, considerando que la entidad confía en gran medida en el almacenamiento y acceso a la información a través de la nube, dada la conveniencia de este enfoque.

  Las Guías Complementarias del Marco Internacional para la Práctica Profesional son un conjunto de recursos y directrices desarrollados por el Instituto de Auditores Internos (IIA). Estas guías brindan orientación a los profesionales de la auditoría interna y establecen los estándares y mejores prácticas para el ejercicio de esta disciplina.

  Mediante el uso de las Guías complementarias del IPPF se busca brindar recomendaciones y medidas de control efectivas que permitan a la entidad proteger sus activos tecnológicos y así poder enfrentar los desafíos en el entorno empresarial.

La alta dirección tiene claro que todas las deficiencias del sistema de control y gestión de riesgo son superables cuando se les brinda servicios de consultoría especializada para lograr fortalecer y corregir aquellos procesos que no se realizan de la mejor manera, todo para garantizar el logro de los objetivos de la entidad.

## 1.2 Formulación del problema

La entidad objeto de estudio presentó una serie de deficiencias en los diferentes controles, siendo uno de estos y el más significativo en el área de TI, debido a que es la actividad principal de la entidad, por ello fue de mucha importancia brindar una consultoría para la identificación y evaluación de riesgos de dicha área.

¿De qué manera impacta la ausencia de un programa de consultoría sobre la identificación y evaluación de riesgos en el área de TI con respecto a la adecuada ejecución de los procesos, el logro de los objetivos y su debida gestión en la entidad que se dedica a la prestación de servicios de gestión empresarial?

## 1.3 Objetivos

### 1.3.1 Objetivo General

Desarrollar una consultoría sobre la identificación y evaluación de riesgos asociados al área de Tecnología de la Información (TI) el cual contribuirá a la mejora en la gestión de riesgos y controles de la entidad objeto de estudio.

### 1.3.2 Objetivos Específicos

- Determinar de qué manera los riesgos del área de Tecnología de Información (TI) afectan en la operatividad del negocio.
- Identificar vulnerabilidades de riesgos de tal forma que se analice como impactan en el cumplimiento de los objetivos de la entidad.

- Elaborar una matriz de riesgos identificando aquellos riesgos que pudieran afectar negativamente para el cumplimiento de los objetivos del área de Tecnología de Información.

## 1.4 Marco Teórico, Conceptual, Técnico y Legal

### 1.4.1 Antecedentes

El riesgo es algo inherente prácticamente en toda actividad empresarial, por lo que se hace necesario que los profesionales aprendan a identificarlo, evaluarlo. Por tal razón, el dominio de las técnicas para evaluar y mitigar los riesgos se convierte en uno de los desafíos más recurrentes que enfrenta cualquier entidad económica.

En la actualidad la expansión de la tecnología ha permitido que más usuarios accedan a información de una entidad lo que significa que tienen un desafío de asegurarse de una buena implementación de controles de prevención y detección.

El riesgo está ligado a la incertidumbre sobre eventos futuros, y resulta imposible eliminarlo. Ante esto, la única forma de enfrentarlo es administrándolo, distinguiendo las fuentes de donde proviene, midiendo el grado de exposición que se asume y eligiendo las mejores estrategias disponibles para controlarlo y conocer los grados de vulnerabilidad que se posee. (*SCIELO, 2018*).

Los riesgos informáticos son amenazas que pueden afectar la seguridad y el funcionamiento de los sistemas informáticos, así como la integridad de los datos. Estos riesgos pueden tener diversas formas y pueden afectar tanto a usuarios individuales como a organizaciones.

La ciberseguridad es un campo en constante evolución que ha surgido en respuesta al aumento de amenazas y ataques cibernéticos.

A medida que las empresas comenzaron a utilizar los distintos programas informáticos estas se volvieron más vulnerables a ataques informáticos, entre ellos los ciberataques, pero estos se intensificaron a principios de la década de 2000, debido a que las organizaciones criminales empezaron a financiar en gran medida para poder robar información y datos personales.

### 1.4.2 Conceptos

**Control:** Cualquier medida que tome la dirección, el Consejo y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. (GLOSARIO INSTITUTO DE AUDITORES INTERNOS, 2019, pág. 1)

**Cumplimiento:** Adhesión a las políticas, planes, procedimientos, leyes, regulaciones, contratos y otros requerimientos. (GLOSARIO INSTITUTO DE AUDITORES INTERNOS, 2019, pág. 1)

**Gestión de riesgos:** La cultura o conjunto de procesos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, controlar, informar y revelar los distintos tipos de riesgos que se encuentra expuesta una empresa, de tal forma que les permita minimizar perdidas y maximizar oportunidades.

**Procesos de control:** Las políticas, procedimientos y actividades, que forman parte de un marco de control, diseñados y operados para asegurar que los riesgos estén contenidos dentro de las tolerancias establecidas que una organización está dispuesta a aceptar. (GLOSARIO INSTITUTO DE AUDITORES INTERNOS, 2019, pág. 3)

**Servicios de consultoría:** Actividades de asesoramiento y servicios relacionados, proporcionadas a los clientes, cuya naturaleza y alcance estén acordados con los mismos y estén dirigidos a añadir valor y mejorar los procesos de gobierno, gestión de riesgos y control de una organización. (GLOSARIO INSTITUTO DE AUDITORES INTERNOS, 2019, pág. 3)

**Tecnología de la información:** se refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. (Pérez Porto, J., Gardey, A., tecnologías de la información, 18 de noviembre de 2014)

### 1.4.3 Generalidades del sector empresarial

**Sector de empresas de gestión empresarial**

Las empresas que se dedican a la prestación de servicios de gestión empresarial son empresas que en la actualidad son muy requeridas por la misma necesidad que tienen las demás entidades en digitalizar sus operaciones.

La gestión empresarial es el conjunto de actividades empresarial que realiza una persona especializada. Además, debe tener la capacidad de poder organizar, controlar y dirigir un grupo de personas. Para conseguir los objetivos que se ha planteado la organización. (NTX PRO, 2019)

Existen empresas especializadas en la prestación de servicios de gestión empresarial, que abarcan desde asesoramiento y consultoría hasta soluciones tecnológicas destinadas a ayudar a diversas organizaciones a optimizar sus procesos y alcanzar sus objetivos estratégicos.

En El Salvador, existen entidades especializadas en brindar asesoría y consultoría en soluciones informáticas para la gestión empresarial. Estos servicios engloban diversas áreas, como el desarrollo de software personalizado, la implementación de sistemas de gestión empresarial (ERP), la oferta de servicios en la nube, la implementación de sistemas SAP, la implementación de sistemas de gestión de clientes (CRM) y la consultoría en infraestructura tecnológica, entre otros.

Para lograr una gestión empresarial idónea para la entidad, es esencial que se cumplan cuatro características fundamentales. Estas cualidades son cruciales para contribuir al logro de los objetivos planteados. A continuación, se detallan estas características:

1. **Planificación:** En toda entidad se requiere una planificación de procesos, con el cual se pueda llegar a alcanzar los objetivos planteados a corto, mediano o largo plazo, así mismo se tendrá el detalle de lo que se necesita para poder llevar a cabo las funciones y desempeñarlas de mejor manera.
2. **Organización:** Es aquí donde se delega y coordina las actividades que se han planificado con anterioridad, con lo cual se busca crear un orden para poder ayudar al alcance de los objetivos.
3. **Dirección:** Se debe contar con personas capaces de liderar y orientar al grupo de trabajo, el cual buscara siempre estar pendiente de su personal a cargo, así como de motivarlos a cumplir sus metas.
4. **Control:** El cual se encuentra relacionado con la coordinación y seguimiento del trabajo de los más integrantes del grupo, con esto se busca conocer los puntos altos

y bajos de la entidad, para así poder proponer acciones ante posibles problemas que puedan ocurrir en el futuro.

**Ventajas**

Entre las ventajas que podemos encontrar sobre la gestión empresarial son las siguientes:

- Logra administrar adecuadamente la entidad, ya que se consigue tener un proyecto desde su planeación hasta que este finalice.
- Contribuye a mejorar la eficiencia en los procesos de la entidad.
- Se logra la integración del equipo de trabajo, ya que cada persona tendrá su nivel de acceso, así como sus funciones asignadas.
- Se logra tener una mejor comunicación entre los individuos y esto facilita aquellos procesos burocráticos que se tuvieren.

  En la actualidad, las Tecnologías de la Información han experimentado un crecimiento significativo, lo que ha generado una mayor demanda de comprensión y conocimiento en este campo. En este contexto, resulta esencial familiarizarse con las diversas características, ventajas y desventajas que estas tecnologías pueden presentar para aprovechar su potencial de manera efectiva.

Las empresas deben ser capaces de adaptarse a las nuevas tecnologías, modificar sus modelos de negocios o adaptar cambios de manera efectiva, por lo que es necesario adoptar controles que ayuden a detectar y mitigar riesgos que enfrentan por el crecimiento y avance tecnológico que se tiene en la actualidad.

**Clasificación de los controles Generales de TI**

Los Controles Generales de TI se podrían definir como el conjunto de Políticas y procedimientos auditables establecidos por una empresa para ayudar a garantizar la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos de TI. Los ITGC incluyen controles sobre la tecnología de la información del ambiente (TI), los cambios de programas, desarrollo de programas, el acceso a los programas y datos y las operaciones de computadora. (*Enterprise, 2015*)

### 1.4.4 Generalidades del Sector Profesional

**Auditoría Interna en los procesos de Gestión de Riesgos.**

La auditoría interna desempeña un papel fundamental en la gestión de riesgos de una organización ya que contribuye a la identificación, evaluación y mitigación de riesgos al proporcionar una evaluación independiente y objetiva de los controles internos, los procesos operativos y la eficacia de la gestión de riesgos en general.

Con la identificación se revisan y evalúan los procesos y actividades de la organización. A través de la realización de auditorías y evaluaciones de riesgos, y los auditores internos pueden identificar áreas y procesos que representan un mayor riesgo para la organización, así como las vulnerabilidades y amenazas asociadas.

Dentro de las evaluaciones pueden estar los controles internos donde la auditoría interna evalúa la efectividad de estos, también evalúa el cumplimiento normativo de leyes, regulaciones y políticas internas relacionadas con la gestión de riesgos.

**Gestión de los Riesgos de Seguridad de la Información.**

Actualmente en la revolución digital, las compañías son conscientes del protagonismo de la información en sus procesos productivos, por lo tanto, la información es el activo principal pero también debemos considerar:

- Infraestructura informática,
- Equipos auxiliares,
- Redes de comunicaciones,
- Instalaciones,
- y personas.

**Procesos del auditor en la evaluación de riesgos.**

La función del auditor interno que evalúa procesos relacionados con Tecnología de la Información (TI), debe seguir pasos clave para presentar una auditoría efectiva, entre esos procesos que debe seguir están:

1. Planificación de la auditoría:
    a. Definir el alcance de la auditoría, identificando los procesos de TI específicos que se evaluarán.
    b. Establecer los objetivos y criterios de auditoría, basados en estándares y mejores prácticas relevantes.
    c. Recopilar información y realizar una evaluación preliminar de riesgos relacionados con los procesos de TI.
2. Recopilación de información:

   a. Obtener y revisar la documentación relevante, como políticas, procedimientos, manuales, informes de seguridad, etc.
   b. Realizar entrevistas con el personal clave responsable de los procesos de TI.
   c. Realizar pruebas y análisis de los controles y sistemas de TI, como pruebas de penetración, evaluaciones de seguridad, revisión de configuraciones, etc.
3. Evaluación de riesgos y controles:
   a. Identificar y evaluar los riesgos asociados con los procesos de TI, incluyendo amenazas de seguridad, vulnerabilidades y exposición a fallas.
   b. Evaluar la efectividad de los controles internos existentes para mitigar los riesgos identificados.
   c. Identificar brechas o deficiencias en los controles y documentar las áreas de mejora necesarias.
4. Análisis y hallazgos:
   a. Analizar los datos y la información recopilada para identificar patrones, tendencias y problemas recurrentes.
   b. Documentar los hallazgos y las recomendaciones de mejora, estableciendo prioridades y niveles de riesgo asociados.
   c. Comunicar los hallazgos a la alta dirección y a los responsables de los procesos de TI, asegurándose de proporcionar explicaciones claras y acciones correctivas sugeridas.
5. Seguimiento y cierre:
   a. Monitorear la implementación de las acciones correctivas propuestas y verificar su efectividad.

b. Realizar un seguimiento regular para asegurarse de que los problemas identificados se hayan resuelto de manera satisfactoria.
c. Preparar informes finales de auditoría que resuman los resultados, conclusiones y recomendaciones.

