UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: Caso estudio Distribuidora AMC
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autora:
Ing. Jácome Tapia Verónica Fernanda
Tutor/a:
Mg. Toasa Guachi Renato Mauricio Ph.D. Maryory Urdaneta

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Toasa Guachi Renato Mauricio con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: **Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: Caso estudio Distribuidora AMC.**

Elaborado por: **Verónica Fernanda Jácome Tapia**, con C.I: 1722641683, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

Mg. Toasa Guachi Renato Mauricio

C.I: 1804724167

APROBACIÓN DEL TUTOR

Yo, Urdaneta Herrera Maryory con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: **Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: Caso estudio Distribuidora AMC.**

Elaborado por: **Verónica Fernanda Jácome Tapia**, con C.I: 1722641683, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Ph.D. Maryory Urdaneta Herrera

C.I: 1804724167

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, **Verónica Fernanda Jácome Tapia** con **C.I: 1722641683**, autora del proyecto de titulación denominado: **Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC.** Previo a la obtención del título de Magister en **Seguridad Informática**.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
VERONICA FERNANDA JACOME TAPIA

Ing. Verónica Fernanda Jácome Tapia

C.I: 1722641683

Tabla de contenidos

APROBACIÓN DEL TUTOR ii
APROBACIÓN DEL TUTOR iii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE iv
INFORMACIÓN GENERAL 5
Contextualización del tema 5
Problema de investigación 6
Objetivo general 7
Objetivos específicos 7
Vinculación con la sociedad y beneficiarios directos: 8
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO 9
1.1. Contextualización general del estado del arte 9
1.2. Proceso investigativo metodológico 10
1.2.1.- Enfoque de la investigación 10
1.2.2.- Tipos de investigación 10
1.2.3.- Población de estudio 11
1.2.4.- Recopilación de información 11
1.3. Análisis de resultados 11
CAPÍTULO II: PROPUESTA 20
2.1. Fundamentos teóricos aplicados 20
2.1.1. ISO/IEC 27005:2022 20
2.1.2. Vulnerabilidad 23
2.1.3. Amenaza informática 23
2.1.4. Riesgo 23
2.2. Descripción de la propuesta 24
a. Estructura general 24
b. Explicación del aporte 25
c. Estrategias y/o técnicas 26
2.3. Validación de la propuesta 28
2.4. Matriz de articulación de la propuesta 29
2.5. Análisis de resultados. Presentación y discusión. 31
2.5.1. Valoración de activos 31
2.5.2. Identificación de amenazas y estimación de riesgos 39
2.5.2. Valoración de riesgos 40

CONCLUSIONES 44
RECOMENDACIONES 45
BIBLIOGRAFÍA 46
ANEXOS 49

Índice de tablas

Tabla 1 *Seguridad informática* 12
Tabla 2 *Evaluación de riesgos* 13
Tabla 3 *Normativa ISO 27005:2022* 14
Tabla 4 *Vulneraciones al sistema informático* 15
Tabla 5 *Controles para mitigar vulnerabilidades* 16
Tabla 6 *Controles actuales para mitigar las vulnerabilidades* 17
Tabla 7 *Monitoreo continuo* 18
Tabla 8 *Estrategias de respuesta ante incidentes* 19
Tabla 9 Matriz de articulación 29
Tabla 10 *Activos primarios* 31
Tabla 11 *Activos de apoyo* 32
Tabla 12 *Identificación de activos* 33
Tabla 13 *Valoración de activos* 34
Tabla 14 *Valoración de Información (I)* 34
Tabla 15 *Valoración de Aplicaciones informáticas (AI)* 35
Tabla 16 *Valoración de equipos informáticos (EI)* 36
Tabla 17 *Evaluación de activos* 37
Tabla 18 *Valoración de activos* 38
Tabla 19 *Evaluación de activos* 38
Tabla 20 *Identificación de amenazas* 39
Tabla 21 *Valoración de riesgos* 40
Tabla 22 *Valoración de riesgos con amenazas de daño físico* 40
Tabla 23 *Valoración de riesgos de amenazas naturales* 41
Tabla 24 *Valoración de riesgos de amenazas de fallas en infraestructura* 41
Tabla 25 *Valoración de riesgos de amenazas de fallos técnicos* 42
Tabla 26 *Valoración de riesgos de amenazas de acciones humanas* 42
Tabla 27 *Valoración de riesgos de amenazas de comprometimiento de funciones o servicios* 43
Tabla 28 *Valoración de riesgos de amenazas organizativas* 43

Índice de figuras

Figura 1 *Seguridad informática* 12
Figura 2 *Evaluación de riesgos* 13
Figura 3 *Normativa ISO 27005:2022* 14
Figura 4 *Vulneraciones al sistema informático* 15
Figura 5 *Controles para mitigar vulnerabilidades* 16
Figura 6 *Controles actuales para mitigar las vulnerabilidades* 17
Figura 7 *Monitoreo continuo* 18
Figura 8 *Seguridad informática* 19
Figura 9 *Proceso de gestión del riesgo* 20
Figura 10 *Seguridad informática* 25
Figura 11 *Investigación en Acción* 27

INFORMACIÓN GENERAL

Contextualización del tema

La seguridad de la información ayuda a proteger la privacidad y los datos personales, lo que es esencial para cumplir con las leyes de protección de datos y preservar la confianza de los clientes y usuarios (Cordero, 2022). Es por eso que es necesario reconocer a la información como un activo valioso para cualquier organización, y su pérdida o compromiso puede tener consecuencias graves en términos de reputación, operaciones y competitividad (Agudelo, 2019).

En consecuencia, nace la necesidad de contar con un plan de mitigación de riesgos para identificar, evaluar y gestionar los posibles riesgos que pueden afectar a una organización (Fernández, 2021). Al hacer un análisis y formulación de riesgos, se pueden tomar medidas proactivas para reducir la probabilidad de que los riesgos ocurran, así como para minimizar su impacto en caso de que sucedan. Esto puede ayudar a proteger los activos, la reputación y la continuidad del negocio, y también puede contribuir a la seguridad y el bienestar de las personas involucradas. En resumen, un plan de mitigación de riesgos es fundamental para la gestión eficaz de cualquier situación potencialmente peligrosa (Gonzales, 2018).

Gracias al avance continuo de la tecnología, el comercio electrónico y las actividades que se relacionan con el manejo de información constituyen uno de los elementos esenciales para la competitividad y la rentabilidad de los negocios. Por otro lado, “las organizaciones están cada vez más expuestas a virus, gusanos, piratas informáticos e ingenieros sociales, es así que un 77.6% de todos los ataques que se producen en el mundo, están dirigidos a empresas, mientras que a particulares un 22.4%” (Granados, 2020, p. 24).

Por otro lado, en la investigación realizada por Páez (2021) se encontró que en la empresa donde se realizó el estudio “no posee implementado en su totalidad controles para el Sistema de Gestión de Seguridad de la Información (SGSI), debido a que tan solo poseen el 30% implementados en su totalidad, es decir un 60% están medianamente implementados, en proceso de implementación o sin implementarse” (p. 59).

En Ecuador se han desarrollado varios esfuerzos para tratar de proteger los datos y es por ello que se publicó el 26 de mayo del 2021 la Ley Orgánica de Protección de Datos Personales cuyo “objeto y finalidad es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos,

obligaciones y mecanismos de tutela" (Ley Orgánica de Protección de Datos Personales, 2021, p. 9).

De los resultados expuestos se tiene que gran parte de empresas en el Ecuador no cuentan con una adecuada implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), tal como lo afirma Puna (2021) en su investigación en donde afirma que en las microempresas de estudio "no se dispone de documentación ni políticas relacionadas a la seguridad de la información que producen este dato equivale al 84% del total, mientras que el 16% de los entrevistados que en número representan a 86 encuestados mencionaron que disponen ya sea documentación o alguna política para proteger su información" (p. 59).

Problema de investigación

Se han producido un número cada vez mayor de ataques a la seguridad de la información que amenazan a los datos que manejan las organizaciones, lo que causa "pérdidas significativas e incluso afectar su existencia continua" (Estrategia Nacional de Ciberseguridad del Ecuador, 2022, p. 8). Junto a los ataques de seguridad generados desde fuera de la organización para Cordero (2022) "por fuga de información técnica por parte de miembros de la organización" (p. 8); y por vulnerabilidades en la seguridad de datos (Raheman et al., 2022).

Para conocer la situación actual, se realizó una encuesta al Ing. Tapia encargado del departamento de TI de la empresa de lo que se obtuvo que en el contexto de seguridad la información fue vulnerada ya que la computadora principal se infectó con virus, también hubo perdida de documentación física, pero la información pudo ser recuperada gracias a los respaldos realizados.

Por otra parte, Tapia (2022) supo manifestar que luego del evento no se ha hecho ninguna aplicación de controles en la privacidad de datos lo que impide contar con una perspectiva real de la situación actual en la seguridad de la información e imposibilita la determinación de brechas de vulnerabilidad. De allí que es necesario hacer un análisis de riesgos para identificar las brechas de seguridad que existan, y de ahí hacer un plan de mitigación de riesgos es de suma importancia, para ello se utilizará la ISO 27005:2022.

Según Moran (2021) las empresas requieren que sus aplicaciones informáticas cumplan con estándares de seguridad de la información ya que son entidades de control y tiene a su disposición información de carácter confidencialidad (Estrategia nacional de ciberseguridad del Ecuador, 2022), la misma que necesita ser resguardada mediante políticas de seguridad

adecuadas que permitan salvaguardar estos activos críticos y de esta manera cumplir con el Sistema de Gestión de Seguridad de la Información (p. 3).

Con la investigación se pretende asegurar la información que la distribuidora AMC maneja, ya que es necesario tener los datos de proveedores, clientes y personal resguardados para evitar que personas inescrupulosas usen esos datos con fines fraudulentos; y así cumplir con el Art. 10 de la "Ley Orgánica de Protección de Datos"; la cual en el literal g establece la confidencialidad:

> El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio. (Ley Orgánica de Protección de Datos Personales, 2021, p. 10)

El artículo 10 de la "Ley Orgánica de Protección de Datos" se cumple con el debido aseguramiento del Sistema de Gestión de Seguridad de la Información (SGSI), y por eso al hacerse un análisis de riesgo se beneficia a la distribuidora AMC.

Objetivo general

Realizar una evaluación de riesgos para para el establecimiento de un enfoque sistemático de Gestión de Riesgos de Seguridad de la Información mediante la normativa ISO 27005:2022: Caso estudio Distribuidora AMC.

Objetivos específicos

- Realizar una investigación teórica sobre la evaluación de riesgos mediante la ISO 27005:2022 para conocer sobre la Gestión de Riesgos de Seguridad de la Información.
- Hacer un diagnóstico de los activos críticos de la distribuidora AMC con la finalidad de priorizar los que requieren la implementación de controles.
- Evaluar los riesgos asociados a los activos considerados como críticos mediante una matriz de riesgos basándose en la evaluación realizada con la Norma ISO 27005:2022.

- Validar la matriz de riesgos para la prevención de vulnerabilidades mediante la normativa ISO 27005:2022 a través de criterio de especialistas expertos en el tema de estudio

Vinculación con la sociedad y beneficiarios directos:

Para el correcto desarrollo de la investigación se toma como referencia el objetivo 9 de los ODS el cual está orientado a la industria, innovación e infraestructura, cuyo fin es "construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación para apoyar el desarrollo económico y el bienestar humano, con especial hincapié en el acceso equitativo y asequible para todos" (Naciones Unidas, 2015).

Además, al implementar medidas de seguridad en la información crítica, se pueden obtener varios beneficios para la Distribuidora AMC, así como para los trabajadores y clientes que trabajan en las diferentes áreas de la empresa. Entre los principales beneficios se tiene la seguridad en la protección de datos personales, ya que se puede salvaguardar la privacidad y proteger los datos personales de los individuos, lo que promueve la confianza en el uso de servicios en línea y aplicaciones que la distribuidora maneja en sus diferentes giros de negocio.

Por otro lado, al garantizar la seguridad de la información crítica, se reduce el riesgo de robo de identidad, fraude financiero y otros delitos cibernéticos que podrían afectar a la empresa. Estas medidas de seguridad en la información crítica contribuyen a la preservación de la estabilidad y la continuidad de servicios esenciales, como la infraestructura pública, los servicios de emergencia y otros sistemas vitales para la sociedad.

