UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

PROPUESTA DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS ENFOCADO EN LA SEGURIDAD DE LA INFORMACIÓN PARA LAS PYMES FINANCIERAS

AUTOR:

HUGO FABIAN CAJAMARCA QUISHPE

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR
2024

Autor:

Hugo Fabian Cajamarca Quishpe
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
hcajamarca@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero en Sistemas.
mquiroz@ups.edu.ec

DEDICATORIA

Dedico este proyecto, en primer lugar, a mi hija Adeline Cristal Cajamarca Gualotuña, quien es mi motor y mi fuente de energía para superarme y seguir adelante cada día. Agradezco profundamente el amor incondicional y el constante apoyo de mis padres durante el desarrollo de este trabajo. También quiero expresar mi profunda gratitud a todas las personas que, de una u otra forma, me brindaron su ayuda invaluable a lo largo de este proyecto. Ya sea con palabras de aliento, consejos útiles, o simplemente estando ahí para apoyarme

Hugo Fabian Cajamarca Quishpe.

AGRADECIMIENTO

Quiero expresar mi profunda gratitud a quienes han sido pilares fundamentales en este camino hacia la culminación de mi maestría.

A Dios por otorgarme salud y la oportunidad de perseguir mis metas académicas.

A mi hija, quien ha sido mi mayor inspiración y fuente de motivación a lo largo de este viaje.

A mis padres, por su amor incondicional, apoyo inquebrantable y constante respaldo durante cada paso de este proceso.

Y finalmente, a todos aquellos que han brindado su valiosa ayuda y apoyo en diversas formas a lo largo de este proyecto.

Hugo Fabian Cajamarca Quishpe.

Tabla de Contenido

Propuesta de una metodología de gestión de riesgos enfocado en la seguridad de la información para las pymes financieras

Autor(es):

HUGO FABIAN CAJAMARCA QUISHPE

Resumen

El propósito de este estudio es establecer una metodología robusta que servirá de ayuda para las pequeñas y medianas empresas financieras a clasificar sus activos de información y realizar análisis de riesgo relacionado con la seguridad de la información. Esta metodología se basa en la misión, principios y valores fundamentales de las pymes financieras. Para evaluar los activos de información, se han considerado factores como el logro de objetivos, la reputación, el valor patrimonial y la continuidad operativa.

Para desarrollar esta metodología, nos hemos apoyado en la normativa NTE INENISO/IEC 27005. Este enfoque ha permitido crear una matriz de autoevaluación que categoriza y evalúa la información de las pymes financieras. Esta matriz proporciona detalles sobre las características de los activos y los responsables asociados, lo que nos permite identificar activos críticos y aplicar medidas para mitigar los riesgos identificados.

Este enfoque garantiza la integridad, confidencialidad, y disponibilidad de la información, así también refuerza la seguridad física y del entorno, protegiendo así los intereses y la reputación de las pequeñas y medianas empresas financieras.

Palabras claves: confidencialidad, integridad, disponibilidad, autenticidad.

Abstract

The purpose of this work is to establish a robust methodology to assist financial SMEs in classifying information assets and conducting risk analysis related to information security. This methodology is grounded in considering their mission, principles, and values. To assess the impact of information assets, criteria such as goal compliance, reputation, asset value, and service continuity have been taken into account.

In developing this methodology, we have relied on the NTE INEN-ISO/IEC 27005 regulations. This approach has enabled us to generate a self-assessment matrix that classifies and weighs XYZ's information. The matrix includes details about asset characteristics and associated stakeholders, allowing us to identify critical assets and implement measures to mitigate identified risks.

This comprehensive approach not only ensures the confidentiality, integrity, and availability of information but also strengthens physical and environmental security, thus safeguarding the interests and reputation of our organization.

Keywords: confidentiality, integrity, availability, authenticity.

1. Introducción

1.1. Antecedentes

Las (PYMES) en el sector financiero enfrentan desafíos significativos para la gestión de riesgos que están afines directamente con seguridad de información. El aumento significativo en la dependencia tecnológica y la proliferación de amenazas cibernéticas, estas empresas están cada vez más expuestas a riesgos mismas que comprometen la integridad del recurso informativo, su disponibilidad y la confidencialidad. Por ejemplo, las causas principales se ven afectado por la falta de recursos y experiencia que puede dificultar la implementación de medidas efectivas de seguridad cibernética, lo que deja a las PYMES vulnerables a ataques como el phishing y el ransomware.

A pesar de las regulaciones existentes en el sector financiero que garantizan la seguridad de información, muchas PYMES carecen de recursos y de la experiencia necesaria para implementar programas de gestión de riesgos de manera proactiva. Por ejemplo, pueden enfrentar dificultades para realizar evaluaciones exhaustivas de riesgos o para permanecer al día con las últimas amenazas cibernéticas y las mejores prácticas de seguridad.

En este contexto, desarrollar una metodología sólida y accesible para la gestión de riesgos de seguridad en información es fundamental, servirá de gran ayuda a las PYMES financieras a proteger los activos críticos y fortalecer la confianza de los clientes en un entorno cada vez más digitalizado y amenazante.

1.2. Determinación del problema

Debido a la limitación de recursos tanto humanos como económicos en las PYMES financieras, y la falta del enfoque específico y flexible que ayude con la gestión de estos riesgos que implican un alto grado de vulnerabilidad en la información que manejan estas entidades, estas empresas tienen dificultades para identificar, evaluar y gestionar riesgos de forma proactiva y eficaz.

1.2.1 Descripción del problema

Debido a la limitación de recursos tanto humanos como económicos las PYMES financieras no están en la capacidad para establecer e implementar un sistema efectivo que este enfocado en la seguridad de información y su gestión, este sistema ayudara a identificar, evaluar y mitigar las amenazas de manera eficiente. Sin una metodología específica y adaptable, estas empresas están en desventaja frente a las crecientes amenazas cibernéticas y los requerimientos normativos.

1.2.2 Formulación del problema

Dada esta situación, surge la necesidad de una solución que permita a las PYMES financieras adoptar un enfoque detallado sobre la gestión de información que límite el riesgo de seguridad. Esto implica realizar la identificación, evaluación y mitigación de amenazas de forma eficaz, asegurando así el cumplimiento normativo y la protección de los activos críticos de la organización.

1.2.3 Justificación del problema

Para proteger datos sensibles, cumplir con normativas, garantizar la continuidad operativa del negocio, mantener la confianza del cliente y proporcionar soluciones efectivas a las PYMES financieras con recursos limitados, es esencial contar con la metodología apropiada para el manejo y gestión de riesgos de seguridad de información.

1.2.4 Delimitación del problema

Nos enfocaremos en el cumplimiento de las normativas específicas reguladas para el sector financiero, excluyendo aquellas que no guarden una relación directa con la seguridad de la información en las PYMES financieras

1.3. Justificación

Un marco de gestión de riesgos de seguridad de información, "*con el propósito de identificar las necesidades de la organización en relación de los requisitos de seguridad de la información* " [1], proporciona una estructura sólida para abordar estratégicamente los riesgos cibernéticos. Esto se traduce en la protección de activos críticos y el fortalecimiento de la capacidad de las pymes financieras para enfrentar los desafíos del entorno digital actual.

- Un marco de gestión de riesgos permite comprender las diversas amenazas que podrían afectar a las pymes financieras.
- Mediante un enfoque de riesgos, se puede evaluar y clasificar estas vulnerabilidades, priorizando aquellas que representan un riesgo significativo para el negocio.
- Un marco de gestión de riesgos facilita una mejora continua, permitiendo a las pymes financieras adaptarse y estar preparadas para enfrentar los desafíos futuros.

1.4. Objetivo

1.3.1. Objetivo general

Realizar una propuesta metodológica de gestión de riesgos para mejorar la gestión de seguridad de la información aplicando la norma ISO 27005

1.3.2. Objetivos Específicos

1. Analizar la situación actual de las pymes financieras del segmento uno para establecer el contexto de la gestión del riesgo en la seguridad de la información.

2. Diseñar un marco de Gestión de Riesgos de Seguridad de la Información basado en las fases y principios establecidos por la Norma ISO 27005:2022, con el fin de mejorar la gestión de riesgos en las pymes financieras.

3. Realizar una evaluación teórica de la eficiencia de la metodología, mediante la creación de una tabla comparativa entre la Norma ISO 27005:2022 y la metodología Magerit V3, con el propósito de medir su viabilidad.

2. Marco Teórico Referencial

2.1. Glosario de términos y/o definiciones

Para los fines del presente documento se ha de considerar el siguiente glosario de términos, basados en las normas internacionales, ISO/IEC 24765:2017, ISO/IEC 27000:2018, ISO/IEC 27002:2022, ISO/IEC 27005:2022:

2.1.1. Definiciones

- **Activo de información:** Se refiere a cualquier información o recurso relacionado con la información que tiene valor para una organización y que necesita ser protegido. [1].
- **Aceptación del Riesgo:** Es la decisión razonada a favor de asumir un riesgo particular (ISO/IEC 27000:2018, 2018).
- **Amenaza:** Se define como cualquier circunstancia o evento potencial que puede causar daño a los activos de información mediante el aprovechamiento de una vulnerabilidad.[2].
- **Análisis del Riesgo:** Es el proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo [2].
- **Análisis del Impacto:** Proceso de análisis de todas las funciones operativas y el efecto que una interrupción operativa podría tener sobre ellas [3].
- **Comunicación y Consulta:** Es el proceso de establecer canales efectivos de comunicación y consulta dentro de una organización en relación con la gestión de riesgos de seguridad de la información[2].
- **Confidencialidad:** Es la propiedad de que la información no se difunde o revela a personas, o procesos no autorizados [4].
- **Consecuencia:** Es el resultado de un evento que afecta los objetivos [2]..
- **Contexto Interno:** Es el ambiente interno en el que la organización busca lograr sus objetivos [2].

