UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

TRABAJO DE GRADO EN MODALIDAD DE INVESTIGACIÓN: "GESTIÓN DE RIESGOS FINANCIEROS EN LA ERA DIGITAL APLICADA A UNA ORGANIZACION NO GUBERNAMENTAL UBICADA EN EL DEPARTAMENTO DE SAN SALVADOR"

TRABAJO DE INVESTIGACION PRESENTADO POR:

ROSALES MARTÍNEZ, ELIS JOHANNA ALEYDA

SANABRIA LÓPEZ, MOISÉS ORLANDO

PARA OPTAR AL GRADO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA

19 DE FEBRERO DE 2025

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AUTORIDADES UNIVERSITARIAS

RECTOR:	ING. JUAN ROSA QUINTANILLA QUINTANILLA
VICERRECTORA ACADÉMICA:	DRA. EVELYN BEATRIZ FARFÁN MATA
SECRETARIO GENERAL:	LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

AUTORIDADES DE LA FACULTAD DE CIENCIAS ECONÓMICAS

DECANA:	LICDA. CELINA AMAYA DE CALDERÓN
SECRETARIO:	LIC. JUAN PABLO MARÍN
COORDINADOR GENERAL DE PROCESOS DE GRADO:	MAF. RONALD EDGARDO GÁLVEZ RIVERA
DIRECTOR DE LA ESCUELA DE CONTADURÍA PÚBLICA:	MSC. MAURICIO ERNESTO MAGAÑA MENÉNDEZ
COORDINADOR DE PROCESOS DE GRADO DE LA ESCUELA DE CONTADURÍA PÚBLICA:	LIC. ABRAHAM DE JESÚS ORTEGA CHACÓN
DOCENTE ASESOR:	MSC. MAURICIO ERNESTO MAGAÑA MENÉNDEZ
TRIBUNAL EVALUADOR:	LIC. BENITO MIRANDA BELTRÁN
	LIC. WILMER EDMUNDO PÉREZ DÍAZ
	MSC. MAURICIO ERNESTO MAGAÑA MENÉNDEZ

DEDICATORIAS

Agradezco a Dios por darme sabiduría y poder concluir mis estudios, también agradezco a mi madre Edith Xenia López de Sanabria quién me ha apoyado durante todo este proceso y a lo largo de mi vida. A mi padre Moisés Arnulfo Sanabria Anaya espero me pueda ver desde el cielo, a mis amigos que me han apoyado en cada una de las etapas de mi vida y me han alentado a seguir siempre adelante. Gracias a cada uno de los docentes de la Universidad de El Salvador que han aportado en toda mi carrera profesional.

Moisés Orlando Sanabria López

A Elena Recinos, por su apoyo incondicional, a Nessycka Sosa por animarme a terminar este proceso y a todos los docentes de la Facultad de Ciencias Económicas que han aportado a mi formación profesional.

Elis Johanna Aleyda Rosales Martínez

ÍNDICE

Índice de tablas

Índice de figuras

RESUMEN EJECUTIVO

El presente estudio responde a la creciente preocupación de las organizaciones no gubernamentales (ONG) en San Salvador ante su vulnerabilidad financiera y operativa frente a amenazas digitales. En un entorno de constante avance tecnológico, la adopción de nuevas herramientas digitales ha generado importantes desafíos, especialmente en la integración de software y la implementación de sistemas adecuados para la gestión de riesgos financieros. Esto impacta negativamente en la capacidad de las ONG para tomar decisiones oportunas y alcanzar sus objetivos institucionales.

El objetivo principal de la investigación fue diseñar una herramienta técnica para la gestión de riesgos financieros en la era digital, orientada a fortalecer la toma de decisiones y el cumplimiento de metas organizacionales. Esta herramienta establece un marco para identificar, evaluar y mitigar riesgos financieros, con el propósito de minimizar pérdidas económicas y garantizar la continuidad operativa de las ONG.

La metodología empleada fue el enfoque hipotético-inductivo, adecuado cuando no es posible comprobar directamente una hipótesis, basándose en la observación y análisis de casos concretos. Se realizaron entrevistas a responsables clave dentro de diversas ONG, con el fin de conocer sus desafíos en materia de gestión de riesgos y explorar posibles soluciones. Estas entrevistas permitieron entender mejor las necesidades específicas de cada unidad organizativa.

Los resultados revelaron que, pese a la adopción de nuevas tecnologías, las ONG enfrentan problemas significativos debido a la incompatibilidad de los sistemas de software financiero, especialmente en el uso del ERP. Las entrevistas a cuatro unidades organizacionales evidenciaron la ausencia de un sistema efectivo de gestión de riesgos,

lo cual limita la toma de decisiones basada en información confiable. Asimismo, se identificó la necesidad de implementar controles internos robustos como una oportunidad clave para reducir la exposición al riesgo financiero y mejorar la gestión integral.

En conclusión, la investigación confirma la urgencia de implementar una herramienta técnica que permita a las ONG identificar y evaluar los riesgos inherentes a sus operaciones. Se propone el uso de una matriz de riesgos financieros, acompañada por un sólido marco de controles internos, como estrategia fundamental para proteger la estabilidad financiera y operativa de estas organizaciones frente a eventos adversos.

Se recomienda que las ONG realicen revisiones continuas y mejoras en sus sistemas de gestión de riesgos y control interno, asegurando su eficacia y adaptabilidad a un entorno cambiante. También se destaca la importancia de capacitar al personal responsable en prácticas óptimas para la identificación, evaluación y mitigación de riesgos financieros.

Finalmente, se resalta la necesidad de integrar eficientemente las tecnologías disponibles, mediante la adaptación de software que facilite una gestión ágil y precisa de los riesgos. El uso adecuado de herramientas tecnológicas fortalecerá la toma de decisiones y garantizará la sostenibilidad de las operaciones de las ONG en San Salvador.

INTRODUCCIÓN

Las Organizaciones No Gubernamentales (ONG) tienen como objetivo ayudar y beneficiar a los menos privilegiados de un país, ciudad o comunidad, brindando apoyo en áreas como salud, familiar, académica, recursos naturales (agua potable) y muchas otras que probablemente han sido descuidadas por los gobiernos. Estas organizaciones, en su mayoría, ejecutan planes sin el ánimo de ser lucrativas, por lo cual, resulta necesario buscar fuentes de ingresos que puedan sostener cada proyecto, asimismo, es importante que la administración de los recursos sea de una manera eficiente y eficaz.

En ese contexto, la investigación que presenta este documento está basada en los resultados obtenidos de la organización no gubernamental denominada "La Fundación la Aurora", en la cual se desarrolla un conjunto de análisis sobre la gestión de los riesgos financieros en la era digital. En resumen, los capítulos se dividen de la siguiente manera:

En el capítulo uno, se desarrolla el planteamiento del problema, con el cual se identifica el origen de la problemática, para conocer de una manera detallada a la organización en estudio. Además, se establecen los objetivos que dirigen la investigación, tanto de forma general como específica.

Así mismo, se definen algunos conceptos básicos y relevantes para tener una mejor compresión de tema, y por último, pero no menos importante, se da a conocer la base técnica que es aplicable en el país.

En el capítulo dos, se detalla el proceso metodológico usado en la investigación, en el cual se adopta un enfoque cualitativo para el desarrollo del estudio. De esa manera se define así, las unidades de análisis, el universo, muestra, hipótesis, y variables para finalizar con las técnicas utilizadas para la obtención de resultados.

Y, en el capítulo tres, como producto del proceso de investigación se presenta una herramienta denominada Guía para la Gestión de Riesgos en Organizaciones no Gubernamentales de El Salvador, una propuesta de elaboración propia pero que toma como base la información proporcionada por la entidad en análisis.

Las conclusiones obtenidas de este análisis revelan que, a pesar de contar con un personal competente y una estructura organizativa sólida, la fundación carece de herramientas técnicas adecuadas para gestionar los riesgos financieros, especialmente en el ámbito digital. Además, se detectó un alto riesgo en el área de informática, ya que la gestión de la información financiera depende de un proveedor externo. Estos hallazgos subrayan la necesidad urgente de implementar estrategias de gestión de riesgos en las ONG para prevenir fraudes y asegurar una adecuada operación en el mediano y largo plazo.

En base a estas conclusiones, las recomendaciones propuestas incluyen fomentar una cultura organizacional de gestión de riesgos, la implementación de guías específicas para la evaluación y monitoreo de riesgos financieros, y la contratación de personal especializado tanto en el área informática como en auditoría interna. También se hace énfasis la

importancia de la capacitación continua del personal para asegurar que las decisiones se tomen con un conocimiento adecuado de los riesgos.

Los anexos presentados incluyen guías de entrevistas dirigidas a los diferentes actores clave dentro de la organización, lo que permitió obtener información detallada y precisa para evaluar los riesgos financieros y proponer soluciones adecuadas. Estas entrevistas fueron fundamentales para comprender las dinámicas internas y los desafíos enfrentados en la gestión de riesgos, particularmente en el contexto digital.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA Y MARCO TEÓRICO

1.1 Antecedentes del problema

Las Organizaciones No Gubernamentales (ONG) se desempeñan en varias áreas, incluyendo el intercambio científico, la religión, la ayuda de emergencia y los asuntos humanitarios. Estas organizaciones son efectivas y han tenido, a lo largo del tiempo, un amplio apoyo económico. La ONG opera de manera independiente, sin una injerencia directa de los gobiernos. Esto le otorga una mayor flexibilidad para llevar a cabo sus proyectos y programas. También son aceptadas como parte de las relaciones internacionales, en España y Latinoamérica se han desarrollado de la mejor manera, y esto permite que en América Latina se sigan desarrollando iniciativas de cooperación que permiten el desarrollo, la sanidad, la educación y el bienestar social.

Bajo este enfoque de desarrollo y bienestar nace en 1992 *La Fundación la Aurora* como una organización no gubernamental, con el propósito de mejorar las condiciones de vida de los habitantes más desfavorecidos de las comunidades de Soyapango y zonas aledañas a través de una educación de calidad y del cuidado de la salud mediante la construcción y la gestión de un complejo de 19 hectáreas donde se encuentran ubicados, quien beca y forma a más de 1,500 alumnos provenientes de entornos vulnerables bajo los pilares de la excelencia académica y humana y la clínica asistencial que atiende a 60.000 pacientes al año, donde se trabajan más de 29 especialidades médicas y ontológicas, con precios notablemente inferiores a los del sistema de salud privado en El Salvador.

En 1990, nace la gestión de riesgo a partir del desarrollo de las primeras normas internacionales en los países de Australia y Nueva Zelanda que emitieron la norma de Administración de Riesgos (AS/NZS 4360, 1999) y que, junto con el país de Canadá (CAN/CSA Q850-97) se volvieron únicas para su tiempo. En 2010 la ISO (Organización Internacional de Normalización) emitieron las primeras normas de gestión de riesgos: ISO 31000 e ISO 31010, la primera dedicada a las directrices y conceptos de riesgos, y la segunda a las técnicas de evaluación y medición de riesgos.

Para el año de 2018 la ISO 31000 fue actualizada, los principales cambios son en el entorno empresarial y tecnológico. Dentro de la ISO 31000:2018 se define principalmente la gestión de riesgo como la incertidumbre en los objetivos, creando amenazas y oportunidades sobre su logro. (ISO, 2018) En este contexto, la tecnología de la información emerge como un actor central, generando, procesando y almacenando vastas cantidades de datos que influyen significativamente en la gestión del riesgo.

La era digital ha generado grandes cambios en la economía y en la sociedad tecnológica ya que, incide directamente en el desarrollo de los mercados, creando oportunidades de lograr ventajas competitivas. La transformación digital está vinculada a los sistemas de información y comunicación, marketing e ingeniería de software, por lo que, si una organización no está preparada y no desarrolla la capacidad de transformarse, esta oportunidad se le convierte en amenaza; por ejemplo, el “Big Data” define un gran volumen de datos los cuales son complejos o difíciles de procesar mediante los métodos comunes. Lo cual, lo convierte en un desafío tecnológico para el desarrollo y uso de las herramientas digitales; sin embargo, es una oportunidad para mejorar y optimizar los recursos de las instituciones.

1.2 Caracterización del problema

La gestión de riesgos en las Organizaciones No Gubernamentales (ONG) es un proceso esencial que abarca la identificación, evaluación y mitigación de diversos tipos de riesgos, tales como financieros, operativos, de reputación y legales. La falta de una cultura sólida de gestión de riesgos puede acarrear consecuencias graves, incluyendo la pérdida de fondos, el daño a la reputación, el cierre de programas y, en última instancia, la incapacidad de cumplir con su misión.

En un entorno operativo que es complejo, donde las Organizaciones No Gubernamentales (ONG) dependen en gran medida de donaciones y deben ejecutar proyectos en condiciones desafiantes, muchas de estas organizaciones no cuentan con las herramientas y metodologías necesarias para gestionar sus riesgos de manera proactiva. La resistencia al cambio y la falta de conciencia sobre la importancia de la gestión de riesgos son obstáculos significativos que impiden la implementación de prácticas efectivas en este sector. La era digital ha transformado fundamentalmente el entorno operativo de las ONG, introduciendo riesgos financieros y cibernéticos que requieren una adaptación constante de sus estrategias de gestión de riesgos. La volatilidad del suministro en línea, los ciberataques y la dependencia de las tecnologías digitales son sólo algunos de los desafíos que enfrentan estas organizaciones.

1.3 Formulación del problema

¿En qué grado la ausencia de procedimientos y políticas especializadas en materia de gestión de riesgo financieros en la era digital para Organizaciones No Gubernamentales (ONG) afecta la toma de decisiones y la consecución de los objetivos?

1.4 Objetivos

1.4.1 General

Proponer una herramienta técnica que oriente sobre la gestión de riesgo financieros en la era digital para el fortalecimiento de la toma de decisiones y el alcance de los objetivos institucionales en Organizaciones No Gubernamentales (ONG).

1.4.2 Específicos

- Identificar los principales riesgos financieros que las organizaciones sin fines de lucro enfrentan en la era digital.
- Proporcionar estrategias técnicas que permitan gestionar los riesgos financieros en las organizaciones.
- Adquirir los conocimientos necesarios en la normativa técnica y legal que sea aplicable directamente a la gestión de riesgos financieros y la transformación digital.
- Indicar a través de una guía la aplicación de herramientas técnicas que ayuden a gestionar los riesgos financieros en organizaciones sin fines de lucro y en un entorno tecnológico.

1.5 Marco teórico

1.5.1 Antecedentes de las Organizaciones No Gubernamentales

Las Organizaciones No Gubernamentales (ONG) iniciaron sus actividades en El Salvador a principios de la década de 1960 surgieron de la Iglesia Católica las organizaciones de asistencia para la población bajo el nombre de CÁRITAS, estas instituciones católicas se dedicaban a la recolección y distribución de alimentos, ropa y medicinas a las poblaciones más vulnerables. En los años 80 este tipo de instituciones que trabajan en el campo de la ayuda alimentaria se veían fortalecidas con fondos de Naciones Unidas, Europa y América del Norte. Según el informe de la Comisión Kissinger, Estados Unidos aporta un promedio de 100 millones de dólares anuales a la región en ayuda alimentaria a través del programa PL-480. Esta ayuda, según el citado informe, tiene como objetivo paliar la situación de desnutrición en la región.

La Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) y el Catholic Relief Service (CRS) están trabajando con CARITAS locales para canalizar estos recursos. Sin embargo, las causas y soluciones de la crisis socioeconómica de Centroamérica son objeto de debate entre los distintos actores. (Informe de la Comisión Nacional Bipartita Sobre Centroamérica., 1984.)

La ONG que esta investigación tiene como objeto de estudio y a la cual se hace referencia como *Fundación La Aurora*, a fin de respetar la confidencialidad de la información otorgada, fue constituida por un sacerdote jesuita español en 1992 en el distrito de Soyapango, considerada la cuarta ciudad más peligrosa del mundo, según el Igarape Institute, ha trabajado para brindar oportunidades a la infancia y juventud salvadoreña con un proyecto educativo y sanitario de calidad, que la ha convertido en una institución comprometida con la transformación de la educación y la salud en el país.