### 1.4.5 Base Técnica

Se desarrollo la investigación bajo las normativas técnicas siguientes:

- **Guías Complementarias del Marco Internacional para la Práctica Profesional**

Las Guías Complementarias del Marco Internacional para la Práctica Profesional (IPPF) son una serie de documentos desarrollados por el Instituto de Auditores Internos (IIA) que proporcionan orientación práctica y detallada sobre diversas áreas relacionadas con la auditoría y los controles internos.

El Marco IPPF establece los estándares y principios fundamentales para la práctica de la auditoría interna a nivel global. Las Guías Complementarias, por su parte, se centran en aspectos más específicos y ofrecen orientación técnica para abordar desafíos y riesgos particulares en el ámbito de la auditoría interna.

Estas guías abordan temas como la gestión de riesgos, el control interno, la gobernanza corporativa, la auditoría de TI, la ética y la calidad de la auditoría interna. Cada guía proporciona una descripción detallada del tema, incluyendo conceptos clave, enfoques de auditoría, mejores prácticas y consideraciones relevantes.

Las Guías Complementarias del IPPF son herramientas valiosas para los profesionales de la auditoría interna, ya que les brindan conocimientos y recursos prácticos para llevar a cabo evaluaciones efectivas, promover la mejora continua y proporcionar un valor añadido a las organizaciones. Estas guías se actualizan regularmente para reflejar los cambios y avances en el entorno empresarial y tecnológico, y asegurar que los profesionales de la auditoría interna cuenten con información actualizada y relevante para desempeñar su labor de manera eficiente.

Prácticamente las Guías Complementarias del Marco Internacional para la Práctica Profesional (IPPF) son documentos técnicos que ofrecen orientación práctica sobre diversos aspectos de la auditoría y los controles internos ya que contribuyen a fortalecer la calidad y efectividad de sus actividades.

- **Guías Complementarias GTAG**

Dentro del IPPF, se encuentran las Guías Complementarias (GTAG, por sus siglas en inglés) que proporcionan orientación específica sobre temas relacionados con la auditoría y los controles internos.

Las Guías Complementarias del IPPF (GTAG) son una serie de documentos técnicos que brindan información detallada y práctica sobre una amplia gama de temas relevantes para los profesionales de la auditoría interna. Estas guías son desarrolladas por el IIA en colaboración con expertos de la industria y cubren diversas áreas temáticas, como la gestión de riesgos, la seguridad de la información, la auditoría de TI y el gobierno corporativo.

El objetivo de las GTAG es proporcionar a los auditores internos herramientas y conocimientos prácticos para abordar los desafíos y riesgos actuales en sus organizaciones. Estas guías están diseñadas para ser aplicadas en el contexto de la auditoría interna y ofrecen orientación sobre enfoques, metodologías y mejores prácticas para llevar a cabo evaluaciones y revisiones efectivas.

- **GTAG: Evaluación de riesgos de ciberseguridad**

Cuando se aborda el tema de la ciberseguridad se refiere a las tecnologías, los procesos y las prácticas concebidas a fin de proteger del acceso no autorizado los activos de información entre los cuales se tienen las computadoras, redes, programas y datos que se encuentran en una organización, por lo cual la actividad de auditoría interna desempeña una función crucial en lo referente a la evaluación de los riesgos de ciberseguridad de una organización mediante evaluaciones como:

- ¿Quién tiene acceso a la información más valiosa de la organización?
- ¿Cuáles son los activos con mayor probabilidad de sufrir un ciberataque?
- ¿Qué sistemas ocasionarían la alteración más significativa?
- ¿Qué datos, si los obtuvieran partes no autorizadas, provocarían pérdidas competitivas o financieras, ramificaciones legales o perjuicios a la reputación de la organización?

Al evaluar el rol de la auditoría en una organización especialmente en el contexto de la ciberseguridad se trata de asegurar que el modelo de las tres líneas de IIA estén adecuadamente separadas y funcionando eficazmente.

Cuando se observa la dirección como la primera línea y a cargo de los datos, procesos, riesgos y controles, en cuanto a la ciberseguridad, esta función suele recaer en los administradores del sistema y demás personal al que se asigna la protección de los activos de la organización. Luego la segunda línea de defensa está compuesta por las funciones de supervisión de cumplimiento, control y riesgos responsables de asegurar que los controles y procesos de la primera línea existan y funcionen eficazmente. Estas funciones pueden incluir grupos a cargo de garantizar una gestión de riesgos efectiva y de supervisar riesgos y amenazas en el espacio de la ciberseguridad.

Como tercera línea de defensa, la actividad de auditoría interna brinda a la alta dirección y al Consejo aseguramiento independiente y objetivo respecto a gobierno, controles y gestión de riesgos, lo que incluye la evaluación de la eficacia general de las actividades que realizan la primera y segunda líneas de defensa para gestionar y mitigar amenazas y riesgos de ciberseguridad.

Cuando se evalúan los riesgos de TI, se puede observar que el alcance del riesgo en el ámbito de la ciberseguridad se presenta como un ejercicio interdependiente. En este contexto, es esencial que la auditoría interna planifique de manera conjunta con las funciones de cumplimiento en la segunda línea de defensa. La planificación de la auditoría alcanza su máxima eficacia cuando se integra con las funciones de cumplimiento, las cuales tienen la capacidad de priorizar el impacto comercial y conocen con qué partes colaborar durante el proceso y después de la finalización de la auditoría interna.

La Norma 2050 del IIA, titulada "Coordinación", establece la necesidad de lograr una cobertura efectiva de los riesgos de ciberseguridad a través de la colaboración con las primeras y segundas líneas de defensa. Esto asegura que la auditoría interna identifique y

aborde la información más crítica y relevante para la organización en el ámbito de la ciberseguridad

Por lo que la actividad de auditoría interna debe identificar los sistemas y las tecnologías que abren vías de acceso a la visualización de información crítica (por ejemplo, los datos de los empleados, la información de identificación personal, los números de tarjeta de crédito de los clientes y el historial de transacciones de proveedores). Al trabajar con la dirección operativa, también se garantiza que se supervisen los elementos pertinentes a las vulnerabilidades de ciberseguridad en forma continua. Para determinar el alcance de la auditoría de ciberseguridad, la auditoría interna debe considerar quién tiene acceso a la información crítica y evaluar la tecnología sobre su ruta de acceso.

**Enfoque para evaluar riesgos y controles de ciberseguridad**

Existen seis componentes interdependientes que pueden emplearse para evaluar tanto el diseño como la eficacia operativa de los controles y el gobierno de ciberseguridad a nivel directivo. La interconexión de estos componentes y su flujo de seguimiento se pueden observar en la imagen siguiente:

En la Figura 1, se muestran seis componentes interdependientes del marco para evaluar el diseño y la eficacia operativa de los controles y el gobierno de ciberseguridad a nivel de la dirección.

**Figura 1. Marco para la evaluación de Riesgos de ciberseguridad.**


*Fuente: (Instituto de Auditores Internos, 2016)*

- **Auditoría de programas contra amenazas internas**

Se hace referencia a la amenaza interna como la posibilidad de que cualquier entidad con acceso autorizado, es decir, dentro del ámbito de la seguridad, pueda causar daño a un sistema de información o a una iniciativa, ya sea a través de la destrucción, divulgación o modificación de datos, o mediante la denegación del servicio. Esto se diferencia de una amenaza externa, que ocurre cuando una entidad que no tiene acceso autorizado a los sistemas de la organización busca afectar dichos sistemas.

Entre los riesgos relacionados con las amenazas internas, se incluyen los siguientes:

- Fraude
- Sabotaje
- Robo de propiedad intelectual (PI) o secretos comerciales
- Divulgación de datos delicados

- Uso de recursos de TI para actos ilegales.

Los auditores internos pueden agregar valor significativo a la organización, ayudando a fortalecer los procesos de control, gobierno y gestión de riesgos para abordar de manera efectiva las amenazas internas.

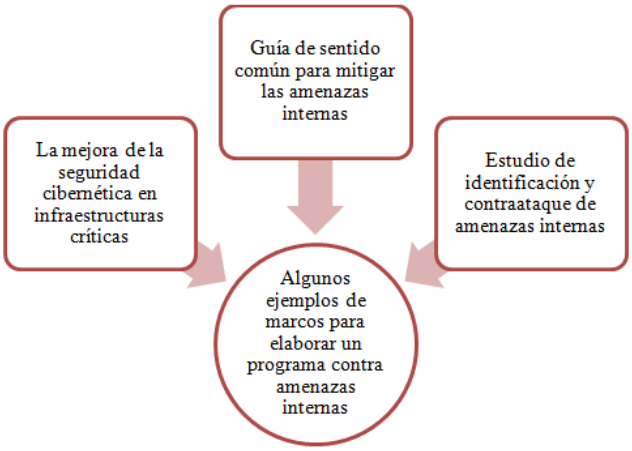
**El rol de la auditoría interna al auditar la gestión de amenazas internas**

Se hace referencia a que la actividad de auditoría interna utiliza un enfoque sistemático, disciplinado y basado en riesgos para proporcionar aseguramiento, asesoramiento y visión con objetividad. En cuanto a la gestión de amenazas internas, la responsabilidad de la auditoría interna es proporcionar servicios de aseguramiento y consultoría que ayuden a la organización a alcanzar sus objetivos mediante la evaluación y la contribución a la mejora de los procesos de gestión de riesgos, control y gobierno de la organización, tal como se establece en la Norma 2100 (Naturaleza del trabajo).

En este contexto, se menciona una consultoría que agrega valor cuando el personal de operaciones de TI se encuentra limitado en cuanto a tiempo y recursos para evaluar los riesgos asociados a las amenazas internas y para identificar los controles necesarios. Los auditores internos pueden respaldar al equipo de administración de sistemas y redes al llevar a cabo evaluaciones de riesgos relacionados con amenazas internas, identificando posibles problemas que los administradores de sistemas y seguridad podrían haber pasado por alto o áreas donde las políticas no se están siguiendo adecuadamente. A continuación, se presentan ejemplos de marcos para la elaboración de programas.

En la Figura 2, se muestran algunos ejemplos de marcos de trabajo que pueden utilizarse para elaborar un programa contra amenazas internas.

**Figura 2. Marco de trabajo para elaboración de programa contra amenaza internas.**




*Fuente: (Instituto de Auditores Internos, 2018).*

## ISO 27000

Las normas que forman la serie ISO/IEC-27000 son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.

En estos momentos la información es uno de los activos más importantes de una compañía, por lo que es necesario que esta se encuentre debidamente protegida. Las normas de la familia de ISO 27000 tratan la gestión de la seguridad de la información y pueden ser combinadas para proporcionar un marco reconocido a nivel mundial.

Estas normas están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la

Información (SGSI) o por su denominación en inglés *Information Security Management System* (ISMS).

Las normas esenciales en el tratamiento para una buena gestión de riesgos son:

ISO 27004: Proporciona pautas orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI.

ISO 27005: Define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información, orientado en cómo establecer la metodología a emplear.

ISO 27008: Define cómo se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos.

ISO 27014: Establece principios para el gobierno de la seguridad de la información.

ISO 27034: Proporciona orientación en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación. (*Solutions, 2023*)

Referente a la ISO/IEC 27002 esta norma internacional que establece el código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones.

El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. (*OSTEC, 2016*)

## Matriz de riesgos

Según (SINGWEB, s.f.), "la matriz de riesgos es una herramienta de control y gestión que se utiliza comúnmente para identificar las actividades o procesos de mayor importancia en una empresa, así como para determinar el tipo y nivel de riesgos a los que están expuestas estas actividades". Además, esta matriz también facilita la evaluación de la eficacia de una gestión adecuada de riesgos que podría tener un impacto negativo en los resultados y en el logro de los objetivos de una organización.

## Fases para la elaboración de una matriz de riesgo.

### Identificación de riesgos

La identificación de riesgos es un proceso continuo y reiterado en el tiempo, que se realiza para potenciar la capacidad de la organización de lograr sus objetivos. (COSO, 2013).

Esto puede lograrse mediante entrevistas con los responsables de los procesos y la realización de evaluaciones detalladas de los mismos. Este enfoque garantiza que la organización este debidamente preparada y anticiparse a posibles eventos futuros. En este contexto, se recomienda incluir la siguiente información:

- Nombre del riesgo
- Descripción del riesgo
- Clasificación del riesgo
- Causas del riesgo
- Consecuencias o impactos

**Probabilidad de ocurrencia y valorización**

Probabilidad representa la posibilidad de que se produzca un evento determinado mientras que impacto representa su efecto.