La seguridad en la información fomenta la confianza en las transacciones comerciales en línea, lo que beneficia tanto a los consumidores como a la empresa al reducir el riesgo de fraude y la pérdida de datos financieros. Finalmente, al poner en práctica estrategias y tecnologías de seguridad de la información, se fortalece la relación entre la sociedad y el entorno digital, proporcionando a los ciudadanos un entorno más seguro y confiable para interactuar, trabajar con la empresa de estudio.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

La seguridad de la información es de suma importancia debido a que la información personal y confidencial debe estar protegida para preservar la privacidad de las personas y evitar posibles usos indebidos o violaciones de privacidad. Por otro lado, la preservación de la integridad de los datos garantiza que los datos permanezcan íntegros, precisos y confiables, lo que es crucial para la toma de decisiones y el funcionamiento eficiente de las organizaciones.

Es esencial para proteger los activos digitales, preservar la confianza del cliente, cumplir con las normativas y salvaguardar la privacidad en un entorno cada vez más digitalizado y conectado. De allí que para la investigación se toman como referencia los siguientes trabajos:

La investigación realizada por Gonzales (2018) titulada "Diseño de un plan estratégico de seguridad de la información, mediante la aplicación de análisis de riesgos con la norma ISO/IEC 27005:2022. Caso de estudio INAMHI" en la que se encontró como principales hallazgos que mediante "la metodología planteada como ISO 27005:2022 con OCTAVE-S se logra establecer controles, procedimientos para mitigar el riesgo y gestionar la información de manera ordenada la seguridad de la información basado en riesgos". Esta investigación hace un gran aporte ya que mediante la metodología OCTAVE permite establecer un modelo viable para la identificación de riesgos mediante la normativa ISO 27005:2022, además permite que todos los miembros de la organización asuman la responsabilidad de lo que implica la seguridad de la información que se maneja dentro de la empresa o institución.

Por otro lado, la investigación realizada por Tuabanda (2023) titulada "Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO 27001; A9 control de acceso" se encontró que "la utilización de controles tales como generación de accesos, firewall de contenidos permitirán mejorar la calidad de seguridad informática evitando filtración de información y brindando al personal administrativo, docentes y estudiantes la navegación segura", de ahí que se sustenta la necesidad d implementar seguridades en las empresas ya que en la actualidad la información es uno de los bienes más importantes para cualquier organización (Tuabanda, 2023).

De acuerdo a la investigación realizada por Cevallos (2023) indica que "es necesario identificar los riesgos que se presenten en cada uno de los procesos de la compañía y realizar un análisis y evaluación de cada uno de ellos, para tomar las acciones necesarias" (p. 29). De allí

que la identificación de procesos en la empresa es importante para la identificación de activos en la empresa.

Otro de los trabajos tomados como referencia se tiene la investigación realizada por Cueva (2022) indica que “la comunidad se conecta a la red Wi-Fi para hacer documentos legales delicados y transferencias bancarias sin usar ninguna protección, a esto se agrega que muchos de los usuarios desconocen de algún protocolo de seguridad o protección a nivel de la infraestructura que les permita navegar de manera segura a través de la red” (Cueva, 2022, p. 49).

1.2. Proceso investigativo metodológico

1.2.1.- Enfoque de la investigación

El enfoque para la presente investigación es mixto es decir cualitativo debido a que se procede a hacer una entrevista para conocer la situación actual de la empresa de estudio. También se considera que es cuantitativo ya que mediante este se pretende obtener datos que puedan ser tabulados para Hernández et al. (2014) “el enfoque cuantitativo utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población” (p. 165). Es decir, se obtendrán cifras que ayuden a la “evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC”.

1.2.2.- Tipos de investigación

Para el desarrollo de la presente investigación se considera una investigación de tipo bibliográfica debido a que se utilizara fuentes confiables como lo son revistas, papers, artículos científicos para la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC. Bernal (2010), indica que: “La investigación documental es aquella que se celebra través de la consulta de documentos (libros, revistas, publicaciones periódicas, anualmente, registros, etc.). Toda investigación requiere de una revisión exhaustiva de las fuentes de consulta” (p. 50).

También, se considera una investigación de campo ya que la información utilizada para la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información se la obtiene directamente de la Distribuidora AMC que es el lugar de estudio.

Finalmente, se considera una investigación descriptiva ya que según Hernández et. al (2014) señalan que una "investigación descriptiva consiste en presentar la información tal cual es, indicando cual es la situación en el momento de la investigación analizando, interpretando, imprimiendo, y evaluando lo que se desea". Es decir, se utiliza para la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC.

1.2.3.- Población de estudio

Para elaborar la propuesta de evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC, se considera como población de estudio a los trabajadores de la Distribuidora AMC la cual posee 20 empleados. No se tomará muestra y se procederá a trabajar con toda la población ya que es pequeña.

1.2.4.- Recopilación de información

La información relacionada con la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC, es obtenida mediante una revisión documental que permita identificar los riesgos a los cuales está expuesta la empresa mediante la normativa ISO 27005:2022.

Para la recolección de información se utiliza cómo técnica de investigación la encuesta, la misma que permite conocer la situación actual de la empresa. El instrumento usado para la recolección de datos es un cuestionario conformado por ocho preguntas. La encuesta es aplicada a los 20 trabajadores con preguntas cerradas las mismas que poseen una escala de Likert para su respuesta (ver Anexo 1).

También se considera un análisis documental con la finalidad de recolectar la información necesaria para realizar la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC con información que proporciona el estado actual del SGSI de la empresa de estudio.

1.3. Análisis de resultados

Una vez aplicadas las encuestas se procede a hacer la tabulación de las mismas como se muestra a continuación:

Pregunta 1: ¿Ha escuchado sobre el término seguridad informática?

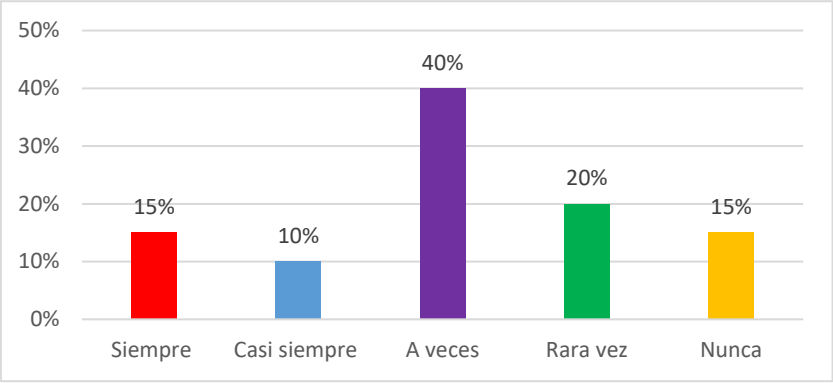
Tabla 1

Seguridad informática

	Frecuencia	Porcentaje
Siempre	3	15%
Casi siempre	2	10%
A veces	8	40%
Rara vez	4	20%
Nunca	3	15%
Total	**20**	**100%**

Figura 1

Seguridad informática



Análisis e interpretación:

Al investigar sobre si los encuestados han escuchado el término seguridad informática (figura 1) se encontró que el 15% lo ha escuchado siempre, el 10% casi siempre, el 40% lo ha hecho a veces, el 20% rara vez y el restante 15% nunca lo ha hecho. Estos resultados evidencian que gran parte de empleados desconocen sobre el término seguridad informática es por ello que no todos los empleados toman acciones para proteger los activos digitales, garantizar la continuidad del negocio, cumplir con las regulaciones y mantener la confianza del cliente en un entorno cada vez más interconectado y digitalizado.

Pregunta 2: ¿Con que frecuencia ha escuchado el término evaluación de riesgos en la empresa?

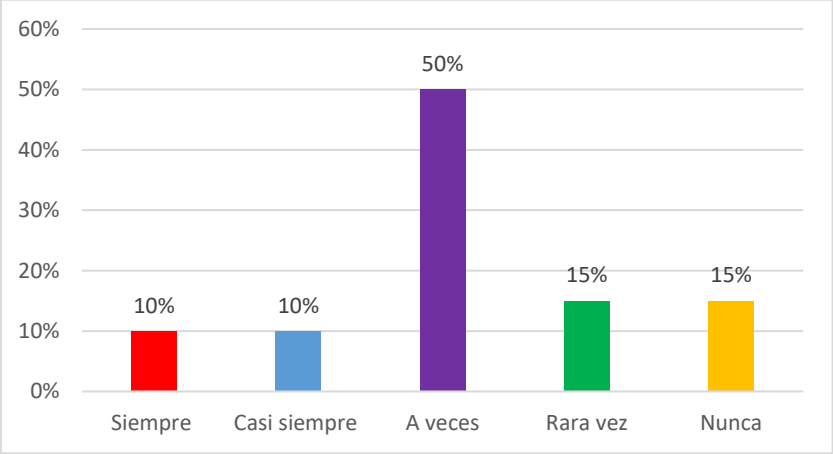
Tabla 2

Evaluación de riesgos

	Frecuencia	Porcentaje
Siempre	2	10%
Casi siempre	2	10%
A veces	10	50%
Rara vez	3	15%
Nunca	3	15%
Total	**20**	**100%**

Figura 2

Evaluación de riesgos



Análisis e interpretación:

Los datos obtenidos de la pregunta dos relacionada con la frecuencia ha escuchado el término evaluación de riesgos de la figura 2 se obtuvo que el 10% lo han escuchado siempre, el otro 10% casi siempre, el 50% a veces, el otro 15% rara vez y el restante 15% nunca lo han escuchado.

La mayor parte de entrevistados afirman haber escuchado el término evaluación de riesgos y esto se da debido a que en la empresa han ocurrido eventos en los cuales se ha comprometido la información de clientes y estudiantes.

Pregunta 3: ¿Ha escuchado sobre la normativa ISO 27005?

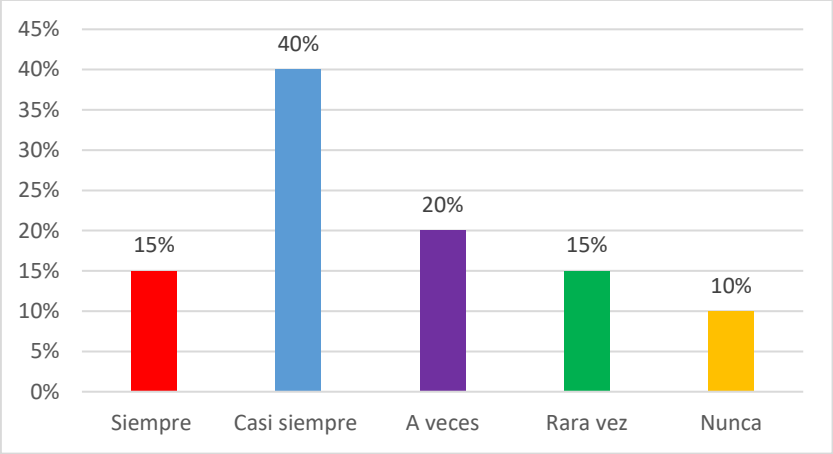
Tabla 3

Normativa ISO 27005:2022

	Frecuencia	Porcentaje
Siempre	3	15%
Casi siempre	8	40%
A veces	4	20%
Rara vez	3	15%
Nunca	2	10%
Total	**20**	**100%**

Figura 3

Normativa ISO 27005:2022



Análisis e interpretación:

Con respecto a la normativa ISO 27005:2022 se encontró que el 15% de encuestados siempre han escuchado sobre la normativa, el 40% casi siempre, el 20% a veces, el 15% rara vez y el restante 10% nunca lo ha escuchado como se muestra en la figura 3.

Los empleados aseguran conocer sobre la normativa ISO 27005:2022 y esto es debido a los eventos por los cuales la empresa ha tenido que pasar luego de haber sufrido vulneraciones en su información y datos que esta maneja.

Pregunta 4: ¿Con que frecuencia ha existido vulneraciones al sistema informático de la empresa?