- **Contexto Externo:** Es el entorno externo en el que la organización busca lograr sus objetivos [2].
- **Control:** Es la medida que mantiene y/o modifica el riesgo [2]
- **Criterios de Riesgos:** Son los términos de referencia contra los cuales se evalúa la importancia de un riesgo [4].
- **Degradación:** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza. [5].
- **Disponibilidad:** Es la propiedad de la información para ser accesible y utilizable bajo demanda por una entidad autorizada [4].
- **Estimación de Riesgo:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable [4].
- **Evaluación del Riesgo:** Es el proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su importancia es aceptable o tolerable [2].
- **Evento:** Es la ocurrencia o cambio de un conjunto particular de circunstancias [2].
- **Evitar el Riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Frecuencia:** Tasa de ocurrencia de una amenaza. Número de sucesos o de efectos en una unidad de tiempo [6]
- **Gestión de Riesgo:** Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo [2].
- **Identificación del Riesgo:** Es el proceso de encontrar, reconocer y describir los riesgos [2].
- **Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza. Consecuencia resultada de un suceso que afecta a los objetivos. [6]
- **Integridad:** Es la propiedad de la información para ser relativa a su exactitud y completitud [4].

- **Inventario de Activos:** Lista completa, sistemática y estructurada de todos los activos de información de una organización (o parte de ella) que se utilizan o se manejan para alcanzar los objetivos comerciales, cumplir con los requisitos legales o contractuales, o respaldar la operación de los procesos organizativos [4]
- **Plan de tratamiento de riesgos:** Es aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo [2]
- **Riesgo:** Es el efecto de la incertidumbre sobre los objetivos, en la seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información y por lo tanto, causen daños a una organización [2]
- **Umbral de riesgo:** Es la medida del nivel de incertidumbre o el nivel de impacto en el que una parte interesada puede tener un interés específico. Por debajo de ese umbral de riesgo, la organización aceptará el riesgo. Por encima de ese umbral de riesgo, la organización no tolerará el riesgo [7]
- **Alcance:** Es la delimitación sobre la cual se ejecutará el análisis de riesgos de seguridad de la información, asociados a los procesos de la institución [2]
- **Amenaza:** Causa potencial de un incidente de seguridad de la información que puede resultar en daño a un sistema o daño a una organización [2]
- **Confidencialidad:** Es la propiedad de que la información no se difunde o revela a personas, o procesos no autorizados [4]
- **Custodio del activo de información:** Es la persona encargada del procesamiento y almacenamiento del activo de información [1]
- **Disponibilidad:** Es la propiedad de la información para ser accesible y utilizable bajo demanda por una entidad autorizada [4]

- **Incidente de seguridad de la información:** Es un evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información [2]
- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios previamente procesados en varios datos que pueden ser almacenado o distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio [4]; y se constituye en un activo de información de las pymes financieras.
- **Integridad:** Es la propiedad de la información para ser relativa a su exactitud y completitud [4].
- **Responsable del activo de información:** Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de los activos de información; tiene autoridad para especificar y exigir las medidas de seguridad necesarias a los custodios de los activos de información para cumplir con sus responsabilidades [3].
- **Riesgo de seguridad de la información:** Es la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización [2].
- **Vulnerabilidad:** Debilidad de un activo o control que puede explotarse para que ocurra un evento con una consecuencia negativa [2].
- **Plan de tratamiento de riesgos:** Es aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo [2].
- **Riesgo:** Es el efecto de la incertidumbre sobre los objetivos, en la seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información y por lo tanto, causen daños a una organización [2].

- **Umbral de riesgo:** Es la medida del nivel de incertidumbre o el nivel de impacto en el que una parte interesada puede tener un interés específico. Por debajo de ese umbral de riesgo, la organización aceptará el riesgo. Por encima de ese umbral de riesgo, la organización no tolerará el riesgo [7].

2.1.2. Términos

- **SI:** Seguridad de la Información [4].
- **FODA:** Fortaleza Oportunidades Debilidades Amenazas [8].
- **CID:** Confidencialidad, Integridad y Disponibilidad.

2.2. Estrategias de Administración de Riesgos

Las estrategias de administración aplicables para los distintos riesgos son las siguientes:

- **Aceptar el riesgo:** Consiste en la decisión informada de asumir un riesgo sin implementar ninguna acción para mitigarlo o eliminarlo. Esta opción solo se aplica a los riesgos de nivel bajo, y requiere un seguimiento y una revisión constante para asegurar que no varíen [1].
- **Evitar el riesgo:** Se refiere a eliminar la fuente que genera el riesgo o prevenir que se produzca la causa que da lugar al efecto no deseado [2]
- **Mitigar el impacto:** Es implementar controles para disminuir la probabilidad o las consecuencias de un evento negativo. Para ello, se pueden emplear diferentes tácticas, como asumir el riesgo, prevenirlo, eliminar la fuente o transferirlo. Esta estrategia no elimina el riesgo, pero sí disminuye el daño que podría causar si se materializa [2].
- **Reducir la probabilidad de ocurrencia:** Son acciones tomadas para disminuir la probabilidad o las consecuencias negativas asociadas a la ocurrencia [1]. Significa que se han identificado actividades de control, cuya implementación permitirá reducir la probabilidad de ocurrencia al nivel más bajo posible.

- **Transferir el riesgo:** La transferencia de riesgo es una de las formas de tratamiento que implica la distribución acordada con otras partes que están en riesgo. Esta estrategia permite reducir o eliminar los riesgos repartiéndolos entre varios grupos. Cuando la transferencia es parcial, se denomina "compartir el riesgo" [2].

3. Situación actual de las PYMES financieras

De acuerdo con lo publicado por la Superintendencia de Economía Popular y Solidaria (SEPS) en su reporte *"LISTADO DE ENTIDADES DEL SFPS CON SEGMENTACIÓN 2023"* se identificó que existe 145 entidades financieras registradas en el segmento 4 y 65 entidades financieras registradas en el segmento 5

De acuerdo con lo publicado por el Banco Central del Ecuador (BCE), en el catálogo de "*Cooperativas de Ahorro y Crédito Calificadas al Sistema Nacional de Pagos por Segmentos*" se identificó que existen 40 instituciones del segmento 4 registradas en este sistema

De acuerdo con la Resolución No. SEPS-IGT-IR-IGJ-2018-0279, de 26 de noviembre de 2018: *"Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario, bajo el control de la Superintendencia de Economía Popular y Solidaria" en la SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO Artículo 4.- Administración de Riesgo Operativo, numeral 4.5.- Para mantener una adecuada administración del riesgo operativo las entidades de los segmentos 4 y 5, sin perjuicio de lo dispuesto en el Capítulo III Administración de riesgos en las cooperativas de ahorro y crédito de los segmentos 4 y 5 de las, "Normas para la administración integral de riesgos en las cooperativas de ahorro y crédito, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda", emitida por la Junta de Política y Regulación Monetaria y Financiera, deberán:*

a) Definir adecuadamente los procesos de la entidad, los mismos que incluyan: actividades, responsables, fecha de actualización y fecha de aprobación por parte del consejo de administración;

b) Mantener un registro de sus eventos de riesgo, el mismo que contemple como mínimo, fecha de ocurrencia, descripción, solución e impacto financiero de ser el caso;

c) Garantizar una adecuada separación de funciones que evite la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo;

d) Implementar políticas y niveles de aprobación para las distintas líneas de negocio y procesos con el fin de evitar conflictos de interés; y,

e) Elaborar un manual de administración del personal que contemple las políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal.

La Resolución No. SEPS-IGT-IR-IGJ-2018-0279, en su numeral 4.4, establece que las entidades de los segmentos 1, 2 y 3 deberán implementar lo determinado en los siguientes numerales:

4.4.1 Manual de Riesgo Operativo

4.4.2 Tipos de eventos de riesgo operativo

4.4.3 Metodologías

4.4.4 Base de eventos de riesgo

4.4.5 Esquema de reportes

4.4.6 Capacitación de riesgo operativo

Por otro lado, las entidades clasificadas en los segmentos 4 y 5 solo deberán cumplir lo establecido en el numeral 4.5. Debido a su tamaño y limitados

recursos, no están obligadas a desarrollar metodologías propias de la gestión de riesgos en la seguridad de información.

A medida que estas empresas crecen, se vuelve necesario adoptar metodologías de administración de riesgos para cumplir con los requisitos normativos y avanzar hacia el segmento 3. Ante esta necesidad, muchas PYMES financieras optan por adoptar estándares internacionales como ISO 27005 o Magerit.