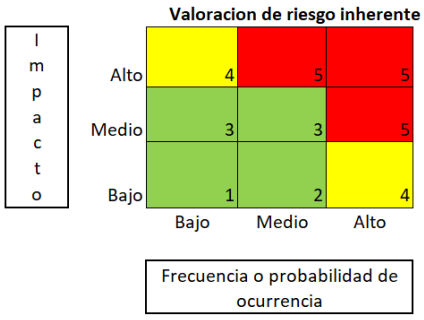
La dirección utilizará parámetros de desempeño para determinar hasta qué punto se están logrando los objetivos y, normalmente, usará las mismas unidades de medida, o similares, para valorar el impacto potencial de un riesgo en la consecución de un objetivo. (COSO, 2013).

Por lo cual es esencial calcular tanto la probabilidad de que el riesgo se materialice como el grado de impacto potencial que podría tener en la entidad. La valoración del riesgo, por su parte, involucra un análisis que se relaciona directamente con la probabilidad de ocurrencia y puede llevarse a cabo tanto en términos cualitativos como cuantitativos.

La valorización cualitativa es la que utiliza solo escalas descriptivas para evaluar la probabilidad de ocurrencia de cada evento, mientras que la evaluación cuantitativa utiliza valores numéricos o datos estadísticos.

La valorización consiste en asignar a los riesgos calificaciones dentro de un rango, el cual podría ser entre 1 a 5 (insignificante (1), baja (2), media (3), moderada (4), alta (5), la cual depende del impacto y de la probabilidad (SIGWEB, s.f.) como se observa en la imagen siguiente:

**Figura 3. Referente de valoración del riesgo.**




***Fuente:*** *Elaboración propia.*

**Evaluación de la calidad de gestión.**

La organización dispone de mecanismos de evaluación de riesgos efectivos que implican a los niveles adecuados de la dirección con conocimientos adecuados. (COSO, 2013).

La evaluación de la calidad de la gestión tiene como objetivo principal determinar la eficacia de los controles implementados por la entidad para mitigar los riesgos.

**Calcular el riesgo neto o residual.**

La evaluación del riesgo inherente, además del riesgo residual, puede ayudar a la organización a comprender hasta qué punto es necesario adoptar respuestas ante los riesgos. (COSO, 2013).

Por lo cual el cálculo del riesgo neto o residual se basa en la consideración tanto del grado de materialización de los riesgos inherentes como de las acciones de mitigación implementadas por la administración.

### 1.4.6 Base Legal

La entidad objeto de estudio, es una empresa constituida en El Salvador, sujeta a la legislación nacional aplicable y vigente. Sus actividades son la prestación de servicio en gestión empresarial enfocada en la implementación de desarrollo y soluciones informáticas.

Debido a sus procesos bajo los cuales se identificarán riesgos la normativa legal que se aplicará será:

**LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS**

Esta ley generalmente establece disposiciones legales y reglamentos para prevenir y sancionar los delitos informáticos y proteger la seguridad de la información en entornos digitales.

El objeto de aplicación de esta ley establecido en su Art. 1.- es el proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes.

También esta ley se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. Sea este hecho cometido por cualquier persona, natural o jurídica, nacional o extranjera, y si estos afectan a bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador.

En diciembre de 2021, se ratifican reformas que ayudan a extender de manera más puntual ciertos artículos de dicha ley, donde se agregan más conceptos aplicables a esta ley y se dan con una mejor explicación algunos artículos. (ASAMBLEA LEGISLATIVA, 2021).

**LEY DE FIRMA ELECTRÓNICA.**

La firma electrónica se define como cualquier símbolo o proceso electrónico que permite a una persona manifestar su voluntad sobre un documento electrónico. Esto puede incluir desde una simple firma escaneada hasta métodos más avanzados de autenticación electrónica.

Entre el objeto de esta ley se encuentra la facilitación referente a las transacciones electrónicas, ya que promueve la adopción de tecnologías electrónicas en las transacciones comerciales y legales, eliminando barreras que pudieran existir para el uso de documentos y firmas electrónicas.

La ley establece que las firmas electrónicas tienen la misma validez legal que las firmas manuscritas, siempre que cumplan con los requisitos y estándares de seguridad especificados en la ley; entre los requisitos de autenticación se establecen aquellos que garanticen la identidad del firmante, como contraseñas, certificados digitales u otros métodos de autenticación.

Esta ley puede incluir disposiciones para prevenir el repudio de una firma electrónica, lo que significa que una vez que una persona ha firmado electrónicamente un documento, no puede negar su autoría, asimismo, puede requerirse que las soluciones de firma electrónica sean interoperables con otros sistemas y cumplan con estándares técnicos

específicos. También se establecen requisitos para el almacenamiento seguro y a largo plazo de documentos firmados electrónicamente.

Referente a penalidades por incumplimiento pueden establecerse sanciones y penalidades por el uso indebido de firmas electrónicas o por el incumplimiento de las disposiciones legales relacionadas con ella, y debe cumplirse con las leyes de protección de datos personales cuando se recopilen, almacenen y procesen datos personales en el contexto de firmas electrónicas. (ASAMBLEA LEGISLATIVA, 2015)

**LEY DE COMERCIO ELECTRÓNICO.**

El objeto de esta ley es establecer un marco legal de las relaciones electrónicas de índole comercial, contractual, y es aplicable a todo tipo de relación contractual celebrado de forma electrónica, digital o tecnológicamente equivalente.

Y los obligados a cumplirla será toda persona natural o jurídica, pública o privada establecida en El Salvador, que realice por sí mismo o por medio de intermediarios transacciones comerciales o intercambio de bienes o servicios contractuales, mediante la utilización de cualquier clase de tecnología o por medio de redes de comunicación interconectadas.

Las actividades reguladas en la presente ley se regirán por los siguientes principios:

- Principio de equivalencia funcional.
- Principio de neutralidad tecnológica.
- Principio de no repudiación.

En el Art. 20 establece que lo relativo a la protección de datos personales se estará a lo dispuesto en la legislación pertinente.

Los proveedores de servicios de intermediación en el ejercicio de sus actividades estarán obligados a:

a) Informar de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que permitan entre otros, la protección frente a virus informáticos y programas espía.

b) Contar con un mecanismo de recepción y gestión de reclamos de forma permanente, fácil, directa y gratuita. (ASAMBLEA LEGISLATIVA, 2020).

# CAPÍTULO II. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

## 2.1 Tipo de estudio

La investigación se basó en un enfoque cualitativo utilizando técnicas como la recolección de datos, las entrevistas abiertas y bajo proceso inductivo, donde se explora la perspectiva teórica. En este método, se examinó la información de manera gradual, partiendo de lo específico hacia lo general. El propósito principal es abordar una problemática, encontrar posibles consecuencias y entregar una conclusión. A través de las técnicas e instrumentos aplicados se dio respuesta a la problemática que se había formulado inicialmente.

## 2.2 Unidad de Análisis

La unidad de análisis de la investigación fue el jefe del área de TI de la empresa que se dedica a servicios de gestión empresarial ubicada en San Salvador ya que no cuenta con departamento de auditoría interna

## 2.3 Técnica e instrumento a usar en la investigación

Teniendo acceso a información y al personal de la empresa de estudio se consideraron las siguientes técnicas documentales y de campo:

**Técnicas:**

**Entrevistas:** Técnica que permitió obtener información necesaria sobre el tema de investigación, la cual se realizó al personal del área de tecnología de la información.

**Instrumentos:**

**Cuestionario de preguntas:** Se detallaron preguntas para poder realizar una entrevista a la unidad de análisis.

**Fuente bibliográfica:** Se obtuvo información necesaria de fuentes bibliográficas confiables.

## 2.4 Procesamiento de Información

Con la información obtenida de la investigación se realizó un análisis y fue trasladado el resultado a una hoja de trabajo con el fin de organizar una propuesta de solución a la entidad objeto de estudio.

## 2.5 Determinación de variables

Variable Dependiente

Fortalecimiento de la Gestión de Riesgos para mejorar los procesos en el área TI.

Variable Independiente

Programa de consultoría para la identificación y evaluación de riesgos en el área de TI de acuerdo con las NIEPAI.

### 2.6 Operacionalización de variables

**Tabla 1. Operacionalización de variables**

| **formulación del Problema** | **Objetivo General** | **Hipótesis del Trabajo** | **Elemento de la hipótesis** | **Variables** | **Indicadores** | **Instrumentos** |
|---|---|---|---|---|---|---|
| ¿De qué manera impacta la ausencia de un programa de consultoría sobre la identificación y evaluación de riesgos en el área de TI con respecto a la adecuada ejecución de los procesos, el logro de los objetivos y su debida gestión en la entidad que se dedica a la prestación de servicios de gestión empresarial? | Desarrollar una consultoría sobre la identificación y evaluación de riesgos asociados al área de Tecnología de la Información (TI) el cual contribuirá a la mejora en la gestión de riesgos y controles de la entidad objeto de estudio. | La elaboración de un programa de consultoría sobre la identificación y evaluación de riesgos en el área de TI contribuirá al fortalecimiento de la gestión de riesgos de la entidad objeto de estudio. | Programa de consultoría.<br><br>Evaluación de riesgos.<br><br>Identificación de riesgos. | **<u>Variable Independiente</u>**<br>Programa de consultoría para la identificación y evaluación de riesgos en el área de TI de acuerdo con las NIEPAI. | Marco Internacional para la Práctica Profesional de la auditoría interna.<br><br>Programa de consultoría de auditoría interna. | *Guías de Preguntas tipo entrevista<br>*Fichas bibliográficas para sustentar la investigación |
| | | | Riesgos en el área de TI | **<u>Variable Dependiente</u>**<br>Fortalecimiento de la gestión de Riesgos para mejorar los procesos en el área TI | Guías complementarias sobre Evaluación de riesgos en ciberseguridad y auditoria de programas contra amenazas internas | **parámetros de medición**<br>*Mejora de los procesos claves.<br>*Resultados de retroalimentación con las partes interesadas. |

***Fuente**: Elaboración propia*

## 2.7 Cronograma de Actividades.

**Tabla 2. Cronograma de actividades.**

| **Meses** | **Marzo** | | | | | **Abril** | | | | **Mayo** | | | | | **Junio** | | | | **Julio** | | | | **Agosto** | | | | | **Septiembre** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Semanas | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 |
| Actividades | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Inicio de Especializacion en Auditoria Interna | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Selección del tema | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enunciado del problema | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Capitulo I: Planteamiento del problema y marco teórico** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Justificación de la investigación | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Objetivos de la investigación | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Marco Teorico | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hipótesis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Entrega de Anteproyecto | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **b) Capitulo II : Metodología de la investigación** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enfoque y tipo de investigación | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Unidades de análisis, población y muestra. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Variables e indicadores | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **c) Capitulo III: Propuesta de solución:** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Propuesta de la Matriz de Riesgo, resultante de la consultoria | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Entrega Final | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

***Fuente**: Elaboración propia*

## 2.8 Diagnóstico.

Con la realización de una entrevista al encargado del área de Tecnología de la Información, esto con el objetivo de obtener detalles sobre los riesgos a los cuales se encuentra expuesto el departamento antes mencionado de la entidad objeto de estudio, y así, poder contribuir a la implementación de un programa de auditoría que ayude a minimizar la materialización de dichos riesgos, y contribuya al logro de los objetivos en la entidad.

De acuerdo con los resultados obtenidos de dicha entrevista, permitieron diagnosticar lo siguiente:

- Por el funcionamiento y giro de la entidad esta presenta un mayor riesgo en recibir ataques cibernéticos con los cuales se busca robar información como datos de clientes, contraseñas, usuarios, así como también eliminar información confidencial de clientes.
- Al no llevarse a cabo auditorias de la infraestructura tecnológica; sino que, solamente se han realizado observaciones sobre algunos puntos a mejorar esto puede ocasionar que no se dé una respuesta eficaz ante los sucesos; así mismo las recomendaciones que se han brindado no han sido tomadas en cuenta hasta el momento.
- Frecuentemente, la sustitución de los equipos se produce únicamente cuando dejan de funcionar, en lugar de considerar aspectos más precisos, como las actualizaciones necesarias o la verificación de que posean la capacidad requerida para asegurar el cumplimiento de los objetivos establecidos.

- Aunque se cuenta con una zona delimitada (*Demilitarized zone*), la cual es una red perimetral que protege la red de área local interna contra el tráfico de datos no confiable, no se puede garantizar que esté completamente libre de riesgo de ser infectada por *WannaCry* el cual puede acceder a los equipos reflejando vulnerabilidades del sistema operativo.
- Dado que la entidad brinda servicios tecnológicos clave, es fundamental garantizar que todos los servidores estén protegidos contra riesgos y cuenten con rigurosas medidas de seguridad. Sin embargo, es importante señalar que la empresa no dispone de estas medidas en la actualidad.
- La entidad no dispone de una política para administrar contraseñas y la creación de usuarios. Esto es especialmente preocupante en el caso de usuarios que no están relacionados con activos sensibles, pero que aun así pueden representar una posible vulnerabilidad en términos de programas y accesos a computadoras, lo que podría facilitar ataques internos.
- Aunque la entidad dispone de un Plan de Recuperación ante Desastres (DRP) que abarca aspectos como datos, hardware y software, es importante destacar que este plan nunca ha sido sometido a pruebas desde su implementación. Esta falta de pruebas podría generar preocupaciones en cuanto a la capacidad del plan para recuperar datos de manera efectiva en caso de que se materialice un riesgo. Por lo tanto, es esencial considerar la necesidad de realizar pruebas periódicas para garantizar la eficacia del DRP.
- La falta de un proceso de selección de proveedores de servicios complementarios que incluya requisitos de seguridad informática aumenta el riesgo de que estos

proveedores no cumplan con estándares de seguridad, lo que a su vez podría exponer los servicios proporcionados a posibles ataques.