1.5.2 Antecedentes del riesgo financiero

El riesgo financiero se refiere a la probabilidad de que una entidad (organización, individuo o institución financiera) no pueda cumplir con sus obligaciones financieras, lo que puede resultar en pérdidas económicas. Este concepto ha evolucionado a lo largo de la historia en respuesta a los cambios en los mercados, la economía y la regulación financiera. A continuación, se presentan los principales antecedentes y la evolución del riesgo financiero:

El origen del riesgo financiero, data desde la antigüedad; las primeras manifestaciones de riesgo financiero se observaron en actividades comerciales y mercantiles. Los comerciantes enfrentaban riesgos de pérdida de mercancías debido a naufragios, robos o problemas climáticos. Para mitigar estos riesgos, operaron los primeros mecanismos de seguros marítimos, en los que los comerciantes pagaban una prima a cambio de protección ante pérdidas. La práctica de prestar dinero con intereses (usura) también implicaba riesgo financiero, especialmente en caso de impago por parte del deudor.

Durante el Siglos XV al XVIII, con la expansión del comercio mundial, aparecieron las primeras compañías de comercio, como la Compañía Holandesa de las Indias Orientales, que necesitaban financiación para sus expediciones. Los accionistas asumían el riesgo financiero de perder su inversión si la expedición fallaba. Durante esta época, surgieron los primeros mercados financieros y bolsas de valores , lo que permitió la cotización de acciones y la diversificación del riesgo.

Ya en el Siglo XIX con la aparición de la banca moderna y la expansión de los préstamos bancarios se dio lugar a un nuevo tipo de riesgo financiero: el riesgo de crédito. Los bancos

comenzaron a ofrecer préstamos a empresas y particulares, enfrentando el riesgo de que estos no devolvieran el dinero. Para mitigar este riesgo, los bancos desarrollaron mecanismos de evaluación de solvencia y el concepto de "garantías" o "colaterales". También, durante esta época, se producen algunas de las primeras crisis financieras internacionales. , como la Crisis de los Tulipanes (1637) y la Crisis de los Ferrocarriles (1873). Estas crisis evidenciaron la necesidad de controlar el riesgo de mercado y el riesgo de liquidez en las operaciones bancarias.

La formalización del riesgo financiero llegó en el siglo XX. En la década de 1950, Harry Markowitz desarrolló la Teoría de la Cartera (Portfolio Theory) , introduciendo el concepto de diversificación del riesgo. Esta teoría planteó que los inversores pueden reducir el riesgo financiero combinando activos de diferentes características. La medición de la volatilidad y el concepto de beta (propuesto por William Sharpe) permitieron evaluar el riesgo sistemático de los activos financieros. Tras la Gran Depresión de 1929, surgieron las primeras regulaciones. En Estados Unidos, se crearon la Comisión de Bolsa y Valores (SEC) y nuevas leyes bancarias para controlar el riesgo de mercado y proteger a los inversores. Los bancos centrales comenzaron a asumir el rol de "prestamistas de última instancia" para evitar crisis de liquidez.

A partir de la década de 1980, la liberalización de los mercados financieros dio lugar a la creación de nuevos instrumentos, como los derivados financieros (opciones, futuros, swaps, etc.).

Estos productos permitieron a los inversionistas cubrir sus riesgos, pero también introdujeron nuevos riesgos complejos y difíciles de calcular. El riesgo de contraparte (la posibilidad de que la otra parte no cumpla con su obligación) se hizo más relevante.

La crisis asiática de 1997 y la crisis financiera de 2008 destacaron la importancia de controlar el riesgo de mercado, el riesgo de crédito y el riesgo de liquidez. La crisis de 2008 se produjo, en parte, por la acumulación de activos tóxicos (hipotecas subprime) en los balances de los bancos, lo que llevó a la quiebra de Lehman Brothers. Tras esta crisis, los reguladores internacionales (Basilea III) introdujeron requisitos de capitalización bancaria más estrictos para reducir el riesgo de insolvencia.

En la actualidad, con la digitalización de los servicios financieros, el riesgo cibernético ha ganado protagonismo, ya que los ataques informáticos pueden paralizar operaciones financieras. Los inversores ahora consideran los riesgos ESG (ambientales, sociales y de gobernanza) antes de tomar decisiones de inversión. Por ejemplo, las empresas con alto riesgo ambiental pueden enfrentar mayores costos de financiación.

En cuanto a la Gestión del Riesgo con Tecnología (Big Data e IA), los bancos y fondos de inversión ahora utilizan inteligencia artificial (IA) y big data para predecir y gestionar riesgos financieros. Estas tecnologías permiten identificar patrones de riesgo en tiempo real, facilitando la toma de decisiones rápidas y la prevención de crisis.

Así mismo, las criptomonedas introducen un nuevo tipo de riesgo financiero, ya que su volatilidad extrema y la falta de regulación las hacen altamente especulativas, por ello, los reguladores aún están trabajando para controlar el riesgo asociado con los criptoactivos.

1.5.3 Antecedentes de la transformación digital

La transformación digital con el avance de la tecnología, el mayor ataque cibernético de la historia fue en 2017 denominado “WannaCry” el cual se propagó a través de Microsoft Windows

y que afectó más de 200 mil computadores en cerca de 120 países en todo el mundo, dicho suceso fue llamado “ramsomware”, que es un secuestro de información, a través del cual, el ciberdelincuente encripta la información del computador, es decir que lo pone una clave desconocida para que el dueño de la información no la pueda utilizar y pide un dinero para entregar dicha clave. (Páez-Gabriuna, Sanabria, & Gauthier-Umaña, 2022)

En la era digital se ha incrementado la información que las entidades recopilan y almacenan en las diferentes bases de datos, esto hace que la protección de la información, la privacidad, y seguridad sea un aspecto importante en la gestión del riesgo financieros, ante la posibilidad de hackers que causan daño intencional a dispositivos o sistemas digitales por la vulnerabilidad de los sistemas informáticos, las redes y programas, que podrían perpetuar una serie de ciberataques entre los que sobresalen phishing, malware y ransomware.

1.6 Conceptos

Organizaciones No Gubernamentales

Las Organizaciones no Gubernamentales también son conocidas por sus siglas bajo el termino de ONG. Estas son entidades de iniciativa social que tienen fines humanitarios y que no dependen de la administración pública ni tienen fines lucrativos. (Cabezas, 2023)

Según la Real Academia Española (RAE), las ONG son, organizaciones de iniciativa social, independiente de la administración pública, que se dedican a actividades humanitarias, sin fines lucrativos.

Estas organizaciones sin fines de lucro están orientadas al desarrollo y satisfacción de necesidades físicas, económicas e intelectuales; realizando actividades económicas con enfoque social, para lo que requieren controles adecuados que les permitan agilizar los procesos y generar

información confiable para la toma decisiones. (Páez-Gabriuna, Sanabria, & Gauthier-Umaña, 2022)

Riesgo financiero

Según la Real Academia Española (RAE), el riesgo es una contingencia o proximidad de un daño. Todas las actividades que se realizan en cualquier ámbito de la vida cotidiana conllevan un riesgo inherente, algunas en más o menos medida, pero ninguna queda exenta de ello.

Desde el punto de vista de la normativa técnica se tienen las siguientes definiciones:

- La norma ISO 31000:2018 define al riesgo como la incertidumbre que surge durante la consecución de los objetivos. Es decir, son circunstancias o eventos adversos que obstruyen el desarrollo habitual de las actividades de una organización y generan incertidumbre existiendo el riesgo de tener repercusiones económicas en la entidad. (ISO, 2018).
- El Banco Interamericano de Desarrollo entiende el riesgo como la posibilidad de sufrir algún daño y este a su vez consiste en una pérdida de valor económico. (Ramos, y otros, 1999).

Transformación digital

Es un proceso que conduce a las organizaciones no gubernamentales a implementar iniciativas tecnológicas, pero también, a la realización de diversas acciones en lo cultural, político, económico, ecológico y normativo. Es, en resumidas cuentas, la configuración de un proceso de adaptación a las nuevas realidades. También responde a la necesidad de reconfigurar, reinventar y hacer avanzar los esquemas tradicionales de organizarse socialmente, con el interés de alcanzar nuevos estándares de bienestar, desarrollo y prosperidad para la humanidad. Este tipo de

transformación implica la reconfiguración de las organizaciones sin fines de lucro y las lleva a plantearse un modelo de negocio orientado al beneficio social, así como el establecimiento de nuevas formas de comunicarse y de interactuar en todas las esferas entre los diversos actores que dan forma a la sociedad. (Páez-Gabriuna, Sanabria, & Gauthier-Umaña, 2022)

Gestión de riesgo

Se considera esencial para la obtención de resultados efectivos dentro de las organizaciones. Se define como un conjunto de procesos secuenciales que contribuyen a la mejora continua y a la toma de decisiones gerenciales. (Soborit, González Capote, Mata Varela, Fornet Batista, & Cabrera Álvarez, 2020)

También, puede definirse, según Ramos (1999), como un proceso que puede añadir valor a la empresa y debe ser liderado por la alta dirección de la entidad por medio de la fijación de criterios de aceptación de los riesgos que se desean gestionar, de acuerdo con su ámbito de actividad y con los objetivos perseguidos. Así como también, el nivel de riesgo máximo aceptable y finalmente, el análisis y evaluación de los riesgos existentes en cada momento, y de manera desagregada por unidades de negocio. Todo lo anterior, ayudará a la toma de decisiones acerca de nuevas transacciones y cambios en el perfil de rentabilidad versus riesgo de la entidad, de acuerdo con las expectativas acerca del negocio.

La etapa final de este proceso es la evaluación de los resultados obtenidos, explicando su origen y la conexión con los riesgos asumidos. (Ramos, y otros, 1999, pág. 27)

Normas ISO

Constan de reglamentos y disposiciones que pueden utilizarse en todos los países para cumplir con los estándares mínimos de calidad, respuestas de entregas y niveles de servicio aceptables en cualquier tipo de empresas y organizaciones.

Se define como un listado de detalles técnicos u otro documento que está a disposición de todo público, dispuesto con el apoyo, acuerdo y aceptación general de las partes involucradas, fundamentado en los resultados combinados de la ciencia, tecnología y experiencia, que considera beneficios colectivos y es aprobada por un conjunto de profesionales competentes a nivel nacional, regional e internacional. (Unificas.com, 2024)

1.7 Generalidades Organizaciones No Gubernamentales (ONG)

Las Organizaciones No Gubernamentales (ONG) se financian a través de la recaudación de fondos, que puede provenir tanto de donantes públicos como de particulares. Estos son esenciales para llevar a cabo proyectos que buscan desarrollo y satisfacción de necesidades físicas, sociales e intelectuales, la cual es fundamental para su existencia. Por lo tanto, la actividad de obtener fondos implica la necesidad de desarrollar productos o servicio que genere ingresos.

Las ONG poseen características particulares por tener cierta autonomía y liderazgo, entre ellas están:

- Independencia del Estado, por lo que, están dirigidas por personas distintas al poder político.
- Sus operaciones tienen trascendencia social por lo que no tienen fines lucrativos.
- Aunque no poseen dependencia del Estado, están sujetas a las leyes como toda organización.

Según la organización *Ayuda en Acción*, las ONG se clasifican con base a su orientación y área de influencia. Según su orientación se pueden diferenciar cuatro tipos (Cabezas, 2023):

- De caridad: son las que enfocan sus actividades a apoyar a colectivos en vías de desarrollo, aportando herramientas para el auto sostenimiento.
- De servicios: centran sus actividades en proyectos de salud, educación, planificación familiar, entre otros servicios.
- Participativas: desarrollan proyectos de autoayuda en comunidades locales.
- De defensa y empoderamiento: son aquellas que sirven para impulsar un cambio en el sistema político, social y económico.

Según el área de influencia se tienen cuatro tipos de ONG:

- De carácter local: también conocidas como de base comunitaria, ya que surgen de la misma iniciativa de la comunidad.
- Ciudadanas: estas operan a nivel local, pero se distinguen por su enfoque en la promoción de derechos y la participación de los ciudadanos en la vida pública.
- Nacionales: tienen un alcance que abarca todo el territorio nacional. Se dedican a implementar proyectos y programas que responden a las necesidades de diversas comunidades a lo largo del país
- Internacionales: llevan a cabo proyectos en múltiples países, abordando problemáticas globales como la pobreza, la salud y la educación.

1.8 Gestión de riesgo

Se define como un proceso sistemático y analítico que tiene como objetivo evaluar, gestionar y comunicar los riesgos. Este proceso es crucial para mitigar y en la medida de lo posible

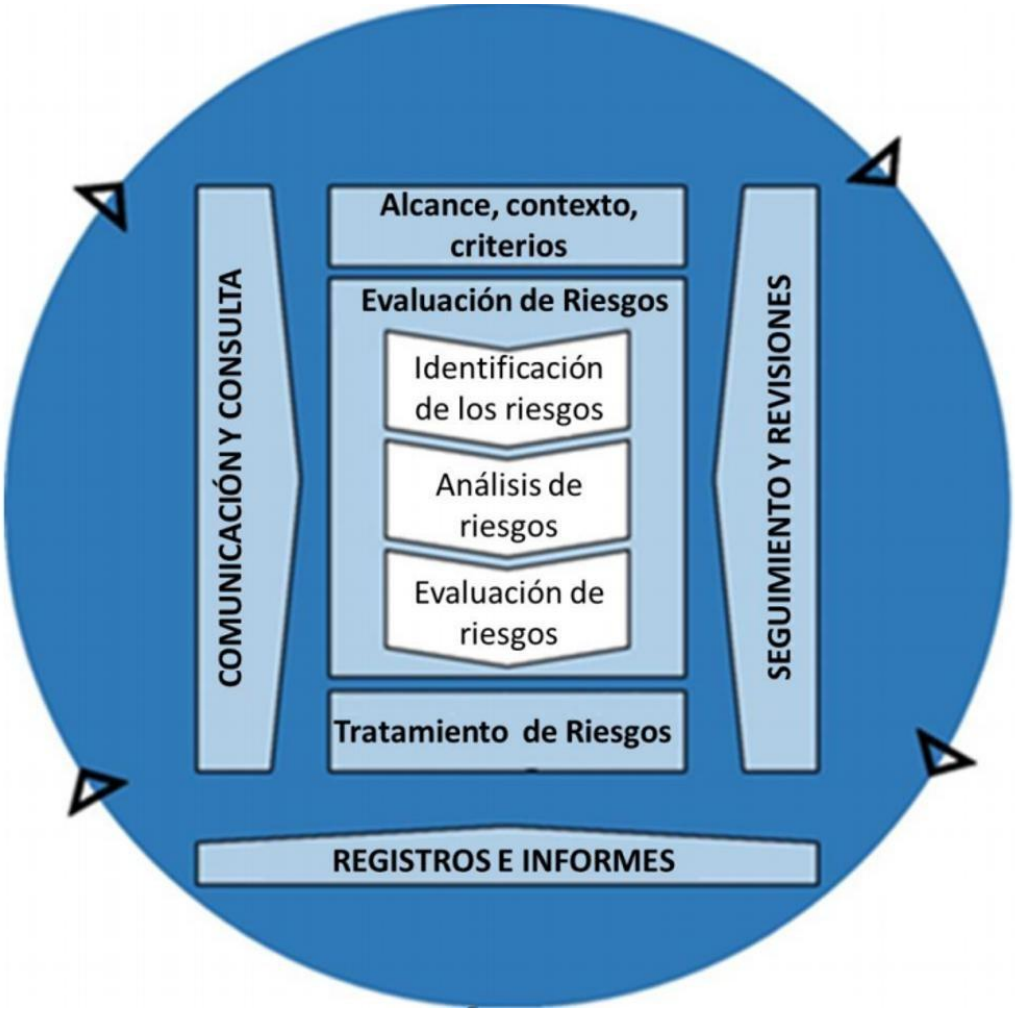
eliminarlos. A través de este enfoque, se busca no solo comprender la naturaleza, sino también establecer estrategias efectivas que permitan a las organizaciones enfrentar y reducir la probabilidad de eventos adversos (Insua & Naveiro Flores, 2022).

Tal como se muestra en la figura numero 1 se puede apreciar el esquema de la gestión de riesgo recomendada por la ISO 31000, la evaluación de riesgos se basa en obtener información sobre las amenazas que podrían afectar potencialmente una entidad y el impacto que tendrían si se materializarán. Dentro de esta fase se encuentran la elaboración de matrices de riesgos y los análisis de posibles escenarios asociados a las amenazas.