La principal problemática radica en la complejidad de estas normativas y en la falta de experiencia interna para su implementación efectiva. Esto puede llevar a deficiencias en la gestión de riesgos, dejando a las instituciones vulnerables a amenazas cibernéticas.

El objeto de este trabajo es crear la metodología específica para estas PYMES financieras, que les guíe paso a paso con la gestión de riesgos en la seguridad de información. Esta metodología personalizada buscará simplificar la interpretación de las normativas, proporcionando una guía clara y práctica para que las instituciones puedan implementar procesos efectivos de gestión de riesgos. Esto incluirá un enfoque adaptado a las necesidades y recursos disponibles de estas PYMES, y mejorar la seguridad, reducir los riesgos relacionados con datos y operaciones financieras.

4. Metodología de gestión de riesgos de seguridad de la información.

4.1. Ámbito de Aplicación

La metodología tiene como alcance utilizar la situación actual de las PYMES financieras y establecer el contexto de la gestión del riesgo en seguridad de la información. Esto incluirá el diseño de un marco para la Gestión de Riesgos de Seguridad en la Información que se basa en las fases y principios establecidos por la Norma ISO 27005:2022 [5], para mejorar la gestión de riesgos en estas pymes.

Análisis de las metodologías del Sistema de Gestión de Riesgo (SGRO)

Etapas del Sistema de Gestión de Riesgo (SGRO)	ISO 27005:2022	Magerit V3	Metodología Propia
Identificar	✔	✔	✔
Medir	✔	✔	✔
Priorizar			✔
Controlar/Mitigar			✔
Monitorear	✔	✔	✔
Comunicar	✔	✔	✔

En este cuadro, un " ✔ " indica que las metodologías cumplen con las etapas del SGRO según lo establecido. ISO 27005 y Magerit incluyen directrices para la priorización y mitigación de riesgos. Sin embargo, sin la experiencia necesaria en su implementación, puede resultar difícil utilizarlas eficazmente. La metodología propuesta cumple con todas las etapas definidas y es consistente con los requerimientos establecidos para un Sistema de Gestión de Riesgo Operativo. El cuadro permite comparar el cumplimiento entre diferentes enfoques, destacando que la metodología propuesta es congruente con los principios y normas establecidos.

Además, se realizará una evaluación teórica de la eficiencia de la metodología mediante la creación de una tabla comparativa entre la Norma ISO 27005:2022 y la metodología Magerit V3, con el propósito de medir su viabilidad.

4.2. Base Metodológica

La " *Propuesta de una metodología de gestión de riesgos enfocado en la seguridad de la información para las pymes financieras*", se alinea a la norma ISO 27005:2022 [5], e ISO 31000:2009.

Para facilitar la comprensión de la " *Propuesta de una metodología de gestión de riesgos enfocado en la seguridad de la información para las pymes financieras* ", la misma se desarrollará siguiendo las fases descritas y sustentadas por la Norma ISO 27005:2012. Ref.: Ilustración 1.

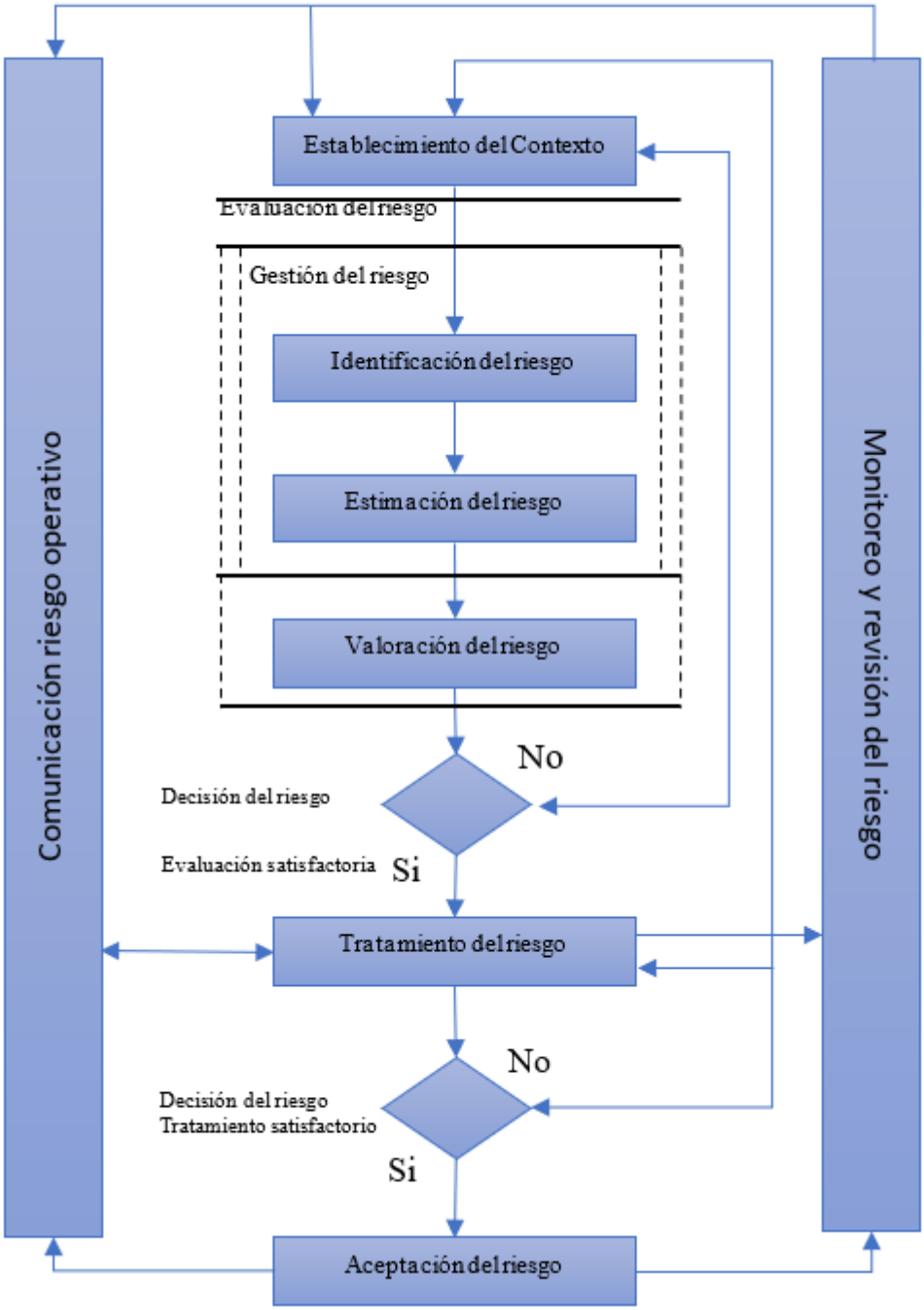

Ilustración 1. Gestión de Riesgos de la Seguridad de la Información.

4.3. Fase de Comunicación de Riesgos

La etapa de socialización del riesgo deberá ser un aspecto primordial para las etapas que implican el proceso de gestión del riesgo. El inicio debe ser:

a) Determinar cada uno de los elementos involucrados en la fase de identificación del riesgo a fin de tomar occisiones:

- Internas: Son los encargados de las Unidades Administrativas, Propietarios de Información y de los Custodios de Activos de Información entre otros.
- Externas: Proveedores, Entes Reguladores, Clientes, entre otros.

b) Definir la información a considerarse en el proceso que implica la Gestión de Riesgos en Seguridad de Información, abarcando aspectos como el tratamiento, causa, probabilidad de ocurrencia, consecuencias, entre otros.
c) Definir los mecanismos para la correcta comunicación, tomando en consideración algunos mecanismos como: la capacitación, los circulares, concientización y los informes de riesgos e impacto.
d) Establecer los medios de información para cada etapa:

- Comunicación inicial: Iniciamos con la introducción de los conceptos generales sobre el riesgo, las implicaciones que estas conlleva y los beneficios de su gestión, además de otros ítems pertinentes.
- Comunicación efectiva sobre la marcha: se debe comunicar los avances en el proceso de gestión a fin de obtener el apoyo y participación de todos los involucrados.

e) Las operaciones en información estarán orientadas a:

- Determinar y evaluar el riesgo, tomando en cuenta tanto su afectación como su probabilidad.
- Establecer la priorización y el tratamiento adecuado de los riesgos identificados.
- Comunicar e involucrar a cada uno de los interesados en esta fase.
- Supervisar y evaluar la metodología y el procedimiento.
- Implementar programas de capacitación y concienciación en toda la organización misma que deberá tratar temas de relevancia de los tipos

de ataques que ponen en riesgo la información y a su vez de las estrategias de acción correspondientes.

f) Determinar los objetivos de la comunicación:

- Presentar de manera adecuada los resultados alcanzados durante el proceso de gestión.
- Recopilar datos relevantes vinculados directamente con el riesgo de seguridad de información en las PYMES financieras.
- Cruzar información de los resultados obtenidos en la evaluación y en el plan de tratamiento de riesgos.
- Ofrecer apoyo en la ejecución acciones relacionadas con la seguridad de la información.
- Coordinar acciones a ejecutar en el plan de respuesta oportuna y la gestión de acontecimientos o sucesos de riesgos que impliquen vulnerabilidad de seguridad.
- Establecer tareas y acciones a cada una de las áreas que implican riesgos.
- Identificar mecanismos de percepción que faciliten la detección del riesgo de seguridad en la información.

g) Definir la metodología de evaluación de riesgos a utilizar.