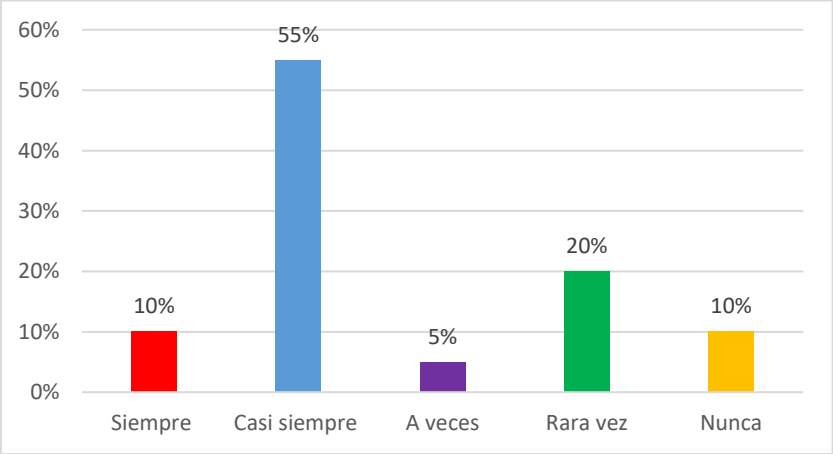
Tabla 4

Vulneraciones al sistema informático

	Frecuencia	Porcentaje
Siempre	2	10%
Casi siempre	11	55%
A veces	1	5%
Rara vez	4	20%
Nunca	2	10%
Total	**20**	**100%**

Figura 4

Vulneraciones al sistema informático



Análisis e interpretación:

El 10% de encuestados afirman que siempre ha existido vulneraciones en el sistema informático, otro 55% afirman que casi siempre, el 5% a veces, un 20% lo han hecho rara vez y el restante 10% nunca lo ha notado como se muestra en la figura 4.

Las vulneraciones al sistema de la empresa comprometieron su funcionamiento y se perdió la información relacionada con clientes, así como información de estados financieros, procesos e informes importantes que pararon a la empresa por varias semanas.

Pregunta 5: ¿En la empresa se han implementado controles para mitigar vulnerabilidades?

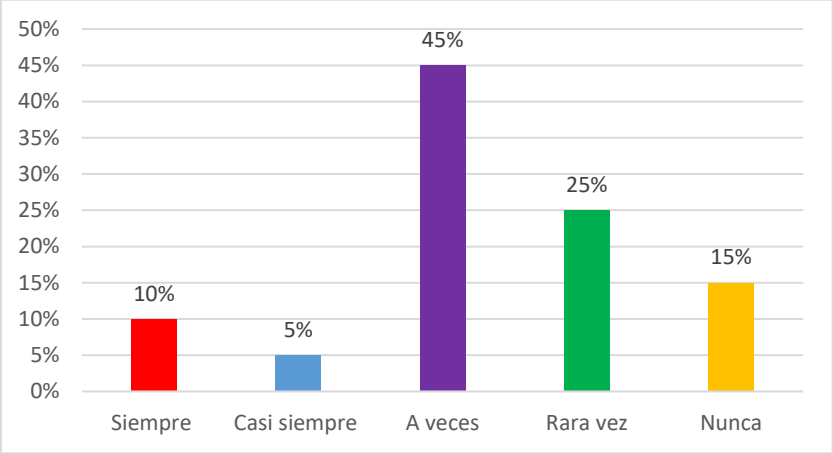
Tabla 5

Controles para mitigar vulnerabilidades

	Frecuencia	Porcentaje
Siempre	2	10%
Casi siempre	1	5%
A veces	9	45%
Rara vez	5	25%
Nunca	3	15%
Total	**20**	**100%**

Figura 5

Controles para mitigar vulnerabilidades



Análisis e interpretación:

Al investigar si se han implementado controles para mitigar vulnerabilidades de la figura 5 se obtuvo que el 10% lo ha hecho casi siempre, el 5% lo ha hecho casi siempre, el 45% a veces, el 25% rara vez y el restante 15% nunca lo han hecho.

En la empresa los controles implementados para mitigar vulnerabilidades son ineficientes lo que hace que se tomen acciones con la finalidad de proteger los activos de la organización, para así mantener la confianza del cliente, cumplir con las regulaciones y garantizar la continuidad del negocio en un entorno cada vez más digital y conectado.

Pregunta 6: ¿Considera que son suficientes los controles actuales para mitigar las vulnerabilidades?

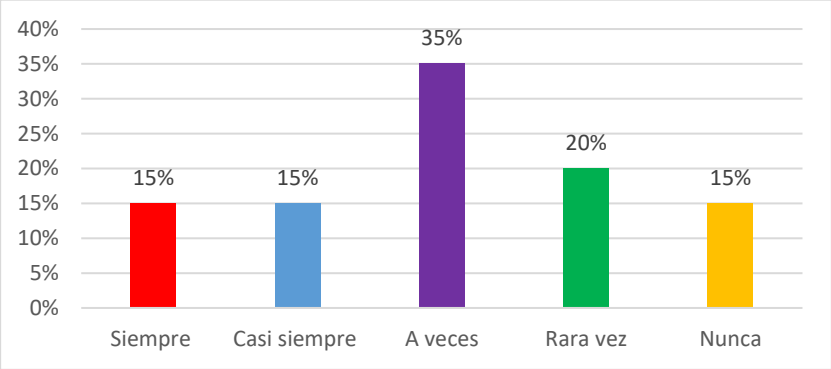
Tabla 6

Controles actuales para mitigar las vulnerabilidades

	Frecuencia	Porcentaje
Siempre	3	15%
Casi siempre	3	15%
A veces	7	35%
Rara vez	4	20%
Nunca	3	15%
Total	**20**	**100%**

Figura 6

Controles actuales para mitigar las vulnerabilidades



Análisis e interpretación:

Una vez realizada la encuesta se encontró que el 15% consideran que siempre son suficientes los controles actuales para mitigar las vulnerabilidades, el otro 15% lo han hecho casi siempre, el 35% lo han hecho a veces, el otro 20% rara vez y el restante 15% nunca, como se muestra en la figura 6.

La mayor parte de empleados consideran que los controles actuales implementados para mitigar vulnerabilidades son insuficientes, de ahí que es importante considerar que los ataques cibernéticos pueden interrumpir las operaciones comerciales normales, lo que resulta en tiempo de inactividad costoso y pérdida de ingresos. Los controles de seguridad ayudan a garantizar la continuidad del negocio al reducir la probabilidad de interrupciones causadas por brechas de seguridad.

Pregunta 7: ¿En la empresa se realiza el monitoreo continuo para asegurar la información que esta maneja?

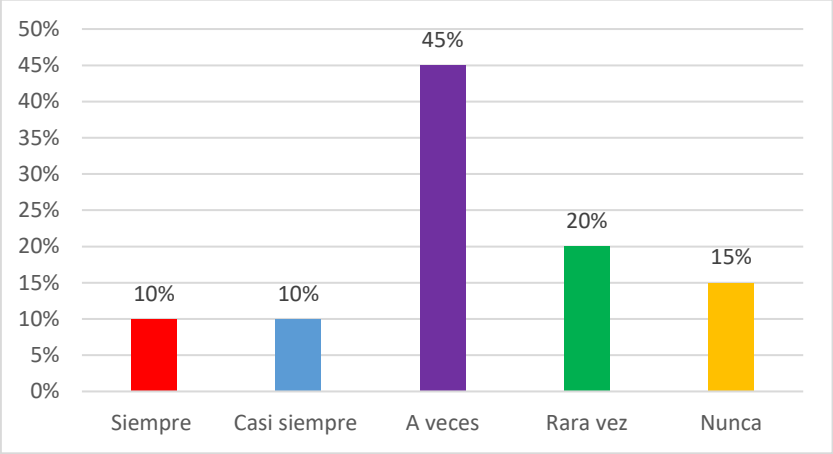
Tabla 7

Monitoreo continuo

	Frecuencia	Porcentaje
Siempre	2	10%
Casi siempre	2	10%
A veces	9	45%
Rara vez	4	20%
Nunca	3	15%
Total	**20**	**100%**

Figura 7

Monitoreo continuo



Análisis e interpretación:

Al investigar si en la empresa se realiza el monitoreo continuo para asegurar la información que esta maneja se encontró que el 10% lo han hecho casi siempre, el 10% casi siempre, el 45% lo ha hecho a veces, el 20% lo ha hecho rara vez y el restante 15% nunca lo han hecho (figura 7).

En la empresa no se ha hecho un monitoreo continuo para asegurar la información, de ahí que es importante que se considere que este es esencial para proteger los activos de información de una empresa, detectar y prevenir amenazas cibernéticas, cumplir con las regulaciones de seguridad y mantener la confianza del cliente en un entorno digital en constante evolución.

Pregunta 8: ¿Considera que es necesario implementar estrategias de respuesta ante incidentes en caso de que una vulnerabilidad sea explotada?

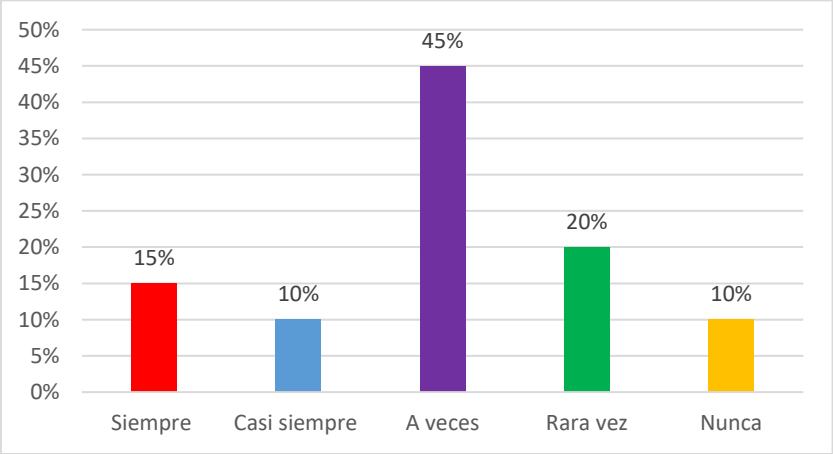
Tabla 8

Estrategias de respuesta ante incidentes

	Frecuencia	Porcentaje
Siempre	3	15%
Casi siempre	2	10%
A veces	9	45%
Rara vez	4	20%
Nunca	2	10%
Total	**20**	**100%**

Figura 8

Seguridad informática



Análisis e interpretación:

Al investigar sobre si es necesario implementar estrategias de respuesta ante incidentes en caso de que una vulnerabilidad sea explotada se encontró que el 15% lo hace siempre, el 10% casi siempre, el 45% a veces, el 20% rara vez y el restante 10% nunca lo hacen, como se muestra en la figura 8.

Los encuestados consideran que se debería implementar estrategias de respuesta ante incidentes relacionados con vulnerabilidades para así evitar ataques cibernéticos que puedan interrumpir las operaciones comerciales normales, así como evitar inactividad costosa y pérdida de ingresos.

CAPÍTULO II: PROPUESTA

A continuación, se hace una recopilación teórica para que sustenten la investigación relacionada con la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC.