Por otra parte, la gestión de riesgos se constituye por las actividades realizadas para controlar las amenazas y reducir la posibilidad de materializar o minimizar el impacto. Y finalmente, la comunicación de riesgos se orienta al intercambio de información relacionada con los riesgos entre todas las partes interesadas.

Figura 1

El proceso de la administración gestión de riesgos



Nota: Diagrama del proceso de gestión de riesgos, que incluye la identificación, análisis y evaluación de riesgos, así como su tratamiento.

1.9 Proceso de gestión de riesgos

La norma ISO 31000:2018 se enfoca en identificar, evaluar, mitigar y comunicar riesgos, para minimizar su efecto negativo y maximizar los positivos. Por ello, la implementación de un Sistema de Gestión de Riesgos debe seguir una serie de etapas para que sea eficaz. A continuación, se explica en qué consiste cada una en el esquema siguiente:

Etapa 1: Establecer el contexto

Es una etapa previa que permite conocer a la organización por dentro, elaborando un diagnóstico preliminar con base en datos de otros procesos, para entender el contexto interno y externo en el que se desenvuelve. Posteriormente, se establece un método de evaluación, una estructura del análisis y se plantean alternativas, hasta que se selecciona la más conveniente al finalizar el proceso.

Etapa 2: Identificación de riesgos

En esta fase se identifican los eventos ocurridos y con posibilidad de acontecer, así como las áreas de impacto. Es importante responder a las preguntas "¿qué?, ¿por qué? y ¿cómo?" para identificar los factores de riesgo, sobre todo aquellos que pueden causar pérdidas.

Etapa 3: Análisis de riesgos

La tercera etapa se orienta a analizar la frecuencia de los eventos y la gravedad de posibles u ocurridas pérdidas, con base en la lista de los riesgos elaborada en la etapa 2, para gestionar el riesgo del que se trate. Según Soborit, González Capote, Mata Varela, Fornet Batista, & Cabrera Álvarez, 2020 se advierten sobre la importancia de no subestimar ningún riesgo, aunque parezca insignificante. Además, tener en cuenta que la frecuencia y gravedad no se manifiestan de la misma forma en todos los riesgos.

Según la ISO 31000:2018 el objetivo del análisis del riesgo es asimilar, y entender las condiciones del entorno con tendencia al riesgo y sus principales componentes e incluso identificar

los niveles adecuados del mismo. Esta investigación incluye una descripción específica de la incertidumbre, las consecuencias y orígenes, los resultados, probabilidades, atributos, tendencias, controles y efectividad. Un suceso puede tener causas y efectos que perjudican los objetivos planteados. (ISO, 2018)

Etapa 4: Evaluación de los riesgos

Está etapa está destinada a comparar los niveles estimados de riesgos, como resultado de la etapa anterior, con criterios ya preestablecidos según prioridades de gestión. Si el grado considerado de los riesgos es bajo, se catalogan como aceptables y, por tanto, no requieren gestión o tratamiento inmediato. Por el contrario, si los niveles estimados de riesgos no son bajos, será necesario realizar las actividades de la etapa 5.

Etapa 5: Tratamiento de los riesgos

En esta etapa se tratan los riesgos que no se catalogaron como aceptables en la etapa 4. Para ello, se identifican las opciones de tratamiento, se evalúan y se selecciona la más convenientes para el proceso. Posteriormente, se preparan los planes de tratamiento y se implementan.

El propósito de la gestión del riesgo es elegir, evaluar y poner en ejecución los planes alternativos para controlarlo, lo cual sugiere el siguiente proceso:

- Formular y seleccionar opciones para el tratamiento del riesgo
- Planificar e implementar el tratamiento del riesgo
- Evaluar la eficacia de ese tratamiento
- Determinar si el nivel de vulnerabilidad restante es tolerable.
- En caso de que el nivel de exposición persista, implementar medidas complementarias.

Las organizaciones cuentan con diferente conjunto de controles y medidas para gestionar los riesgos y generalmente adoptan una combinación de estrategias para minimizar los efectos negativos. Entre estas se encuentran:

1. Prevención. Identifique y aborde las amenazas antes de que se conviertan en un problema. Esto incluye establecer políticas, procedimientos y controles para prevenir o reducir la probabilidad de estas amenazas.
2. Transferencia. Transferir la responsabilidad de los riesgos a otra entidad, como una compañía de seguros, mediante la compra de pólizas. Esto también puede incluir la subcontratación de ciertas funciones a terceros que estén mejor capacitados para gestionar estas amenazas.
3. Mitigación. Implementar acciones que reduzcan el impacto o la probabilidad de un peligro. Por ejemplo, invertir en tecnología para mejorar la ciberseguridad o diversificar las carteras de inversión para reducir la exposición a problemas financieros.
4. Aceptación. Reconocer la existencia de amenazas y estar preparado para afrontar sus posibles consecuencias. Esta estrategia puede resultar útil cuando el costo de la mitigación del riesgo supera el posible impacto negativo.
5. Evitación. Elimine la exposición a amenazas evitando actividades o situaciones que puedan causar problemas. Aunque eficaz, esta estrategia puede limitar las oportunidades de crecimiento o desarrollo.
6. Gestión proactiva. Implementar un enfoque integral que combine monitoreo continuo, evaluación de amenazas y adaptación a condiciones cambiantes, analizando escenarios futuros.

La combinación de estas estrategias dependerá del tipo de amenazas que enfrenta una organización, su tolerancia, los recursos disponibles y sus objetivos de negocio. En la práctica, las entidades suelen realizar evaluaciones periódicas y adaptar sus enfoques de gestión en consecuencia.

La gestión de amenazas en una organización se basará en la naturaleza de los riesgos, la tolerancia, los recursos y los objetivos comerciales.

Según ISO 31000:2018, seleccionar estrategias adecuadas para abordar estas amenazas implica equilibrar los beneficios potenciales con los costos y los esfuerzos de implementación. Estas estrategias pueden incluir evitar, aceptar, eliminar, cambiar la probabilidad o las consecuencias de los riesgos, dividir o detener. La elección de estas tácticas debe ser coherente con los objetivos de la organización, los criterios de evaluación y los recursos disponibles. Los planes de tratamiento especifican cómo se implementarán estas estrategias seleccionadas y deben integrarse en los procesos de gestión de la organización. La información en los planes de tratamiento debe incluir la lógica de la selección de la estrategia, los responsables, las acciones propuestas, los recursos necesarios, medidas de desempeño, umbrales, requisitos de presentación de informes y plazos previstos para la ejecución y finalización de las acciones. (ISO, 2018)

Etapa 6: Monitoreo, revisión y comunicación de los riesgos

Finalmente, en esta etapa se materializa la toma de decisiones, con relación a la alternativa de gestión de riesgos que resultó más conveniente en la etapa anterior encaminada a reducir el mínimo costo o pérdida posible, se monitorea su comportamiento y se implementa un plan de gestión y revisión.

Los tres elementos de esta etapa intervienen en todo el ciclo de vida del proceso de gestión de riesgos, ya que, la comunicación con los interesados internos y externos es vital a fin de obtener los datos, unificar criterios y experiencias para identificar, estimar y evaluar los riesgos sin desconocer ninguna de las etapas del proceso.

1.10 Clasificación del riesgo

Como se explicó anteriormente los riesgos están presentes en cualquier actividad de las organizaciones, y ellos se pueden clasificar de la siguiente manera:

- **Estratégico.** Está relacionado con los objetivos estratégicos de la organización, su materialización se relaciona con el desconocimiento de las consecuencias de incumplir las expectativas de los clientes y usuarios.
- **Operacional:** Se vinculan con el propósito de los procesos que constituyen la actividad de la entidad. Es decir que están presentes en la ejecución de estos y, al materializarse, pueden provocar que la organización no opere adecuadamente.
- **Tecnológico.** Se refiere a los equipos de tecnologías de información y comunicación y/o sus operaciones. Incluyen sistemas operativos, aplicaciones, comunicaciones en las redes, entre otros. De igual manera ciberseguridad, privacidad y seguridad de la información.
- **Financiero.** Se orienta hacia las operaciones financieras, como pagos, deudas, ofertas, cobros y costos.
- **Legal.** Se encuentra ligado al cumplimiento de los requisitos legales y reglamentarios.
- **Reputacional.** Tiene que ver con la imagen de la entidad ante terceros.
- **Procesos.** Se relaciona con los resultados de un proceso y sus interacciones, afectando la eficacia y la eficiencia de la organización al materializarse.

- **Proyecto.** Está presente durante el ciclo de vida de un proyecto y pueden tener las mismas características de los riesgos operacionales.

1.11 Tipología de los riesgos financieros

- De crédito: La pérdida crediticia, que se refiere al capital no recuperado de los prestatarios. Está presente en todas las áreas de operación, es un costo inherente a las actividades de crédito. Aunque el nivel puede variar con el tiempo, se puede estimar estadísticamente mediante la Pérdida Anticipada (PA), que representa el costo promedio esperado, que se considera parte de los gastos operativos.

  Es importante destacar que la PA en sí misma no representa una amenaza, ya que el riesgo implica incertidumbre. Si las pérdidas reales siempre coincidieran con la PA, no habría incertidumbre. El riesgo real surge de las fluctuaciones en el nivel crediticio, conocidas como Pérdidas No Anticipadas (PNA). Estadísticamente, la PNA es la desviación estándar de las pérdidas crediticias. (España, 2014)

- De tasas de interés: Es el que se deriva de las fluctuaciones en los tipos de interés de los activos y pasivos que cualquier agente económico mantiene en cartera. Las posibles causas de estas variaciones son:

- Política monetaria de control de la cantidad de dinero en circulación.
- Déficit público, compitiendo con el sector privado por los recursos disponibles.
- Tasa de inflación, como explicación del tipo nominal.
- Tipos de interés exteriores.

Actualmente, tanto las entidades financieras como las empresas, los inversores institucionales y individuales se ven amenazados por una variedad de riesgos, entre los que destacan los de interés, mercado, liquidez y operación.

- **Interés**: constituye una preocupación para todas las entidades económicas, ya que está relacionado con las fluctuaciones en el costo del dinero. Estas variaciones pueden impactar negativamente en el valor de los activos y pasivos, lo que a su vez afecta la rentabilidad y solvencia de las empresas y entidades financieras. La magnitud de este riesgo varía en función de la sensibilidad de cada entidad a los cambios en las tasas de interés.
- **Mercado**: también conocido como riesgo sistemático, se refiere a la posibilidad de que el valor de un activo disminuya debido a factores generales del mercado, como cambios en los precios de los activos, tipos de interés o materias primas. Este tipo de riesgo afecta a todas las entidades que invierten en activos financieros y puede ocasionar pérdidas significativas.
- **Liquidez**: se centra en la capacidad de una entidad para convertir rápidamente sus activos en efectivo con el fin de cumplir con sus obligaciones. Surge cuando una entidad carece de la liquidez necesaria para hacer frente a sus pagos a corto plazo, lo que puede desencadenar problemas de solvencia y dificultades financieras.
- **Operacional**: abarca las posibles pérdidas que pueden surgir debido a fallas en los procesos internos de una organización, errores humanos, interrupciones en las operaciones o eventos externos como desastres naturales o fraudes. Este tipo de riesgo puede tener un impacto negativo en la reputación, rentabilidad y continuidad del negocio de las entidades. En conclusión, estos riesgos forman parte integral del entorno financiero actual y es

fundamental gestionarlos de manera efectiva para mitigar sus efectos negativos en las organizaciones y los inversores.

1.12 Transformación digital

El proceso de transformación digital varía según la fuente y el enfoque, pero una estructura común a menudo se basa en diferentes etapas o fases. Uno de los modelos comúnmente referenciados es el de George Westerman, Didier Bonnet y Andrew McAfee en su libro "*Leading Digital: Turning Technology Into Business Transformation*". (Michel Tamayo Saborit, 2020)

Este modelo describe el proceso de transformación digital en cuatro etapas:

3.11 Digitalización: implica adoptar tecnologías digitales para mejorar la eficiencia, esto incluye la automatización de procesos manuales y la creación de sistemas más eficientes, pero no necesariamente cambia fundamentalmente el negocio.

3.12 Transformación digital: va más allá de la digitalización y se centra en el cambio de modelos de negocio y procesos fundamentales; aquí, las empresas redefinen sus estrategias aprovechando las capacidades de la tecnología digital para generar valor de nuevas maneras.

3.13 Negocio digital: es el siguiente nivel en el que las empresas crean nuevos productos, servicios y experiencias que antes eran imposibles. Esto implica una integración más profunda de la tecnología en todas las áreas del negocio.

3.14 Corporación digital: es parte integral de la cultura de la empresa y se utiliza constantemente para innovar y mantener la relevancia en un entorno en constante cambio.

Las tecnologías de la información y las comunicaciones (TIC) están tomando relevancia en los diferentes sectores económicos. El mundo presenta grandes cambios, destacando los sociales, culturales, medioambientales, entre otros, esto ha influido en la vida del ser humano,

conduciéndolo a la transformación digital y al uso de nuevas tecnologías, abriendo brechas que permiten que el mundo esté conectado y en el que cada vez es más fácil comprar ropa, alimentos, productos de belleza y más, sin tener que salir del hogar.

El Salvador no es ajeno a esta nueva era, un ejemplo claro ha sido la implementación de un nuevo sistema para la declaración de impuestos (Ministerio de Hacienda) totalmente digitalizado, donde hoy día los formularios que se imprimían y eran presentados de forma física ya no son utilizados. En el 2021 el Gobierno de El Salvador, a través del Ministerio de Hacienda habilitó los servicios en línea, lo que permite que los procesos sean más rápidos y ayudan a minimizar los riesgos de evasión de impuestos.

La gestión de riesgos financieros tiene como fin identificar y evaluar los peligros a los que una organización se enfrenta y de esta manera implementar estrategias que permitan reducir el impacto. La transformación digital es clave en este proceso, ya que proporciona herramientas para enfrentar los riesgos de manera eficaz. Por ejemplo: con el análisis de datos, el volumen de información financiera a diario es vasto, y la tecnología de la Big Data, que ayuda a recopilar y analizar grandes volúmenes de datos, detectando e identificando riesgos financieros.

La automatización de procesos ayuda a agilizar y optimizar sus actividades, disminuyendo los errores humanos y aumentando la operatividad.

La transformación digital comprende una serie de pasos a considerar para obtener buenos resultados en su ejecución, algunos son:

- Conocer la situación actual: es muy importante conocer los procesos que una organización tiene, los recursos con los que cuenta y políticas internas, así será efectiva la transformación digital permitiendo identificar los problemas o desafíos a abordar.

- Establecer necesidades: ¿qué se quiere lograr con la transformación digital?, esa tendrá que ser una pregunta clave para definir lo que se espera alcanzar con la transformación digital; los objetivos deben ser SMART (por sus siglas en inglés: específico, medible, alcanzable, relevante y temporal).
- Responsabilidad de la dirección: para lograr alcanzar los objetivos establecidos en la transformación digital, es esencial que la dirección esté comprometida al cumplimiento de las metas trazadas, proporcionando lo recursos, políticas para la adaptabilidad al cambio y tomando decisiones estratégicas que beneficien a la buena implementación.
- Adoptar las herramientas necesarias: para ello es importante conocer las necesidades de la organización, así, las tecnologías a adoptar serán las adecuadas para la actividad que desarrolla, pudiendo utilizar software de gestión empresarial, automatización de procesos, inteligencia artificial, entre otros, que puedan servir para alcanzar los objetivos definidos.
- Formación y desarrollo: proporcionar herramientas útiles para la capacitación continua del personal que ejecutará los recursos tecnológicos adoptados por la organización, fomentando la mejora en los procesos digitales que ayudarán a gestionar los riesgos.
- Adaptabilidad: se debe estar conscientes que la transformación digital está en un cambio continuo, lo cual permite mejoras en los procesos, pero implica permanecer en constante evolución.

Claramente no todo es bueno en la era digital, como consecuencia que toda la información se encuentre digitalizada están los "ciberataques", cuentas de banco, información personal, datos empresariales, etc. Son vulnerables ante los ataques de “hackers” que fácilmente podrían dejar en bancarrota a una organización que no esté debidamente protegida.