- Identificar a los encargados de la parte ejecutora de la gestión y a los interesados de salvaguardad información, mismos que se encargaran en la toma de decisiones y acciones específicas a seguir.
- Fomentar una correcta comunicación de ambos sentidos entre todas las partes involucradas.

4.4. Fase de establecimiento del contexto

En esta fase, se dispondrá de algunos pasos a seguir:

a) Determinar el alcance de la metodología para la seguridad y la gestión de riesgos que implican:

- Describir cada uno de los requerimientos que implican para un producto o servicio.

b) Considerar el argumento externo, para lo cual vamos a tomar en cuenta los siguientes factores:

- Factores ambientales, culturales, legales, sociales, reglamentarios, económicos, tecnológicos y competitivo.
- La relación con los interesados externos, se considera las normativas y reglamentos del ente de control también las leyes en vigencia dentro del marco legal.
- Establecer el contexto interno: Se alinea a los procesos, la cultura, la estrategia y la estructura de las PYMES financieras. Se consideran factores que pueden influir en la forma en que se gestiona el riesgo, como:
    - Resultados producto del análisis FODA.
    - Productos de los datos obtenidos en auditoría interna.
    - Procedimiento elaborado para la continuidad de negocio.
    - Productos obtenidos del estudio sobre los riesgos tecnológicos.
    - Productos obtenidos de la información de los Activos críticos

4.5. Alcance y Limites

Se establece en varios aspectos que a continuación se detalla:

- Los agentes internos y externos.
- Políticas que norman la Seguridad de la Información.
- La ubicación y delimitación geográfica.

La forma de estructurar esta gestión se compone de:

- Determinar la relación existente del flujo de información en los procesos de funcionamiento.
- Determinar los procesos críticos.

- Identificar el tipo de información que se catalogara como críticos.
- Identificar probabilidades de riesgo, impacto y fragilidades.
- Estructurar una estrategia de mitigación para los riesgos en información.

4.6. Organización para la Gestión del Riesgo de Seguridad de la Información

Para realizar la organización para la gestión se debe seguir estos lineamientos:

- Determinar compromisos para la evaluación, tipificación y procedimiento de gestión.

Para desarrollar un proceso adecuado de gestión también se debe incluir:

- Identificar los actores interesados e involucrados.
- Determinar los roles y responsabilidades a fin de asignar a los actores interesados e involucrados actividades.

Los encargado, responsables y propietarios de información, junto al responsable de seguridad de información, llevarán a cabo una valoración de riesgos para cada uno de los activos de información crítica, identificando así las acciones u estrategias para su tratamiento.

Durante la sesión del Comité de Administración Integral de Riesgos (CAIR), se presentará la valoración al riesgo de seguridad en la información, siguiendo el debido proceso de gestión y se definirá el mecanismo de acción ante dicho riesgo [6].

Se definirán la información que deben conservarse y almacenarse en cada unidad de administración y se notificarán para su debido registro en el documento inventariado a cargo del responsable de riesgos.

4.7. Fase de Análisis de Riesgo

Esta fase comprende el análisis del riesgo, identificándose inicialmente los activos de información, y su criticidad en cada proceso.

4.7.1 Identificación de activos de información

Para incluir la información de los activos en el documento que lleva el inventario de cada unidad administrativa, se deben considerar algunos parámetros:

a) Identificación del Activo: Se identificará utilizando la abreviatura del área correspondiente acompañado de un número que llevará la secuencia. Por ejemplo: Gerencia de Riesgos GR_001.

b) Descripción: Se proporcionará una descripción a detalle de la importancia del activo y su función dentro de la cadena de información. Por ejemplo: Contiene información sobre los activos de TI.

c) Tipo: Se determinará con una letra distintiva a la inicial de su descripción como se detalla a continuación en el ejemplo: "Actividades (A), Procesos (Pr), Información (I), Hardware (H), Software (S), Redes (R), Personas (P), u otros (O) [6].

d) Medio: Se debe especificarás el medio en donde se encuentra almacenado el activo de información siendo así un medio físico (carpetas, archivos, etc.), lógico (aplicaciones, discos externos, etc.) o humano (empleados).

e) Ubicación: Se indicará de manera específica el lugar de ubicación ya sea física o un medio lógico.

f) Criticidad: Se determinará si el activo es crítico mediante la ayuda de la tasación del CID. Se utilizará como referencia la Tabla 2.

g) Asignaciones: Se identificará con una letra distintiva acorde a la persona que esta a cargo de dicha información, ejemplo: propietario (P), custodio (C) o el usuario(U).

h) Responsable: Se indicará al área pertinente y el nombre del responsable.

5. Descripción de Actividades

De acuerdo con esta metodología, se desglosan algunas actividades:

a) Identificación de activos de información.

b) Clasificación de activos de información.

c) Determinación de activos críticos de información.

d) Identificación del universo de amenazas y vulnerabilidades.

e) Análisis y evaluación de riesgos en seguridad de la información.

5.1. Identificación de Atributos Estratégicos de la Organización

Para identificar los atributos estratégicos de la organización, se recomienda, pero sin limitarse a los siguientes elementos:

- Misión
- Principios y Valores
- Objetivos Estratégicos

Estos atributos se utilizarán para evaluar el impacto que sufre la integridad, exclusividad y disponibilidad asociadas con los activos en información.

La determinación de atributos estratégicos de la organización es esencial para alinear la seguridad de la información.

Considerando los elementos mencionados anteriormente, se han definido los siguientes atributos estratégicos:

a) Cumplimiento de objetivos

b) Reputación

c) Valor patrimonial

5.2. Definición de Criterios para análisis y Evaluación de Riesgos de Seguridad de la Información

Una vez establecido el atributo estratégico de la PYMES, iniciamos a aplicar los siguientes criterios para evaluar y analizar el riesgo de seguridad en la información que se maneja:

a) Criterio de evaluación de impacto: Este criterio permite calificar cualitativamente los desgastes de integridad, exclusividad y vacancia de los activos de información. Este a su vez se emplea de manera consistente durante el análisis de riesgos y permite ponderar el nivel de impacto de los activos de información. (Ver Anexo 2). Se refiere a evaluar los posibles impactos resultantes de la pérdida, alteración o divulgación no autorizada de la información, así como de la falta de disponibilidad de los activos de información dentro de las pymes financieras.

b) Criterio de evaluación de vulnerabilidad: Este criterio permite determinar a ciencia cierta la probabilidad que ocurra una amenaza y se lleve a cabo debido a la vulnerabilidad que presenta un activo de información por los niveles de control. (Ver Anexo 1). Se refiere a evaluar las posibles debilidades o puntos críticos en los sistemas, procesos o activos de información que podrían ser blanco fácil a amenazas que comprometan la seguridad de la información.

c) Criterio de clasificación de riesgos: Este criterio define cuándo un riesgo es considerado inaceptable o aceptable. El análisis depende de los criterios de evaluación de impacto y vulnerabilidad. (Ver Anexo 1. Criterios de evaluación de riesgos de la Seguridad de la Información). Se refiere a cómo se determina, categoriza la importancia de los riesgos identificados durante la evaluación de riesgos.

5.3. Identificación de Activos de Información de Los Procesos

Para la identificación de los activos de información, es esencial determinar qué información se utiliza o genera durante la ejecución de los procesos en las pymes financieras. En este levantamiento de información, la participación de los responsables de los procesos o sus delegados es fundamental para llevar a cabo las siguientes actividades:

Conocer los procesos: Esto implica identificar principalmente las entradas (información que se utiliza como insumo para la ejecución del proceso), las salidas (información generada como resultado de la ejecución del proceso), los procesos de soporte y los actores que intervienen en esta etapa.

Identificar los activos de información: Se entienden a los activos como recursos que procesan, generan y/o resguardan información clave para la operación y el correcto cumplimiento de objetivos dentro de las pymes financieras. Toda la información ingresada o producida en un proceso puede estar relacionada con uno o varios activos de información. El responsable del proceso entregará el mapa de los procesos involucrados para observar la interacción entre ellos.

Tipos de activos de información: Incluyen archivos físicos (como reportes, actas, resoluciones, entre otros), archivos digitales (como políticas, normativas, procedimientos en formato electrónico), hardware (servidores, equipos de redes, etc.), instalaciones físicas (infraestructura tecnológica y acceso al centro de datos), personas (personal clave con conocimientos especializados) y software (programas de computadora y procedimientos).

Registro en el formato “Inventario de activos de información”: Esta actividad implica registrar todos los activos de información identificados en un formato específico, como se detalla en el Anexo 2.