- La ausencia de un plan de respuesta ante incidentes cibernéticos, como las brechas de seguridad o ataques, coloca a la entidad en una situación de riesgo actual en lo que respecta a la posible fuga de información.

Tras el diagnóstico de los riesgos, que se llevó a cabo mediante una entrevista con el responsable del área de TI, se ha llegado a la conclusión de que la entidad necesita implementar un programa de consultoría con el objetivo de mitigar los riesgos identificados y asegurar que se aborden de manera adecuada a través de procesos y controles eficaces.

La implementación de este programa de consultoría fortalecerá significativamente la calidad del servicio ofrecido a los clientes, así como la protección de la información confidencial y los activos de la entidad.

# CAPÍTULO III. PROPUESTA DE CONSULTORÍA PARA EL ÁREA DE TI DE UNA EMPRESA QUE SE DEDICA A LA PRESTACIÓN DE SERVICIOS DE GESTIÓN EMPRESARIAL.

## 3.1 Generalidades

### 3.1.1 Objetivo

Proporcionar una consultoría que permita identificar, evaluar y mitigar los riesgos en el área de Tecnología de la Información (TI) con el fin de garantizar la seguridad, disponibilidad e integridad de los sistemas, datos y recursos tecnológicos de la entidad objeto de estudio.

### 3.1.2 Alcance

Las guías que se presentan a continuación tienen como objetivo facilitar la identificación y evaluación de los riesgos, monitoreo y revisión de la matriz de riesgos, en el área de tecnología de información (TI) de una empresa que se dedica a la prestación de servicios de gestión empresarial y garantizar la operatividad de la empresa.

## 3.2 Planteamiento del caso práctico

La empresa "Entidad Objeto de Estudio S.A. de C.V.", fue fundada en el año 2015 en El Salvador, se dedica a ofrecer servicios de gestión empresarial, poniendo énfasis en herramientas informáticas y métodos analíticos, por esta razón, la infraestructura tecnológica es esencial para la satisfacción del cliente y operaciones efectivas del negocio.

Con el propósito de garantizar la seguridad y funcionamiento de la entidad, se propone una evaluación de riesgos en el área de tecnología de la información (TI), motivo por el cual se ha contratado a "Nemax S.A. de C.V."

Nemax S.A. de C.V. realiza un diagnóstico, previo a la realización de la consultoría donde se determina que la entidad presenta riesgos los cuales pudieran presentar un impacto en el logro de los objetivos, a su vez aquellos se identifican controles muy bajos que hacen que la entidad no logre el cumplimiento de sus objetivos estratégicos.

Con esta consultoría se pretende dar valor a la entidad, ya que permitirá la optimización de recursos y controles a modo de dar eficacia en sus operaciones, y así generar beneficios financieros y aumentar la capacidad de funcionamiento en un área tan fundamental como lo es el área de tecnología de la información.

## 3.3 Desarrollo del Caso.

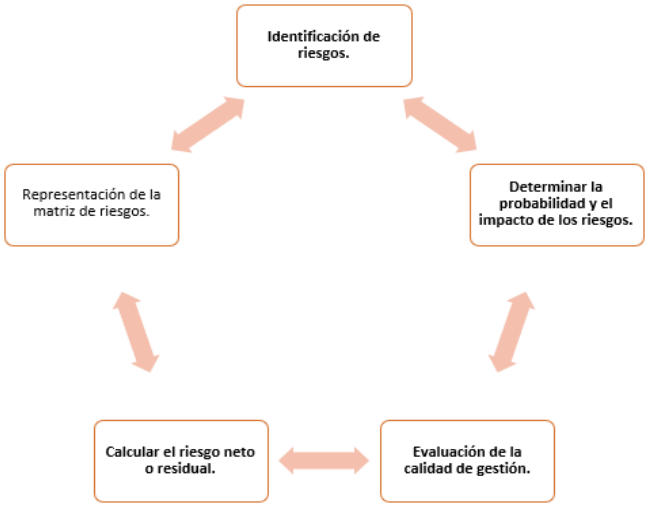
### 3.3.1 Proceso para prestar servicios de consultoría.

**Figura 4. Proceso para prestar servicios de consultoría.**


***Fuente:*** *Elaboración propia*

### 3.3.2 Pasos para elaborar una matriz de riesgo.

**Figura 5. Pasos para elaborar una matriz de riesgo.**

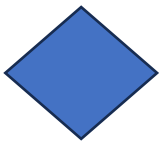
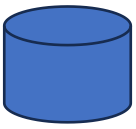



***Fuente:*** *Elaboración propia*

### 3.3.3 Flujogramas de Procesos.

**Simbología de flujograma de Procesos.**

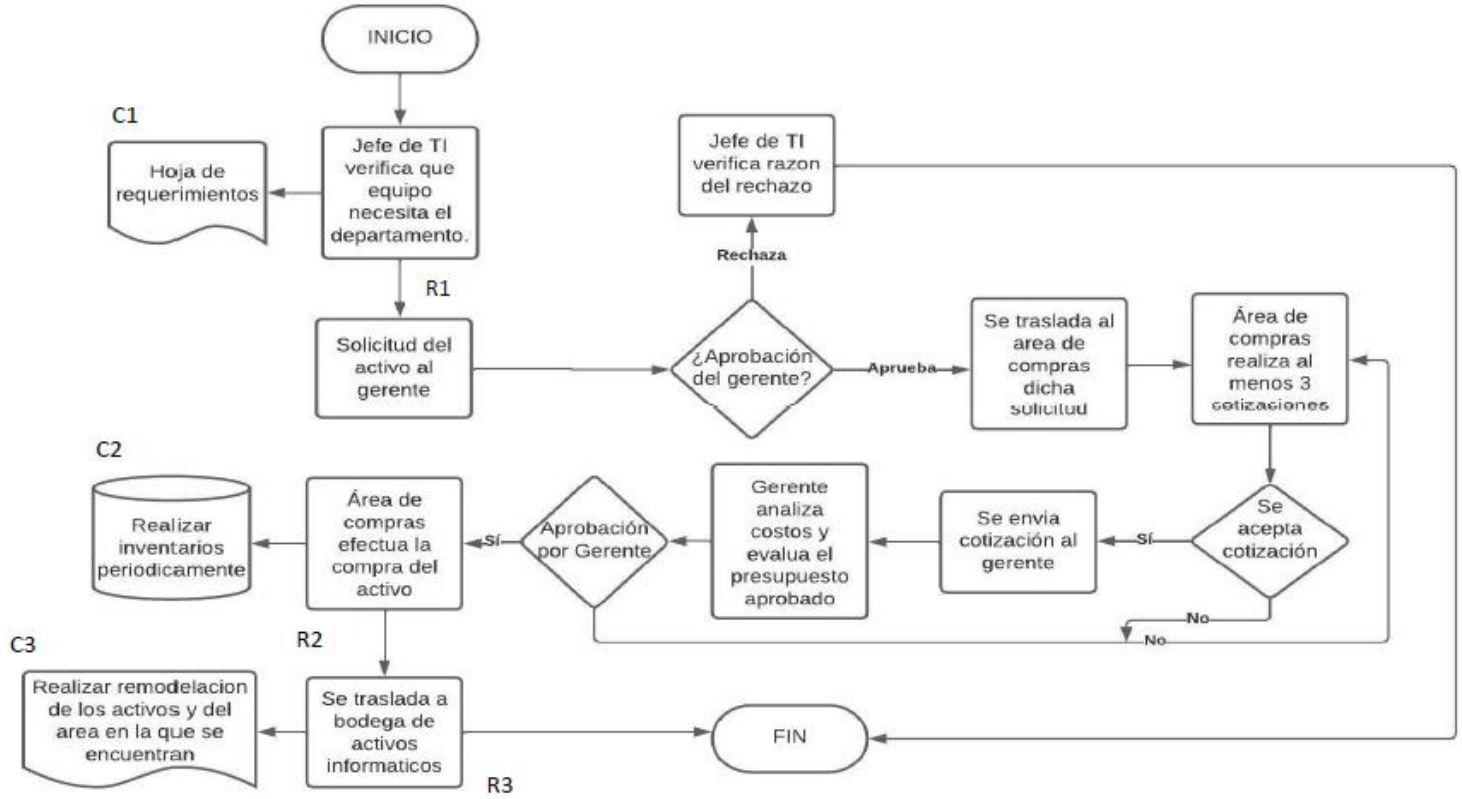
**Figura 6. Simbología de flujograma de Procesos.**

| SÍMBOLO | NOMBRE | FUNCIÓN |
|---|---|---|
|  | Inicio/Final | Representa el inicio y el final de un proceso. |
|  | Entrada/Salida | Representa la lectura de datos en la entrada y la impresión de datos en la salida. |
|  | Linea de Flujo | Indica el orden de la ejecución de las operaciones. La flecha indica la siguiente instrucción. |
|  | Proceso | Representa cualquier tipo de operación. |
|  | Decisión | Nos permite analizar una situación, con base en los valores verdadero y falso. |
|  | Documento | Documento utilizado en el proceso. |
|  | Base de datos | Empleado para representar la grabación de datos. |

***Fuente:*** *Símbolos de diagramas de flujo (smartdraw.com)*

**Proceso de compra de activo tecnológico.**

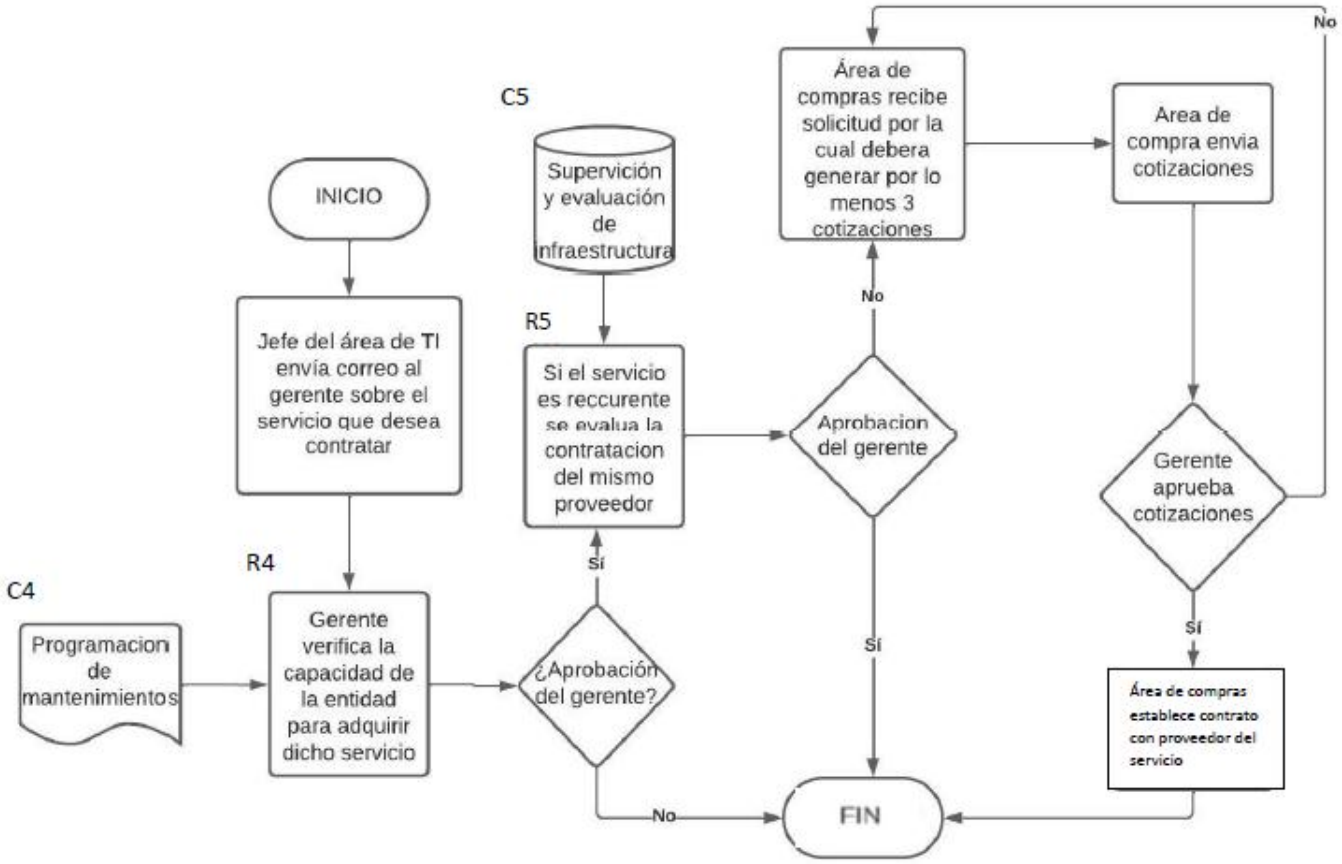
**Figura 7. Proceso de compra de activo tecnológico.**