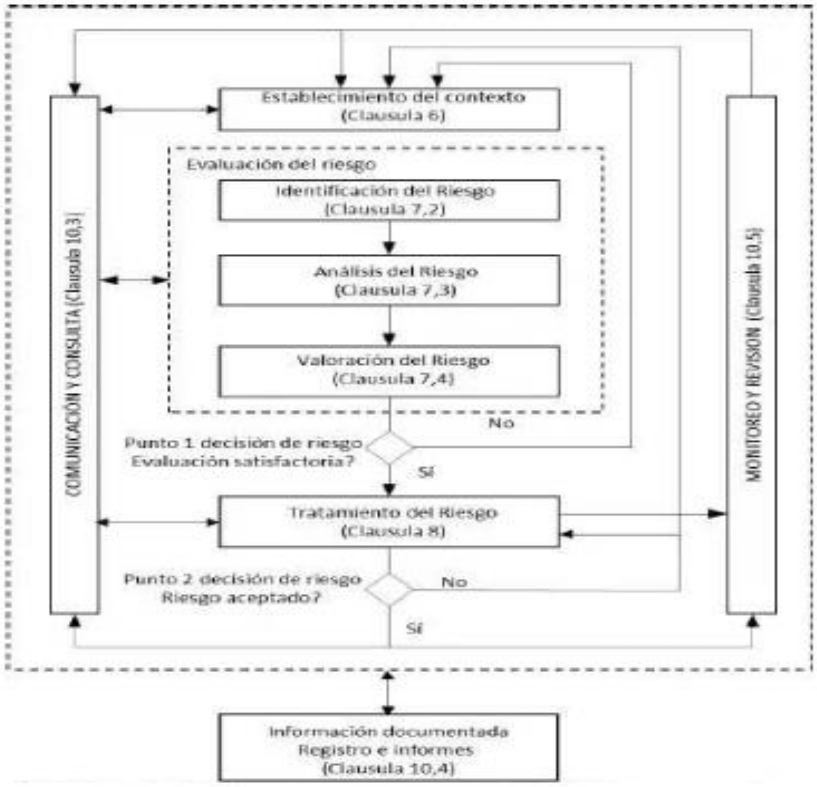
2.1. Fundamentos teóricos aplicados

2.1.1. ISO/IEC 27005:2022

ISO/IEC 27005:2022 proporciona soporte para los conceptos generales especificados en "ISO/IEC 27001 e ISO/IEC 27002 para la comprensión completa de la norma". Se puede aplicar a todo tipo de organizaciones que necesiten salvaguardar su información. En la normativa se considera el proceso de la figura 9 para la gestión del riesgo, como se muestra a continuación: (ISO/IEC 27002, 2011)

Figura 9

Proceso de gestión del riesgo



Nota: En la figura se muestra el proceso establecido en la normativa ISO 27005:2022 para el proceso de gestión de riesgo. Tomado de ISO 27005 (2022).

En la figura se muestra el proceso iterativo de evaluación de riesgos y las actividades de tratamiento en la normativa. Primero se empieza por la evaluación del contexto establecido, luego se realiza la identificación de riesgos. Se continua con el análisis de los mismos para obtener la información suficiente y de esta manera realizar la evaluación de los mismos y finalmente tomar las acciones necesarias "para modificar los riesgos a un nivel aceptable, luego se sigue el tratamiento de riesgos. Si la información no es suficiente, se realiza otra iteración con un contexto revisado" (Gonzales, 2018).

La eficacia del tratamiento de riesgos depende de los resultados de su evaluación. "Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual". Este es el caso cuando es necesaria otra iteración con cambios en los parámetros del contexto. La actividad de aceptación de riesgos debe garantizar que los riesgos residuales sean aprobados explícitamente por los directores de la organización.

Según lo indicado en la normativa se empieza por la **etapa 1:** En la cual se establece el contexto como se detalla a continuación: (ISO/IEC 27002, 2011).

1) Actividad 1: Establecimiento del Alcance: "El alcance se determina en relación con las características de la empresa, la organización, ubicación, bienes y tecnología". El alcance de las entidades del sector público dependerá directamente de su presupuesto y tamaño. La gestión de riesgos debe realizarse a todos los procesos críticos que son esenciales para el cumplimiento de los objetivos estratégicos de la organización.

2) Actividad 2: Selección de Procesos Críticos: "Para iniciar con el proceso, es importante tener en cuenta la información y documentación de la organización relacionada con la planificación estratégica y los procesos existentes". Es importante indicar que la participación del personal de la organización es indispensable. Esta actividad se logra a través de encuestas, entrevistas, visitas a las instalaciones y otras actividades que permitan recolectar la información necesaria.

3) Actividad 3: Descripción de Criterios de Evaluación: Este paso se establece como una metodología cualitativa para la estimación de riesgos. La estimación cualitativa utiliza las escalas ya establecidas para describir la probabilidad de ocurrencia de las amenazas. "Para evaluar el impacto en el negocio de la organización, es necesario determinar las consecuencias que pueden resultar de la pérdida de confidencialidad, integridad o disponibilidad de los activos".

El riesgo se define como la medida de la probabilidad y gravedad de los efectos adversos. Considerando como probabilidad cualquier ocurrencia hipotética de un evento y está condicionada a un conocimiento previo.

Etapa 2: Identificación de riesgos

Se necesita un marco de evaluación de riesgos con un enfoque para categorizar y compartir información sobre los riesgos de TI. Además, los riesgos deben identificarse claramente; no basta con hacer referencia a las probabilidades y al valor esperado. Por lo tanto, la identificación de riesgos debe hacerse detalladamente para que los resultados sean los esperados.

1) Actividad 1: Identificación de Activos: Los activos pueden ser documentos en papel, documentos electrónicos, aplicaciones, bases de datos, personas, equipos de TIC, "infraestructura y servicios externos o procesos subcontratados. La información almacenada en los activos puede verse afectada por los riesgos en tres aspectos principales: confidencialidad, integridad y disponibilidad". Se debe identificar el conjunto de activos de información, es decir, se debe identificar cualquier elemento que represente valor para los procesos previamente seleccionados en el alcance. Al identificar los activos, también es necesario identificar a sus propietarios, es decir, la persona o unidad organizativa responsable de cada activo. En resumen, es necesario identificar los activos, su categoría general, su categoría específica y su propietario y asociar esta información al proceso organizacional.

2) Actividad 2: Valoración de activos críticos: Como se mencionó anteriormente, las tres dimensiones de la información que pueden sufrir ataques son la confidencialidad, la integridad y la disponibilidad. Para contribuir a un mejor proceso de toma de decisiones y garantizar una correcta gestión de riesgos, los riesgos más importantes deben cuantificarse y analizarse de acuerdo con los criterios de aceptación definidos. Por ello, para priorizar los riesgos se identifican los activos más importantes. Los propietarios calificarán los activos desde la perspectiva de las tres dimensiones de la seguridad de la información y según "el nivel de impacto en una escala del 1 al 5, siendo 5 la calificación más alta. La tasación de activos se realizará para cada proceso crítico, detallando todos los activos involucrados e identificando al propietario y la categoría específica a la que pertenece". Las calificaciones se promedian y se obtiene una puntuación única por activo.

2.1.2. Vulnerabilidad

La vulnerabilidad se define como una debilidad que se desencadena accidental o intencionalmente. La debilidad en la seguridad o los controles de los activos puede ser aprovechada por amenazas. Las vulnerabilidades generalmente son un problema técnico, pero a veces los incidentes fueron causados por humanos; por ejemplo, el empleado usa una contraseña débil que es vulnerable a ataques. de un extraño. A veces, sin previo aviso o conocimiento, alguien descarga software sin saber que contiene código malicioso. Tanto la organización como los productos de la organización son vulnerables a las amenazas (Hamita et al., 2020).

La identificación de vulnerabilidades es esencial para la implementación de los estándares ISO/IEC 27005:2022 mediante el uso de controles para mitigar la vulnerabilidad identificada y proteger los activos mediante medidas preventivas, correctivas o de detección. Cuando no se ejerce ninguna vulnerabilidad, no hay riesgo de una fuente de amenaza (Gonzales, 2018).

2.1.3. Amenaza informática

Una amenaza se define como cualquier acción potencial que pueda causar daño o pérdida a un servicio o producto. Se ve como una acción, una acción potencial o ninguna acción que puede causar daño y daño que se puede dividir en amenazas naturales, amenazas humanas y amenazas ambientales. El número de amenazas humanas en incidentes de seguridad y privacidad está creciendo. También se considera amenaza informática a cualquier evento, acción o circunstancia que pueda causar daño, comprometer la integridad, la confidencialidad o la disponibilidad de los sistemas de información, los datos o las redes de una organización. Estas amenazas pueden provenir de diversas fuentes, como individuos malintencionados, malware, errores humanos, desastres naturales, entre otros (Hamita et al., 2020).

2.1.4. Riesgo

El riesgo se define como una incertidumbre que podría afectar a uno o más objetivos. Para que un riesgo esté presente en el sistema, una amenaza debe explotar una vulnerabilidad a través de cualquier acción potencial y causar daños o pérdidas a los activos. Es importante entender qué significa riesgo en la seguridad de los sistemas de información. Para identificar fácilmente los riesgos de seguridad, es necesario conocer o identificar los activos, las posibles amenazas a los activos y las vulnerabilidades explotadas por estas amenazas. El análisis de

riesgos es la parte más compleja en la implementación de ISO/IEC 27005:2022 (Hamita et al., 2020).

El origen del acceso no autorizado puede ser por amenazas externas e internas; Debido al control de acceso inadecuado, la organización quedó expuesta a acceso no autorizado a sus datos importantes. Las amenazas internas, como los usuarios autorizados, pueden representar un riesgo para la organización si no se controlan adecuadamente. Siempre que la red se ve comprometida, los intrusos, como los piratas informáticos, pueden atacar fácilmente el sistema. Los riesgos de las amenazas externas e internas son muy costosos, pérdida de credibilidad, la reputación de la organización está en riesgo y pérdida de participación de mercado. Los riesgos incluyen la divulgación no autorizada de información confidencial, la interrupción de los servicios, la pérdida de productividad de los empleados, pérdidas financieras, implicaciones legales de los clientes, el público o los inversores, y puede ocurrir chantaje al amenazar con exponer información confidencial (Gonzales, 2018).

2.2. Descripción de la propuesta

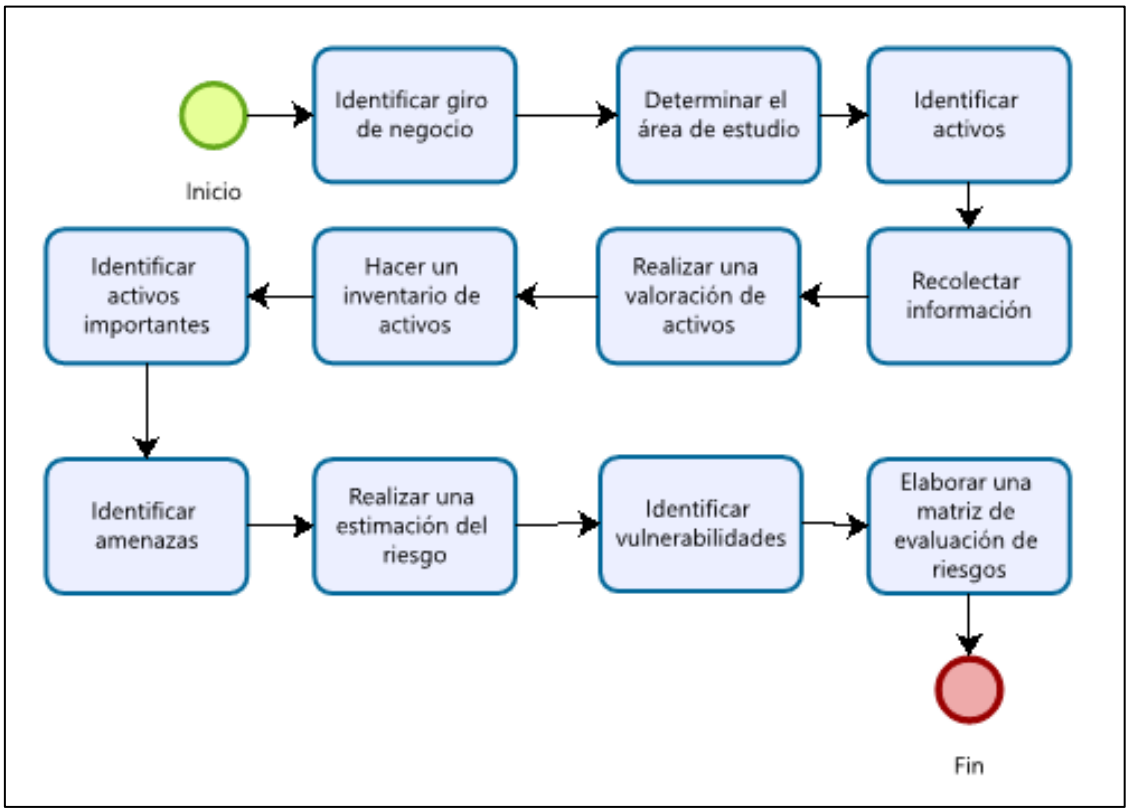
A continuación, se desarrolla la investigación iniciando con la identificación de activos, la valoración, estimación de riesgos, análisis de vulnerabilidades y finalmente la evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC:

a. Estructura general

Para el desarrollo adecuado de la Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC se toma como referencia la figura 10 mostrada a continuación:

Figura 10

Seguridad informática



b. Explicación del aporte

Para el desarrollo de la presente investigación se inicia de la siguiente manera:

Estudio de negocio:

Mediante el estudio de negocio se pretende conocer el giro de negocio de la empresa, además este paso ayuda a entender cuáles son los documentos considerados cómo importantes dentro de la organización. Ayuda a entender la información que la empresa maneja y el tratamiento que hay que darle a la misma.