1.13 Base técnica

Tabla 1

Normativa técnica relacionada con el funcionamiento y gestión de riesgos de las ONG

Norma	Descripción y uso
Norma de Contabilidad Financiera 21 – NCF para ONGS	Para minimizar los riesgos y cumplir aspectos legales en la norma, se tratan los elementos contables que requieren una consideración especial por el tipo de entidades a las que aplica. Las organizaciones sin fines de lucro y orientadas al desarrollo realizan actividades económicas y sociales, pero la contabilidad debe resumir la información que esos eventos generan, el tamaño de la organización debe contar con la tecnología para el proceso de la información como: computadoras, programas, software contable.
ISO 31000	Las organizaciones actualmente se encuentran en contantes cambios adaptándose a nuevas necesidades y forma de operación en sus procesos por eso el estándar es utilizado en todo tipo de riesgo como de instalaciones, operaciones, financiero entre otros, también es su conjunto de directrices y principios internacionales que proporcionan un enfoque sistemático y estructurado para la identificación, evaluación, tratamiento y monitoreo de riesgos en cualquier organización. Su objetivo principal es ayudar a proteger sus activos, cumplir con sus objetivos y mejorar la toma de decisiones. Tiene tres componentes principales: los principios de la administración de riesgo, marco de trabajo y proceso.
ISO 27000	Permite a las organizaciones la evaluación de riesgo y la aplicación en cualquier tipo, incluyendo pequeñas y medianas empresas, grandes corporaciones, instituciones gubernamentales y sin fines de lucro. Para proteger la confidencialidad, integridad y disponibilidad de la información, se logra cuáles son los potenciales problemas que podrían afectar en la evaluación del riesgo, y luego definir qué es necesario para prevenir y minimizar estos problemas.

Norma	Descripción y uso
Coso ERM y La Gestión de Riesgos	Considerando que las organizaciones se enfrentan a una gran cantidad de riesgos que afectan las diferentes partes, el COSO fue diseñado para reconocer los eventos que perjudican, evalúa y responde a los riesgos detectados de modo que estuvieran preparados para situaciones que limiten los objetivos.
NRP-36 Normas Técnicas Para La Gestión De Los Riesgos De Lavado De Dinero Y De Activos, Financiación Del Terrorismo Y La Financiación De La Proliferación De Armas De Destrucción Masiva	La implementación de metodologías efectivas para mitigar los riesgos de lavado de dinero exige un enfoque integral que abarque desde la evaluación del perfil de riesgo específico de la entidad hasta el análisis detallado de sus productos, servicios y relaciones con los clientes. (NRP-36, 2022)

1.14 Base legal

Tabla 2

Base legal aplicable al funcionamiento y gestión de riesgos de las ONG

Ley	Descripción y uso
Ley de Emisión de Activos Digitales	Dentro de la gestión de riesgo financieros se consideran esta ley con las transferencias de cualquier título de activos digitales que se utilicen dentro del territorio de El Salvador. Así como regular los requisitos y obligaciones de los emisores, proveedores, y demás participantes que operen en el proceso. Como características los activos digitales pueden ser poseídos, intercambiados, transferidos, negociados y promovidos por persona natural o jurídica. (1, Art. Ley de Emisión de Activos Digitales, 2022)
Ley de Delitos Informáticos	Para poder minimizar los riesgos financieros en la transformación digital con la presente ley que tiene por objeto proteger los bienes jurídicos, de aquellas conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de la información almacenada, transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad imagen de las personas naturales o jurídicas en los términos aplicables. (Art. 1 Ley de Delitos Informáticos, 2016)
Ley de Asociaciones y Fundaciones sin Fines de Lucro	El objetivo de regular las organizaciones sin fines de lucro es aplicar un régimen jurídico especial, que toda asociación y fundación tiene el derecho de establecer su régimen interno de conformidad de la ley. Dentro de estas normas jurídicas se regula el riesgo legal minimizándolo. (Art. 8 Ley de Asociaciones y Fundaciones sin Fines de Lucro, 1996)
Ley Contra el Lavado de Dinero y de Activos y su Reglamento.	En la presente ley contiene el conjunto normas jurídicas para prevenir, detectar, sancionar, y erradicar el delito de lavado de dinero y de activos, así como su encubrimiento. La ley será aplicable para persona natural o jurídica quienes deberán presentar la información de cualquier operación, transacción, acción u omisión a la autoridad competente. (Art.1 Ley Contra el Lavado de Dinero y de Activos y su Reglamento., 2000)

Ley	Descripción y uso
Instructivo para la Prevención, Detección y Control del Lavado de Dinero y Activos, Financiación del Terrorismo y la Financiación Proliferación de Armas de Destrucción Masiva.	Para el control del riesgo financiero en el instructivo se desarrollan las obligaciones de los sujetos obligados para la detección de operaciones inusuales y reporte de operaciones sospechosas que puedan estar vinculadas al lavado de dinero y de activos, la financiación del terrorismo y de la proliferación de armas de destrucción masiva, así como para el control y reporte de operaciones sospechosas a la Unidad de Investigación Financiera (UIF) (Art. 5 Instructivo para la Prevención, Detección y Control del Lavado de Dinero y Activos, Financiación del Terrorismo y la Financiación Proliferación de Armas de Destrucción Masiva, 2003)
Ley de Impuestos Sobre la Renta	Para establecer la exclusión de sujetos pasivos al pago del impuesto, como organizaciones de utilidad pública. (Art. 6 Ley Impuesto sobre la renta, 1963)
Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios	La ley regula el impuesto aplicable a la transferencia de bienes o servicios, por emisión y control de documentos fiscales, y la presentación de declaraciones mensuales sobre operaciones gravadas o exentas. (Art.93 Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, 1992)
Ley De Protección De Datos Personales Y Habeas Data	La presente ley se aplicará a cualquier tipo de dato personal, ya sea almacenado en bases de datos automatizadas o manuales, que se encuentre bajo el control de entidades públicas o privadas en El Salvador. Su ámbito de aplicación abarca todas las etapas del tratamiento de datos personales, desde su recolección hasta su uso final, por parte de cualquier actor público o privado. (Ley de proteccion de datos personales y habeas DATA, 2024)
Las Recomendaciones Del Gafi	La evaluación y gestión de riesgos de LA/FT son pilares fundamentales para la construcción de un régimen ALA/CFT robusto y eficaz. El EBR permite a los Estados optimizar la asignación de recursos, focalizando los esfuerzos en las áreas más vulnerables. Al adoptar un enfoque diferenciado, los países pueden adaptar sus medidas a la realidad de sus respectivos contextos, sin comprometer la efectividad de su régimen ALA/CFT. (LAS RECOMENDACIONES DEL GAFI, 2023)

CAPÍTULO II: METODOLOGÍA DE LA INVESTIGACIÓN

2.3 Enfoque de la investigación

El enfoque utilizado en el presente trabajo de grado es cualitativo orientado y aplicado a la metodología de investigación derivada al objeto de estudio. Dicho enfoque se centró en recoger información que se ha traducido en ideas y conceptos implementados al ámbito concreto investigado.

2.4 Tipo de estudio

El tipo de estudio desarrollado en la investigación fue con base al método hipotético inductivo ya que no se pueden comprobar directamente la hipótesis, por ello, se partió de la observación de hechos particulares para llegar a la generalización del caso en estudio.

2.5 Unidades de análisis

Para el desarrollo de la investigación se tomó como unidad de análisis a los colaboradores que estaban facultados para la toma de decisiones, entre ellos, el director general, el subdirector Financiero, la Contadora General y el Director de Tecnología e Información (DTI) de la organización “La Fundación la Aurora”.

2.6 Universo y muestra

La investigación se basó en las organización no gubernamentales, el estudio se delimito a una ONG, “La Fundación la Aurora” para respetar la confidencialidad de la institución que proporcionó la información. “La Fundación la Aurora” es una organización legalmente constituida en el departamento de San Salvador y posee programas de autosuficiencia orientados a la salud y educación.

2.7 Hipótesis y Variables

Hipótesis: la implementación de una guía para la gestión de riesgos financieros en la era digital fortalece la toma de decisiones y contribuye al alcance de los objetivos institucionales en las Organizaciones No Gubernamentales de San Salvador

Variable independiente: la implementación de una guía para la gestión de riesgos financieros en la era digital.

Variable dependiente: fortalece la toma de decisiones y contribuye al alcance de los objetivos institucionales en las Organizaciones No Gubernamentales de San Salvador

2.8 Técnicas e instrumentos utilizadas en la investigación

2.8.1 Instrumentos de medición

Los instrumentos utilizados para la obtención de la información fue la guía de preguntas con las que se prepararon las entrevistas realizadas al Contador General, el Director General, el

subdirector administrativo y financiero y el director de Tecnología e Información (DTI) y las fichas bibliográficas que permitieron anotar y sustentar las fuentes consultadas al momento de indagar sobre las actualizaciones y novedades informáticas en torno a la gestión de riesgos en la era digital de las organizaciones sin fines de lucro.

2.9 Procesamiento de la información

La información recopilada en la entrevista sirvió para interpretar la información y se complementó con la bibliografía consultada para diagnosticar el problema.

2.10 Análisis e interpretación de los resultados

El instrumento utilizado para recopilar información de la organización fue la entrevista que estuvo dirigida a cuatro unidades de análisis claves en la toma de decisiones. Se diseñó con una guía de preguntas que permitió analizar el proceso de gestión de riesgos financieros y plantear posibles soluciones a los hallazgos que así lo requieran.

Procesada esta información se muestran a continuación los resultados:

Tabla 3

Unidad de análisis: Contador General

Generales

Pregunta	Respuesta	Comentario
1. ¿Cuántos años tiene de trabajar en la institución?	**Cuatro años**	Denota conocimiento y experiencia en cuanto a las operaciones y funcionalidad de la Organización.
2. ¿Qué nivel académico posee?	**Licda. En Contaduría Pública**	Existe congruencia con el puesto de trabajo
3. ¿Cuántos años de experiencia posee en la presentación de informes financieros?	**Seis años**	Denota que cuenta 6 años con experiencia para realizar la información de manera oportuna y según las necesidades de los directivos para la toma de decisiones.

Planeación

Pregunta	Respuesta	Comentario
4. ¿Cuáles son los principales riesgos para la generación de información financiera que enfrenta la ONG en la era digital?	**El riesgo que considero más grande son las inconsistencias que genera el sistema, como todavía se encuentra en el proceso de transición al DTE, el proveedor actualiza con frecuencia la versión del sistema de facturación y el contable.**	Es conocedora de los procesos operativos y sabe la importancia de que la información se procese de forma correcta para evitar errores en los resultados. Sin embargo, existen procesos que son nuevos y es necesario seguirse adaptando.
5. ¿Cuáles son los principales aspectos contables que deben considerarse para la gestión de riesgo en la era digital?	**El proceso que se lleva para la recolección de documentos y la posterior contabilización, también la revisión e integración de las cuentas contables, sobre todo aquellas que tienen que ver con efectivo.**	Se realizan muchos procesos manuales para la revisión de la información contable, pudiendo aprovechas las herramientas de las Tecnologías de la Información
6. ¿Cuáles son los errores contables más comunes que podrían surgir durante la gestión de riesgo en la era digital?	**Quizá ingresar de forma equivocada los registros contables, también, a veces, depende de la inducción que se les dé a los auxiliares, porque si no se les enseña bien el sistema y a cómo utilizarlo, los errores son más frecuentes.**	Poca comprensión de la capacitación de personal, o no es el adecuado para realizar la actividad.

Pregunta	Respuesta	Comentario
7. ¿Cómo se realiza la revisión de los estados financieros de las ONG?	**Por mi parte los reviso en el proceso de elaboración de las integraciones de las cuentas contables, al revisar registro por registro voy validando los saldos de las cuentas, sobre todo aquellas que tienen que ver con el efectivo, como las cajas, banco, cuentas por cobrar, por pagar, etc.**	Hay un importante interés por las cuentas relacionadas con el efectivo, lo que da seguridad a los directivos en cuanto al tratamiento de este, pero el proceso de revisión no es el más optimo, pues lleva más tiempo la revisión cuenta por cuenta y registro por registro.
8. ¿Cuáles son los desafíos contables comunes durante la integración de sistemas financieros en la gestión de riesgo en la era digital?	**Considero que el desafío más grande es la falta de confianza en los sistemas informáticos contables, ya que, nos ha pasado, que se nos duplican números de partida, o permite realizar registros después de cerrado el mes, entonces, hay que revisar bien, en ocasiones registro por registro.**	El desafío se puede convertir en debilidad dado que depender del riesgo humano por la falta de confianza en los sistemas genera trabajo y preocupación extra.
9. ¿Cómo coordina su trabajo con el jefe de Informática para garantizar una evaluación integral de la gestión de riesgo de los estados financieros?	**Reportando cualquier inconsistencia, también tomando capturas de pantalla de las inconsistencias para validar y descartar que sea error humano**	Existe buena comunicación entre el departamento contable y el de sistemas lo que puede ayudar a que las inconsistencias se resuelvan más rápido.

Control Interno

Pregunta	Respuesta	Comentario
10. ¿Cómo considera usted la evaluación y el fortalecimiento de controles internos en la administración de la ONG?	**Algunos controles son deficientes, otros los establecemos nosotros mismos en el día a día por inconsistencias que resultan a veces, porque no hay un manual de controles o procedimientos.**	La falta de un manual de procedimientos podría llevar a cometer errores operativos, ya que, guiarse por el criterio de cada colaborador no siempre puede prevenir los errores.
11. ¿Considera usted que la organización tiene herramientas tecnológicas que ayuden a la generación de información para la mitigación de riesgos financieros en la era digital?	**Tenemos los sistemas, tanto contable como de facturación, pero como le dije anteriormente, no son del todo fiable por las inconsistencias que genera a veces y creo que en lugar de mitigar los riesgos los incrementa.**	La implementación de la Factura electrónica presenta deficiencia y reprocesos, perjudicando la atención al cliente.
12. ¿Qué controles tiene la empresa para prevenir el fraude financiero?	**Entiendo que cuando dice fraude se refiere a la sustracción de efectivo, en ese sentido, el sistema genera de una vez el corte de efectivo de todas las cajas, también hay cámaras de seguridad en toda el área de cajas, tesorería y contabilidad.**	El control del efectivo y la seguridad es alto ante una amenaza de perdida de dinero por algún empleado encargado.
13. ¿Considera usted que la organización está monitoreando adecuadamente las actividades financieras para detectar fraudes?	**Considero que sí**	Es positivo que se monitoree constantemente disminuyendo algún riesgo posible.

Interacción con Otros Profesionales:

Pregunta	Respuesta	Comentario
14. ¿Qué desafíos ha enfrentado en la colaboración con departamento de informática y cómo se han superado?	**A veces cuesta que encuentren las inconsistencias, puesto que no son los desarrolladores del sistema contable, se ha superado comunicándonos las tres áreas: el proveedor del sistema, el DTI y yo.**	El servicio que prestan los desarrolladores del sistema contable y presenta deficiencia.

Tabla 4

Unidad de análisis: Director General

Generales

Pregunta	Respuesta	Comentario
1. ¿Cuántos años tiene de trabajar en la institución?	**Desde 1997, veintisiete años**	Denota conocimiento pleno de la organización.
2. ¿Qué nivel académico posee?	**Lic. En Artes dramáticas**	A pesar de que no cuenta con un título académico acorde a sus funciones, el conocimiento y experiencia en la organización le permiten desempeñar correctamente su cargo.
3. ¿Cuántos años de experiencia posee en la presentación de informes financieros?	**Tres años**	El director general tiene 3 años de experiencia en el análisis de la información financiera de la organización.
Planeación		
4. ¿Cuál es la visión de la ONG sobre la gestión de riesgos financieros en la era digital?	**Seguir estableciendo controles y procedimientos que nos permitan minimizar los riesgos, también será importante seguir formando a todas las personas involucradas en el área financiera y administrativa.**	Hay intención de aprender y mejorar los procesos sin ignorar la importancia de que el equipo desarrolle competencias que ayuden al logro de los objetivos de la organización.