5.4. Ponderación de Activos de Información

5.4.1 Calificación del nivel de impacto a los activos de información

El nivel de impacto por pérdida de confidencialidad (C), integridad (I) y disponibilidad (D) se determina en colaboración con el responsable del activo de información. Para ello, se califica el impacto para cada uno de los atributos estratégicos de las pymes financieras, previamente identificados en la sección 5, y para cada activo de información. A continuación, se presenta un ejemplo de cómo llevar a cabo este proceso:

Confidencialidad			*Integridad*			*Disponibilidad*		
A1	*A2*	*A3*	*A1*	*A2*	*A3*	*A1*	*A2*	*A3*
1	*3*	*5*	*1*	*3*	*5*	*1*	*3*	*5*

Tabla 1. Ejemplo de calificación de impacto de los Activos de Información

Para evaluar el impacto, se emplearán los criterios establecidos en el Anexo 1, que abordan el tema de riesgos de seguridad que pone en riesgo la información. Para la calificación del impacto para los aspectos de exclusividad, integridad y disponibilidad de los activos se documentará en el formato "Ponderación y Clasificación de Activos de Información" detallado en el Anexo 3. El impacto total de cada activo se calculará a partir del promedio de las calificaciones obtenidas. Los niveles de impacto se clasifican como Bajo (menor a 2.5), Medio (2.5 o más) y Alto (3.5 o más).

5.5. Clasificación de los Activos de Información

Para iniciar con la codificación de los activos de información, se consideran dos criterios principales: el nivel de importancia y la sensibilidad de la información contenida o producida.

En cuanto al nivel de importancia:

Crítica: La información es vital para la continuidad de procesos esenciales de las pymes financieras o está requerida por la ley. Su disponibilidad debe ser preservada a toda costa debido a su impacto directo en las operaciones.

Esencial: La información es necesaria y de ser el caso puede ser reconstruida en caso el caso fortuito de pérdida, una de las cosas a tomar en cuenta es que su recuperación podría no ser alcanzada dentro del tiempo definido como máximo tolerable por la empresa sin consecuencias legales, operativas o económicas.

No Esencial: Información útil para tareas habituales del personal, pero que no es crítica ni esencial para la operación general.

Respecto al nivel de sensibilidad:

Confidencial: Información personal no sujeta a divulgación pública, protegida contra acceso no autorizado.

Reservada: Información que requiere acceso autorizado y cuyo tratamiento inadecuado puede representar riesgos significativos para la empresa.

Privada o No Reservada (Información de acceso autorizado): este apartado trata de la información cuyo acceso debe ser expresamente autorizado y restringido a un grupo reducido de usuarios para evitar riesgos potenciales.

Pública: Información no confidencial que no representa riesgos significativos para la empresa y tiene requerimientos de control limitados.

La clasificación de los activos se registra según estos criterios en el formato "Ponderación y Clasificación de Activos de Información" mencionado en el Anexo 3.

MATRIZ DE CALOR DE LA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

En el eje "x", se registrará el indicador de sensibilidad en la seguridad de la información, relacionado con el atributo de exclusividad. En el eje "y", se registrará el nivel de importancia, relacionado con el atributo de Disponibilidad.

La matriz de calor de la clasificación de activos de información es de tipo cartesiano y establece tres niveles de acuerdo con la importancia y cuatro niveles de sensibilidad de la información. En cada casillero, se registrará el número correspondiente del activo de información identificados.

MATRIZ DE CALOR DE LA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

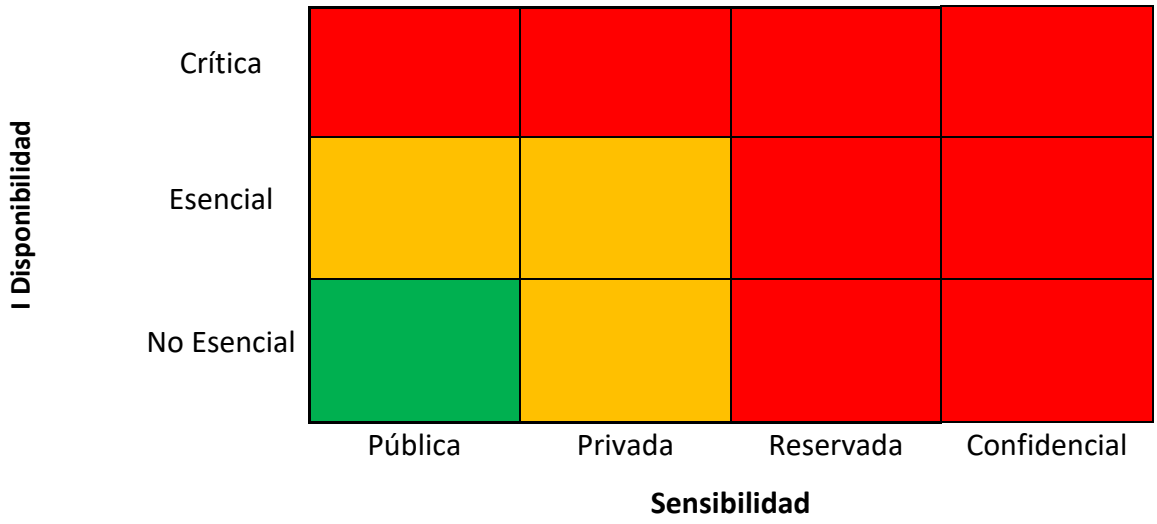

Tabla 2. Matriz de calor.

Nivel de Importancia o Criticidad

Es un mecanismo que nos ayudara a identificar la información requerida para la continuidad de las operaciones normales o para el cumplimiento de leyes y normas.

- No Esencial 
- Esencial 
- Crítica 

Nivel de Sensibilidad

Refiere al riesgo que implica su divulgación para de las pymes financieras.

- Pública 
- Privada 
- Reservada 
- Confidencial 

5.6. Determinación de Activos de Información Críticos

Para determinar a los activos de información que serán considerados como críticos iniciamos diciendo que son aquellos que se encuentran en una escala de importancia crucial o crítico y en una escala de sensibilidad de confidencialidad, ya sea discreta o privada, todas estas deben encontrarse en una escala de impacto medio o alto, mismo que determinara el resultado final de la ponderación realizada. Se aplicará el análisis de riesgos de seguridad de la información a estos activos.

Al concluir esta actividad, se registrará el inventario de activos de información críticos en el formato establecido en el Anexo 4.

5.7. Identificación de universo de amenazas y vulnerabilidades

Es un paso importante para tomar en cuenta en el análisis de riesgos la identificación de posibles ataques y vulnerabilidades que están sujetos los

activos de información. Para llegar a este punto es necesario una revisión periódica a las amenazas y vulnerabilidades, hay que considerar diversos cambios que pueden afectar a las pymes financieras, como:

Reformas a la normativa legal aplicable a las pymes financieras.

Introducción de nuevos procesos y productos.

Avances y cambios tecnológicos, entre otros.

La matriz de amenazas y vulnerabilidades ayuda en encontrar resultados analizando el tipo de activo de información que manejan las pymes financieras (todo el conjunto de equipos, talento humano, instalaciones, archivos y la tecnología que poseen). Esta matriz se detalla en el Anexo 5.

IDENTIFICACIÓN DE CONTROLES

Los requisitos de seguridad asignados a los activos de información están en las listas de verificación de controles, que se detallan en el Anexo 6. Estas listas están diseñadas considerando que cada control está directamente relacionado con la protección del activo de información frente a una o varias vulnerabilidades.

La lista de verificación incluye los controles de seguridad cuya existencia debe ser validada para determinar si se está mitigando adecuadamente las posibles vulnerabilidades de los activos de información.

Al aplicar la lista de verificación de controles, es posible identificar los controles existentes y las vulnerabilidades asociadas a los activos de información. Los controles incluidos en la lista de verificación y sus respectivas vulnerabilidades están vinculados con al menos uno de los siguientes tipos que servirán para el control de seguridad de la información:

TIPOS DE CONTROLES	CRITERIOS DE SEGURIDAD
Administrativos	▪ Segregación de funciones ▪ Continuidad ▪ Capacidad de respuesta a incidentes ▪ Revisión periódica de controles de seguridad ▪ Investigaciones del personal y sus referencias ▪ Análisis de Riesgos ▪ Capacitación técnica y de seguridad ▪ Asignación de funciones ▪ Autorización del sistema ▪ Plan de seguridad de aplicación o sistema
Técnicos	▪ Comunicaciones ▪ Criptografía ▪ Control de acceso discrecional ▪ Identificación y autenticación ▪ Detección de intrusos ▪ Reutilización de objetos ▪ Auditoría de Sistemas
Físicos	▪ Controles para asegurar la calidad del sistema de suministro eléctrico ▪ Acceso y disponibilidad de los medios de datos ▪ Distribución y etiquetado externos de los datos ▪ Protección de instalaciones (ej. oficina, centro de cómputo, data center) ▪ Control de humedad ▪ Control de temperatura ▪ Estaciones de trabajo, portátiles y computadores personales

Tabla 3. Identificación de Controles

El listado de controles administrativos, técnicos y físicos proporciona datos de referencia para una evaluación preliminar y no necesariamente se incluyen todos para el análisis de riesgos. El cálculo de la probabilidad que ocurra se

fundamenta en la presencia o ausencia de estos controles para cada activo de información. La probabilidad de que una vulnerabilidad potencial se materialice debido a una amenaza se clasifica según el criterio establecido en la evaluación de vulnerabilidad. Para más detalles, consulta el Anexo 1 y el Anexo 5.

5.8. Análisis y evaluación de riesgos de seguridad de la información

Este proceso permite encontrar las posibles amenazas que se enfrentan los activos de información de las pymes financieras y determinar así la acción adecuada para los eventos de riesgo con un nivel de impacto medio o alto. Aquellos eventos de riesgo con un nivel de impacto bajo se consideran aceptados por el responsable del activo de información.

