**FACULTAD DE POSTGRADO**
**TRABAJO FINAL DE GRADUACIÓN**

# DISEÑO DE UNA ESTRATEGIA DE CIBERSEGURIDAD BASADA EN LAS NORMAS ISO/IEC 27001:2022 Y 27032:2023. CASO: MICROFINANCIERA PRISMA DE HONDURAS, 2025

**SUSTENTADO POR:**

**RAÚL HUMBERTO AGUILAR MEDINA**
**MARÍA EUGENIA CHACÓN MACÍAS**

**PREVIA INVESTIDURA AL TÍTULO DE**

**MÁSTER EN**
**GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN**

**TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.**

**ABRIL, 2025**

**UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA**

**UNITEC**

**FACULTAD DE POSTGRADO**

**AUTORIDADES UNIVERSITARIAS**

**RECTORA**

**ROSALPINA RODRÍGUEZ**

**VICERRECTOR ACADÉMICO NACIONAL**

**JAVIER ABRAHAM SALGADO LEZAMA**

**SECRETARIO GENERAL**

**ROGER MARTÍNEZ MIRALDA**

**DECANA FACULTAD DE POSTGRADO**

**ANA DEL CARMEN RETTALLY VARGAS**

# DISEÑO DE UNA ESTRATEGIA DE CIBERSEGURIDAD BASADA EN LAS NORMAS ISO/IEC 27001:2022 Y 27032:2023. CASO: MICROFINANCIERA PRISMA DE HONDURAS, 2025

**TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE**

**MÁSTER EN**

**GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN**


**ASESOR**

**JESÚS RICARDO RODRÍGUEZ RIVERA**

**MIEMBROS DE LA TERNA:**

**CARLOS ROBERTO AMADOR ALVARENGA**
**JOSÉ RODOLFO SORTO BUESO**
**ANTHONY STEVE BARAHONA ESPINOZA**

# FACULTAD DE POSTGRADO

# DISEÑO DE UNA ESTRATEGIA DE CIBERSEGURIDAD BASADA EN LAS NORMAS ISO/IEC 27001:2022 Y 27032:2023. CASO: MICROFINANCIERA PRISMA DE HONDURAS, 2025

**Raúl Humberto Aguilar Medina**
**María Eugenia Chacón Macías**

**Resumen**

La presente investigación diseñó una estrategia de ciberseguridad para la Microfinanciera PRISMA, alineada con las normas ISO/IEC 27001:2022, ISO/IEC 27032:2023 y el marco NIST CSF. Se utilizó una metodología de enfoque mixto, con un diseño no experimental y alcance descriptivo. La recolección de datos se realizó mediante entrevistas semiestructuradas y la aplicación de dos herramientas: la Matriz de Diagnóstico de Seguridad Global basada en ISO/IEC 27002:2022 y la herramienta MASS, dirigidas a una muestra de 8 colaboradores clave. Se evaluaron 93 controles distribuidos en los dominios organizativo, de personas, físicos y tecnológicos. Los resultados reflejaron que 31 controles (33.3%) presentaban niveles bajos de madurez: 8 en estado Existente, 19 en Inicial y 4 no aplicaban. El dominio organizativo fue el más crítico, con el 54% de sus controles en estados bajos, seguido del tecnológico con el 35.2%. En contraste, los dominios tecnológico y físico alcanzaron mayores niveles de madurez, con 15 controles tecnológicos en nivel Definido y 9 entre Cuantitativo y Optimizado. Se concluyó que PRISMA mantiene una madurez general entre los niveles Inicial y Gestionado, lo que evidencia la necesidad de una estrategia integral. Con base en estos hallazgos, se diseñó una propuesta estructurada en cinco fases, con definición de controles, indicadores, cronograma, presupuesto y mecanismos de mejora continua, orientada a fortalecer las capacidades de identificación, protección, detección, respuesta y recuperación frente a amenazas cibernéticas.