Determinación de área de estudio:

Una vez entendido el negocio se evalúa el área en la que se va a realizar la investigación y es aquí en donde se define el alcance y el procedimiento a seguir dependiendo del área de estudio.

Identificación de activos:

Mediante este paso puede hacer un inventario de activos que refleje todos aquellos que se relacionan con el manejo de la información dentro del área de estudio.

Valoración de activos:

Una vez identificada la organización, segregada el área de estudio y conociendo los activos se continua con la valoración de activos a través de juicio de expertos para conocer aquellos que son considerados como importantes para la organización.

Identificación de amenazas

Mediante la identificación de amenazas que se detalla en la ISO 27005:2002 se las puede evaluar dependiendo de las categorías que esta normativa detalla.

Estimación de riesgo

La estimación de riesgo se la realiza según las categorías indicadas en la normativa y a través de cálculos matemáticos.

Matriz de valoración de ISO 27005:2022

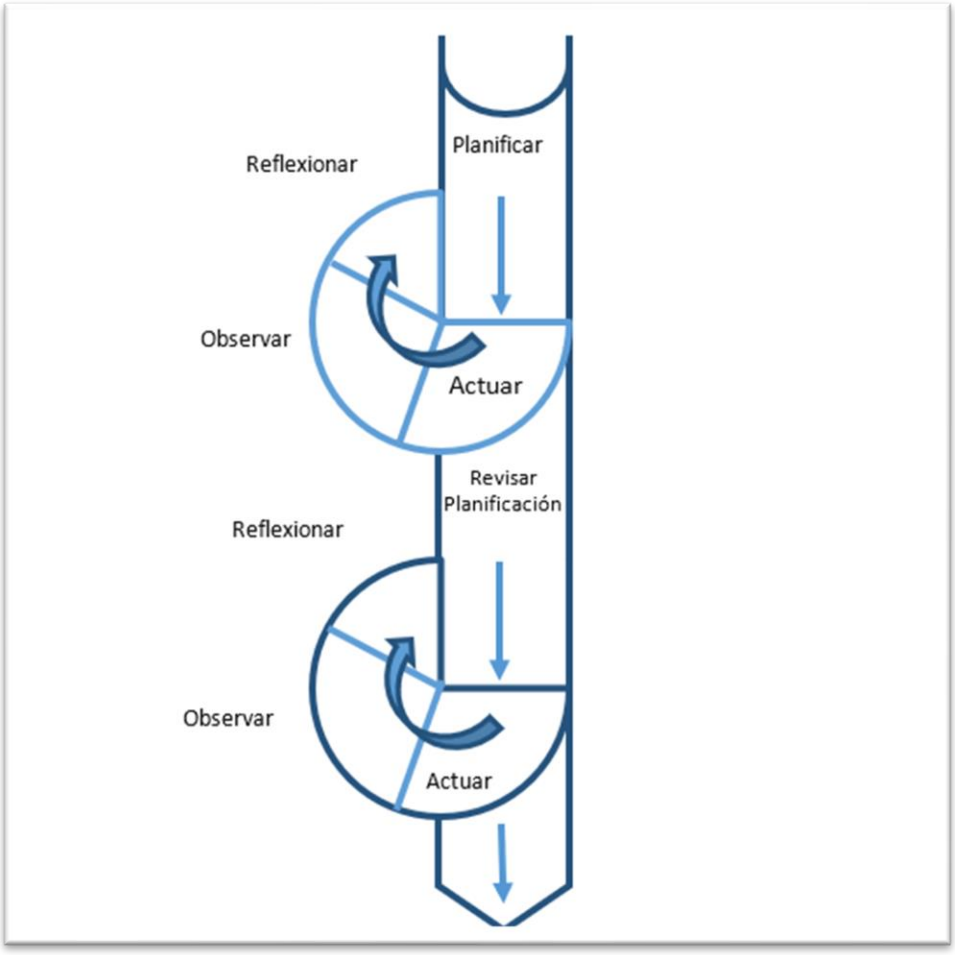
Finalmente se implementa una matriz basada en la ISO 27005:2022 en la cual se detalla todo el proceso desde el inventario de activos, valoración de activos, análisis y evaluación, plan de acción.

c. Estrategias y/o técnicas

Para la construcción del presente producto se tomó como referencia la metodología Investigación en Acción (Action Research) descrita por Baskerville y Wood Harper (1996), mostrada en la figura 11.

Figura 11

Investigación en Acción



Nota: Modelo de investigación en acción según Baskerville y Wood-Harper. Tomado de Baskerville & Wood-Harper (p. 3), 1996

La descripción general de la metodología a usarse se detalla a continuación:

Planificación e Identificación del Problema

En esta etapa se identifica los problemas específicos o las áreas de mejora en la gestión de riesgos de seguridad de la información dentro de la organización. Esta fase involucra la consulta con partes interesadas para comprender sus preocupaciones y expectativas.

Planificación

Basado en la identificación del problema, se procede a elaborar un plan de acción que detalle cómo se aplicarán los principios de ISO/IEC 27005 para gestionar los riesgos. Define objetivos claros, pasos específicos y criterios de éxito.

Actuar

En esta etapa se lleva a cabo las actividades de gestión de riesgos siguiendo los pasos de ISO/IEC 27005, que incluyen identificación, evaluación, tratamiento y monitoreo de riesgos.

Observar y reflexionar

Aquí se analiza los datos recopilados para evaluar la efectividad de las estrategias de gestión de riesgos. Identifica qué aspectos están funcionando bien y cuáles necesitan ajustes.

Revisar planificación

En esta etapa se realiza el análisis y la reflexión, ajustes en el plan de acción. Esto puede implicar revisar las estrategias de tratamiento de riesgos, mejorar los controles, o ajustar los métodos de evaluación.

2.3. Validación de la propuesta

La validación de la propuesta será realizada por medio de juicio de expertos tales como la Mgtr. Mónica Vargas la cual es una experta en seguridad informática. Desempeña el cargo de jefe de TI en una minera, la cual consideró que el proyecto está bien estructurado y puede servir de base para la gestión de riesgos en cualquier empresa que desee implementar esta ISO como seguridad para la protección de la información. (Anexo 2)

El Mgtr. Jaime Salgado en su validación también consideró que el trabajo se encuentra bien estructurado y presenta buenas bases parala implementación de la normativa en la gestión de riesgos en las diferentes empresas. (Anexo 3)

.

2.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 9

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
ISO/IEC 27005:2022	Proporciona las directrices para la gestión del riesgo en la seguridad de la información en una organización, ayuda a dar soporte al Sistema de Gestión de Seguridad de la Información (SGSI).	Enfoque cualitativo	Investigación bibliográfica	El conocer sobre la normativa ayuda a implementarla de manera adecuada, y de esta manera poder definir el enfoque de la gestión del riesgo	Revisión Documental
Valoración de activos	La valoración de activos es crucial para una gestión efectiva de riesgos, la protección de la información crítica de la organización y el cumplimiento de las regulaciones de seguridad. Proporciona una base sólida para la toma de decisiones estratégicas y la asignación de recursos en materia de seguridad de la información. (Agudelo Mira, 2019)	Enfoque cuantitativo	Investigación de campo, observación	El conocer los activos ayuda a identificar los más importantes para la organización, y de esta manera poder definir el enfoque de la gestión del riesgo	Observación

Vulnerabilidad	La vulnerabilidad se define como una debilidad que se desencadena accidental o intencionalmente. (Hamita et al., 2020)	Enfoque cuantitativo	Investigación de campo	Es importante identificar las vulnerabilidades para reducir el riesgo de explotación por parte de los atacantes y a proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos de la organización	Revisión Documental
Riesgo	Los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las consecuencias pueden ser muy graves en relación a la información que se está manejando. (Muñoz et al., 2019)	Enfoque cuantitativo	Investigación bibliográfica	El conocer el riesgo es esencial para proteger los activos de información de una organización, garantizar la continuidad del negocio, cumplir con las regulaciones de seguridad y mantener la confianza del cliente en un entorno cada vez más digital y conectado.	Revisión Documental
Matriz de gesti{on de riesgos	Un plan de mitigación de riesgos es una herramienta crucial para gestionar los riesgos de una organización de manera efectiva, reduciendo la probabilidad de ocurrencia de eventos adversos y minimizando su impacto potencial en los objetivos y operaciones de la empresa. (Raheman et al., 2022)	Enfoque cualitativo	Investigación bibliográfica y de campo	Elaborar un plan de mitigación ayuda a gestionar los riesgos, reduciendo la probabilidad de ocurrencia.	Revisión Documental

*Nota***:** Elaboración propia

2.5. Análisis de resultados. Presentación y discusión.

2.5.1. Valoración de activos

En el Anexo A.2.2 de la norma ISO 27005:2022 Se encuentra relacionado con los activos y permite evaluar el riesgo que se relaciona a estos. De ahí que los activos pueden ser de carácter primario o de apoyo, para el cumplimiento de los objetivos se inicia con la valoración de activos mostrada a continuación en la tabla 10.

Tabla 10

Activos primarios

Código de Activo	Área/ Subproceso	Clase de Activo	Tipo de Activo	Nombre de Activo	Intención del Uso	Propietario del activo (Cargo)
AP001	Sección Desarrollo Técnico GIS	Primario	Servidor 1	Servidor 1	Procesos internos del negocio	Ingeniero de Sistemas
AP002	Sección Desarrollo Técnico GIS	Primario	Servidor 2	Servidor 2	Procesos internos del negocio	Ingeniero de Sistemas
AP003	Sección Desarrollo Técnico GIS	Primario	Laptop	Laptop 1	Procesos internos del negocio	Ingeniero de Sistemas
AP004	Sección Desarrollo Técnico GIS	Primario	Pc	Computadora de escritorio 1	Procesos internos del negocio	Ingeniero de Sistemas

En la tabla 11 se detallan los activos considerados como importantes para la institución que son 4 computadoras de uso general y un servidor en donde se recopila toda la información considerada como importante tanto de docentes, padres de familia y estudiantes.

Tabla 11

Activos de apoyo

Código de Activo	Área/ Subproceso	Clase de Activo	Tipo de Activo	Nombre de Activo	Intención del Uso	Propietario del activo (Cargo)
A001	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 1	Es usado por el público en general	Ingeniero de Sistemas
A002	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 2	Es usado por el público en general	Ingeniero de Sistemas
A003	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 3	Es usado por el público en general	Ingeniero de Sistemas
A004	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 4	Es usado por el público en general	Ingeniero de Sistemas
A005	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 5	Es usado por el público en general	Ingeniero de Sistemas
A006	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 6	Es usado por el público en general	Ingeniero de Sistemas
A007	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 7	Es usado por el público en general	Ingeniero de Sistemas
A008	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 8	Es usado por el público en general	Ingeniero de Sistemas
A009	Sección Desarrollo Técnico GIS	De apoyo	Laptop	Laptop 1	Sistema para Facturación	Contador
A010	Sección Desarrollo Técnico GIS	De apoyo	Laptop	Laptop 2	Sistema de Diseño	Diseñador
A011	Sección Desarrollo Técnico GIS	De apoyo	Copiadora Ricoh MP5000	Copiadora 1	Sistema de Diseño	Diseñador
A012	Sección Desarrollo Técnico GIS	De apoyo	Copiadora Ricoh MPC35002	Copiadora 2	Sistema de Diseño	Diseñador
A013	Sección Desarrollo Técnico GIS	De apoyo	Copiadora Ricoh MPC30000	Copiadora 3	Sistema de Diseño	Diseñador
A014	Sección Desarrollo Técnico GIS	De apoyo	Impresora Epson L3250	Impresora 1	Sistema de Diseño	Diseñador

Código de Activo	Área/ Subproceso	Clase de Activo	Tipo de Activo	Nombre de Activo	Intención del Uso	Propietario del activo (Cargo)
A015	Sección Desarrollo Técnico GIS	De apoyo	Plotter de Impresión 1,60 m	Plotter de impresión	Sistema de Diseño	Diseñador
A016	Sección Desarrollo Técnico GIS	De apoyo	Plotter de corte 1,5 m	Plotter de corte	Sistema de Diseño	Diseñador
A017	Sección Desarrollo Técnico GIS	De apoyo	Cortadora laser 30x20 cm	Cortadora Laser	Sistema de Diseño	Diseñador

Para el análisis y valoración de activos se los clasifica en tres categorías que son: Información en la que se agrupan aquellos activos que manejan la información de la empresa, Aplicaciones informáticas que se manejan en la empresa y Equipos informáticos. Categorías que se indican en la tabla 12.