Pregunta	Respuesta	Comentario
5. ¿La ONG está dispuesta a invertir recursos para implementar nuevas tecnologías en la gestión de riesgos financieros?	**De momento, con la tecnología que tenemos hemos hecho una gran inversión, si es necesario irla actualizando, se hará.**	Sí hay intenciones de invertir más en tecnología, no se descarta la posibilidad a largo plazo.
6. ¿Cómo se asegura la organización de que su cultura de gestión de riesgos está alineada con su estrategia general?	**Se ha invertido con el propósito de alcanzar los objetivos propuestos y todas las decisiones se toman con ese fin.**	A pesar de la poca experiencia en la dirección general hay objetivos propuestos y se trabaja orientados al cumplimiento de estos.
Ejecución		
7. ¿Cómo identifican en la ONG los riesgos financieros emergentes en el entorno digital?	**El equipo de informática se mantiene actualizado mediante formación continua, lo que les permite identificar amenazas y actuar adecuadamente. Durante la implementación del DTE, estuvieron en constante comunicación con el proveedor para asegurar que los equipos cumplieran con los requisitos necesarios.**	Hay interés por preparar constantemente al equipo informático y actualizarlos.
8. ¿Cómo minimizan los riesgos financieros para que la ONG pueda enfocar sus recursos de manera efectiva?	**Revisando constantemente los procesos y resolviendo de manera inmediata las inconsistencias**	La revisión constante puede ser un factor positivo para evitar errores, pero también podría ser resultado de inseguridad al momento de tomar decisiones.

Pregunta	Respuesta	Comentario
9. ¿Cómo coordina su trabajo con el subdirector Financiero y el jefe de Informática para garantizar una evaluación integral de la gestión de riesgos financieros?	**Para minimizar los riesgos operativos hay comunicación y seguimiento constante, por correo electrónico o llamadas del subdirector Financiero con todas las áreas bajo su cargo y con el área de sistemas informáticos.**	La comunicación es un factor importante y positivo porque permite que la información fluya y se resuelvan los errores de forma inmediata.
Control Interno		
10. ¿Qué estrategias utiliza la ONG para mitigar los riesgos financieros?	**Resolución inmediata a las inconsistencias encontradas o las que se generan durante la ejecución y registros en el sistema.**	Falta un protocolo claro para resolver inconsistencias o errores, y actuar sin un plan definido puede llevar a decisiones equivocadas.
11. ¿Qué herramientas y tecnologías están disponibles para ayudar a la ONG a gestionar sus riesgos financieros en la era digital?	**Las que tenemos en uso son el sistema de facturación, el sistema contable, el sistema de marcación de entrada, el sistema de cámaras de videovigilancia.**	La organización hace uso de tecnologías disponibles para minimizar sus riesgos financieros.
12. ¿Qué controles tiene la empresa para prevenir el ciberataque en el área financiera?	**No lo sé, creo que habría de preguntar a los expertos, quizá los de sistemas le puedan ayudar con esta pregunta.**	El director general debería conocer los controles que protegen la información de la organización, aunque no domine los aspectos técnicos. No obstante, su desconocimiento podría reflejar una confianza excesiva en su equipo.

Pregunta	Respuesta	Comentario
13. ¿Cómo está monitoreando la empresa sus actividades financieras para detectar fraudes?	**Se monitorizan constantemente las operaciones con pruebas de efectivo como arqueos de caja, conciliaciones bancarias, además se poseen dos firmas autorizadas en los cheques, lo que permite que los egresos pasen por más de un filtro.**	Existen carencias en el monitoreo de actividades financieras ya que no se toman en cuenta todos los tipos de riesgos que existen en al ejecutar estas actividades.
Interacción con Otros Profesionales:		
14. ¿Cómo colabora con otras áreas de la ONG para gestionar los riesgos financieros en la era digital?	**Con la constante comunicación y el trabajo en equipo**	La comunicación es un pilar importante en la organización

Tabla 5

Unidad de análisis: Subdirector Administrativo y Financiero

Generales

Pregunta	Respuesta	Comentario
1. ¿Cuántos años tiene de trabajar en la institución?	**20 años**	Denota conocimiento pleno de la organización.
2. ¿Qué nivel académico posee?	**MBA En Administración Financiera**	Existe idoneidad académica para el cargo
3. ¿Cuántos años de experiencia posee en la presentación de informes financieros?	**Tres años**	Posee experiencia en el análisis e interpretación de la información financiera de la organización
Planeación		
4. ¿Cuáles son los principales riesgos que enfrenta la ONG en la era digital?	**Basándome en nuestra Fundación, los riesgos podrían ser mayoritariamente operativos y de liquidez.**	Existe conocimiento de los procedimientos de la organización lo que permite identificar puntualmente las áreas de riesgo.
5. ¿Qué áreas considera la organización en la planeación para la gestión de riesgo en la era digital?	**Dentro del área administrativa, los procesos y canales de operación; dentro del área financiera todas las áreas considero que son de riesgo, por lo tanto, se incluyen todas dentro de la planificación.**	Un punto positivo es que se valoran todas las posibilidades y se busca cubrir todas las áreas.

Pregunta	Respuesta	Comentario
6. ¿Cuáles áreas considera más vulnerables en la gestión de riesgos en la era digital?	**Considero que las áreas que tienen que ver con el flujo de efectivo y las que garantizan la integridad de los registros, ya que se parten de ellos para la emisión de reportes para elaborar los informes financieros.**	Se reafirma la preocupación por el efectivo lo que asegura la atención al riesgo asociado a este rubro, pero se limitan los riesgos solo a esta área lo que lo aumenta en otras.
Ejecución		
7. ¿Cómo realiza la revisión o evaluación de los procesos operativos? ¿toma en cuenta el factor digital?	**La revisión previa la realiza la jefatura del área, quién posteriormente se encarga de compartir los hallazgos e inconsistencias conmigo, los analizamos y tomamos decisiones si hay que modificar los controles o los procesos. El factor digital siempre se toma en cuenta dado que todos los procesos están basados en el sistema informático de contabilidad o de facturación, según sea el caso.**	Denota trabajo en equipo y más de una opinión podría significar decisiones más acertadas valorando todos los escenarios posibles.
8. ¿Cuáles son los desafíos administrativos en cuanto a la gestión de riesgo en la era digital?	**A veces las personas son reacias a cumplir algunos procedimientos porque les parece irrelevantes o a llevar controles porque consideran que son una pérdida de tiempo, pero es porque no ven el panorama completo de lo que se quiere lograr.**	Esto podría indicar que los colaboradores no tienen claro todos los procedimientos a seguir.

Pregunta	Respuesta	Comentario
9. ¿Cómo coordina su trabajo con la dirección general para garantizar una toma de decisiones integral con enfoque basado en gestión de riesgo?	**La comunicación constante permite tomar decisiones coordinadas y detectar mejor los riesgos al contar con diferentes perspectivas.**	Los colaboradores tienen claro que la comunicación es clave para que se pueda trabajar de forma sincronizada.
10. ¿Aplica normativa técnica para medir o gestionar el riesgo?	**Si se refiere a alguna ISO, no; en la parte contable la Norma de contabilidad 21.**	La base técnica es limitada, ya que la Norma Contable 21 se enfoca en registros y estados financieros, pero no abarca la gestión de riesgos.
Interacción con Otros Profesionales:		
11. ¿Ha gestionado, propuesto o ejecutado formación continua en gestión de riesgos para el personal de la organización?	**Sí, los auditores han brindado como parte del servicio capacitaciones sobre la gestión de riesgo y lavado de dinero y activos**	Denota apoyo de parte de la auditoría externa, esto podría facilitarles el trabajo de identificación y diagnóstico de los riesgos potenciales que podrían afectar la organización
12. ¿Qué áreas ha tomado en cuenta para la formación en gestión de riesgos?	**Todas las áreas de la administración financiera: cajas, tesorería, contabilidad y asistencia administrativa**	Esto es un factor positivo porque permite tener protegidas todas las áreas de posibles pérdidas o amenazas a su funcionamiento continuo.
13. ¿Con qué periodicidad se reciben las capacitaciones?	**Una vez al año de forma general, pero se apoya de manera individual cuando se requiere.**	La falta de calendarización de capacitaciones puede dejar abierto a la voluntad del colaborador, provocando deficiencias en algunas áreas de conocimiento.

Tabla 6

Unidad de análisis: Director de Tecnología e Información (DTI)

Unidad de análisis: director de tecnología e información (DTI)

Generales

Pregunta	Respuesta	Comentario
1. ¿Cuántos años tiene de trabajar en la institución?	**14 años**	Tiene conocimiento de la operatividad de la organización lo que le permitiría desarrollar los sistemas informáticos para la organización.
2. ¿Qué nivel académico posee?	**Ingeniero en Sistemas de Computación**	Posee idoneidad académica para el área lo cual es positivo para apoyar informáticamente en todas las áreas.
3. ¿Cuántos años de experiencia posee en la presentación de informes financieros?	**No elaboro informes financieros**	Aunque no sea su área de especialidad, es fundamental que tenga un entendimiento básico de los componentes de un informe financiero.
Planeación		
4. ¿Cómo el departamento de informática implementa la medida de seguridad en la era digital que garanticé el uso de herramientas tecnológicas?	**Con utilización de usuarios y contraseñas con niveles de permiso y perfiles.**	Ejecuta estrategias de seguridad que permite delegar responsabilidades ante cualquier error o inconsistencia.

Pregunta	Respuesta	Comentario
5. ¿Qué nuevas herramientas tecnológicas se está utilizando para gestionar los riesgos financieros en la era digital?	**De nuestro lado ninguno, habría que preguntar al proveedor del sistema**	Delegar la gestión de la información financiera fuera de la organización expone a la empresa a riesgos significativos.
6. ¿Cómo se está comunicando los riesgos financieros en la era digital a las demás partes interesadas en la ONG?	**Por medio de correo electrónico y mensajes**	Como no se gestiona la información financiera y el control del sistema ERP, se desconoce a qué riesgos se enfrentan como organización
Ejecución		
7. ¿Cómo realiza el departamento de informática la identificación y evaluación de los riesgos financieros en la era digital?	**No se administra la información financiera dentro de la Fundación**	Denota que hay necesidad de involucrar al departamento informático en la gestión de riesgos para que puedan evaluarlos desde su área de trabajo. Además, indica que, carecen de procesos y procedimientos establecidos para recopilar, registrar, analizar y reportar los datos financieros en la era digital.
8. ¿Cómo está asegurando el departamento de informática que los sistemas y datos financieros estén protegidos contra ciberataques?	**Mediante el uso de firewall**	Aparte del firewall, no se conoce si cuenta con otras medidas, que les permite proteger los datos financieros de accesos no autorizados y garantizar la confidencialidad.

Pregunta	Respuesta	Comentario
9. ¿Cómo coordina su trabajo con el Contador para garantizar una evaluación integral de la gestión de riesgo de los estados financieros?	**Mediante llamadas y mensajes de textos**	Denota que hay buena comunicación entre las áreas involucradas.
Control Interno		
10. ¿Realizan ustedes autoevaluación de las medidas informáticas implementadas para garantizar el manejo de la información financiera?	**No**	La falta de estas medidas pone en riesgo a la organización, ya que impide evaluar la eficacia del manejo de la información y la expone a ciberataques.
11. ¿Qué herramientas y tecnologías están disponibles para ayudar a la ONG a gestionar sus riesgos financieros en la era digital?	**Uso de llaves token para el ingreso a los sistemas, seguridad biométrica**	Estos insumos serían útiles para gestionar riesgos si los sistemas informáticos del área financiera se desarrollaran y administraran internamente.
12. ¿Qué controles tiene la empresa para prevenir el ciberataque en el área financiera?	**No tenemos el control de los sistemas financieros, el proveedor es quien se encarga de ello.**	Se reafirma el riesgo de pérdida de información o mal gestión de esta.
13. ¿Participa el departamento de informática en el monitoreo de las actividades financieras con el propósito de prevenir fraudes?	**No**	Denota alto riesgo de que se generen fraudes internos y externos.

Pregunta	Respuesta	Comentario
Interacción con Otros Profesionales:		
14. ¿Cuenta el departamento de informática la colaboración con otras áreas de la ONG para gestionar los riesgos financieros en la era digital?	**No porque no gestionamos los riesgos internamente**	La comunicación en este tema es nula puesto que no se administra la información financiera desde el departamento de informática

2.11 Diagnóstico de la investigación

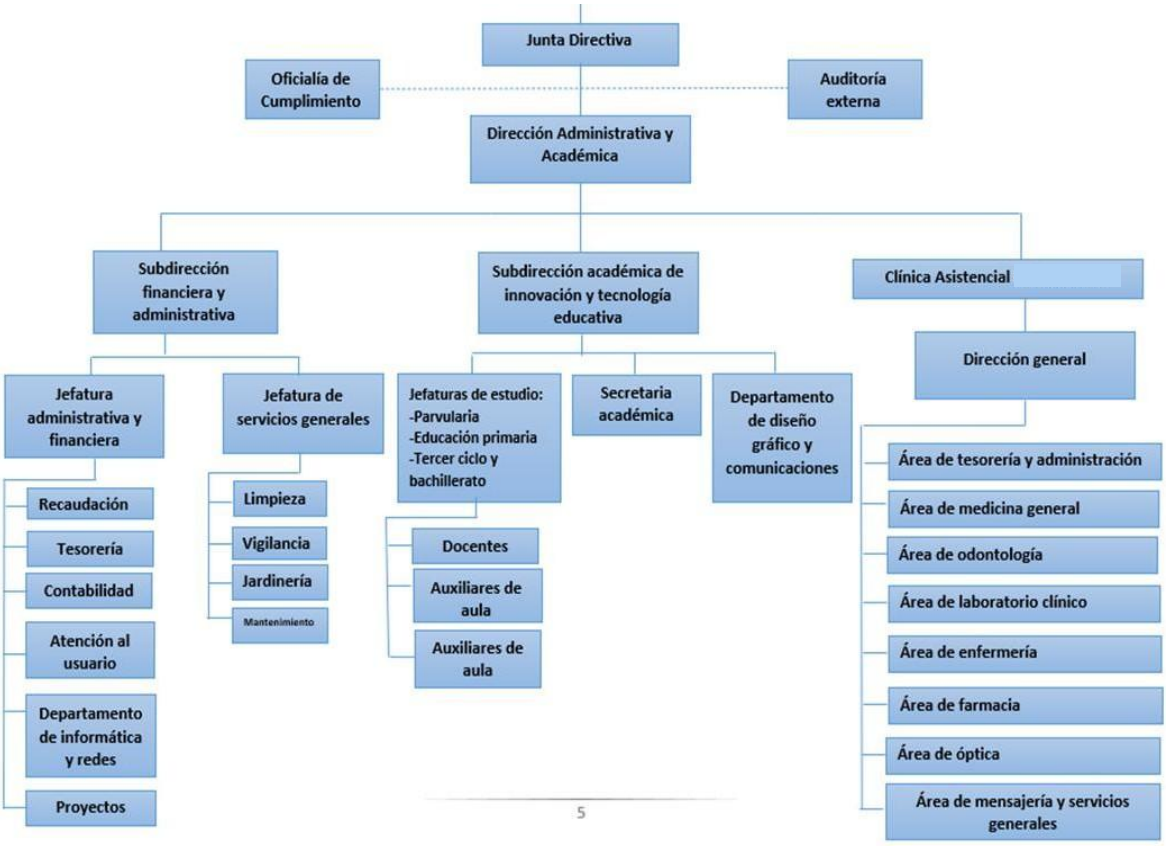
El presente diagnóstico se hizo con base en las entrevistas realizadas a las unidades de análisis seleccionadas para la presente investigación, con el fin de identificar los principales riesgos financieros a los que se enfrentan las Organizaciones No Gubernamentales en la era digital.

También, se consideró importante, para el diagnóstico, partir desde una matriz de riesgo proporcionada por la organización, para realizar el análisis de la gestión de riesgos actual y proponer áreas de mejora en una nueva matriz elaborada como resultado y aporte de esta investigación.

Las cuatro unidades de análisis entrevistadas dieron su aporte de acuerdo con el alcance que cada una tenía desde su cargo en la organización y para ello se presenta el organigrama del que dispone actualmente la Fundación:

Figura 2

Organigrama de la Fundación La Aurora



Nota: Estructura organizativa de la ONG, mostrando la distribución de funciones y responsabilidades entre las diferentes áreas.