**Palabras claves: (Ciberataques, Ciberseguridad, Estrategia, Normativas, Riesgos)**

# GRADUATE SCHOOL

# DESIGN OF A CYBERSECURITY STRATEGY BASED ON ISO/IEC 27001:2022 AND 27032:2023 STANDARDS. CASE: MICROFINANCIERA PRISMA DE HONDURAS, 2025

**Raul Humberto Aguilar Medina**
**Maria Eugenia Chacon Macias**

**Abstract**

This research designed a cybersecurity strategy for Microfinanciera PRISMA, aligned with ISO/IEC 27001:2022, ISO/IEC 27032:2023 standards and the NIST CSF framework. A mixed-method approach was employed, with a non-experimental design and descriptive scope. Data was collected through semi-structured interviews and the application of two tools: the Global Security Diagnostic Matrix based on ISO/IEC 27002:2022 and the MASS tool, applied to a sample of 8 key collaborators. A total of 93 controls were evaluated across four domains: organizational, people, physical, and technological. Results revealed that 31 controls (33.3%) presented low maturity levels, with 8 classified as "Existing", 19 as "Initial," and 4 were deemed not applicable. The organizational domain was the most critical, with 54% of its controls in low maturity states, followed by the technological domain with 35.2%. The technological and physical domains showed higher maturity, with 15 technological controls at the "Defined" level and 9 at "Quantitative" or "Optimized" levels. It was concluded that PRISMA maintains a general maturity between "Initial" and "Managed" levels, highlighting the need for a comprehensive cybersecurity strategy. Based on these findings, a five-phase proposal was developed, detailing control definitions, indicators, implementation schedule, budget, and continuous improvement mechanisms, aimed to strengthen the organization's capabilities for identification, protection, detection, response, and recovery against cyber threats.

**Key Words: (Cyberattacks, Cybersecurity, Regulations, Risks, Strategy)**

# DEDICATORIA

El presente trabajo está dedicado, primero a mi familia, y segundo, a mis amigos por ser todos juntos, los pilares fundamentales de mi vida y celebrar junto a mí cada logro alcanzado.

Raúl Humberto Aguilar Medina

Dedico este trabajo a mi familia y seres queridos, quienes han sido mi soporte, mi equilibrio y mi razón de ser. Gracias a su fe inquebrantable en mí y su apoyo incondicional, he logrado culminar este capítulo de mi vida que hoy celebramos con profunda gratitud. Su felicidad sincera me llena y me motiva, pues ustedes son con quienes más deseo compartir este logro. Asimismo, lo dedico a las nuevas generaciones, especialmente a mis alumnos, con la esperanza de que este proyecto sirva como inspiración y ejemplo de que, con esfuerzo, valentía y compromiso, es posible alcanzar grandes metas. Este triunfo también es de ustedes.

María Eugenia Chacón Macías

# AGRADECIMIENTO

En primera instancia a Dios por ser el dador de la vida y permitirme avanzar en este hermoso desafío; a mi familia, por apoyarme en cada uno de los retos que he tenido en mi vida; a mi madre, por ser mi inspiración de perseverancia, esfuerzo, y siempre estar presente en cualquier circunstancia de mi vida; a mis hermanas y hermano, que siempre han creído en mí y me motivan a seguir adelante; a mis amigos y compañeros, que en más de una forma me han ayudado en este proceso de formación profesional.

Raúl Humberto Aguilar Medina

Al culminar este proyecto, agradezco profundamente las bendiciones y el apoyo recibido durante este significativo capítulo de mi vida. Agradezco a Dios por su guía, sabiduría y fortaleza, fuente constante de inspiración en cada paso del camino. A mi familia, especialmente a mis hijos, quienes con su amor incondicional han sido el pilar de este logro. A mis maestros y asesores, cuya orientación y enseñanzas me han enriquecido inmensamente, y a mis amigos y compañeros de trabajo, por su ánimo y compañía en los momentos desafiantes. A todos, mi gratitud eterna.

María Eugenia Chacón Macías

# ÍNDICE DE CONTENIDO

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

En este primer capítulo, se establece el marco general de la investigación, abordando la temática principal y contextualizándola a través de antecedentes basados en estudios previos. Asimismo, se define el problema de investigación, se plantean los objetivos y preguntas clave, y se expone la justificación del estudio. Además, se analiza el entorno en el que se desarrolla el proyecto, considerando su posible aplicabilidad en el futuro.