***Fuente**: Elaboración propia*

***Proceso de contratación de servicio.***

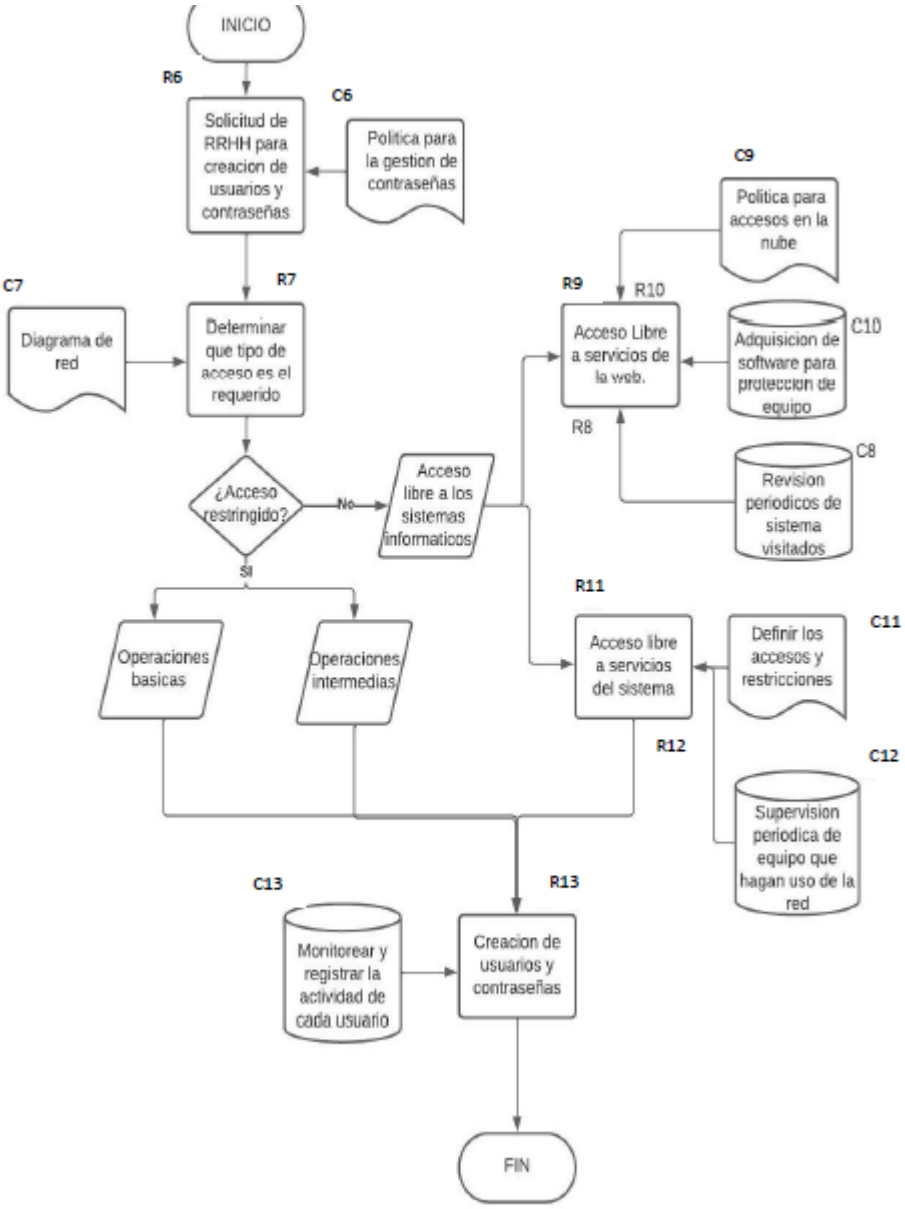
**Figura 8. Proceso de contratación de servicio.**




***Fuente:*** *Elaboración propia.*

**Proceso de control sobre accesos al sistema**

**Figura 9. Proceso de control sobre accesos al sistema.**




***Fuente:*** *Elaboración propia.*

### 3.3.4 Parámetros de medición.

**Tabla 3.Ponderación magnitud de Impacto.**

| Clasificación | Nivel | Económico ($) | Proceso (T) | Reputacional |
|---|---|---|---|---|
| **Insignificante** | **1** | Pérdida menor o igual al 1% del patrimonio | Reproceso/interrupción del proceso menor/ igual a 2 días | Al interior del proceso |
| **Menor** | **2** | Pérdida entre el 1,01% y 3% del patrimonio | Reproceso/interrupción del proceso entre 3 y 8 días | A nivel de compañía |
| **Moderada** | **3** | Pérdida entre el 3,01% y 6% del patrimonio | Reproceso/interrupción del proceso entre 9 y 16 días | A nivel de gremio Asociación o similar |
| **Mayor** | **4** | Pérdida entre el 6,01% y 10% del patrimonio | Reproceso/interrupción del proceso entre 17 y 24 días | A nivel de cliente |
| **catastrófica** | **5** | Pérdida superior al 10,01% del patrimonio | Reproceso/interrupción del proceso superior a 24 días | Medios de comunicación |

***Fuente:*** *Elaboración propia.*

**Tabla 4.Ponderacion de Probabilidad de Ocurrencia.**

| Clasificación | Nivel | Descripción |
|---|---|---|
| Casi seguro | **5** | La vulnerabilidad se materializa más de diez veces en el año |
| Muy probable | **4** | La vulnerabilidad se materializa a lo sumo de siete a diez veces en el año |
| Posible | **3** | La vulnerabilidad se materializa a lo sumo de cuatro a seis veces en el año |
| Improbable | **2** | La vulnerabilidad se materializa a lo sumo de dos a tres veces en el año |
| Muy improbable | **1** | La vulnerabilidad se materializa a lo sumo una vez en el año |

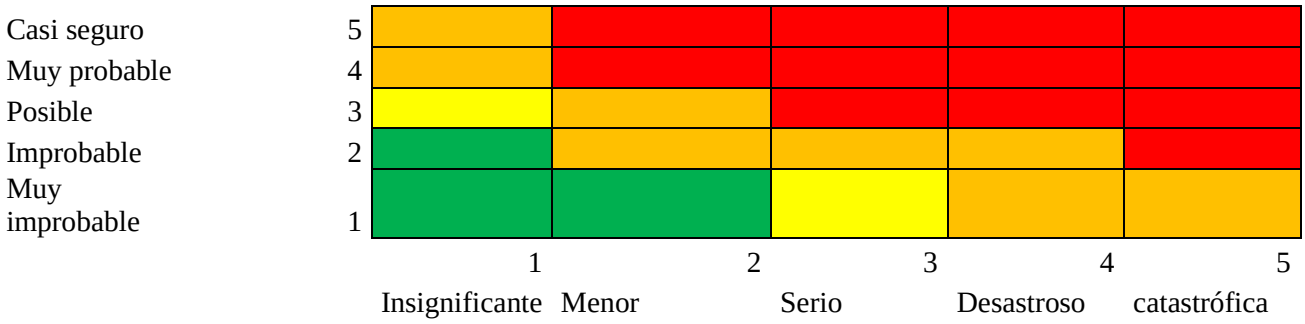
***Fuente:*** *Elaboración propia.*

**Tabla 5. Medida de efectividad de los controles.**

| Periodicidad (P) | Función/oportunidad | Naturaleza | Eficiencia del control | Nivel de control |
|---|---|---|---|---|
| Permanente | Preventivo | Automatizado | Optimo | 5 |
| | | Semiautomatizado | | |
| | | Manual | | |
| | Correctivo | Automatizado | | |
| | | Semiautomatizado | | |
| | | Manual | | |
| | Detectivo | Automatizado | | |
| | | Semiautomatizado | | |
| | | Manual | | |
| Periodico | Preventivo | Automatizado | Bueno | 4 |
| | | Semiautomatizado | | |
| | | Manual | | |
| | Correctivo | Automatizado | | |
| | | Semiautomatizado | | |
| | | Manual | | |
| | Detectivo | Automatizado | | |
| | | Semiautomatizado | | |
| Ocasional | Preventivo | Manual | Medio | 3 |
| | | Automatizado | | |
| | | Semiautomatizado | | |
| | Correctivo | Manual | | |
| | | Automatizado | | |
| | | Semiautomatizado | | |
| | Detectivo | Manual | Regular | 2 |
| | | Automatizado | | |
| | | Semiautomatizado | | |
| | | Manual | Deficiente | 1 |