Tabla 7

Matriz de riesgo proporcionada por la Fundación La Aurora

Riesgo	Descripción	Probabilidad	Impacto	Calificación del riesgo	Medidas de control
Contratación de empleados con antecedentes penales relacionados	Un empleado recién contratado tiene antecedentes penales por tráfico de drogas.	Baja	Alto	Medio	* Verificar los antecedentes penales de todos los empleados nuevos. *Realizar renovación anual.
Realización de transacciones inusuales o sospechosas por parte de empleados	Un empleado realiza una serie de transferencias electrónicas de alto valor a cuentas en el extranjero.	Baja	Medio	Medio	* Establecer límites de transacción para los empleados. * Monitorear las transacciones de los empleados para detectar actividades inusuales. * Requerir que los empleados proporcionen justificación para las transacciones inusuales.
Falsificación de documentos por parte de empleados	Un empleado falsifica documentos para obtener un préstamo de la empresa.	Baja	Alto	Medio	* Implementar controles internos para detectar la falsificación de documentos. * Capacitar a los empleados sobre cómo identificar documentos falsificados. * Investigar todas las denuncias de falsificación de documentos.
Uso indebido de información confidencial por parte de empleados	Un empleado vende información confidencial de clientes a un competidor.	Baja	Alto	Medio	* Restringir el acceso a la información confidencial. * Firmar contrato de confidencialidad

Riesgo	Descripción	Probabilidad	Impacto	Calificación del riesgo	Medidas de control
Soborno de empleados por parte de proveedores	Un proveedor ofrece un pago a un empleado para obtener un contrato.	Baja	Alto	Medio	* Firma de política institucional * Establecer un canal confidencial para que los empleados denuncien el soborno.
Apropiación indebida de activos por parte de empleados	Un empleado roba dinero en efectivo	Baja	Alto	Medio	* Implementar controles internos fuertes para proteger los activos. * Arqueos periódicos.
Lavado de activos a través de la nómina	Un empleado crea empleados ficticios para desviar fondos de la empresa.	Baja	Alto	Medio	* Realizar verificaciones de identidad de los empleados. * Investigar todas las discrepancias en la nómina.
Financiamiento del terrorismo a través de donaciones benéficas	Un empleado desvía donaciones benéficas a una organización terrorista.	Baja	Alto	Medio	* Monitorear el uso de fondos donados. * Investigar todas las donaciones sospechosas.
Uso indebido de la tecnología de la información por parte de empleados	Un empleado utiliza la tecnología de la información de la empresa para acceder a información confidencial o para cometer delitos.	Baja	Medio	Medio	* Implementar controles y monitorear el uso de la tecnología de la información por parte del personal.
Incumplimiento de las leyes y regulaciones de la Ley Contra el Lavado de Dinero	Un empleado no cumple con los requisitos de presentación de informes	Baja	Medio	Medio	* Implementar y monitorear procedimientos para garantizar el cumplimiento de las leyes y regulaciones

Riesgo	Descripción	Probabilidad	Impacto	Calificación del riesgo	Medidas de control
Selección de proveedores de alto riesgo	Hacer negocios con un proveedor que está involucrado en actividades ilícitas.	Baja	Alto	Medio	* Realizar la debida diligencia
Falta de transparencia en la propiedad o estructura del proveedor	No poder verificar la propiedad o estructura real del proveedor.	Medio	Alto	Medio	* Realizar la debida diligencia
Transacciones inusuales o sospechosas con proveedores	Un proveedor realiza una serie de pagos de alto valor a cuentas en el extranjero.	Medio	Medio	Medio	* Realizar la debida diligencia * Requerir que los proveedores proporcionen justificación para las transacciones inusuales.
Falsificación de documentos por parte de proveedores	Un proveedor presenta documentos falsificados para obtener un contrato o un pago.	Baja	Alto	Medio	* Implementar controles para detectar documentos falsificados. * Verificar la autenticidad de los documentos con fuentes independientes. * Realizar la debida diligencia
Soborno de empleados por parte de proveedores	Un proveedor ofrece un pago a un empleado para obtener una ventaja comercial.	Baja	Alto	Medio	* Implementar una política de anticorrupción clara y concisa. * Capacitar a los empleados sobre cómo reconocer y denunciar el soborno.
Uso indebido de información confidencial por parte de proveedores	Un proveedor accede o utiliza información confidencial de la empresa sin autorización.	Medio	Medio	Medio	* Restringir el acceso a la información confidencial a los proveedores que la necesitan. * Implementar acuerdos de confidencialidad con proveedores.

Riesgo	Descripción	Probabilidad	Impacto	Calificación del riesgo	Medidas de control
Lavado de activos a través de las cuentas por pagar	Un proveedor infla las facturas o crea facturas ficticias para lavar dinero.	Baja	Alto	Medio	* Implementar controles para detectar facturas fraudulentas. * Reconciliar las cuentas por pagar con otros registros financieros. * Realizar verificaciones de antecedentes de los proveedores y sus asociados. * Monitorear las actividades de los proveedores para detectar comportamientos sospechosos. *Realizar la debida diligencia. * Exigir a los proveedores que cumplan con las leyes y regulaciones. * Monitorear el cumplimiento de los proveedores con las leyes y regulaciones.
Financiamiento del terrorismo a través de proveedores	Un proveedor desvía fondos para apoyar actividades terroristas.	Baja	Alto	Medio	
Incumplimiento de las leyes y regulaciones por parte de proveedores	Un proveedor no cumple con los requisitos, como los requisitos de presentación de informes.	Medio	Medio	Medio	

Nota: Fuente proporcionada por la administración financiera de Fundación La Aurora

La contadora general expresó su preocupación por las discrepancias encontradas en el software contable, lo que genera incertidumbre en los registros financieros de la empresa.

El ERP implementado no fue diseñado a medida para las necesidades específicas de la Fundación, presentando una interfaz y módulos poco adecuados para optimizar sus procesos contables y la información financiera.

Estas deficiencias exponen a la organización a mayores riesgos operativos y financieros, ya que la complejidad del sistema aumenta la probabilidad de errores humanos y fraudes.

Estas deficiencias incrementan los riesgos operativos y financieros, ya que, al no ser un sistema amigable con el usuario incrementa la probabilidad de que los colaboradores asociados al área operativa comentan errores involuntarios, por un lado, y por otro, que se cometan delitos asociados y que no se puedan rastrear.

La necesidad de realizar actualizaciones constantes al software indica que este no fue desarrollado con una visión a largo plazo, lo que genera incertidumbre en la planificación contable, dificultando en el cumplimiento de los plazos establecidos para la entrega de reportes y esto limita la toma de decisiones oportunamente.

Estas inconsistencias informáticas también interfieren en el proceso de inducción de las nuevas contrataciones, ya que no permiten la adaptación del equipo debido a la improvisación con el uso del sistema.

Otra debilidad del área administrativa es que no existen manuales de procedimientos que permitan tener claro a los y las colaboradoras del área contable la forma de proceder ante los obstáculos operativos que surjan en el día a día. Al no contar con manuales de

procedimientos, las operaciones contables se realizan de manera informal, lo que genera inconsistencias en la información financiera.

La unidad DTI, al no estar involucrada directamente en el desarrollo o administración del software, no pudo ofrecer soluciones inmediatas a las problemáticas identificadas. Su dependencia del proveedor externo limita la capacidad de respuesta del sistema. En este punto es importante destacar que la información financiera no se administra en la organización y esto implica un riesgo alto de pérdida o manipulación de la información. Además, existe poco o nulo conocimiento de cómo se gestionan los riesgos financieros desde el punto de vista informático.

Por otra parte, tanto la dirección general como la subdirección financiera tienen amplio conocimiento acerca de la organización, sin embargo, no existe un manual o instructivo que brinde los lineamientos por áreas para gestionar los riesgos financieros. La matriz compartida indica que no se miden los riesgos por áreas o procesos.

En cuanto a las máximas autoridades de la Fundación, se considera que es importante que se realice una inversión a corto plazo, ya sea interna o externa, que les permita desarrollar un software que se ajuste a las necesidades de la organización, dado que tienen operaciones diversas pero que por su misma naturaleza no están integradas dentro del servicios informático contable que poseen actualmente.

Lo anterior conlleva a que como directivos no conozcan de primera mano los procesos que el servidor del software contable realiza con la información financiera que procesa el departamento contable lo que expone a la organización a riesgos financieros digitales como: manipulación o fraude interno, incumplimiento normativo y regulatorio,

ciberataques y robos de datos financieros, dependencia excesiva de terceros, integridad de la información, entre otros.

En cuanto a la gestión de riesgos, este es un tema clave para el éxito y la sostenibilidad de cualquier organización, por lo que es importante que se apoyen en un marco de referencia que les ayude; la ISO 31000 sería una buena herramienta para iniciar con este proceso hacia la mejora continua, ya que su fin, según la Organización Internacional de Normalización, es proteger activos y mejorar la toma de decisiones para cumplir objetivos de la Fundación. También, existen otras normas y leyes como las Normas Técnicas del Banco Central de Reserva, la Ley de Supervisión y Regulación del Sistema Financiero, entre otras que, aunque son aplicables al sistema bancario, también pueden adecuarse a una ONG para garantizar una gestión basada en el riesgo financiero.

Finalmente, no se concretó que existiera una calendarización de capacitación constante, a pesar de que se indicó en las entrevistas que se capacitaba periódicamente a los colaboradores, pero adicional a las capacitaciones especializadas en cada área, es importante que se preste atención a las relacionadas con la gestión de riesgo.

CAPÍTULO III: GUÍA PARA LA GESTIÓN DE RIESGOS FINANCIEROS EN LA ERA DIGITAL EN LA ORGANIZACIONES NO GUBERNAMENTALES DE EL SALVADOR

Introducción

En la era digital, las Organizaciones No Gubernamentales (ONG) de El Salvador enfrentan un entorno cada vez más dinámico y complejo, caracterizado por la globalización de los mercados, el acceso a nuevas tecnologías y la creciente dependencia de los sistemas digitales para el desarrollo de sus actividades. A pesar de los avances tecnológicos y el acceso a nuevas herramientas, las ONG también están expuestas a riesgos financieros significativos, que van desde la malversación de fondos hasta ataques cibernéticos, fraudes y fluctuaciones económicas.

La gestión de riesgos financieros se ha consolidado como un elemento clave para garantizar la sostenibilidad a largo plazo y el rendimiento eficiente de las organizaciones sin fines de lucro. Dada la limitación de sus recursos y la incertidumbre en los contextos de financiamiento, estas organizaciones deben crear un enfoque integral para identificar, evaluar y reducir riesgos, con el fin de salvaguardar su misión y maximizar el aprovechamiento de los fondos disponibles

Esta guía tiene como objetivo proporcionar a las ONG salvadoreñas un conjunto de herramientas y mejores prácticas para que gestione los riesgos financieros en un entorno digital cada vez más complejo. Con base en las normas ISO 31000 e ISO 31010, esta investigación tiene como objetivo fortalecer la capacidad de las organizaciones actuar de manera sostenible y transparente, adaptándose a las peculiaridades del contexto salvadoreño.

GUÍA PARA LA GESTIÓN DE RIESGOS FINANCIEROS EN LA ERA DIGITAL EN LAS ORGANIZACIONES NO GUBERNAMENTALES DE EL SALVADOR

Contenido

➢ OBJETIVOS

General

Proporcionar a las Organizaciones No Gubernamentales (ONG) un marco normativo y teórico que permita identificar, evaluar y mitigar los riesgos que puedan afectar la capacidad de la organización para cumplir con su misión y objetivos**.**

Específicos

- Ayudar a la organización a identificar los riesgos potenciales que podrían impactar sus operaciones, finanzas, reputación, y efectividad en la consecución de sus objetivos.
- Evaluar y priorizar los riesgos según su probabilidad de ocurrencia y el impacto que podrían tener, para enfocar las acciones de manera más efectiva.
- Facilitar el desarrollo de estrategias y medidas preventivas para reducir la probabilidad o el impacto de los riesgos identificados, asegurando así una gestión proactiva.
- Proteger los recursos de la organización, incluyendo el personal, fondos, y activos, al anticipar posibles problemas y minimizar su impacto.
- Verificar que la ONG cumpla con las leyes, regulaciones y estándares relevantes relacionados con la gestión de riesgos.

A. MARCO NORMATIVO

A.1. Normativa Técnica

a. Norma ISO 31000 Gestión de Riesgo en las Organizaciones

b. Norma ISO 31010/2019 Gestión de Riesgos. Técnicas de Evaluación del Riesgo

c. NRP-36 "Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos, Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva"

A.2. Normativa Legal

d. Ley Especial para la Prevención, Control y Sanción del Lavado de Activos, Financiamiento al Terrorismo y de la Proliferación de Armas de Destrucción Masiva

e. Reglamento de la Ley Contra Lavado de Dinero y Activo

f. Ley de Asociaciones y Fundaciones sin Fines de Lucro

g. Recomendaciones GAFI

h. Ley para el Fomento de Entidades Fintech y Regulación de Servicios Financieros Digitales

i. Ley de Emisión de Activos Digitales

B. MARCO APLICATIVO SOBRE GESTIÓN DEL RIESGO

La gestión de riesgos es un proceso fundamental en cualquier organización o proyecto, ya que ayuda a identificar, evaluar y mitigar los riesgos que podrían afectar negativamente los objetivos. A continuación, se presentan aspectos generales importantes sobre la gestión de riesgos y que se han desarrollado en la presente guía:

a. **Identificación de riesgos**: Este es el primer paso y consiste en identificar todos los posibles riesgos que podrían impactar un proyecto o una organización. Esto puede incluir riesgos financieros, operativos, tecnológicos, legales, ambientales, entre otros. La identificación puede hacerse a través de métodos como análisis FODA, lluvia de ideas, entrevistas con expertos, y revisión de documentación histórica.

b. **Evaluación de riesgos**: Una vez identificados, los riesgos deben evaluarse para determinar su probabilidad de ocurrencia y el impacto que tendrían en caso de materializarse. Esto se ha realizado mediante el inventario de riesgos mostrados en la primera tabla y posteriormente en una matriz de riesgos, que clasifica los riesgos en términos de su gravedad y probabilidad. Esto ayuda a priorizar los riesgos que necesitan una atención inmediata.

c. **Desarrollo de estrategias de mitigación**: Para cada riesgo significativo identificado, se deben desarrollar estrategias para mitigarlo o gestionarlo. Las estrategias pueden incluir la implementación de controles para reducir

la probabilidad de que el riesgo ocurra, desarrollar planes de contingencia para manejar el impacto si el riesgo se materializa, o transferir el riesgo a terceros (por ejemplo, mediante seguros).

d. **Implementación de estrategias**: Una vez que se han desarrollado las estrategias de mitigación, es esencial implementarlas de manera efectiva. Esto puede incluir la asignación de recursos, la modificación de procesos, y la comunicación de las estrategias a todas las partes involucradas.

e. **Monitoreo y revisión**: La gestión de riesgos no es un proceso estático; los riesgos pueden cambiar con el tiempo. Por lo tanto, es crucial monitorear continuamente los riesgos y las estrategias de mitigación para asegurarse de que siguen siendo efectivas. Esto puede implicar la revisión regular de los riesgos, la evaluación de la efectividad de las estrategias de mitigación y la actualización de los planes según sea necesario.

f. **Comunicación y reporte**: La comunicación efectiva es clave en la gestión de riesgos. Es importante informar a todas las partes interesadas sobre los riesgos y las estrategias de mitigación, y mantener una transparencia continua. Los informes regulares sobre el estado de los riesgos y la efectividad de las estrategias son esenciales para una gestión eficaz.

g. **Cultura de gestión de riesgos**: Fomentar una cultura organizacional que valore la gestión de riesgos puede ayudar a mejorar la capacidad para identificar y abordar los riesgos de manera proactiva. Esto incluye la formación del personal, la promoción de una actitud positiva hacia la

identificación de riesgos y la integración de la gestión de riesgos en todos los niveles de la organización.

La gestión de riesgos es dinámica y requiere un enfoque sistemático y disposición para adaptarse a cambios y nuevas amenazas. El objetivo de la presente guía es proporcionar un camino a las organizaciones sin fines de lucro para que puedan reducir la incertidumbre y mejorar su capacidad para alcanzar sus objetivos de manera efectiva. Las etapas de este proceso se aplican de la siguiente manera:

B.1. IDENTIFICACIÓN DEL RIESGO

En esta etapa, se propone, primeramente, conocer todos aquellos factores internos y externos que pueden afectar al cumplimiento de los objetivos. Posteriormente, para visualizarlos es necesario la elaboración de una matriz, la cual permite hacer un inventario de los riesgos, la frecuencia con que ocurren y el impacto que tienen dentro de la Organización.