Para catalogar el nivel de vulnerabilidad, se analiza el impacto y la probabilidad de ejecución de dicha amenaza, para lo cual hay que tomar en cuenta los criterios que se encuentran en el Anexo 1. Posteriormente, iniciamos con el registro en la matriz de riesgos de seguridad de la información (Anexo 7) las amenazas (eventos), las vulnerabilidades (causas), los controles existentes identificados, y se complementará con la selección del factor de riesgo y el tipo de control

5.8.1. Determinación del riesgo residual

El Riesgo Residual se define como el nivel de riesgo considerando los controles existentes. Para cada uno de los activos de información críticos identificados, se utilizará el impacto calculado de cada atributo estratégico, que se encuentra en el "Resumen de impactos" del documento de ponderación y clasificación de activos de información (Ver Anexo 3).

A continuación, se aplicarán algunos criterios que serán tomados en cuenta para realizar la estimación de vulnerabilidad que nos permitirá establecer la probabilidad de ocurrencia para cada uno de los activos de información críticos, según se detalla en el Anexo 1. Las calificaciones de impacto y probabilidad de riesgose registrarán en la matriz que se encuentra en el Anexo 7.

5.8.2. Determinación del riesgo administrado

La siguiente actividad implica la selección de estrategias de administración en función del nivel de riesgo residual determinado. Estas estrategias pueden incluir aceptar el riesgo, mitigar el impacto, reducir la probabilidad, transferir el riesgo o evitar el riesgo.

Si después de evaluar el riesgo residual y las estrategias de administración, se determina que el nivel de riesgo no es adecuado, se acordará la implementación de opciones de mejora para reducir la probabilidad de ocurrencia, mitigar el impacto o transferir el riesgo.

Cada opción de mejora se analiza en términos de viabilidad, como su compatibilidad con el entorno de control de las pymes financieras y la aceptación por parte de los usuarios y su eficacia, es importante saber el grado de protección y el nivel de mitigación del riesgo que proporciona. Se considerarán factores como la capacidad de reacción y control frente a un ataque identificado, el régimen de control y las regulaciones aplicables de ser el caso y las políticas organizacionales y el análisis costo-beneficio.

Las opciones de mejora seleccionadas deben ser acordadas con los responsables de los activos de información de las pymes financieras. Toda la información resultante de esta actividad se registrará en la Matriz de Riesgos (ver Anexo 7).

Finalmente, para obtener el riesgo administrado, se medirá el impacto y la probabilidad después de implementar las opciones de mejora, y se ubicarán los eventos en la matriz de Riesgos de Seguridad de la Información.

5.8.3. Determinación e implementación de los planes de administración de riesgos

Una vez seleccionada la opción de mejora y su respectivo control para los diferentes eventos de riesgo, en colaboración con el responsable del activo o la contraparte designada para la gestión de riesgos, se elaborarán los planes de administración de riesgos. Estos planes contendrán las estrategias elegidas y la

forma en que serán implementadas, utilizando el formato proporcionado en el Anexo 7.

Los planes especificarán las acciones necesarias de las personas o áreas involucradas en la implementación de cada plan, de manera que se pueda monitorear fácilmente su progreso. Por lo general, se establecerán compromisos con los responsables o la contraparte designada para la gestión de riesgos de las áreas involucradas.

5.8.4. Matriz de calor de riesgos de la seguridad de la información

Sobre el eje horizontal (eje x) servirá para registrar la probabilidad de ocurrencia, mientras que en el eje vertical (eje y) se registrarán los niveles de impacto.

La matriz de riesgo de seguridad de la información es de tipo cartesiano y establece tres niveles. Estos niveles han sido categorizados de acuerdo con el impacto y la probabilidad. Es decir, a mayor impacto y probabilidad, el nivel será alto, mientras que, a menor impacto y menor probabilidad, el nivel será bajo. Esto se determina siguiendo las siguientes relaciones:

Nivel de riesgo	Impacto	Probabilidad
Alto	5	1 - 2 -3 - 4 - 5
	4	3 - 4 -5
Medio	4	1 – 2
	3	2 – 3 – 4 - 5
	2	5
Bajo	3	1
	2	1 - 2 – 3 – 4
	1	1 - 2 - 3 - 4 - 5

Tabla 4. Relación Impacto Probabilidad según el Nivel de Riesgo

A continuación, disponemos de una matriz de calor resultante del análisis de riesgos en seguridad de la información.

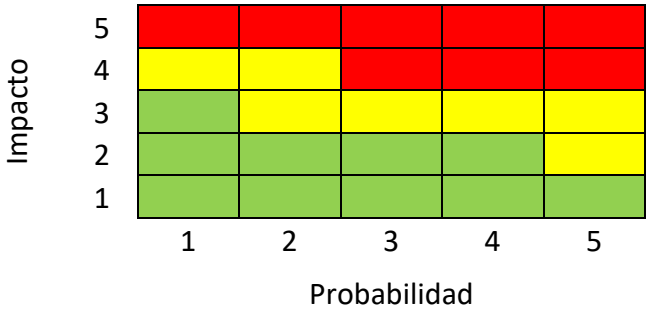

Tabla 5. Matriz de Riesgos de la seguridad de la Información

- Nivel bajo

Eventos de riesgo encontrados y clasificados que sean ubicados en este nivel, estos a su vez se consideran tolerables por lo que no requieren de ningún plan de acción.

- Nivel medio

Eventos de riesgo encontrados y clasificados que son ubicados en este nivel, indica que los responsables de acción deben considerar la implementación de medidas de mitigación oportunas.

- Nivel alto

Los eventos de riesgo encontrados y clasificados que son ubicados en este nivel, indica a los responsables tomar acciones inmediatas que deberán informarán y solicitarán sin demora la pronta intervención en los eventos de riesgo. Se elaborarán las posibles medidas de mitigación de ser necesario se solicitará al comité de administración la aceptación de dichas medidas de así requerirlo. Para

acceder a la Matriz de calor de riesgos de la seguridad de la información, consulte el Anexo 7

6. Evaluación teórica de la metodología de gestión de riesgos de seguridad de la información propuesta

Realizar una evaluación teórica de la eficiencia de la metodología, mediante la creación de una tabla comparativa entre la Norma ISO 27005:2022 y la metodología Magerit V3, con el propósito de medir su viabilidad.

La Junta de Política y Regulación Monetaria y Financiera expidió la Resolución No. 521-2019-F, en la que se estableció las reformas a la Norma para la segmentación de las entidades del Sector Financiero Popular y Solidario. [5]

La SEPS de acuerdo con la información remitida por cada una las entidades del Sector Financiero Popular y Solidario, ha realizado la actualización de la segmentación para el año 2023. [5]

NORMA PARA LA SEGMENTACIÓN DE LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

Artículo 1.- Las entidades del sector financiero popular y solidario de acuerdo con el tipo y al saldo de sus activos se ubicarán en los siguientes segmentos:

Segmento	Activos
1	Mayor a 80'000.000,00
2	Mayor a 20'000.000,00 hasta 80'000.000,00
3	Mayor a 5'000.000,00 hasta 20'000.000,00
4	Mayor a 1'000.000,00 hasta 5'000.000,00
5	Hasta 1'000.000,00

4.2.- Etapas del Sistema de Gestión de Riesgo Operativo: Las entidades y la Corporación deben ejecutar las etapas definidas para el Sistema de Gestión de Riesgo Operativo que consisten en:

4.2.1 Identificar: Debe realizarse con anterioridad a la ejecución de cualquier proceso, con el fin de determinar los riesgos operativos que han ocurrido, así como aquellos riesgos operativos en potencia que van a suponer una serie de obstáculos al logro de los objetivos definidos. En esta etapa de identificación pueden a su vez diferenciarse dos subetapas:

- *Inventario de procedimientos*
- *Recolección de información*

4.2.2 Medir: Una vez que los riesgos operativos de los diferentes procesos han sido identificados, el siguiente paso es evaluar la posibilidad de materialización de los mismos (en función de la frecuencia con la que los mismos suceden) así como, definir el impacto que los mismos podrían generar en caso de ocurrencia.

Como resultado de esta segunda etapa, establecemos el llamado riesgo inherente, que no es más que el nivel de riesgos que presenta una actividad concreta, sin aplicarle ningún tipo de control.

4.2.3 Priorizar: Los resultados de la matriz de probabilidad e impacto, permiten identificar aquellos riesgos que representan una mayor amenaza, a los cuales se les puede dar mayor prioridad o gestión de respuesta, con los recursos de los que dispone la entidad.

4.2.4 Controlar/mitigar: En esta etapa se busca definir las medidas de control que permitan reducir la probabilidad de ocurrencia y/o impactos ocasionados por los riesgos inherentes detectados.

Tras esta etapa, la entidad obtiene el conocido riesgo residual, que es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados por la entidad.

4.2.5 Monitorear: En esta etapa se debe llevar a cabo el seguimiento adecuado a los riesgos con el fin de ir analizando su evolución.

4.2.6 Comunicar: Las entidades deben definir una política sobre los eventos de riesgo operativo que deban informar interna o externamente y que esté sujeta a revisión periódica, en función de las estrategias organizacionales. Además, deben implementar

un proceso para evaluar el impacto de la información a comunicar en función a su gestión de riesgos.
(Numeral incluido por el numeral 2 del Artículo 2 de la Resolución No. SEPS-IGT-IGSINR-INGINT-2022-0211 de 7 de julio de 2022.)