Tabla 12

Identificación de activos

Categoría	Activo
Información (I)	Datos de clientes Datos de empleados Datos de procesos internos de la empresa
Aplicaciones informáticas (AI)	Windows 11 Windows 10 Windows 7 Windows server Office 2024 Office 2019 Office 2016q Maintopq Cura Photqoshop Ilustrador Corell Drawn Laser DRW Inventor Autocad
Equipos informáticos (EI)	Copiadoras Impresoras Router Computadoras de escritorio Computadoras personales Servidor

En el apartado 7.2.1 de la normativa titulado “Proceso de evaluación de los riesgos para la seguridad para la seguridad de la información” se indica que se “deben identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información” (IEC/ISO 27005, 2012). La valoración considerada para la investigación se detalla a continuación en la tabla 13.

Tabla 13

Valoración de activos

Disponibilidad		
Valor	**Criterio**	**Escala**
0	No aplica/ no es relevante	Bajo
1	Debe estar disponible al menos el 50% del tiempo	Medio
2	Debe estar disponible al menos el 90% del tiempo	Alto
3	Siempre debe estar disponible	Crítico
Integridad		
Valor	**Criterio**	
0	No aplica/ no es relevante	Bajo
1	Tiene que estar correcto o completo al menos en un 60%	Medio
2	Tiene que estar correcto o completo al menos en un 85%	Alto
3	Tiene que estar correcto o completo al menos en un 99%	Crítico
Confidencialidad		
Valor	**Criterio**	
0	No aplica/ no es relevante	Bajo
1	Daños relevantes, afectan a varios dispositivos	Medio
2	Daños considerables, afectan a casi todos los dispositivos	Alto
3	Daños catastróficos, afectan la imagen y reputación de la empresa	Crítico

Una vez establecida la escala para la valoración de activos se procede a evaluar cada, con el fin de identificar los riesgos a los que se encuentren expuestos. En las categorías señaladas la primera valoración se la realiza a la información(I), como se puede observar en la tabla 14.

Tabla 14

Valoración de Información (I)

Datos clientes	
Dimensión	**Valor**
Disponibilidad	2
Integridad	3
Confidencialidad	3
Datos de empleados	
Dimensión	**Valor**
Disponibilidad	1
Integridad	3
Confidencialidad	3

Datos de procesos internos de la empresa	
Dimensión	**Valor**
Disponibilidad	3
Integridad	3
Confidencialidad	3

A continuación, se hace la valoración de aplicaciones informáticas con las que se trabaja en la empresa como se muestra en la tabla 15.

Tabla 15

Valoración de Aplicaciones informáticas (AI)

Windows 11	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	0
Windows 10	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	0
Windows 7	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	0
Windows server	
Dimensión	**Valor**
Disponibilidad	3
Integridad	3
Confidencialidad	3
Office 2024	
Dimensión	**Valor**
Disponibilidad	2
Integridad	2
Confidencialidad	2
Office 2019	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	1
Office 2016	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	1
Maintop	
Dimensión	**Valor**
Disponibilidad	1
Integridad	1
Confidencialidad	0

Cura	
Dimensión	**Valor**
Disponibilidad	1
Integridad	1
Confidencialidad	0
Photoshop	
Dimensión	**Valor**
Disponibilidad	1
Integridad	1
Confidencialidad	0
Ilustrador	
Dimensión	**Valor**
Disponibilidad	1
Integridad	1
Confidencialidad	0
Corell Drawn	
Dimensión	**Valor**
Disponibilidad	2
Integridad	1
Confidencialidad	0
Laser DRW	
Dimensión	**Valor**
Disponibilidad	2
Integridad	1
Confidencialidad	0
Inventor	
Dimensión	**Valor**
Disponibilidad	2
Integridad	1
Confidencialidad	0
Autocad	
Dimensión	**Valor**
Disponibilidad	2
Integridad	1
Confidencialidad	0

Luego se procede a hacer la valoración de equipos informáticos (EI), como se muestra en la tabla 16.

Tabla 16

Valoración de equipos informáticos (EI)

Copiadoras	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	0

Impresoras	
Dimensión	**Valor**
Disponibilidad	3
Integridad	2
Confidencialidad	0

Router	
Dimensión	**Valor**
Disponibilidad	3
Integridad	3
Confidencialidad	0
Computadoras de escritorio	
Dimensión	**Valor**
Disponibilidad	3
Integridad	3
Confidencialidad	3
Computadoras personales	
Dimensión	**Valor**
Disponibilidad	3
Integridad	3
Confidencialidad	3
Servidor	
Dimensión	**Valor**
Disponibilidad	3
Integridad	3
Confidencialidad	3

Una vez terminada la valoración de activos se procede con su evaluación, para ello se considera los aspectos de la tabla 17.

Tabla 17

Evaluación de activos

Aspecto	**Abreviatura**	**Descripción**
Ámbito	Amb	Información (I), Aplicaciones informáticas (AI), Equipos informáticos (EI)
Función	Fun	Se relaciona con la importancia de los bienes informáticos al realizar una tarea.
Costo	Cos	Considera el valor económico y valor de uso de los bienes informáticos.
Imagen	Img	Repercusión interna y/o externa que ocasionaría la pérdida de los bienes informáticos.
Confidencialidad	Con	Se considera como la necesidad de proteger la información.
Integridad	Int	Se relaciona con que la información no se modifique o destruya.
Disponibilidad	Dsp	Los bienes informáticos deben puedan dar la información adecuada solo a las personas autorizadas.
Importancia	Imp	Se obtiene de la suma de la función, costo, imagen, confidencialidad, integridad y disponibilidad.

En la tabla 18 se indica la escala a usarse para la valoración de activos según la escala de Likert indicado en la ISO 27005 “insignificante, muy bajo, bajo, medio, alto, muy alto y crítico” (IEC/ISO 27005, 2012).

Tabla 18

Valoración de activos

Criterio	Valor
Bajo	0
Medio	1
Alto	2
Crítico	3

Según Páez (2019) “la importancia de los bienes informáticos se calcula mediante el promedio de la función, costo, imagen, confidencialidad, integridad y disponibilidad” (p. 34); como se indica en la tabla 19.

$$Imp = \frac{Fun + CoS + Im + Con + Int + Disp}{6}$$

Tabla 19

Evaluación de activos

Activo	Amb	Fun	Co	Img	Con	Int	Dsp	Imp
Datos de clientes	I	3	3	3	3	3	3	3.00
Datos de empleados	I	2	2	3	3	2	2	2.33
Datos de procesos internos	I	3	3	3	3	3	3	3.00
Windows 11	AI	2	2	1	3	2	3	2.16
Windows 10	AI	2	2	1	3	2	3	2.16
Windows 7	AI	2	2	1	3	2	3	2.16
Windows server	AI	3	3	3	3	3	3	3.00
Office 2024	AI	2	2	1	3	2	3	2.16
Office 2019	AI	2	2	1	3	2	3	2.16
Office 2016	AI	2	2	1	3	2	3	2.16
Maintop	AI	2	2	1	0	2	1	1.33
Cura	AI	2	2	1	0	2	1	1.33
Photoshop	AI	2	2	1	0	2	1	1.33
Ilustrador	AI	2	2	1	0	2	1	1.33
Corell Drawn	AI	2	2	1	0	2	1	1.33
Laser DRW	AI	2	2	1	0	2	1	1.33
Inventor	AI	2	2	1	0	2	1	1.33
Autocad	AI	2	2	1	0	2	1	1.33
Copiadoras	EI	2	2	1	0	2	1	1.33
Impresoras	EI	2	2	1	0	2	1	1.33
Router	EI	3	3	3	3	3	3	3.00
Computadoras de escritorio	EI	1	2	2	1	1	3	1.66
Computadoras personales	EI	1	2	2	1	1	3	1.66
Servidor	EI	3	3	3	3	3	3	3.00

Luego de hacer la valoración de activos se tiene que los bienes considerados como críticos relacionados con la información son los datos de clientes, datos de procesos internos. En relación con aplicaciones informáticas se tiene Windows server y en relación con equipos informáticos se tiene el servidor.

2.5.2. Identificación de amenazas y estimación de riesgos

Los bienes informáticos críticos que necesitan ser resguardados son datos de clientes, datos de procesos internos, Windows server y el servidor, para ello se procede a identificar las amenazas que se relacionan a estos según las categorías indicadas en la ISO 27005 como se indica en la tabla 20.

Tabla 20

Identificación de amenazas

CATEGORIA	AMENAZA
Amenazas físicas (AF)	Fuego Agua Accidente grave Explosión
Amenazas naturales (AN)	Fenómeno climático Fenómeno sísmico Fenómeno volcánico Inundación Pandemia/fenómeno epidémico
Fallas en infraestructura (FI)	Fallo de un sistema de suministro Pérdida de suministro eléctrico Fallo de una red de telecomunicaciones
Fallos técnicos (FT)	Fallo del dispositivo o sistema Saturación del sistema de información Violación de la mantenibilidad del sistema de información
Acciones humanas (AH)	Ingeniería Social Interceptación de comunicaciones privadas Robo de soportes o documentos Robo de equipos Recuperación de medios reciclados o desechados. Divulgación de información Manipulación de hardware Manipulación de software Tratamiento no autorizado de datos personales Uso no autorizado de dispositivos Dispositivos o medios dañinos Uso de software falsificado o copiado Tratamiento ilegal de datos
Comprometimiento de funciones o servicios (CF)	Error en uso Abuso de derechos o permisos Falsificación de derechos o permisos Denegación de acciones
Amenazas organizativas (AO)	Falta de personal Falta de recursos Fallo de los proveedores de servicios Violación de leyes o reglamentos

Nota: En la tabla se muestran los diferentes tipos de amenazas. Tomado de ISO 27005 (2022). Creación propia

2.5.2. Valoración de riesgos

Con las amenazas detalladas en la Tabla 20 se procede a hacer la valoración de riesgos, para ello se toma como referencia la valoración detallada en la Tabla 21, que se toma como referencia de la ISO 27005.

Tabla 21

Valoración de riesgos

Criterio	Valor		
Riesgo bajo	0	-	2
Riesgo medio	3	-	5
Riesgo alto	6	-	8

También se considera el peso, que se obtiene del producto del riesgo total por la importancia.

$$Peso = Riesgo\ total * Importancia$$

Para iniciar se considera el daño físico de los bienes considerados como críticos; como se observa en la tabla 22.

Tabla 22

Valoración de riesgos con amenazas de daño físico

Ámbito	Activo	Amenazas (Ocurrencia)				Riesgo total	Importancia	Peso
		AF1	AF2	AF3	AF4			
Información (I)	Datos de clientes	2	2	6	3	3.25	3.00	9.75
	Datos de procesos internos	2	2	6	3	3.25	3.00	9.75
Aplicaciones Informáticas (AI)	Windows Server	4	3	5	3	3.75	3.00	11.25
Equipos informáticos (EI)	Router	6	4	6	4	5.00	3.00	15.00
	Servidor	6	4	6	4	5.00	3.00	15.00
						Total	**9.00**	**60.75**

Una vez obtenido el peso e importancia se procede a hacer el cálculo del peso total como se indica a continuación:

$$Peso_{total} = \frac{Peso}{Importancia}$$

$$Peso_{total} = \frac{60.75}{9.00} \qquad Peso_{total} = 6.75$$

De acuerdo a la valoración de riesgos se tiene un riesgo alto de que ocurran amenazas físicas. El mismo proceso se lo realiza para cada campo de amenazas detalladas anteriormente. Se continua

con la evaluación de amenazas naturales de los bienes considerados como críticos como se observa en la tabla 23.