***Fuente:*** *Elaboración propia.*

**Figura 10. Valoración del riesgo.**




| | | |
|---|---|---|
| 0-2.99 | | MENOR |
| 3-3.99 | | MEDIA |
| 4-7.99 | | MAYOR |
| 8-25 | | INACEPTABLE |

***Fuente:*** *Elaboración propia.*

### 3.3.5 Identificación de Riesgos.

**Tabla 6. Identificación de riesgos.**

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. | | | | | | | |
|---|---|---|---|---|---|---|---|
| IDENTIFICACIÓN DE RIESGOS | | | | | | | |
| | | | | | | | |
| **N.º** | **ÁREA** | **PROCESO** | **RIESGO IDENTIFICADO** | **OBJETIVO** | **DESCRIPCIÓN DEL RIESGO** | **TIPO DE RIESGO** | **PROPIETARIO** |
| 1 | Tecnología de la Información | Solicitud de cambio de activo fijo en el área | R1: Adquisición de activo inadecuado | Incorporar eficientemente nuevos activos tecnológicos en la infraestructura de la empresa para satisfacer las necesidades y optimizar recursos. | Posibilidad de adquirir activos que no cumplan con las capacidades técnicas requeridas por especificaciones incorrectas y selección de proveedores inadecuados. | Financiero | Jefe de área |
| 2 | Tecnología de la Información | Adquisición de activo tecnológico | R2: Riesgo de obsolescencia de activo | Minimizar el impacto financiero de la obsolescencia de inventario a través de una gestión eficiente de activos con las capacidades requeridas para el área. | Los activos tecnológicos pueden volverse obsoletos rápidamente en términos de soporte, lo que puede requerir costos adicionales para mantenerse actualizados. | Financiero | Jefe de área |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **IDENTIFICACIÓN DE RIESGOS** | | | | | | | |
| | | | | | | | |
| **N.º** | **ÁREA** | **PROCESO** | **RIESGO IDENTIFICADO** | **OBJETIVO** | **DESCRIPCIÓN DEL RIESGO** | **TIPO DE RIESGO** | **PROPIETARIO** |
| 3 | Tecnología de la Información | Mantenimiento de área lógica y física | R3: Infraestructura tecnológica sin mantenimiento | Implementar un programa de mantenimiento preventivo y correctivo en la infraestructura tecnológica. | Los sistemas y equipos de la empresa no reciben el mantenimiento necesario lo que puede conducir a fallos inesperados e interrupciones operativas. | Operativo | Jefe de área |
| 4 | Tecnología de la Información | Adquisición de servicios | R4: Soporte deficiente | Identificar y evaluar de manera proactiva las posibles debilidades en los procesos de soporte del área, con el fin de anticipar problemas, mejorar la calidad de los servicios de asistencia técnica, garantizar la continuidad operativa. | Posibilidad de que el departamento de TI no pueda proporcionar un nivel adecuado de asistencia técnica, lo cual puede derivar en interrupciones operativas y mala experiencia de los usuarios. | Reputacional | Departamento de Compras |
| 5 | Tecnología de la Información | Adquisición de servicios | R5: Condiciones no adecuadas para el buen funcionamiento de los equipos. | Identificar problemas potenciales en el | Posibilidad de que las condiciones de temperatura y humedad en las áreas | Operativo | |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. | | | | | | | |
|---|---|---|---|---|---|---|---|
| IDENTIFICACIÓN DE RIESGOS | | | | | | | |
| | | | | | | | |
| **N.º** | **ÁREA** | **PROCESO** | **RIESGO IDENTIFICADO** | **OBJETIVO** | **DESCRIPCIÓN DEL RIESGO** | **TIPO DE RIESGO** | **PROPIETARIO** |
| | | | | sistema de enfriamiento del área de TI para prevenir fallos y garantizar la continuidad operativa. | de alojamiento de servidores y centros de datos no sean adecuados, lo que puede derivar en sobrecalentamiento de los equipos y sistemas informáticos, fallos, daños y pérdida de datos. | | Departamento de Compras |
| 6 | Tecnología de la Información | Control al acceso del sistema | R6: Deficiente control de accesos. | Evitar posibles deficiencias en los controles de acceso de TI para prevenir accesos no autorizados y mantener la seguridad de la información. | Falta de protección apropiada contra accesos no autorizados a sistemas y recursos de la empresa lo que puede llevar al robo de datos confidenciales. | Seguridad | Jefe de área |
| 7 | Tecnología de la Información | Mantenimiento de área lógica y física | R7: Equipo de Red no ordenado | Implementar buenas prácticas de gestión de red, como documentar y etiquetar adecuadamente los dispositivos, mantener un inventario | En caso de problemas o fallas en la red, la falta de organización puede prolongar el tiempo necesario para identificar y resolver los problemas, lo que podría resultar en períodos de inactividad más largos | Operativo | Jefe de área |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **IDENTIFICACIÓN DE RIESGOS** | | | | | | | |
| | | | | | | | |
| **N.º** | **ÁREA** | **PROCESO** | **RIESGO IDENTIFICADO** | **OBJETIVO** | **DESCRIPCIÓN DEL RIESGO** | **TIPO DE RIESGO** | **PROPIETARIO** |
| | | | | actualizado de hardware | | | |
| 8 | Tecnología de la Información | Control al acceso del sistema | R8: Amenaza por software malicioso | Identificar posibles amenazas de software malicioso y proteger la tecnología de la información de la organización. | Posibilidad de que programas dañinos, como virus o programas maliciosos puedan romper la seguridad de los sistemas de la empresa y causar problemas como el robo de la información e interrupción de la operatividad. | Seguridad | Jefe de área |
| 9 | Tecnología de la Información | Conexión a la red local | R9: Libre acceso a la nube | Garantizar que el personal de la empresa tenga acceso a la nube de manera restringida. | Exposición de información confidencial al alcance de cualquier persona ajena a la empresa. | Seguridad | Jefe de área |
| 10 | Tecnología de la Información | Conexión a la red local | R10: Ciberataques por *phishing* | Implementar medidas de seguridad para prevenir la exposición de información confidencial de la empresa. | Amenaza de que los empleados reciban correos electrónicos o mensajes falsos, engañando a las personas para robar información confidencial. | Seguridad | Jefe de área |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. | | | | | | | |
|---|---|---|---|---|---|---|---|
| **IDENTIFICACIÓN DE RIESGOS** | | | | | | | |
| | | | | | | | |
| **N.º** | **ÁREA** | **PROCESO** | **RIESGO IDENTIFICADO** | **OBJETIVO** | **DESCRIPCIÓN DEL RIESGO** | **TIPO DE RIESGO** | **PROPIETARIO** |
| 11 | Tecnología de la Información | Control al acceso del sistema | R11: Eliminación de datos sensibles por personal no autorizado | Evitar que personal no autorizado o ajeno a la entidad tenga acceso al sistema. | Posibilidad de que información confidencial o delicada sea eliminada por personal no autorizado o por personas externas a la entidad. | Seguridad | Jefe de área |
| 12 | Tecnología de la Información | Conexión a la red local | R12: Uso de equipo personales | Evitar que personal de la empresa utilice equipos electrónicos personales y que tengan acceso a la red local. | Amenaza que surge cuando los empleados utilizan sus propios dispositivos personales para acceder a los sistemas de la empresa y datos corporativos. | Seguridad | Jefe de área |
| 13 | Tecnología de la Información | Control al acceso del sistema | R13: Acceso no autorizado al sistema | Gestionar y asignar accesos, permisos de manera específica para cada área de manera más eficiente. | Si los empleados tienen acceso a áreas o datos para los que no están autorizados, puede ocurrir la fuga de información confidencial, lo que podría tener graves consecuencias para la organización | Seguridad | Jefe de área |
| 14 | Tecnología de la Información | Adquisición nuevo personal | R14: Falta de capacitación al personal de la empresa | Invertir en capacitación y desarrollo del | Ineficiencia operativa debido a la falta de capacitación de los empleados, lo que | Operativo | RRHH |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. | | | | | | | |
|---|---|---|---|---|---|---|---|
| IDENTIFICACIÓN DE RIESGOS | | | | | | | |
| | | | | | | | |
| **N.º** | **ÁREA** | **PROCESO** | **RIESGO IDENTIFICADO** | **OBJETIVO** | **DESCRIPCIÓN DEL RIESGO** | **TIPO DE RIESGO** | **PROPIETARIO** |
| | | | | personal del área de TI | podría provocar retrasos en la ejecución de sus asignaciones. | | |

***Fuente**: Elaboración propia.*

### 3.3.6 Identificación de Controles.

**Tabla 7. Identificación de controles.**

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| IDENTIFICACIÓN DE CONTROLES |
| CONTROLES PARA MITIGAR EL RIESGO |

| Nº | PROCESO | PROPIETARIO | RIESGO IDENTIFICADO | CONTROL | PERIODICIDAD | FUNCIÓN | NATURALEZA | EVIDENCIA | NIVEL DE EFECTIVIDAD |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Solicitud de cambio de activo fijo en el área. | Jefe de área | R1: Adquisición de activo inadecuado | C1: Cuando se solicite un activo informático, es esencial proporcionar una lista detallada de requerimientos que estén directamente relacionados con el propósito específico para el cual se destinará el activo. | Ocasional | Preventivo | Manual | Solicitud formal que incluya las características técnicas y funcionalidades necesarias del activo. | 2 |
| 2 | Adquisición de activo tecnológico | Jefe de área | R2: Riesgo de obsolescencia de activo | C2: Realizar inventarios de activos que presentan mal funcionamiento o que han quedado fuera de su capacidad óptima, | Periódico | Correctivo | Manual | Registro con fecha y motivo por el cual se ha dado de baja el activo fijo. | 3 |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| IDENTIFICACIÓN DE CONTROLES |
| CONTROLES PARA MITIGAR EL RIESGO |

| Nº | PROCESO | PROPIETARIO | RIESGO IDENTIFICADO | CONTROL | PERIODICIDAD | FUNCIÓN | NATURALEZA | EVIDENCIA | NIVEL DE EFECTIVIDAD |
|---|---|---|---|---|---|---|---|---|---|
| | | | | y proceder a darlos de baja adecuadamente. | | | | | |
| 3 | Mantenimiento de área lógica y física | Jefe de área | R3: Infraestructura tecnológica sin mantenimiento | C3: Hacer una remodelación adecuada para los activos informáticos y también del área. | Ocasional | Detectivo | Manual | Facturas donde se compruebe que se han realizado remodelaciones y plan detallado futuros. | 1 |
| 4 | Adquisición de servicios | Departamento de Compras | R4: Soporte deficiente. | C4: Realizar programación de los mantenimientos que se le deben de dar a los equipos informáticas con anticipación. | Periódico | Preventivo | Manual | Registro de la programación de mantenimientos preventivos donde incluya fecha programadas. | 4 |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| IDENTIFICACIÓN DE CONTROLES |
| CONTROLES PARA MITIGAR EL RIESGO |

| Nº | PROCESO | PROPIETARIO | RIESGO IDENTIFICADO | CONTROL | PERIODICIDAD | FUNCIÓN | NATURALEZA | EVIDENCIA | NIVEL DE EFECTIVIDAD |
|---|---|---|---|---|---|---|---|---|---|
| 5 | Adquisición de servicios | Departamento de Compras | R5: Condiciones no adecuadas para el buen funcionamiento de los equipos. | C5: Supervisar el área constantemente y evaluar la infraestructura para evitar una pérdida de información también programar mantenimientos preventivos del equipo. | Periódico | Preventivo | Manual | Ordenes de trabajo de mantenimiento preventivo aprobados y firmados de acuerdo al calendario programado. | 4 |
| 6 | Control al acceso del sistema | Jefe de área | R6: Deficiente control de accesos | C6: Proponer una política en cuanto a las gestiones de contraseñas para los equipos del área | Periódico | Preventivo | Automático | Política de contraseñas aprobada y firmada. | 4 |
| 7 | Mantenimiento de área lógica y física | Jefe de área | R7: Equipo de Red no ordenado | C7: Documentar y etiquetar los componentes de red de la entidad con el fin de mantener un registro actualizado de | Periódico | Preventivo | Manual | Diagramas de red actualizados que permitan reflejar con precisión la infraestructura de red. | 4 |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| IDENTIFICACIÓN DE CONTROLES |
| CONTROLES PARA MITIGAR EL RIESGO |

| Nº | PROCESO | PROPIETARIO | RIESGO IDENTIFICADO | CONTROL | PERIODICIDAD | FUNCIÓN | NATURALEZA | EVIDENCIA | NIVEL DE EFECTIVIDAD |
|---|---|---|---|---|---|---|---|---|---|
| | | | | configuraciones y diagramas. | | | | | |
| **8** | Control al acceso del sistema | Jefe de área | R8: Amenaza por software malicioso | C8: Revisar periódicamente los sitios visitados por los empleados, y gestionar una política para no permitir el acceso a páginas que no sean seguras. | Periódico | Correctivo | Automático | Política de bloqueos de sitios web. | 3 |
| **9** | Conexión a la red local | Jefe de área | R9: Libre acceso a la nube | C9: Gestionar una política donde los empleados tenga acceso restringido a ciertos sitios web. | Permanente | Preventivo | Automático | Política documentada en donde especifique que sitios web estarán restringidos para el personal. | 5 |
| **10** | Conexión a la red local | Jefe de área | R10: Ciberataques por *phishing* | C10: Gestionar un software que proteja los equipos de | Periódico | Preventivo | Automático | Contrato de adquisición de un software de | 4 |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| IDENTIFICACIÓN DE CONTROLES |
| CONTROLES PARA MITIGAR EL RIESGO |

| Nº | PROCESO | PROPIETARIO | RIESGO IDENTIFICADO | CONTROL | PERIODICIDAD | FUNCIÓN | NATURALEZA | EVIDENCIA | NIVEL DE EFECTIVIDAD |
|---|---|---|---|---|---|---|---|---|---|
| | | | | amenazas maliciosas, y también capacitar a los empleados sobre las practicas seguras de navegación. | | | | protección contra amenazas internas y externas. | |
| **11** | Control al acceso del sistema | Jefe de área | R11: Eliminación de datos sensibles por personal no autorizado | C11: Definir los accesos y restricciones para cada empleado de la entidad. | Periódico | Detectivo | Automático | Documento formal que detalle los niveles de acceso y las restricciones para cada empleado. | 4 |
| **12** | Conexión a la red local | Jefe de área | R12: Uso de equipo personales | C12: Supervisión periódica de equipos que están conectados a la red o los que los empleados utilizan en asignaciones laborales. | Periódico | Preventivo | Manual | Reporte de equipos tecnológicos que están conectados a la red. | 4 |
| **13** | Control al acceso del sistema | Jefe de área | R13: Acceso no autorizado al sistema | C13: Monitorear y registrar la actividad de cada | Permanente | Preventivo | Semi-automático | Bitácoras de actividades de cada | 5 |

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| IDENTIFICACIÓN DE CONTROLES |
| CONTROLES PARA MITIGAR EL RIESGO |

| Nº | PROCESO | PROPIETARIO | RIESGO IDENTIFICADO | CONTROL | PERIODICIDAD | FUNCIÓN | NATURALEZA | EVIDENCIA | NIVEL DE EFECTIVIDAD |
|---|---|---|---|---|---|---|---|---|---|
| | | | | usuario y solicitar el acceso requerido al coordinar o jefe inmediato del empleado. | | | | maquina asignada al personal. | |
| **14** | Adquisición nuevo personal | RRHH | R14: Falta de capacitación al personal de la empresa | C14: Realizar programas de capacitación y desarrollo del personal | Periódico | Preventivo | Manual | Programas de capacitación a los empleados del área. | 4 |