En la PYME financiera XYZ se ha implementado la metodología de evaluación de riesgos propuesta en este trabajo para PYMES financieras. Este modelo propio combina conceptos de metodologías internacionales y se basa en un análisis de la estructura organizacional de la empresa, utilizando indicadores cualitativos. Estos indicadores permiten evaluar la situación de la PYME y asignar una calificación de riesgo a sus activos de información, categorizándolos como Alto, Medio o Bajo.

Para aplicar el modelo, se definieron los indicadores relevantes que componen cada categoría de riesgo. La selección y ponderación de estos indicadores se realizaron con la ayuda de expertos de riesgos de operaciones de la Gerencia de Riesgos de XYZ. Se recopiló la mejor información disponible para medir el riesgo de los activos de información, permitiendo así una evaluación cualitativa de los riesgos operativos. Los tres indicadores definidos para este análisis cualitativo son: Reputacional, Patrimonial y Continuidad de los Servicios. Cada uno de estos indicadores se evalúa por separado y luego se consolidan para cuantificar el riesgo dentro del modelo.

La metodología desarrollada y las calificaciones de riesgo otorgadas a la PYME financiera del segmento 1 se ajustan adecuadamente a las características de dicho segmento y cumplen con la resolución establecida. Esto describe de manera precisa su posición relativa dentro del segmento al que pertenece. Además, se ha determinado el cumplimiento de las etapas del SGRO solicitadas por el ente de control. Para ello, se presenta un cuadro comparativo que muestra la metodología propuesta en este trabajo en comparación con las metodologías ISO 27005 y Magerit

Cuadro comparativo metodologías del Sistema de Gestión de Riesgo (SGRO)

Etapas del SGRO	Norma ISO 27005:2022	Magerit V3	Metodología Propia
Identificar	Se centra en identificar amenazas y vulnerabilidades para evaluar riesgos. Incluye herramientas para identificar riesgos en diferentes contextos.	Ofrece un proceso estructurado para identificar riesgos en sistemas de información, con un enfoque en amenazas, vulnerabilidades y escenarios de riesgo.	Enfoca la identificación de riesgos en procesos internos y externos, con énfasis en inventario de procedimientos y recolección de información.
Medir	Proporciona herramientas para medir el impacto y la probabilidad de riesgos identificados. El riesgo inherente se determina sin aplicar controles.	Define métricas para medir la probabilidad y el impacto de riesgos, estableciendo una matriz de riesgos. Se centra en riesgo inherente antes de controles.	Mide la posibilidad de materialización de riesgos y su impacto. Incluye la evaluación del riesgo inherente basado en la frecuencia y gravedad.
Priorizar	Ofrece directrices para priorizar riesgos según su nivel de amenaza, permitiendo la asignación de recursos según la importancia de los riesgos.	Establece un molde de probabilidades de ataque permitiendo la gestión de respuesta adecuada.	Utiliza la matriz de probabilidad e impacto para priorizar riesgos y enfocar los recursos en los más críticos.
Controlar/Mitigar	Se centra en definir controles y medidas para mitigar riesgos identificados, reduciendo la probabilidad e impacto de riesgos inherentes.	Propone una serie de controles y estrategias para mitigar riesgos, reduciendo el riesgo inherente y obteniendo el riesgo residual.	Define medidas de control para reducir la probabilidad e impacto de riesgos inherentes, obteniendo el riesgo residual tras aplicar controles.
Monitorear	Incluye directrices para el monitoreo continuo de riesgos para evaluar su evolución y efectividad de controles.	Ofrece mecanismos para monitorear y controlar riesgos de manera continua, permitiendo ajustes según la evolución de riesgos.	Establece un seguimiento continuo para analizar la evolución de riesgos y la efectividad de controles aplicados.
Comunicar	Enfatiza la importancia de	Define procesos para comunicar riesgos a	Proporciona un proceso para

	comunicar riesgos interna y externamente, estableciendo políticas para eventos de riesgo operativo.	partes interesadas internas y externas, con políticas de comunicación claras y sujetas a revisión periódica.	comunicar eventos de riesgo operativo y evalúa su efectividad.

7. Recomendaciones.

- Se recomienda que las PYMES financieras adopten el marco de gestión de riesgos propuesto de manera gradual. Comenzar con procesos clave y expandir el alcance a lo largo del tiempo ayudará a evitar sobrecargar a la organización y permitirá una mejor adaptación a los cambios.
- La implementación por etapas también facilita la capacitación del personal y la incorporación de nuevos controles.
- Se recomienda establecer sesiones de capacitación periódicas y campañas de concienciación para mantener al personal informado y comprometido.
- Se recomienda que las PYMES financieras implementen un sistema de monitoreo para seguir la evolución de los riesgos y la eficacia de los controles.
- Mantener la metodología actualizada y adaptada a los cambios en el entorno de seguridad, asegurando que la gestión de riesgos sea efectiva y sostenible a largo plazo.

8. Conclusiones.

- La metodológica proporciona un marco sólido para las PYMES financieras, permitiéndoles clasificar, evaluar y gestionar riesgos de seguridad de la información de una manera eficaz.
- Usando esta metodología, las PYMES financieras pueden reducir la vulnerabilidad a amenazas cibernéticas y mejorar su capacidad para proteger información sensible, lo que contribuye a la estabilidad y continuidad del negocio.
- Las PYMES financieras pueden personalizar la metodología según sus necesidades y recursos, lo que facilita la implementación y la adopción de mejores prácticas de seguridad.
- La evaluación teórica mediante la tabla comparativa demuestra que la metodología propuesta es viable y cumple lo establecido en el Sistema de Gestión de Riesgo Operativo por lo que puede ser utilizada por las PYMES financieras para mejorar su gestión en temas de riesgos de seguridad que atenta contra la información.
- A comparación con otras metodologías establece que la propuesta puede ser eficaz para abordar los desafíos únicos de las PYMES financieras y para proporcionar un camino claro hacia el cumplimiento normativo y la reducción de riesgos.

9. Anexos

9.1. Anexo 1. Criterios de evaluación de riesgos de la Seguridad de la Información

Criterios para la evaluación del impacto

El impacto es el efecto adverso en los procesos de las pymes financieras y en el logro de sus objetivos. El impacto se califica para cada atributo estratégico de las pymes financieras: Cumplimiento de Objetivos, Reputacional, Patrimonial y Continuidad de los servicios.

- **Impacto en el Cumplimiento de Objetivos:** La materialización de la acción que puso en riesgo la información ocasiona incumplimiento de las leyes y normativas de privacidad y sigilo.

Los criterios de evaluación de impacto para el atributo son:

Escalas / Impacto		Cumplimiento de Objetivos
3	Alta	Incumplimiento parcial de los objetivos establecidos en la Ley o incumplimiento de los objetivos institucionales
2	Media	Errores o retrasos significativos en el desarrollo de las funciones vinculadas a la Ley o incumplimiento parcial de los objetivos
1	Baja	Cumplimiento de los objetivos establecidos en la Ley y/o institucionales, aunque la calidad y rapidez en el desarrollo de las funciones pueden verse alteradas

Tabla 6. Cumplimiento de Objetivos

- **Impacto de imagen (Reputación):** La ejecución de una amenaza detectada del riesgo podría ocasionar un duro golpe la imagen de las pymes financieras.

Escalas / Impacto		Reputacional (Imagen)	
3	Alta	La ocurrencia del riesgo generaría: - Cobertura de los medios de comunicación (prensa, televisión, radio e internet) a nivel local - Impacto de mediano plazo en la imagen de la pyme financiera	Reputación afectada entre 3 meses y 6 meses
2	Media	La ocurrencia del riesgo generaría: - Cobertura de los medios de comunicación (prensa, televisión, radio e internet) - Impacto pasajero en la imagen de la pyme financiera	Reputación afectada entre 1 mes y 3 meses
1	Baja	La ocurrencia del riesgo generaría cobertura en algún medio de comunicación (prensa, televisión, radio e internet) a nivel local, con acusaciones puntuales que afecten la imagen de la pyme financiera	Reputación afectada entre 1 semana y 1 mes

Tabla 7. Impacto Reputacional

- **Impacto Patrimonial:** La ejecución de un ataque de riesgo podría ocasionar fallas en las operaciones de las pymes financieras, generando perdidas en la Entidad.

Escalas / Impacto		Patrimonial
3	Alta	Daño patrimonial igual o superior a USD 100.000 e inferior a USD 1'000.000
2	Media	Daño patrimonial igual o superior a USD 10.000 e inferior a USD 100.000
1	Baja	Daño patrimonial igual o superior a USD 1.000 e inferior a USD 10.000

Tabla 8. Impacto Patrimonial

- **Impacto en la Continuidad de los Servicios:** La ejecución de un ataque de riesgo podría ocasionar un retraso temporal en la prestacion de servicios en la entidad.