Para facilitar este análisis se propone inventariarlos de la siguiente manera:

Área o departamento o unidad de análisis: área administrativa

Factor	Tipo de factor	Descripción	Riesgo	Tipo de riesgo	Consecuencia
Contratación de empleados	Interno	Gestionar antecedentes penales y solvencia policial al iniciar el proceso de contratación.	Que la persona contratada tenga antecedente penales o procesos judiciales en curso.	Reputacional y contagio	Pérdida de confianza de los donantes y deterioro de la imagen social de la organización
Falsificación de documentos de contratación por parte de empleados	Interno	Recopilación de documentos para el expediente de empleados	Que los empleados falsifiquen documentos legales para alcanzar el perfil de contratación requerido.	Operativo y reputacional	Sanciones penales, daño a la imagen pública, incapacidad para participar en proyectos.
Soborno a empleados	Externo	Que proveedores o usuarios de la Fundación ofrezcan pagos o dadivas a empleados a cambio de ser beneficiados en la asignación de proyectos o programas	Incumplimiento de estatutos y fines para los que fue creada la organización.	Legal, reputacional, operativo y contagio	Retiro de los fondos otorgados para la ejecución de proyectos los cuales se verían reflejados en una disminución en las donaciones restringidas o no restringidas, dependiendo el origen, privado o público, de la aportación.

Factor	Tipo de factor	Descripción	Riesgo	Tipo de riesgo	Consecuencia
Puestos de trabajo ficticios.	Interno	Creación de plazas inexistentes a fin de justificar erogaciones periódicas.	Uso indebido de los fondos en la organización que no justifica los fines para los que fue creada.	Reputacional, legal y operativo.	Las sanciones penales y el daño reputacional pueden impedir la participación en proyectos y acceso a subvenciones, además de causar pérdida de apoyo internacional. Financiera y contablemente, esto se refleja en mayores gastos operativos y menor excedente.
Conocimiento de usuarios o proveedores	Externo	Indagar sobre la operatividad de los usuarios o proveedores de la organización para conocer el origen y procedencia de los fondos mediante el formulario "Conoce a tu cliente"	Que la procedencia de los fondos provenga de actividades ilícitas.	Reputacional, legal, operativo y de contagio	La ejecución de proyectos con fondos ilícitos implica complicidad en lavado de dinero, con posibles sanciones penales y cierre de la Fundación. En lo financiero, se evidencian aumentos de activos y préstamos simulados para justificar los fondos.

Factor	Tipo de factor	Descripción	Riesgo	Tipo de riesgo	Consecuencia
Desconocimiento de políticas de control interno	Interno	Los colaboradores desconocen las políticas de control interno generando inconsistencias en el ejercicio de sus funciones	Incumplimiento de obligaciones operativas, formales, técnicas o tributarias, según sea el caso.	Legal, operativo y de contagio	Observaciones por parte de auditoría interna y externa y sanciones por parte de entidades gubernamentales o reguladoras, en el área financiera se vería reflejado en gastos por multas e intereses por pagos extemporáneos lo que a su vez disminuye el excedente obtenido al final del ejercicio.

Área o departamento o unidad de análisis: área financiera

Factor	Tipo de factor	Descripción	Riesgo	Tipo de riesgo	Consecuencia
Transacciones inusuales o sospechosas por parte de empleados	Interno	Un empleado realiza cuantiosas transferencias electrónicas a cuentas locales o en el extranjero	Que desvíe fondos recaudados para uso propio o para financiar actividades ilícitas.	Reputacional, legal, operativo y de contagio	Sanción por parte de organismos nacionales o internacionales y pérdida de reputación organizacional. En el área financiera, estas actividades se podrían evidenciar en la disminución de activos como efectivo y equivalente y propiedad planta y equipo por la venta o donación de bienes y en las cuentas por cobrar para justificar el egreso.

Factor	Tipo de factor	Descripción	Riesgo	Tipo de riesgo	Consecuencia
Donaciones de dudosa procedencia	Externo	Donaciones irregulares en montos y frecuencia y cuantiosos donativos en efectivo	Que los aportes del donante provengan de actividades ilícitas	Reputacional y legal	Sanción por parte de la FGR si no se reporta y pérdida reputacional de la organización.
Donaciones a terceros	Interno y externo	Donaciones a terceros, en efectivo o especies sin conocimiento o cumplimiento de controles hacia el destinatario.	Que los aportes sean para financiar actividades ilícitas o no sean para el cumplimiento de los fines de la organización.	Reputacional, legal, operativo y de contagio	El cierre de operaciones por intervención de organismos fiscalizadores.

Área o departamento o unidad de análisis: área tecnológica

Factor	Tipo de factor	Descripción	Riesgo	Tipo de riesgo	Consecuencia
Creación de usuarios y contraseñas por colaborador	Interno	Que los colaboradores tengan acceso a todos los usuarios y contraseñas	Que algún colaborador suplante identidad de otro para realizar operaciones	Operativo y de contagio	Realizar operaciones indebidas que perjudiquen el funcionamiento y resultados financieros de la Organización
Creación de perfiles con niveles de permisos	Interno	Que cada usuario tenga asignado un perfil de acceso de acuerdo con las operaciones que realiza.	Que algún colaborador tenga acceso a información confidencial o innecesaria para ejercer sus funciones	Operativo y de contagio	Realizar operaciones indebidas que perjudiquen el funcionamiento y los resultados financieros de la Organización
Protección y acceso controlado a las bases de datos o servidores de la Organización	Interno y externo	Existen estrategias de prevención como la autenticación, automatización y protección de seguridad informática	Probabilidad de hackeo cibernético a la Organización ya sea por lucro o por malicia	Reputacional, legal, operativo y de contagio	Robo de la información confidencial de la organización, manipular la información financiera que podría ocasionar el cierre de esta

B.2. ANÁLISIS DEL RIESGO

Este análisis depende de la información recaudada en la fase de identificación, y con ello se pretende buscar la probabilidad de ocurrencia y sus consecuencias, esto ayudará a la clasificación por nivel de riesgo y las acciones que se tomarán a fin de mitigarlo.

A continuación, se proponen los siguientes pasos:

1. Determinar la frecuencia del evento en un periodo de tiempo estimado, que por lo general es un año.
2. Describir el impacto o consecuencias que ya se ha hecho en la primera fase
3. Clasificarlo, según el nivel de exposición, tomando como base la información obtenida en el paso 1 y 2, en bajo, medio, alto y muy alto; según la frecuencia y el impacto.

Tabla de frecuencia de ocurrencia de los eventos

Criterio	Descripción
Bajo	puede ocurrir solo bajo ciertas circunstancias
Medio	puede ocurrir ocasionalmente
Alto	ocurre con frecuencia
Muy alto	ocurre constantemente

Tabla de impacto de la ocurrencia de los eventos

Criterio	Descripción
Bajo	Si el evento ocurre tiene consecuencias mínimas en la institución
Medio	Si el evento ocurre tiene consecuencias moderadas en la institución
Alto	Si el evento ocurre tiene consecuencias importantes en la institución
Muy alto	Si el evento ocurre tiene consecuencias catastróficas en la institución

B.3. EVALUACIÓN DEL RIESGO

La evaluación del riesgo permite determinar los niveles de riesgo y compararlos mediante el uso de tabla de frecuencia e impacto 5X5 para establecer el grado de exposición al riesgo y el impacto que tendrá dentro de la Organización y esto se logra mediante el uso de la ecuación *probabilidad x gravedad =impacto del riesgo.*

Los riesgos se plantean en función de su probabilidad y gravedad, obteniendo el nivel de impacto del riesgo; este impacto, se puede codificar por color de verde a rojo y clasificarlo en una escala de 1 a 25. Para facilitar la clasificación (hecha en el numeral III) y la evaluación de los riesgos se propone la siguiente matriz:

Probabilidad de ocurrencia	Impacto				
Gravedad	Insignificante (1)	Menor (2)	Significativo (3)	Mayor (4)	Crítico (5)
1. Improbable	Bajo (1)	Bajo (2)	Bajo (3)	Bajo (4)	Medio (5)
2. Poco probable	Bajo (2)	Bajo (4)	Medio (6)	Medio (8)	Alto (10)
3. Ocasional	Bajo (3)	Medio (6)	Medio (9)	Alto (12)	Alto (15)
4. Muy probable	Bajo (4)	Medio (8)	Alto (12)	Alto (16)	Muy alto (20)
5. Recurrente	Medio (5)	Alto (10)	Alto (15)	Muy alto (20)	Muy alto (25)

Los resultados se leerán de la siguiente manera:

a) Bajo (1-4): es probable que los eventos de bajo riesgo no sucedan y, si suceden, no tendrán consecuencias significativas para la organización.

b) Medio (5-9): son una molestia y pueden causar contratiempos en la organización, lo mejor será tomar medidas para prevenir y mitigar estos riesgos; no se deben ignorar, pero tampoco es necesario que sean prioridad.

c) Alto (10-16): pueden poner en riesgo el logro de los objetivos de la organización. Si la probabilidad de que ocurran es alta, las consecuencias serán graves, por lo tanto, es importante darles prioridad.

d) Muy alto (17-25): ponen en riesgo la marcha de la organización. Si su probabilidad de que ocurran es muy alta, las consecuencias serán tan graves que pueden llevar al cierre del negocio.

B.4. MATRIZ DE RIESGO

FUNDACIÓN LA AURORA
MATRIZ PROPUESTA PARA LA GESTIÓN DEL RIESGO FINANCIERO

FACTOR	DESCRIPCIÓN DEL RIESGO	UNIDAD DE ANÁLISIS	ANÁLISIS DEL RIESGO			ACCIONES DE CONTROL
			Probabilidad	Impacto	Gravedad	
Contratación de colaboradores	Los colaboradores contratados tienen antecedentes penales o procesos judiciales en curso.	Subdirector administrativo y financiero	**Poco probable**	**Bajo**	**Menor**	Solicitar antecedentes penales y solvencia de la PNC en original y con código QR legible para poder escanear y consultar la veracidad del documento.
Falsificación de documentos de contratación por parte de los colaboradores	Los colaboradores falsifican documentos de contratación para alcanzar el perfil requerido por la organización.	Subdirector administrativo y financiero	**Poco probable**	**Bajo**	**Menor**	Solicitar documentos originales certificados para confrontar las copias
Soborno a colaboradores	Los proveedores o usuarios de la organización ofrecen pagos o dadivas a los colaboradores a cambio de obtener beneficios o preferencias en la asignación de proyectos.	Subdirector administrativo y financiero	**Poco probable**	**Bajo**	**Menor**	Crear una política donde se prohíba a los colaboradores el recibir obsequios, incentivos o propinas por parte de los usuarios.

FACTOR	DESCRIPCIÓN DEL RIESGO	UNIDAD DE ANÁLISIS	ANÁLISIS DEL RIESGO			ACCIONES DE CONTROL
			Probabilidad	Impacto	Gravedad	
Puestos de trabajo ficticios	Creación de plazas inexistentes con el fin de justificar erogaciones periódicas.	Director general	**Poco probable**	**Medio**	**Mayor**	Uso de controles de asistencias como marcaciones biométricas
Conocimiento de usuarios o proveedores	La procedencia de los fondos de los usuarios o los insumos adquiridos por los proveedores provienen de actividades ilícitas	Subdirector administrativo y financiero	**Poco probable**	**Alto**	**Crítico**	Realizar la debida diligencia según el instructivo de la UIF
Divulgación de políticas y reglamento interno	Faltas e inconsistencias en el ejercicio de las funciones de los colaboradores	Director general	**Ocasional**	**Medio**	**Significativo**	Realizar capacitaciones o convivios periódicos que permitan dar a conocer las políticas y reglamento interno
Transacciones monetarias inusuales de los colaboradores	Desvío de fondos para uso propio o para financiar actividades ilícitas	Contador general	**Poco probable**	**Medio**	**Significativo**	Uso de firmas electrónicas conjuntas entre dos jefaturas, previo a la validación y revisión de la operación.
Transferencias por donaciones	Donaciones irregulares con montos y frecuencia inusuales	Contador general	**Muy probable**	**Alto**	**Mayor**	Solicitar comprobante de procedencia de fondos e informar a la UIF

FACTOR	DESCRIPCIÓN DEL RIESGO	UNIDAD DE ANÁLISIS	ANÁLISIS DEL RIESGO			ACCIONES DE CONTROL
			Probabilidad	Impacto	Gravedad	
Creación de usuarios y contraseñas	Los colaboradores tienen acceso a todos los usuarios y contraseñas	Área tecnológica	**Poco probable**	**Bajo**	**Menor**	Crear usuarios únicos con contraseñas actualizables a corto plazo
Creación de perfiles asociados a permisos	Los usuarios tienen perfiles con permisos que no van de acuerdo con las funciones que desempeñan	Área tecnológica	**Poco probable**	**Bajo**	**Menor**	Asignar permisos a los perfiles de acuerdo con las funciones que tienen asignadas
Acceso controlado a la base de datos y servidores	Hackeo interno o externo, manipulación de la información o del funcionamiento de los sistemas	Área tecnológica	**Poco probable**	**Alto**	**Crítico**	Implementar mecanismos de autenticación, protección endpoints, seguridad de navegación web, inteligencia de tráfico de datos y desarrollar una cultura de ciberseguridad

B.5. CONTROL DEL RIESGO

El riesgo se puede minimizar mediante acciones de control que permitan reducir la ocurrencia y el impacto de los eventos identificados mediante la matriz de riesgo sugerida en el capítulo anterior.

A continuación, se proponen las siguientes acciones de control:

B.5.1. Controles de gestión

a. Implementar políticas y procedimientos financieros

Para garantizar la transparencia, la eficiencia y la seguridad en la gestión financiera se deben establecer y formalizar políticas y procedimientos financieros que sirvan como guías en el manejo de los recursos. Estas políticas deben ser comprensibles, actualizadas y accesibles a todos los involucrados en la gestión financiera de la organización; además, deben incluir elementos claves como la aprobación de jerarquías, distribución de responsabilidades y controles internos.

b. Seguimiento al plan de trabajo anual

El seguimiento al plan de trabajo anual es una actividad esencial para garantizar el cumplimiento de los objetivos estratégicos y operativos dentro de los plazos y presupuestos establecidos. El plan de trabajo anual debe incluir claramente los proyectos, los indicadores de éxito, el cronograma y los recursos financieros asignados. Realizar un seguimiento periódico permite identificar desviaciones a tiempo, corregir problemas y asegurar que los resultados esperados se alcancen de

manera eficiente. A continuación, se detallan tres componentes clave del seguimiento.

a. Presupuesto

b. Cumplimiento de indicadores

c. Ejecución del cronograma

El seguimiento al plan de trabajo anual mediante la revisión del presupuesto, el cumplimiento de indicadores, y la ejecución del cronograma permite que se mantenga el control sobre los proyectos, asegurando una correcta asignación de recursos y un impacto positivo en sus beneficiarios. Estas acciones de control aseguran que la organización pueda responder de manera ágil y eficaz a cualquier desviación, garantizando el éxito de sus objetivos anuales.

c. Presentación de informes

Este documento es un proceso clave dentro de la gestión organizacional, ya que permite la rendición de cuentas, el seguimiento del progreso de las actividades y la evaluación del impacto de los proyectos implementados. Estos informes pueden ser internos, para la dirección y el equipo, o externos, dirigidos a donantes, socios o entidades reguladoras. La correcta elaboración y presentación de informes asegura la transparencia en el uso de los recursos y la alineación de las acciones con los objetivos establecidos.

Estos informes se pueden clasificar en dos tipos:

a. Técnicos

Donde se informan todas las actividades realizadas en el proyecto, así como el cumplimiento de los indicadores. Con base en el instructivo para la administración de recursos financieros del estado, Acuerdo N°15-0393 se sugieren los siguientes apartados para su elaboración:

- Introducción
- Objetivos del proyecto
- Metas
- Alcance
- Actividades desarrolladas
- Fases del proyecto
- Indicadores
- Datos estadísticos
- Metodología utilizada
- Presupuesto ejecutado
- Valoraciones y recomendaciones
- Anexos

b. Financieros

Consta de un reporte detallado, por operación, del uso de los fondos asignados, debe incluir fecha del desembolso, números de cheques emitidos, beneficiarios y descripción de la actividad para las que fueron utilizados.