***Fuente:*** *Elaboración propia.*

### 3.3.7 Matriz de riesgos.

**Tabla 8. Matriz de Riesgos.**

| ENTIDAD OBJETO DE ESTUDIO, S.A. DE C.V. |
|---|
| MATRIZ DE RIESGOS |

| N.º | PROCESO | RIESGO IDENTIFICADO | CATEGORIA DEL RIESGO POR OBJETIVO (3) | EVALUACIÓN DEL RIESGO | | | CONTROL (7) | PERIODICIDAD (8) | FUNCIÓN (9) | NATURALEZA (10) | RIESGO DE CONTROL (11) | RIESGO RESIDUAL (12) (6)/(11) | NIVEL DE EXPOSICIÓN (13) | RIESGO RESIDUAL POR CATEGORIA (14) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | CALIFICACIÓN | | RIESGO INHERENTE (6) (4)*(5) | | | | | | | | |
| | | | | PROBABILIDAD (4) | IMPACTO (5) | | | | | | | | | |
| 1 | Adquisición de activo tecnológico | R2: Riesgo de obsolescencia de activo | Financiero | 3 | 4 | 12 | C2: Realizar inventarios de activos que presentan mal funcionamiento o que han quedado fuera de su capacidad óptima, y proceder a darlos de baja adecuadamente. | Periódico | Correctivo | Manual | 3 | 4.00 | MAYOR | 4.50 |
| 2 | Solicitud de cambio de activo fijo en el área. | R1: Adquisición de activo inadecuado | Financiero | 2 | 5 | 10 | C1: Cuando se solicite un activo informático, es esencial proporcionar una lista detallada de requerimientos que estén | Ocasional | Preventivo | Manual | 2 | 5.00 | MAYOR | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | directamente relacionados con el propósito específico para el cual se destinará el activo | | | | | | | |
| 3 | Adquisición de servicios | R4: Soporte deficiente. | Reputacional | 3 | 5 | 15 | C4: Realizar programación de los mantenimientos que se le deben de dar a los equipos informáticas con anticipación. | Periódico | Preventivo | Manual | 4 | 3.75 | MEDIA | 3.75 |
| 4 | Adquisición de servicios | R5: Condiciones no adecuadas para el buen funcionamiento de los equipos. | Operativo | 5 | 5 | 25 | C5: Supervisar el área constantemente y evaluar la infraestructura para evitar una pérdida de información también programar mantenimientos preventivos del equipo. | Periódico | Preventivo | Manual | 4 | 6.25 | MAYOR | 6.25 |
| 5 | Control al acceso del sistema | R6: Deficiente control de accesos | Seguridad | 2 | 4 | 8 | C6: Proponer una política en cuanto a las gestiones de contraseñas para los equipos del área | Periódico | Preventivo | Automático | 4 | 2.00 | MENOR | 4.14 |
| 6 | Control al acceso del sistema | R11: Eliminación de datos sensibles por personal no autorizado | Seguridad | 1 | 5 | 5 | C11: Definir los accesos y restricciones para cada empleado de la entidad. | Permanente | Detectivo | Automático | 4 | 1.25 | MENOR | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | Control al acceso del sistema | R13: Acceso no autorizado al sistema | Seguridad | 1 | 2 | 2 | C13: Monitorear y registrar la actividad de cada usuario y solicitar el acceso requerido al coordinar o jefe inmediato del empleado. | Permanente | Preventivo | Semi-automático | 5 | 0.40 | MENOR |
| 8 | Control al acceso del sistema | R8: Amenaza por software malicioso | Seguridad | 1 | 5 | 5 | C8: Revisar periódicamente los sitios visitados por los empleados, y gestionar una política para no permitir el acceso a páginas que no sean seguras. | Periódico | Correctivo | Automático | 3 | 1.67 | MENOR |
| 9 | Conexión a la red local | R12: Uso de equipo personales | Seguridad | 2 | 5 | 10 | C12: Supervisión periódica de equipos que están conectados a la red o los que los empleados utilizan en asignaciones laborales. | Periódico | Preventivo | Manual | 4 | 2.50 | MENOR |
| 10 | Conexión a la red local | R10: Ciberataques por phishing | Seguridad | 1 | 4 | 4 | C10: Gestionar un software que proteja los equipos de amenazas maliciosas, y también capacitar a los empleados sobre las practicas seguras de navegación. | Periódico | Preventivo | Automático | 4 | 1.00 | MENOR |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | Conexión a la red local | R9: Libre acceso a la nube | Seguridad | 2 | 4 | 8 | C9: Gestionar una política donde los empleados tenga acceso restringido a ciertos sitios web. | Permanente | Preventivo | Automático | 5 | 1.60 | MENOR | |
| 12 | Mantenimiento de área lógica y física | R3: Infraestructura tecnológica sin mantenimiento | Operativo | 2 | 5 | 10 | C3: Hacer una remodelación adecuada para los activos informáticos y también del área. | Ocasional | Detectivo | Manual | 1 | 10.00 | INACEPTABLE | 4.58 |
| 13 | Mantenimiento de área lógica y física | R7: Equipo de Red no ordenado | Operativo | 3 | 3 | 9 | C7: Documentar y etiquetar los componentes de red de la entidad con el fin de mantener un registro actualizado de configuraciones y diagramas. | Periódico | Preventivo | Manual | 4 | 2.25 | MENOR | |
| 14 | Adquisición nuevo personal | R14: Falta de capacitación al personal de la empresa | Operativo | 2 | 3 | 6 | C14: Realizar programas de capacitación y desarrollo del personal | Periódico | Preventivo | Manual | 4 | 1.50 | MENOR | |

***Fuente:*** *Elaboración propia.*

### 3.3.8 Análisis de la matriz de riesgos.

Tras analizar la matriz de riesgos, se han identificado una serie de riesgos que pueden tener un impacto variable en el logro de los objetivos de la entidad. Estos riesgos incluyen la incapacidad para desempeñar adecuadamente las funciones asignadas debido a la falta de equipos adecuados con las características necesarias. Además, existe un riesgo significativo relacionado con el soporte externo insuficiente de los equipos informáticos, lo que podría afectar la eficiencia operativa. También se ha identificado un alto riesgo de eliminación de información por parte de empleados, ya que no existen políticas adecuadas para la gestión de contraseñas y las restricciones de acceso son deficientes. Debido a los casos antes mencionados, es oportuno llevar a cabo la implementación de controles para poder mitigar dichos riesgos y reducirlos de manera eficaz, dentro de los cuales podemos mencionar:

- Definir política de gestión de contraseñas y los accesos brindados a cada empleado
- Realizar una programación de todos aquellos equipos que necesiten soporte con anticipación.
- Llevar un control de las solicitudes de equipo donde se especifique las características que debe cumplir para poder ser utilizado de manera correcta.
- Realizar capacitaciones a los empleados en los temas de ciberataques, *phishing*, etc. Esto para que todas las áreas tengan conocimiento de ello y puedan alertar de manera oportuna y evitar algún tipo de robo de información.

**Categorización de procesos según su impacto y asignación de controles**

Dentro del análisis y revisión de los procesos en el área de informática se identificaron cuáles de estos tienen un impacto alto hasta el que posee un bajo impacto, para ser controlados en su ejecución.

ALTO

a. Adquisición de servicios.
b. Control al acceso del sistema.
c. Mantenimiento de área lógica y física.

Al realizar la entrevista para evaluación de control interno, los procesos más expuestos al riesgo están el de adquisición de servicios, ya que se menciona que el servicio de soporte es bastante deficiente, esto debido a que la entidad se ajusta al presupuesto y no a la necesidad de poseer un servicio de calidad, también dentro de los servicios adquiridos está el de aire acondicionado y este no es el adecuado porque no logra cubrir la necesidad en el área. Así mismo el proceso de control al sistema presenta un alto riesgo porque en muchas ocasiones no hay eliminación de usuarios antiguos o que ya no pertenecen a la entidad lo cual puede provocar la eliminación de datos sensibles para la entidad, también el uso de equipo sin las medidas necesarias para conectarse a la red de la entidad puede provocar que esta se infecte de software maliciosos.

Entre los controles relacionados al soporte deficiente que sufre la entidad está el "realizar programación de los mantenimientos que se le deben de dar a los equipos informáticos con anticipación", para que estos puedan funcionar correctamente dentro de las actividades diarias de la entidad, para el riesgo del aire acondicionado se tiene un

control de “supervisar el área constantemente y evaluar la infraestructura para evitar una pérdida de información también programar mantenimientos preventivos del equipo”, ya que puede existir muchas fallas como un sobrecalentamiento o afectación al servicio que la entidad presta.

El control aplicado a la infección de software maliciosos está el “definir los accesos y restricciones para cada empleado de la entidad”, esto aliviará a la red de la entidad a que sea más seguro para la información que se maneje en el área.

MEDIO

a. Adquisición de activo tecnológico.
b. Solicitud de cambio de activo fijo en el área.

Al observar procesos como la adquisición de activos tecnológicos o cambios de estos en el área, representa un riesgo medio, ya que se da ocasiones en las cuales el activo adquirido no es el correcto o el necesario para la función establecida, pero se tiene el control de que “cuando se solicite un activo informático, es esencial proporcionar una lista detallada de requerimientos que estén directamente relacionados con el propósito específico para el cual se destinará el activo”, motivo por el cual no representa un impacto de gravedad a la entidad.

Referente al cambio de activos se suele aplicar el control de “realizar inventarios de activos que presentan mal funcionamiento o que han quedado fuera de su capacidad óptima, y proceder a darlos de baja adecuadamente.” Esto aliviará a que la entidad cuente con el equipo necesario para proveer un servicio de calidad a sus clientes.

BAJO

a. Adquisición nuevo personal

Dentro de los riesgos con menos impacto se encuentra el proceso para adquirir personal nuevo, ya que se suele gestionar a la hora de las entrevistas las funciones que se desean tenga los aplicadores a las plazas además de aplicar el control de “realizar programas de capacitación y desarrollo del personal”, esto para establecer que el área, está brindado un servicio de calidad y promover así el desarrollo dentro del personal que labora en el área.

# CONCLUSIONES

- La entidad objeto de estudio al no contar con un departamento de auditoría interna que evalué o supervisé los distintos controles internos, dificulta el realizar análisis fiables que agreguen valor a la entidad o fortalezcan los procesos de gestión de riesgos.
- Se determinó que la entidad objeto de estudio no cuenta con un sistema de control o medidas adecuadas para responder ante los distintos riesgos que pueden verse expuesto el área de tecnología de la información.
- La entidad objeto de estudio no lleva a cabo evaluaciones periódicas de los riesgos a los que se ve expuesta el área de TI y no cuenta con un plan con el cual pueda mitigar dichos riesgos.
- Se concluye que la entidad objeto de estudio carece de herramientas indicadas por normativas para evaluar los riesgos como parte integral del proceso en el área de tecnología de la información.

# RECOMENDACIONES

- El establecimiento de una unidad de auditoría interna que brinde aseguramiento de los procesos y controles, a través de la ejecución de un plan de evaluación e identificación de riesgos.
- Implementar un sistema de control interno el cual este adaptado a las necesidades de la entidad en el que se defina quienes son los responsables y cuáles son sus funciones asignadas dentro de ellos.
- Llevar a cabo evaluaciones periódicas con la elaboración de una matriz de riesgos donde se puedan identificar los distintos riesgos a los cuales se ve expuesta el área de TI.
- La adopción de mecanismo y herramientas de normativas para dar seguimiento y tratamiento eficaz a los riesgos que puedan presentarse en el área de tecnología de la información.

**BIBLIOGRAFÍA**

ASAMBLEA LEGISLATIVA. (14 de Diciembre de 2000). CODIGO TRIBUTARIO. San Salvador, El Salvador.

ASAMBLEA LEGISLATIVA. (21 de Octubre de 2015). LEY DE FIRMA ELECTRÓNICA. San Salvador, El Salvador.

ASAMBLEA LEGISLATIVA. (6 de Febrero de 2020). LEY DE COMERCIO ELECTRÓNICO. San Salvador, El Salvador.

ASAMBLEA LEGISLATIVA. (DICIEMBRE de 2021). LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Y CONEXOS. EL SALVADOR.

COSO. (2013). Evaluacion de riesgos 2013. En C. 2013.

Enterprise. (Agosto de 2015). *Enterprise "Controles Generales de TI"*. Obtenido de https://enterpriseit.cl/controles-generales-de-tecnologias-de-informacion/

Instituto de Auditores Internos. (2016). *Evaluación de riesgos de ciberseguridad.* Fundación Latinoamericana de Auditores Internos (FLAI).

Instituto de Auditores Internos. (2018). *Auditoría de programas contra amenazas internas.* 1035 Greenwood Blvd., Suite 401: Fundación Latinoamericana de Auditores Internos (FLAI).

Lopez, S. y. (2010). *La consultoría de gestión humana en empresas medianas.* Research Gate.