Tabla 23

Valoración de riesgos de amenazas naturales

Ámbito	Activo	Amenazas (Ocurrencia)					Riesgo total	Importancia	Peso
		AN1	AN2	AN3	**AN4**	**AN5**			
Información (I)	Datos de clientes	2	2	3	2	3	2.40	3.00	7.20
	Datos de procesos internos	2	2	2	3	3	2.40	3.00	7.20
Aplicaciones Informáticas (AI)	Windows Server	4	3	3	2	3	3.00	3.00	9.00
Equipos informáticos (EI)	Router	3	4	2	3	4	3.20	3.00	9.60
	Servidor	3	2	4	3	4	3.20	3.00	9.60
							Total	**9.00**	**42.60**

$$Peso_{total} = 4.73$$

De acuerdo a los datos obtenidos se tiene que existe un riesgo medio de que ocurran amenazas naturales. Se continua con la evaluación de que ocurran fallas en la infraestructura como se muestra en la tabla 24.

Tabla 24

Valoración de riesgos de amenazas de fallas en infraestructura

Ámbito	Activo	Amenazas (Ocurrencia)			Riesgo total	Importancia	Peso
		FI1	FI2	FI3			
Información (I)	Datos de clientes	2	3	2	2.66	3.00	7.98
	Datos de procesos internos	2	3	2	2.66	3.00	7.98
Aplicaciones Informáticas (AI)	Windows Server	2	3	3	2.66	3.00	7.98
Equipos informáticos (EI)	Router	3	2	2	2.33	3.00	6.99
	Servidor	3	2	3	2.33	3.00	6.99
					Total	**9.00**	**37.92**

$$Peso_{total} = 4.21$$

E la valoración realizada se obtuvo que existe un riesgo medio de que ocurran amenazas relacionadas con fallas en la infraestructura. Luego se realiza la evaluación de fallos técnicos de los bienes considerados como críticos como se observa en la tabla 25.

Tabla 25

Valoración de riesgos de amenazas de fallos técnicos

Ámbito	Activo	Amenazas (Ocurrencia)			Riesgo total	Importancia	Peso
		FT1	FT2	FT3			
Información (I)	Datos de clientes	1	1	6	2.66	3.00	7.98
	Datos de procesos internos	1	2	6	3.00	3.00	7.98
Aplicaciones Informáticas (AI)	Windows Server	2	2	6	3.33	3.00	9.99
Equipos informáticos (EI)	Router	1	1	6	2.66	3.00	7.98
	Servidor	3	2	6	3.66	3.00	10.98
					Total	**9.00**	**44.91**

$$Peso_{total} = 4.99$$

De la valoración realizada se tiene que existe un riesgo medio de que ocurran amenazas de fallos técnicos con un 4.99. Luego se procede a realizar el análisis con las amenazas de acciones humanas a los bienes considerados como críticos como se observa en la tabla 26.

Tabla 26

Valoración de riesgos de amenazas de acciones humanas

Ámbito	Activo	Amenazas (Ocurrencia)											Riesgo total	Importancia	Peso
		AH1	AH2	AH3	**AH4**	AH5	AH6	AH7	AH8	AH9	AH10	AH11			
Información (I)	Datos de clientes	5	5	8	1	8	6	8	8	3	8	3	5.72	3.00	17.16
	Datos de procesos internos	6	6	8	1	8	6	8	8	3	8	3	5.90	3.00	17.70
Aplicaciones Informáticas (AI)	Windows Server	4	6	8	1	6	6	3	6	2	8	3	4.81	3.00	14.43
Equipos informáticos (EI)	Router	1	6	8	3	2	6	3	6	2	8	3	4.36	3.00	13.08
	Servidor	1	6	8	3	6	6	3	8	2	8	3	4.90	3.00	14.70
													Total	**9.00**	**77.07**

$$Peso_{total} = 8.56$$

De acuerdo a la valoración de riesgos se tiene un riesgo alto de que ocurran amenazas relacionadas con los factores humanos. Se continua con la evaluación de comprometimiento de funciones o servicios de los bienes considerados como críticos como se observa en la tabla 27.

Tabla 27

Valoración de riesgos de amenazas de comprometimiento de funciones o servicios

Ámbito	Activo	Amenazas (Ocurrencia)				Riesgo total	Importancia	Peso
		CF1	CF2	CF3	**CF4**			
Información (I)	Datos de clientes	5	2	1	2	2.50	3.00	7.50
	Datos de procesos internos	5	2	1	3	2.75	3.00	8.25
Aplicaciones Informáticas (AI)	Windows Server	4	2	1	2	2.25	3.00	6.75
Equipos informáticos (EI)	Router	3	2	1	3	2.25	3.00	6.75
	Servidor	2	2	1	3	2.00	3.00	6.00
						Total	**9.00**	**35.25**

$$Peso_{total} = 3.91$$

De acuerdo a la valoración de riesgos se tiene un riesgo medio de que ocurran amenazas de comprometimiento de funciones o servicios. Luego se procede a hacer la evaluación de amenazas organizativas de los bienes considerados como críticos como se observa en la tabla 28.

Tabla 28

Valoración de riesgos de amenazas organizativas

Ámbito	Activo	Amenazas (Ocurrencia)				Riesgo total	Importancia	Peso
		AO1	AO2	AO3	AO4			
Información (I)	Datos de clientes	2	2	6	1	2.75	3.00	8.25
	Datos de procesos internos	2	2	6	1	2.75	3.00	8.25
Aplicaciones Informáticas (AI)	Windows Server	3	2	6	1	3.00	3.00	9.00
Equipos informáticos (EI)	Router	1	2	6	1	2.50	3.00	7.50
	Servidor	2	2	6	1	2.75	3.00	8.25
						Total	**9.00**	**41.25**

$$Peso_{total} = 4.58$$

Una vez realizada la valoración de riesgos se tiene un riesgo medio de que ocurra amenazas organizativas. Una vez terminada la valoración de activos se tiene que de acuerdo a los datos obtenidos existe mayor riesgo en amenazas relacionadas con: Amenazas físicas y de factor humano. De allí nace la necesidad de elaborar un proceso de gestión de la seguridad de la información en donde se muestren los controles que se deben implementar en base al EGSI de la empresa AMC. (Anexo 4)

CONCLUSIONES

En la investigación realizada referente al Sistema de Gestión de Seguridad de la Información (SGSI) y la evaluación de riesgos mediante la ISO 27005 se encontró que la ISO 27005 permite encontrar los riesgos mediante sus 10 secciones en las cuales se establecen las consideraciones más importantes para evaluación del riesgo, así como su tratamiento, aceptación y monitoreo y mediante la cual se puede implementar adecuadamente el proceso de gestión de la seguridad de la información en la distribuidora AMC.

Entre los procesos críticos que maneja la Distribuidora, se tienen aquellos en los que se manipula la información de empleados y clientes, así como transacciones comerciales y esto concuerda con la valoración de activos para la implementación de la matriz de la ISO 27005.

En la evaluación de la ISO 27005 se encontró que existe mayor riesgo en amenazas relacionadas con: amenazas físicas y factor humano. Esto es evidente ya que los equipos que contienen la información considerada como importante de la distribuidora AMC no se encuentran en un lugar adecuado, es evidente la falta de planificación para la colocación de los equipos y su exposición a accidentes tales como fuego, agua, accidentes graves o exposiciones. De la misma manera en cuanto al factor humano se evidencia la falta de políticas y procesos adecuados especialmente en la capacitación de personal para evitar perdida de información.

En la evaluación de riesgos identificados mediante la ISO 27005 se encontró que los activos relacionados con la información presentan un riesgo alto de ahí que es necesario implementar controles relacionados con el EGSI.

RECOMENDACIONES

A continuación, se presentan las recomendaciones para la presente investigación:

Se recomienda que se define el alcance de la evaluación, identificando los activos críticos de información, procesos clave, y las responsabilidades dentro de la Distribuidora AMC. Para que este proceso sea implementado en todas las áreas de la empresa.

Como complemento a la investigación realizada se recomienda **que** se implemente un escáner de vulnerabilidades para detectar las debilidades que podrían ser explotadas por las amenazas identificadas, como configuraciones de seguridad deficientes, falta de capacitación del personal, o infraestructura obsoleta.

Para mejorar el análisis de riesgos se recomienda la evaluación de la probabilidad y el impacto de cada riesgo identificado. Mediante una matriz de riesgo para clasificar los riesgos en función de su gravedad.

Con la investigación realizad se recomienda implementar un plan de mitigación de riesgos en el que se defina las medidas de control necesarias para mitigar, transferir, evitar, o aceptar los riesgos identificados. Prioriza las acciones en función del impacto y la probabilidad.

Ajustar el enfoque de gestión de riesgos en función de los cambios en el entorno empresarial, nuevas amenazas o vulnerabilidades, y los resultados de las auditorías.

BIBLIOGRAFÍA

Agudelo Mira, D. (2019). *Propuesta para la implementación de un Plan de Gestión de Riesgos de Seguridad de la Información para el proceso misional de investigación Tecnológico de Antioquia TdeA - Investigación.* Tecnológico de Antioquia - Institución Universitaria. https://dspace.tdea.edu.co/bitstream/handle/tda/465/Propuesta%20para%20la%20implementacion.pdf?sequence=4&isAllowed=y

Baskerville, R. L., & Wood-Harper, T. (1996). A critical perspective on action research as a method for information systems research. *Journal of Information Technology, 11*, 235-245.

Bernal, C. (2010). *Metodología de la investigación.* Pearson. https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Cevallos Campaña, O. A. (2023). *Propuesta de un modelo de gestión de riesgos de la información en Servientrega Ecuador S.A.* Universidad Tecnológica Israel. https://repositorio.uisrael.edu.ec/bitstream/47000/3555/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-003.pdf

Cordero Núñez, M. G. (2022). *Políticas de seguridad de la información basadas en Normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco LTDA.* Ambato: Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/bitstream/123456789/34814/1/t1959si.pdf

Cueva Quintana, J. B. (2022). *Propuesta de un modelo de Sistema de Gestión de seguridad de la información parala Unidad Educativa Fray Jodoco Ricke bajo la norma ISO 27001.* Universidad Tecnológica Israel. file:///C:/Users/Aithana/Downloads/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2022-001.pdf

Dummanaboyina, C. (2020). Cyber segurity and its importance. *ResearchGate*. https://www.researchgate.net/publication/347439655_CYBER_SECURITY_AND_ITS_IMPORTANCE

Estrategia nacional de ciberseguridad del Ecuador. (2022). Ministerio de Telecomunicaciones y Sociedad de la Información. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Fernández Orozco, G. P. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.* Universidad de las Fuerzas Armadas ESPE. https://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf

Gonzales, D. (2018). *Diseño de un plan estratégico de seguridad de la información, mediante la aplicación de análisis de riesgos con la norma ISO/IEC 27005. Caso de estudio INAMHI.* Universidad Internacional SEK Ecuador. https://doi.org/https://doi.org/10.33890/innova.v3.n2.1.2018.672

Hamita, L. C., Sarkan, H. M., Mohd Azmi, N. F., Mohd, N. M., Chuprat, S., & Yahya, Y. (2020). Adopting an ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients from Data Theft. *International Journal on Advanced Science Engineering Information Technology, 10*(3), 914-919. https://typeset.io/pdf/adopting-iso-iec-27005-2011-based-risk-treatment-plan-to-vxglgpu9qy.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodologìa de la investigación (6a. ed.).* McGraw-Hill. https://academia.utp.edu.co/grupobasicoclinicayaplicadas/files/2013/06/Metodolog%C3%ADa-de-la-Investigaci%C3%B3n.pdf

IEC/ISO 27005. (2012). *Tecnología de la información - técnicas de seguridad - gestión del riesgo en la seguridad de la información* (Vol. 1). INEN.

Muñoz Hernández, H., Zapata Cantero, L. G., Requena Vidal, D. M., & Ricardo Villadiego, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia, 2*(1), 528-537. https://www.redalyc.org/articulo.oa?id=29063446029

Naciones Unidas. (21 de septiembre de 2015). *Objetivos de desarrollo sostenible*. https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Oña, C. (22 de octubre de 2022). Entrevista sobre la situación actual de la información en la Unidad Educativa Rumiñahui. (J. Verónica, Entrevistador)

Raheman, F., Bhagat, T., Vermeulen, B., & Van Daele, P. (2022). Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet, 238*(14). https://doi.org/https://doi.org/10.3390/fi14080238

Tuabanda Cayambe, J. E. (2023). *Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO27001; A9 control de acceso.* Universidad Israel. http://repositorio.uisrael.edu.ec/handle/47000/3562

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

UNIVERSIDAD TECNOLÓGICA ISRAEL
ESCUELA DE POSGRADOS "ESPOG"
MAESTRÍA EN SEGURIDAD INFORMÁTICA

El presente instrumento de investigación tiene como objetivo: "Elaborar un plan de mitigación de riesgos para la prevención de vulnerabilidades mediante la normativa ISO 27005:2022 caso estudio Distribuidora AMC".