Escalas / Impacto		Continuidad de los Servicios
3	Alta	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 1 hora e inferior a 4 horas
2	Media	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 4 hora e inferior a 1 día
1	Baja	El tiempo máximo en que el servicio debe ser recuperado es igual o superior a 1 día e inferior a 3 días

Tabla 9. Impacto en la Continuidad de los Servicios

Criterios de Evaluación de Vulnerabilidad

La vulnerabilidad es el nivel de exposición de las pymes financieras ante una amenaza determinada, es decir, la probabilidad de materialización de la amenaza. Se han definido los siguientes factores de vulnerabilidad para medir el criterio:

- **Controles y Mitigación:** evaluar el alcance de la exposición de las pymes financieras a la amenaza producto de ausencia de medidas de reacción como también a posibles errores en las medidas que se establecen previamente.
- **Probabilidad de Ocurrencia de Amenaza:** evaluar la ocurrencia y el periodo de presencia de causas potenciales de ataque que generan efectos de intromisión y a perdida de confidencialidad en la información de las PYMES financieras.

Los criterios para evaluar la probabilidad son los siguientes:

Escalas / Vulnerabilidad		Descripción
3	Alta	Los controles son identificativos, pero no preventivos, no existe reporte efectivo.
2	Media	Los controles son identificativos, pero no preventivos y hay reporte efectivo.
1	Baja	Los controles son apropiadamente identificativos y preventivos, pero no hay reporte efectivo.

Tabla 10. Criterios para Evaluar la Probabilidad

9.2. Anexo 2. Inventario de activos de la información

	INVENTARIO DE ACTIVOS DE INFORMACIÓN	FECHA:
		VERSIÓN: 01

No.	Nombre del activo	Tipo de activo	Activo del cual depende	Responsable del activo	Cargo- Departamento	Custodio del activo	Cargo- Departamento	Descripción	Ubicación	Proceso	Subproceso
1											
2											
3											
4											

9.3. Anexo 3. Ponderación y clasificación de los activos de información

	PONDERACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN	FECHA:
		VERSIÓN: 01

No.	Nombre del activo de información	Descripción	Tipo de Activo	PONDERACIÓN DE ACTIVOS DE INFORMACIÓN																			CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN		ACTIVO DE INFORMACIÓN CRÍTICO
				CONFIDENCIALIDAD (C)				INTEGRIDAD (I)				DISPONIBILIDAD (D)				RESUMEN DE IMPACTOS							IMPACTO TOTAL DEL ACTIVO	Nivel de Importancia	Nivel de Sensibilidad	
				Cumplimiento de Objetivo	Reputacional	Patrimonial	Continuidad de los Servicio	Cumplimiento de Objetiv	Reputacional	Patrimonial	Continuidad de los Servicio	Cumplimiento de Objetiv	Reputacional	Patrimonial	Continuidad de los Servicio	Cumplimiento de Objetivos	Reputacional	Patrimonial	Continuidad de los Servicios	CONFIDENCIALIDAD (C)	INTEGRIDAD (I)	DISPONIBILIDAD (D)				
1				0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	No Esencial		NO
2				0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	No Esencial		NO
3				0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	No Esencial		NO
4				0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	No Esencial		NO
5				0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00	No Esencial		NO

9.4. Anexo 4. Inventario de activos de información críticos

	INVENTARIO DE ACTIVOS DE INFORMACIÓN CRÍTICOS	FECHA:
		VERSIÓN: 01

No.	Nombre del activo	Tipo de activo	Activo del cual depende	Responsable del activo	Cargo- Departamento	Custodio del activo	Cargo- Departamento	Descripción	Ubicación	Proceso	Subproceso	RESUMEN DE IMPACTOS							IMPACTO TOTAL DEL ACTIVO	CLASIFICACIÓN	
												Cumplimiento de Objetivos	Reputacional	Patrimonial	Continuidad de los Servicios	CONFIDENCIALIDAD (C)	INTEGRIDAD (I)	DISPONIBILIDAD (D)		Nivel de Importancia	Nivel de Sensibilidad
1																					
2																					
3																					
4																					
5																					

9.5. Anexo 5. Amenazas y vulnerabilidades – tipo de activo

ESCALAS: PROBABILIDAD		DESCRIPCIÓN
4	ALTA	Los controles son detectivos, pero no preventivos, no existe reporte efectivo
3	MEDIA	Los controles son detectivos, pero no preventivos y hay reporte efectivo
2	BAJA	Los controles son apropiadamente detectivos y preventivos pero no hay reporte efectivo

					Impacto				Riesgo Aceptable		
No.	Nombre de Activo	Tipo de Activo	AMENAZA	VULNERABILIDAD	C	I	D	Probabilidad	C	I	D
1		- Software - Archivo Digital	Acceso no autorizado a datos	Comunicaciones sin cifrado	4.00	2.00	2	2	Si	Si	

9.6. Anexo 6. Lista de chequeo de controles – tipo de activo

	LISTA DE VERIFICACIÓN DE CONTROLES ESPECÍFICOS - TIPO DE ACTIVO	FECHA:
		VERSIÓN: 01

Nombre del Entrevistado	
Nombre del Entrevistador	
Fecha de Entrevista	

I. CONTROLES ADMINISTRATIVOS Y OPERATIVOS

No.	Nombre de Activo	Tipo de Activo	Control	Implementado	Comentarios
1		Software	Documento de configuración de seguridad para la aplicación que incluya: Los requerimientos y especificaciones de seguridad de la aplicación, la configuración o mantenimiento de la seguridad de la aplicación	SI	
2		Archivo Físico	¿Se ha definido una clasificación y etiquetamiento de los archivos físicos?	PARCIAL	
3		Archivo Digital	¿Se mantiene un control de versionamiento de los cambios realizados de archivo digital?	PARCIAL	
4		Hardware	Documento de configuración de seguridad para el Servidor que incluya: · Política y procedimiento de gestión de acceso	NO	
5		Personas	¿Existe documentación respectiva de cargos y/o funciones relacionadas con el proceso?	NO	
6		Instalaciones Físicas	Existe documentación respectiva: · Cargos y/o funciones relacionadas con la administración / Operación del centro de cómputo (Personal XYZ)	NO	
II. CONTROLES TÉCNICOS					
1		Software	Se configuran las políticas de contraseñas de manera adecuada (aplica para el Administrador de la aplicación como para los usuarios finales): · Usuario firma compromiso por uso de contraseña	SI	
2		Software	· Cambio periódico de contraseña	NO	
33		Archivo Físico	¿Se tiene control de acceso físico donde se encuentran los archivos físicos a través de elementos como: · Dispositivo biométrico	NO	
35		Archivo Digital	¿Se encuentra el archivo digital ubicado en una carpeta de red protegida?	NO	
40		Instalaciones Físicas	Existe un sistema de control de acceso al CDC e indicar cuál es: · Dispositivo Biométrico Facial	NO	
III. CONTROLES FÍSICOS					
2		Archivo Físico	· Controles de humedad e inundaciones	NO	
6		Hardware	El Servidor se encuentra dentro del Centro de Cómputo Quito?	NO	
7		Instalaciones Físicas	Se cuenta con: · Piso falso	NO	

Participantes en la Revisión:

9.7. Anexo 7. Matriz de riesgos de la seguridad de la información

	MATRIZ DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	FECHA:
		VERSIÓN: 01

										RIESGO RESIDUAL							RIESGO ADMINISTRADO									PLAN DE ADMINISTRACIÓN DE RIESGOS				
No.	ÁREA	DIRECCIÓN	PROCESO	Fecha ingreso del evento	Evento (Amenaza)	Causa (Vulnerabilidad)	Factor de Riesgo	Controles Existentes	Tipo de Control	Cumplimiento de Objetivos	Reputacional	Patrimonial	Continuidad de los servicios	Riesgo Residual Impacto	Riesgo Residual Probabilidad	Nivel de Riesgo Residual	Alternativas de Tratamiento	Opciones de Mejora	Cumplimiento de Objetivos	Reputacional	Patrimonial	Continuidad de los servicios	Riesgo Administrado Impacto	Riesgo Administrado Probabilidad	Nivel de Riesgo Administrado	Responsable implementación	Tiempo previsto para la implementación	Como la opción de tratamiento será monitoreado	Costo aproximado de implementar la opción	Ámbito de aplicación
1							Personas		Preventivo	0	0	0	0	0	0	BAJO	Mitigar el impacto		0		0	0	0	0	BAJO				No tiene costo	Nacional
2																														
3																														
4																														
5																														

10. Referencias

`

[1] ISO/IEC 27002:2022, «Information security controls,» 2022. [En línea]. Available: https://www.iso27001security.com/html/27002.html.

[2] ISO/IEC 27005:2022, «Information security risk management,» 2022. [En línea]. Available: https://www.iso27001security.com/html/27005.html.

[3] ISO 28002:2011, «ISO 28002:2011,» 2011. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso:28002:ed-1:v1:en:term:3.25.

[4] ISO/IEC 27000:2018, «Information security management,» 2018. [En línea]. Available: https://www.iso27001security.com/html/27000.html.

[5] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[6] Organización Internacional de Normalización, «ISO/IEC 27005:2022,» 2022. [En línea]. Available: https://www.iso.org/standard/80585.html.

[7] ISO/IEC 24765:2017, «Systems and software engineering,» 2017. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:ed-2:v1:en:term:3.3542.

[8] ISO 9001:2015 , «Quality management systems,» 2015. [En línea]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es.