La presentación de informes es una práctica clave para asegurar la rendición de cuentas y la transparencia en el funcionamiento. A través de informes técnicos y financieros la organización solo asegura el cumplimiento de sus obligaciones.

B.5.2. Controles operativos

La implementación de controles operativos efectivos es crucial para minimizar los riesgos financieros y garantizar la sostenibilidad de la organización, estos están relacionados con la gestión de fondos, la contabilidad y la gestión de activos, a continuación, se sugieren los siguientes:

d. Establecer un comité de riesgos financieros:

Constituir un comité ayudará a identificar y evaluar los riesgos financieros, lo que permitirá tomar decisiones informadas y reducir la exposición a las pérdidas; además, puede ser un mecanismo para garantizar la transparencia en la toma de decisiones. Debe estar compuesto por un presidente, miembro de la junta o un ejecutivo financiero; representantes de diferentes áreas de la organización, como finanzas o auditoría interna y expertos externos, como analistas de riesgos o abogados con experiencia en la gestión de riesgos financieros.

e. Identificación y evaluación de riesgos:

El comité constituido debe establecer un proceso para identificar y evaluar los riesgos financieros potenciales, tal como lo hemos indicado anteriormente, mediante la elaboración de la matriz de riesgo.

f. Monitoreo y seguimiento:

Implementar un sistema de monitoreo y seguimiento, haciendo uso de sistemas informáticos que faciliten la supervisión de los flujos de caja, los activos y las deudas, y detectar posibles desviaciones o riesgos.

g. Control de acceso y uso de recursos:

Proporcionar controles efectivos para garantizar que solo las personas autorizadas utilicen los recursos financieros y accedan a la información.

h. Documentación y registro:

Mantener registros precisos y actualizados de todas las transacciones financieras, incluyendo documentos de soporte para auditorías y evaluaciones.

i. Auditoría y revisión:

Realizar auditorías y revisiones periódicas para evaluar la gestión financiera y detectar posibles errores o irregularidades.

j. Capacitación y formación:

Proporcionar capacitación y formación a los empleados, pasantes y voluntarios sobre la gestión de riesgos financieros y la implementación de controles operativos.

k. Comunicación y coordinación:

Establecer líneas de comunicación y coordinación efectivas entre el departamento financiero, informático y de gestión para garantizar la coordinación y el seguimiento de los riesgos financieros.

B.5.3. Controles legales

En virtud de la legislación salvadoreña y las normas internacionales, se debe implementar los siguientes controles:

l. Registro y acreditación:

La organización debe estar registrada ante el Registro de Fundaciones y Asociaciones sin Fines de Lucro, en el Ministerio de Gobernación y obtener una acreditación como entidad sin fines de lucro, según lo establecido en la Ley de Fundaciones y Asociaciones sin Fines de Lucro.

m. Presentación de estados financieros:

Se deben presentar estados financieros anuales ante el Registro de Fundaciones y Asociaciones sin Fines de Lucro, cumpliendo con la *Norma de Contabilidad N°21*.

n. Control de donaciones:

Es necesario implementar mecanismos para controlar la procedencia de las donaciones, incluyendo las anónimas o las realizadas en efectivo, y comprobar si cumplen con la *Ley de Protección de Datos Personales* de sus donantes y beneficiarios.

o. Seguimiento y control de gastos:

Se debe establecer un sistema de seguimiento y control de gastos para garantizar que los recursos sean utilizados de acuerdo con los objetivos y propósitos de la organización.

p. Normas internacionales y salvadoreñas:

Es importante considerar las normas internacionales, como la ISO 37001 (Sistemas de gestión antisoborno), la ISO 31000 y 31010 (Gestión de riesgos) y las normas salvadoreñas, como la *Ley de Fundaciones y Asociaciones sin Fines de Lucro*, la *Ley de Delitos Informáticos, y Ley de Emisión de Activos Digitales*, para garantizar la implementación efectiva de los controles legales y la gestión de riesgos financieros.

CONCLUSIONES

Se llevó a cabo el análisis de la gestión de riesgos financieros que ejecuta la organización no gubernamental “La Fundación la Aurora”, y se concluye que falta una herramienta técnica que oriente y fortalezca los procesos para identificar las áreas más vulnerables que afectan la toma de decisiones y el cumplimiento de los objetivos establecidos.

Al obtener los resultados de las entrevistas realizadas, se verificó un alto riesgo en el área de informática, donde el administrador de la información financiera digital es un agente externo, es decir, el suministro del producto tecnológico es proporcionado por un proveedor que no forma parte de la organización.

A pesar de contar con una organización bien distribuida y profesional en cada área, se concluye que el personal involucrado directamente con la toma de decisiones no cuenta con los estudios académicos específicos y acordes al puesto desempeñado; a pesar de ello, la administración de la entidad está completamente bien dirigida.

Finalmente, se concluye que es indispensable la implementación de estrategias de gestión de riesgo en las Organizaciones No Gubernamentales para evitar fraudes y garantizar la sostenibilidad en el mediano y largo plazo.

RECOMENDACIONES

De las conclusiones anteriores y con la finalidad de mejorar la gestión de riesgo en la era digital de la entidad se recomienda:

Fomentar una cultura de gestión de riesgos en toda la organización, tanto en el área financiera como informática asegurando la participación de todos los colaboradores en la detección y reducción de riesgos.

Implementar la guía de gestión de riesgos que facilite la identificación, evaluación y monitoreo sistemático de los riesgos financieros en el área financiera.

Considerar la opción de contratar a un profesional de TI para el departamento de informática, a tiempo completo para supervisar la información financiera digital y garantizar un mejor control sobre los sistemas y datos.

Contratar a un auditor interno para analizar la eficacia del sistema de gestión de riesgos y asegurar el cumplimiento de las normativas y regulaciones pertinentes.

Crear un plan de capacitación que contemple las deficiencias detectadas, dando prioridad a los conocimientos y habilidades esenciales para el desempeño de las funciones

BIBLIOGRAFÍA

Asamblea Legislativa de la República de El Salvador, D. 1. (1963). Ley Impuesto sobre la renta. Art. 6.

Asamblea Legislativa de la República de El Salvador, D. 2. (1992). Ley de Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios. Art.93.

Asamblea Legislativa de la República de El Salvador, D. 4. (2000). *Ley Contra el Lavado de Dinero y de Activos y su Reglamento.*

Asamblea Legislativa de la República de El Salvador, D. 4. (2022). Ley de Emisión de Activos Digitales. Art.1.

Asamblea Legislativa de la República de El Salvador, D. 8. (1996). Ley de Asociaciones y Fundaciones sin Fines de Lucro. Art. 8.

Cabezas, N. G. (20 de Febrero de 2023). *www.ayudaenccion.org*. Obtenido de https://ayudaenaccion.org/blog/solidaridad/que-es-una-ong/

Domínguez, I. L. (20 de septiembre de 2023). *Expansión.com*. Obtenido de https://www.expansion.com/diccionario-economico/riesgo-de-tipo-de-interes.html

España, C. d. (2014). *CGRE*. Obtenido de https://www.clubgestionriesgos.org/secciones-informacion-riesgos/riesgo-de-credito/

(1984.). *Informe de la Comisión Nacional Bipartita Sobre Centroamérica.* Diana. México.

Insua, D. R., & Naveiro Flores, R. (2022). *Análisis de riesgos.* Madrid: CSIC.

ISO. (2018). Norma Internacional ISO 31000 Traducción Oficial. Vernier, Ginebra, Suiza.

José A. Soler Ramos, K. B. (1999). *Gestión de Riesgos Financieros. Un enfoque práctico para paises latinoamericanos.* Washintong D.C.: Banco Interamericano de Desarrollo.

LAS RECOMENDACIONES DEL GAFI. (Julio de 2023). *ESTÁNDARES INTERNACIONALES SOBRE LA LUCHA CONTRA EL LAVADO DE ACTIVOS, EL FINANCIAMIENTO DEL TERRORISMO, Y EL FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA.*

Ley de proteccion de datos personales y habeas DATA. (12 de 11 de 2024). *DECRETO 144*. San salvador: Asamblea Legislativa de la Republica de El Salvador.

Michel Tamayo Saborit, D. G. (2020). *La Gestión de Riesgos: herramienta estratégica de gestión empresarial.* ISBN: 978-959-257-572-1.

No380, F. G. (2003). Instructivo para la Prevención, Detección y Control del Lavado de Dinero y Activos, Financiación del Terrorismo y la Financiación Proliferación de Armas de Destrucción Masiva. Art. 5.

NRP-36. (10 de 10 de 2022). *NORMAS TÉCNICAS PARA LA GESTIÓN DE LOS RIESGOS DE LAVADO DE DINERO Y DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y LA FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA.*

Páez-Gabriuna, I., Sanabria, M., & Gauthier-Umaña, V. (2022). *Transformación digital en las organizaciones.* Rosario: Editorial Universidad del Rosario.

Ramos, J. A., Staking, K., Ayuso Calle, A., Beato, P., Botín O´Shea, E., Escrig Meliá, M., & Falero Carrasco, B. (1999). *Gestión de Riesgos Financieros, Un enfoque práctico para países latinoamericanos.* New York Avenue: Banco Interamericano de Desarrollo.

Salvador, A. L. (24 de junio de 2019). Ley de proteccion de datos personales y Habeas DATA. San Salvador, El salvador.

Soborit, M. T., González Capote, D., Mata Varela, M. d., Fornet Batista, J. D., & Cabrera Álvarez, E. N. (2020). *LaGestión de Riesgos: Herramienta Estratégica de Gestión Empresarial.* Cuba: Elitorial: "Universo Sur".

Unificas.com. (22 de julio de 2024). *Unificas*. Obtenido de https://www.unifikas.com/es/noticias/que-son-las-normas-iso

Ballarín, E. (2007). "Una aproximación a la historia de la cuantificación del riesgo: de la antigüedad al siglo XVIII" Disponible en : https://aeca.es/old/vi_encuentro_trabajo_historia_contabilidad/pdf/01_ballarin.pdf

Flórez Ríos, LS (2008). «Evolución de la teoría financiera en el siglo XX» . Disponible en: https ://www .redalyc .org /pdf /3290 /329027263004 .pdf

ANEXOS

ÍNDICE DE ANEXOS

Anexo 1

Guía de preguntas para el contador.

15. ¿Cuántos años tiene de trabajar en la institución?
16. ¿Qué nivel académico posee?
17. ¿Cuántos años de experiencia posee en la presentación de informes financieros?

Planeación:

18. ¿Cuáles son los principales riesgos para la generación de información financiera que enfrenta la ONG en la era digital?
19. ¿Cuáles son los principales aspectos contables que deben considerarse para la gestión de riesgo en la era digital?
20. ¿Cuáles son los errores contables más comunes que podrían surgir durante la gestión de riesgo en la era digital?

Ejecución:

21. ¿Cómo se realiza la revisión de los estados financieros de las ONG?
22. ¿Cuáles son los desafíos contables comunes durante la integración de sistemas financieros en de la gestión de riesgo en la era digital?
23. ¿Cómo coordina su trabajo con el Jefe de Informática para garantizar una evaluación integral de la gestión de riesgo de los estados financieros?

Control Interno:

24. ¿Cómo considera usted la evaluación y el fortalecimiento de controles internos en la administración de la ONG?
25. ¿Considera usted que la organización tiene herramientas tecnológicas que ayuden a la generación de información para la mitigación de riesgos financieros en la era digital?
26. ¿Qué controles tiene la empresa para prevenir el fraude financiero?
27. ¿Considera usted que la organización está monitoreando adecuadamente las actividades financieras para detectar fraudes?

Interacción con Otros Profesionales:

28. ¿Qué desafíos ha enfrentado en la colaboración con departamento de informática y cómo se han superado?

Anexo 2

Guía de preguntas para el director general

1. ¿Cuántos años tiene de trabajar en la institución?
2. ¿Qué nivel académico posee?
3. ¿Cuántos años de experiencia posee en la presentación de informes financieros?

Planeación:

4. ¿Cuál es la visión de la ONG sobre la gestión de riesgos financieros en la era digital?
5. ¿La ONG está dispuesta a invertir recursos para implementar nuevas tecnologías en la gestión de riesgos financieros?
6. ¿Cómo se asegura la empresa de que su cultura de gestión de riesgos está alineada con su estrategia general?

Ejecución:

7. ¿Cómo identifican en la ONG los riesgos financieros emergentes en el entorno digital?
8. ¿Cómo minimizan los riesgos financieros para que la ONG pueda enfocar sus recursos de manera efectiva?
9. ¿Cómo coordina su trabajo con el Sub Director y el jefe de Informática para garantizar una evaluación integral de la gestión de riesgos financieros?

Control Interno:

10. ¿Qué estrategias utiliza la ONG para mitigar los riesgos financieros?
11. ¿Qué herramientas y tecnologías están disponibles para ayudar a la ONG a gestionar sus riesgos financieros en la era digital?
12. ¿Qué controles tiene la empresa para prevenir el ciberataque en el área financiero?
13. ¿Cómo está monitoreando la empresa sus actividades financieras para detectar fraudes?

Interacción con Otros Profesionales:

14. ¿Cómo colabora con otras áreas de la ONG para gestionar los riesgos financieros en la era digital?

Anexo 3

Guía de preguntas para el subdirector administrativo y financiero

1. ¿Cuántos años tiene de trabajar en la institución?
2. ¿Qué nivel académico posee?
3. ¿Posee experiencia en toma de decisiones basadas en riesgos?

Planeación:

4. ¿Cuáles son los principales riesgos que enfrenta la ONG en la era digital?
5. ¿Cuáles son las áreas de la organización que considera dentro de la planeación para la gestión de riesgo en la era digital?
6. De las áreas mencionadas anteriormente ¿Cuáles son las que considera más vulnerables en cuanto a la gestión de riesgos en la era digital?

Ejecución:

7. ¿Cómo realiza la revisión o evaluación de los procesos operativos? ¿toma en cuenta el factor digital?
8. ¿Cuáles son los desafíos administrativos en cuanto a la gestión de riesgo en la era digital?
9. ¿Cómo coordina su trabajo con la dirección general para garantizar una toma de decisiones integral con enfoque basado en gestión de riesgo?
10. ¿Aplica normativa técnica para medir o gestionar el riesgo?

Interacción con Otros Profesionales:

11. ¿Ha gestionado, propuesto o ejecutado formación continua en gestión de riesgos para el personal de la organización?
12. ¿Qué áreas ha tomado en cuenta para la formación en gestión de riesgos?
13. ¿Con qué periodicidad se reciben las capacitaciones?

Anexo 4

Guía de preguntas para director de tecnología e información (DTI)

1. ¿Cuántos años tiene de trabajar en la institución?
2. ¿Qué nivel académico posee?
3. ¿Cuántos años de experiencia posee en la presentación de informes financieros?

Planeación:

4. ¿Cómo el departamento de informática implementa la medida de seguridad en la era digital que garanticé el uso de herramientas tecnológicas?
5. ¿Qué nuevas herramientas tecnológicas se está utilizando para gestionar los riesgos financieros en la era digital?
6. ¿Cómo se está comunicando los riesgos financieros en la era digital a las demás partes interesadas en la ONG?

Ejecución:

7. ¿Cómo realiza el departamento de informática la identificación y evaluación de los riesgos financieros en la era digital?
8. ¿Cómo está asegurando el departamento de informática que los sistemas y datos financieros estén protegidos contra ciberataques?
9. ¿Cómo coordina su trabajo con el Contador para garantizar una evaluación integral de la gestión de riesgo de los estados financieros?

Control Interno:

10. ¿Realizan ustedes autoevaluación de las medidas informáticas implementadas para garantizar el manejo de la información financiera?
11. ¿Qué herramientas y tecnologías están disponibles para ayudar a la ONG a gestionar sus riesgos financieros en la era digital?
12. ¿Qué controles tiene la empresa para prevenir el ciberataque en el área financiero?
13. ¿Participa el departamento de informática en el monitoreando las actividades financieras con el propósito de prevenir fraudes?

Interacción con Otros Profesionales:

14. ¿Cuenta el departamento de informática la colaboración con otras áreas de la ONG para gestionar los riesgos financieros en la era digital?