INSTRUCCIONES: Marcar con una X en la casilla lo que mejor describa el logro de los indicadores propuestos en relación a la escala de Likert.

1. ¿Ha **escuchado sobre el término seguridad informática?**

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

2. ¿Con que frecuencia ha escuchado o utilizado un plan de mitigación de riesgos en la empresa?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

3. ¿Ha escuchado sobre la normativa ISO 27005?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

4. ¿Con que frecuencia ha existido vulneraciones al sistema informático de la empresa?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

5. ¿En la empresa se han implementado controles para mitigar vulnerabilidades?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

6. ¿Considera que son suficientes los controles actuales para mitigar las vulnerabilidades identificadas en la empresa?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

7. ¿En la empresa se realiza el monitoreo continuo para asegurar la información que esta maneja?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

8. ¿Considera que es necesario implementar estrategias de respuesta ante incidentes en caso de que una vulnerabilidad sea explotada?

- Siempre ☐
- Casi siempre ☐
- A veces ☐
- Rara vez ☐
- Nunca ☐

Anexo 2: Validación Mgtr. Mónica Vargas

Universidad Israel
ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Mónica Patricia Vargas Salazar
Título obtenido: Máster en Software con Mención Seguridades
C.I.: 1721851416
E-mail: monicavargas9@gmail.com
Institución de Trabajo: INSERCOMP
Cargo: Ingeniera de Datos
Años de experiencia en el área: 8 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC".

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	35				

Observaciones: El trabajo se encuentra correctamente implementado y debería de probarse en varias empresas para contrarrestar los resultados.

Recomendaciones: Indicar a mayor detalle las indicaciones para el uso de la Normativa.

Lugar, fecha de validación: Quito, 31 de agosto del 2024

Universidad Israel

ESPOG | Escuela de Posgrados

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en SEGURIDAD INFORMÁTICA, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

MONICA PATRICIA VARGAS SALAZAR

Firma del especialista
Mónica Patricia Vargas Salazar

Anexo 3: Validación Mgtr. Jaime Salgado

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Jaime Fernando Salgado Romero
Título obtenido: Magister en Ciberseguridad
C.I.: 1716970809
E-mail: jaimef.salgado@cnt.gob.ec
Institución de Trabajo: Corporación Nacional de Telecomunicaciones CNT EP
Cargo: Analista de Solución Técnica Corporativa
Años de experiencia en el área: 13 años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC".

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso		x			
TOTAL	34				

Observaciones: La propuesta es muy interesante sin embargo las indicaciones para la implementación de la Normativa son escasa.

Recomendaciones: Indicar a mayor detalle las indicaciones para el uso de la Normativa.

Lugar, fecha de validación: Quito, 31 de agosto del 2024

Universidad Israel

ESPOG | Escuela de Posgrados

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en SEGURIDAD INFORMÁTICA, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

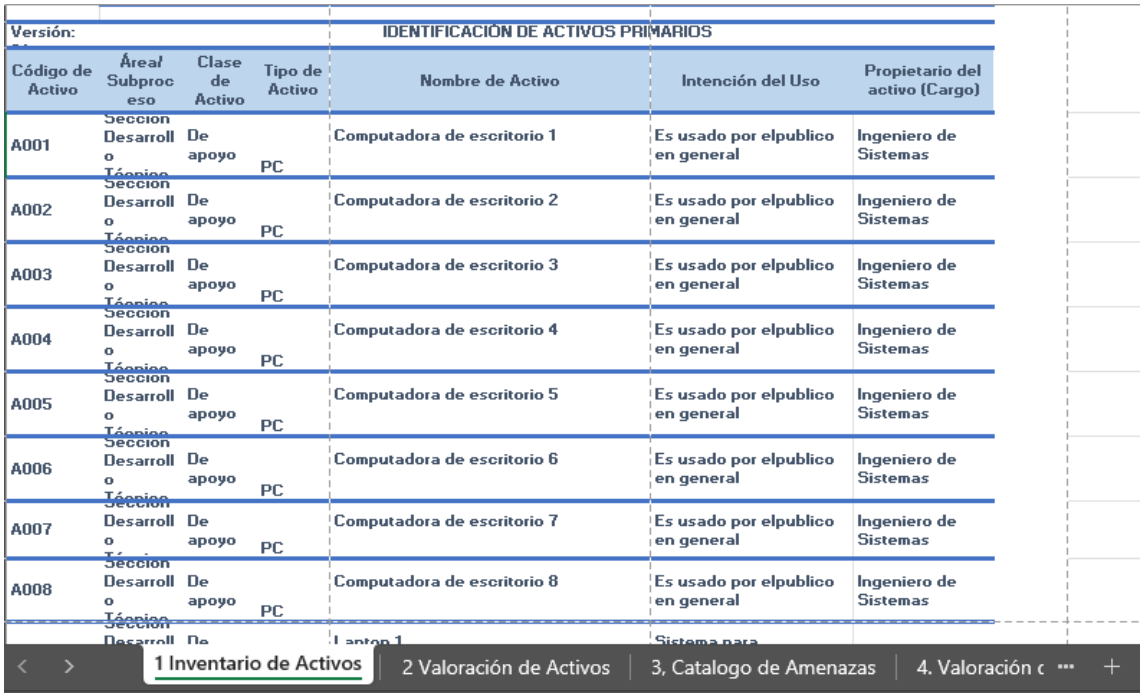
La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista
Mgtr. Jaime Salgado

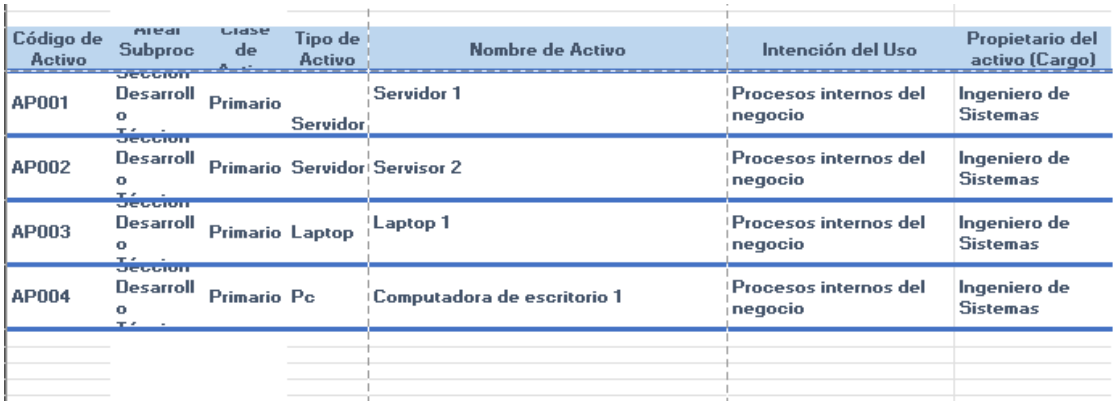
Anexo 3: Matriz de gestión de riesgos



Versión: IDENTIFICACIÓN DE ACTIVOS PRIMARIOS

Código de Activo	Área/ Subproceso	Clase de Activo	Tipo de Activo	Nombre de Activo	Intención del Uso	Propietario del activo (Cargo)
A001	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 1	Es usado por elpublico en general	Ingeniero de Sistemas
A002	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 2	Es usado por elpublico en general	Ingeniero de Sistemas
A003	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 3	Es usado por elpublico en general	Ingeniero de Sistemas
A004	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 4	Es usado por elpublico en general	Ingeniero de Sistemas
A005	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 5	Es usado por elpublico en general	Ingeniero de Sistemas
A006	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 6	Es usado por elpublico en general	Ingeniero de Sistemas
A007	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 7	Es usado por elpublico en general	Ingeniero de Sistemas
A008	Seccion Desarrollo Técnico	De apoyo	PC	Computadora de escritorio 8	Es usado por elpublico en general	Ingeniero de Sistemas
	Seccion Desarroll	De		Laptop 1	Sistema para	

1 Inventario de Activos | 2 Valoración de Activos | 3, Catalogo de Amenazas | 4. Valoración c



Código de Activo	Área/ Subproc	Clase de	Tipo de Activo	Nombre de Activo	Intención del Uso	Propietario del activo (Cargo)
AP001	Seccion Desarrollo Técnico	Primario	Servidor	Servidor 1	Procesos internos del negocio	Ingeniero de Sistemas
AP002	Seccion Desarrollo Técnico	Primario	Servidor	Servisor 2	Procesos internos del negocio	Ingeniero de Sistemas
AP003	Seccion Desarrollo Técnico	Primario	Laptop	Laptop 1	Procesos internos del negocio	Ingeniero de Sistemas
AP004	Seccion Desarrollo Técnico	Primario	Pc	Computadora de escritorio 1	Procesos internos del negocio	Ingeniero de Sistemas

PROCESO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Confidenci	C
Integridad	I
Disponibili	D

Versión: 01

IDENTIFICACIÓN DE ACTIVOS PRIMARIOS

Código de Activo	Área/ Subproceso	Clase de Activo	Tipo de Activo	Nombre de Activo	Intención del Uso	Propietario del activo (Cargo)	C	I	D	Valor
A001	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 1	Es usado por elpublico en general	Ingeniero de Sistemas	2	3	3	8
A002	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 2	Es usado por elpublico en general	Ingeniero de Sistemas	1	2	2	5
A003	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 3	Es usado por elpublico en general	Ingeniero de Sistemas	3	2	1	6
A004	Sección Desarrollo Técnico GIS	De apoyo	PC	Computadora de escritorio 4	Es usado por elpublico en general	Ingeniero de Sistemas	3	2	4	9

CATALOGO DE AMENAZAS TÍPICAS
Fuente: ISO/IEC 27005:2022

CATEGORIA	AMENAZA	TIPO DE FUENTE DE RIESGO
	Amenazas físicas	
Amenazas físicas	Fuego	A, D,E
	Agua	A, D, E
	Contaminación, radiaciones nocivas	A, D, E
	Accidente grave	A, D, E
	Explosión	A, D, E
	Polvo, corrosión, congelación	A, D, E
	Amenazas naturales	
Amenazas naturales	Fenómeno climático	E
	Fenómeno sísmico	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
	Pandemia/fenómeno epidémico	E

D = deliberado
A = accidental
E = ambiental

Identificación del Riesgo							Análisis de Riesgos										Valoración de riesgos Tratamiento de Riesgo			
	Código de Activo	Nombre de Activo	Amenaza	Vulnerabilidad	Controles existentes	Tipo de Controles existentes	Fecha identificación riesgo	Código del riesgo	Propietario Riesgo (Cargo)	Descripción del Riesgo	Consecuencia	Impacto	Probabilidad		Cálculo de Evaluación Riesgo	Nivel de Riesgo	Método de Tratamiento de Riesgos	Tipo de Control	Controles a Implementar	Plan de Acción
												CID (VA)	Nivel de Amenaza	Nivel de Vulnerabilidad						
	A001	Primario				Ninguno		GC-PF-R001	Jefe de facturación	Pérdida de la Planificación de proyectos que maneja la empresa.	Causaría retrasos en la presentación de la programación de los trabajos	3,00	1	3	9	Alto	MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	4.6 Gestión de la capacidad	SI
	A002	De apoyo	Error en uso	Derechos de acceso	Ninguno	Ninguno	14/6/2024	GC-FA-R001	Supervisor	Manipulación del excel sin consentimiento	Falta de integridad en el cálculo	3,00	1	3	9	Alto	MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO	Cifrado	SI
	A003	De apoyo	Denegación de acciones	Interfaz complicada	Ninguno	Ninguno	14/6/2024	GC-FA-R002-a	Supervisor	Error de interpretación	Error de interprtación	3,00	1	3	9	Alto	MODIFICAR / PREVENIR / COMPARTIR	CONTROL CORRECTIVO		SI

Anexo 4: Análisis Anti plagio