OSTEC. (Diciembre de 2016). *ISO 27002: Buenas prácticas para gestión de la seguridad de la información*. Obtenido de https://ostec.blog/es/aprendizaje-descubrimiento/iso-27002-buenas-practicas-gsi/

SIGWEB. (s.f.). *El portal de los exportes en prevencion de riesgos de Chile*. Obtenido de https://www.sigweb.cl/wp-content/uploads/biblioteca/MatrizdeRiesgo.pdf

SINGWEB, E. (s.f.). *EL PORTAL DE LOS EXPERTOS EN PREVENSION DE RIESGOS DE CHILE*. Obtenido de EL PORTAL DE LOS EXPERTOS EN PREVENSION DE RIESGOS DE CHILE: https://www.sigweb.cl/wp-content/uploads/biblioteca/MatrizdeRiesgo.pdf

Solutions, G. S. (27 de Septiembre de 2023). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. Obtenido de https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

The Institute of Internal Auditors . (2017). GLOSARIO. En T. I. Auditors.

# ANEXOS

*ANEXO 1: Entrevista de evaluación de Riesgos.*

**UNIVERSIDAD DE EL SALVADOR**

**FACULTAD DE CIENCIAS ECONÓMICAS**

**ESCUELA DE CONTADURÍA PÚBLICA**

"IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS AL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN, PARA UNA ENTIDAD DEDICADA A LA PRESTACIÓN DE SERVICIOS DE GESTIÓN EMPRESARIAL"

Dirigida a: el encargado del área de Tecnología de Información, de la empresa que se dedica a la prestación de servicios de gestión empresarial.

Objetivo: Obtener información por medio de entrevista realizada al área de Tecnología de Información sobre los riesgos a los cuales se encuentran expuestos en el departamento generando un diagnóstico eficaz sobre los riesgos asociados.

Propósito: Conocer el proceso de identificación y evaluación de riesgos en el área de tecnología de Información de una entidad que se dedica a la prestación de servicios de gestión empresarial y como mitigarlos.

1. **Dentro del área de Tecnología de la Información ¿qué riesgos son los más frecuentes a los que la entidad se encuentra expuesta?**

La entidad se encuentra expuesta en gran medida al robo de información debido a la cantidad de datos confidenciales, que posee de los distintos cliente y esto se debe en +

2. **¿Han tenido lugar auditorías de seguridad en la infraestructura tecnológica, y de ser así, qué vulnerabilidades ha sido identificadas para determinar si la**

**entidad cuenta con una infraestructura adecuada para el resguardo de los equipos tecnológicos?**

Una auditoria completa no se ha realizado desde que ingrese a laborar a la empresa por lo cual no ha habido un parámetro en el cual nos haya servido para determinar si se encuentra con la estructura adecuada, pero si se puede observar deficiencias con respecto a la infraestructura como por ejemplo los aires acondicionados donde se encuentra el servidor fallan muy seguido lo que ocasiona que el servidor se sobrecaliente, así mismo no se tienen controles para el ingreso al área de TI, por lo cual cualquiera pudiera tener acceso a los activos de la entidad.

3. **¿Qué medidas y procedimientos se han implementado hasta la fecha para reducir estos riesgos y vulnerabilidades, en cuanto a la seguridad dentro del área de Tecnología de la Información?**

Se ha planteado la forma de elaborar un sistema de ticket donde se pueda ir registrando de todas las solicitudes realizadas por el demás departamento y el seguimiento de ellas, y así llevar un control y poder identificar aquellos incidentes que son más frecuentes para poder mitigarlos de la manera correcta elaborando un registro de incidentes, por el momento esto solo se tiene en la fase de idea, todavía no se encuentra desarrollado.

Con respecto al aire acondicionado todavía no se toma alguna medida para que pueda solventarse, así como también la entrega de equipo nuevo se da, solamente cuando el equipo en definitiva ya no puede ser usado.

4. **¿Cuáles activos de información y sistemas críticos son utilizados primordialmente en las operaciones de gestión empresarial de la entidad?**

   Los servicios claves de la empresa están relacionados con los servidores para el procesamiento de todas las actividades relacionadas al negocio y la información almacenadas en las mismas, como software tenemos como principal activo a SAP S/4 HANA, el cual gestiona la información clave de empresa.

5. **¿Cuáles son los activos de información con mayor probabilidad de sufrir ciberataques, según su evaluación de la entidad?**

   Los equipos de trabajadores son el mayor riesgo tiene al sufrir un ataque y estos ocasionar un mayor desastre ya que estos equipos son parte de la red interna al ser infectados por un WannaCry y estos afectar a los servidores críticos, aunque existe una DMZ como una buena práctica en la separación de la red.

6. **¿Cómo se administra el acceso y los permisos a los activos que proveen información y datos sensibles en las operaciones de la entidad dentro del área?**

   Los accesos a sistema SAP son absolutamente acceso limitados a pocos usuarios estos deben estar debidamente capacitados al uso del sistema, y debidamente autorizados por la gerencia general la cual nos brindara un correo con la autorización de acceso con ese mismo correo se notifica el grado de acceso que se le debe otorgar o si está relacionado a su puesto de trabajo.

7. **¿Se cuenta con una política adecuada para la gestión de contraseñas, y se verifica su cumplimiento en todos los niveles de la organización, y así descartar posibilidades de abuso en términos de privilegios?**

   Si se cuenta con una política, aunque esta no este establecida como tal, ya que solamente se cuenta con un proceso de seguridad estándar el cual indica que las contraseñas tienen que contener mínimo 8 dígitos, para el caso del personal fuera del área, todo aquel que tiene acceso a los sistemas, se establecen según normativas del sistema SAP.

8. **¿Cuál es la política establecida para los respaldos y la recuperación de datos en caso de incidentes o desastres, y qué tan efectiva es su implementación?**

   Existe un DRP el cual está planteado y al mismo tiempo implementado mas no probado ya que tiene más de 3 años de no ser testeado eso representa un posible fallo en la recuperación de al momento de fallas es el punto más débil actualmente

9. **¿Existe un plan definido y probado para responder a incidentes cibernéticos, que permita hacer frente a posibles ataques o brechas de seguridad?**

   Actualmente no existe ningún plan para realizar una contramedida a un ataque esto debido a que no ha existido un antecedente grave que marque la necesidad de hacer uno, es considerable que es un punto débil de la gestión actual de informática

10. **¿Qué factores externos representan potenciales amenazas que podrían impactar la disponibilidad, integridad y confidencialidad de la información y sistemas tecnológicos de la entidad?**

Los factores externos que podrían impactar negativamente serian:

Los ciberataques tanto como *phishing* e ingeniería social ya que estos pueden robar información confidencial como contraseñas, datos bancarios o incluso interrumpir operaciones.

11. **¿Cómo se evalúa y selecciona a los proveedores de servicios y soluciones tecnológicas para asegurar que cumplen con los estándares de seguridad requeridos?**

    Actualmente no hay un procedimiento para esto se contrata el proveedor que brinde la mejor oferta, no se considera nada más que eso para realizar la contratación.

12. **¿Cuáles riesgos específicos podrían surgir debido a la relación con proveedores externos o al uso de servicios en la nube?**

    Problemas de comunicación
    No tiene equipo técnico necesario
    Tiempo de respuesta muy lentos
    Mala reputación.
    Falta de soporte por parte del proveedor.

13. **¿Con qué periodicidad efectúan evaluaciones internas referentes a programas y equipos que utiliza el personal en el área y que puedan contribuir al conocimiento de amenazas?**

Actualmente no se realiza ninguna evaluación, ya que se asume que ningún personal de otra área participe dentro del área de TI, pero si se observa poca evaluación de los equipos y muchas veces son desfasados y no se eliminan usuarios anteriores, que tal vez ya no laboran en la entidad.

14. **¿Conociendo las amenazas internas o externas que pueden existir en el área de tecnología de la información, que beneficios favorables considera que traería a la entidad la implementación de un sistema de gestión de riesgo?**

Si, tuviera muchos beneficios ya que esto nos ayudaría a identificar y evaluar los riesgos tanto internos como externos para así no afectar la seguridad de la información, y esto contribuiría a que se puedan mitigar aplicando distintas medidas, también ayuda contribuir a identificar las áreas críticas de la infraestructura para así elaborar algún plan de contingencia para que la continuidad del negocio no se vea afectada.

15. **¿Gestionando los riesgos en el área de Tecnología de la Información de qué manera impacta positivamente en las operaciones del negocio?**

Esto impactaría significativamente, ya que esto llegaría a realizar una mejora continua en el área de tecnología, y esto llevaría a favorecer a las demás áreas ya que todo depende de la tecnología para poder desarrollarse de la mejor manera.

***ANEXO 2. Narrativa de Procesos.***

**Cliente:** Entidad Objeto de Estudio, S.A. de C.V.

**Proyecto:** Consultoría sobre identificación de riesgos

**Periodo:** Marzo a Julio 2023

## Área de tecnología de información

### Proceso de adquisición de activo tecnológico

La entidad objeto de estudio, S.A. de C.V. fue creada en el año de 2015 siendo una pequeña empresa que estableció como uno de sus objetivos proporcionar servicios de gestión empresarial dando énfasis a los métodos analíticos y herramientas informáticas.

Por lo que en busca de llevar a cumplimiento sus objetivos en enero del 2023 evalúa contratar servicios de consultoría para identificar los riesgos asociados al área de TI, por lo cual es necesario conocer los procesos que el área de TI emplea para la adquisición de activo tecnológico, adquisición de servicios y control de accesos al sistema.

El proceso para la adquisición de activo tecnológico da inicio cuando el jefe o encargado del área de TI determina que equipo necesita ya sea porque este ha sufrido algún tipo de daño, así como para poder desempeñar las funciones de la manera más eficiente y eficaz posible, por lo cual debe elaborar una hoja de requerimientos donde se especifique las características necesarias que el activo debe cumplir para poder satisfacer las necesidades de dicha área, debido a ello este proceso representa un riesgo importante debido a que si este se omite o no se desarrolla de manera correcta podría generar un error a la hora de realizar la compra y no podrá ser usado de manera óptima, posteriormente la solicitud será trasladada al gerente el cual rechazara o aprobara, si esta es rechazada será devuelta al

jefe o encargado del área de TI para su revisión, si esta procede el encargado traslada la solicitud previamente autorizada hacia el departamento de compras.

El área de compras deberá brindar por lo menos tres cotizaciones del activo, esto para poder optar por el precio más bajo, dicha cotización será trasladad a gerencia la cual se encarga de validar el presupuesto asignado al área solicitante, si el gerente considera que el precio es muy elevado este será rechazado y será enviado nuevamente a compras la cual se encargara de generar nuevas cotizaciones con distintos proveedores, si esta se aprueba se brindara la autorización a compras para que realice la compra, cuando la compra se haya realizado y se tenga el activo físicamente, será enviado a la bodega de activo donde podrá ser solicitado por el área que ingreso la solicitud.

**Procesos de adquisición de servicios**

El proceso inicial se genera cuando el área de TI se ve en la necesidad de contratar servicios ya sea de mantenimiento, soporte, entre otros.

Este inicia cuando el encargado o jefe del área de TI envía la solicitud de contratación de servicios por medio de correo electrónico al gerente, este verificara si la entidad cuenta con la liquidez suficiente para poder adquirir dichos servicios, para esto es indispensable tener una programación de algunos mantenimientos fijos del equipo, debido a que si la entidad no cuenta con la liquidez suficiente estos no se podrán desarrollar lo que pudiera ocasionar alguna falla en el equipo informático, o que los servicios no se puedan prestar de manera regular, si la solicitud es aprobada se verifica con que proveedores se ha trabajado anteriormente y se valida si el proveedor ha desempeñado de manera óptima sus servicios, si es así se vuelve a contratar dicho servicio, si la respuesta fue negativa se

traslada al área de compras la cual se encargar de cotizar con distintos proveedores los servicios solicitados, cuando se tienen las cotizaciones nuevamente se traslada al gerente que podrá aprobar o rechazar dicha cotización, si esta es rechazada el área de compras deberá generar nuevas cotizaciones; si esta es aprobada compras se encargara de establecer el contrato con dicho proveedor.

**Proceso de control sobre acceso del sistema.**

El proceso da inicio desde la contratación del nuevo personal en donde recursos humanos se encarga de brindar las funciones que este desempeñara, y posterior a ello el área de TI recibe el detalle de las funciones y los datos del nuevo empleado, la cual tendrá que asignarle los distintos permisos del sistema de acuerdo a las funciones enviadas por recursos humanos, se puede observar un riesgo a la hora de brindar los permisos a los nuevos empleados, ya que si no se lleva un control y se les deja un libre acceso, esto puede ocasionar que se pueda eliminar datos sensibles de la entidad y esto debido a la falta de capacitación del personal antes de brindarle sus usuarios de acceso, así como también al tener un libre acceso puede verse mayormente expuesto a sufrir ciberataques por medio de *phishing*, o por algún otro software malicioso debido a ello es importante contar con algún software de protección de estos software maliciosos, por último el encargado del área de TI debe compartir la contraseña y usuario al nuevo empleado.