## 1.1 INTRODUCCIÓN

En un mundo cada vez más interconectado, las Tecnologías de la Información y Comunicación (TIC) se han convertido en el pilar fundamental de las operaciones de las organizaciones. Este avance tecnológico ha permitido a las empresas optimizar procesos, acceder a nuevos mercados y mejorar la experiencia del cliente. Sin embargo, también ha incrementado exponencialmente los riesgos asociados a la seguridad de la información, convirtiendo a la ciberseguridad en un elemento crítico para garantizar la continuidad operativa y la protección de activos digitales.

En este contexto, las microfinancieras, como parte esencial del sector financiero, no son ajenas a estas amenazas. Estas instituciones manejan grandes volúmenes de información sensible, tanto de sus clientes como de sus operaciones internas, lo que las convierte en objetivos atractivos para los ciberataques. La Microfinanciera PRISMA, ubicada en Honduras, enfrenta desafíos significativos en términos de protección de la información debido a la ausencia de una estrategia integral de ciberseguridad alineada a estándares internacionales como las normas ISO/IEC 27001 y 27032.

Las normas ISO/IEC 27001 e ISO/IEC 27032 proporcionan marcos metodológicos sólidos para gestionar y mitigar riesgos relacionados con la seguridad de la información y las amenazas cibernéticas. La implementación de estas normativas en la Microfinanciera PRISMA no solo fortalecerá los controles internos y la resiliencia organizacional, sino que también contribuirá a mejorar la confianza de los clientes y a garantizar el cumplimiento de normativas legales y regulatorias.

Esta investigación tiene como propósito diseñar una estrategia de ciberseguridad basada en los lineamientos de las normas mencionadas, adaptada a las características y necesidades

específicas de la Microfinanciera PRISMA.

El presente documento está estructurado en seis capítulos que abordan, de manera integral, el desarrollo de esta investigación:

El primer capítulo expone el planteamiento del problema, los objetivos y la justificación del proyecto.

El segundo capítulo desarrolla el marco teórico, analizando el contexto global, regional y local de la ciberseguridad, las bases conceptuales y las teorías que sustentan la investigación.

En el tercer capítulo, se describe la metodología utilizada, incluyendo el diseño de la investigación, el enfoque metodológico y los instrumentos aplicados para la recolección de datos.

El capítulo cuarto presenta los resultados obtenidos y el análisis de estos, destacando los hallazgos más relevantes.

En el quinto capítulo, se establecen las conclusiones y recomendaciones derivadas del estudio, orientadas a fortalecer la seguridad de la información en la Microfinanciera PRISMA.

Finalmente, el sexto capítulo se centra en la aplicabilidad de la propuesta, detallando las fases en las que se estructura, las medidas de control, el cronograma y el presupuesto estimado.

## 1.2 ANTECEDENTES DEL PROBLEMA

Durante los últimos años, se ha observado un aumento alarmante en la cantidad y sofisticación de los ciberataques, incidentes de seguridad y filtraciones de datos en diversas organizaciones. Estos eventos pueden tener consecuencias devastadoras, desde pérdidas económicas hasta daños en la reputación de las organizaciones, comprometiendo tanto su estabilidad como su credibilidad ante clientes, socios y reguladores. Algunos ejemplos recientes incluyen ataques masivos de ransomware, como WannaCry y NotPetya, que afectaron a empresas e instituciones en todo el mundo, bloqueando el acceso a sus sistemas críticos y exigiendo pagos para restaurar el acceso (Kaspersky, 2024).

El Informe Brecha de Competencias en Ciberseguridad (Fortinet, 2024) señala que, los riesgos son altos para las organizaciones, afectando principalmente las finanzas y la reputación de la empresa; y en respuesta, las organizaciones más actualizadas se enfocan en una triple ciberseguridad que combina: capacitación, concientización y tecnología (Fortinet, 2024). Además,

dicho informe destaca que los cinco principales ataques experimentados con más frecuencia entre 2022-2023 fueron: malware (44%), ataques de suplantación de identidad (36%), ataques web (31%), ataques de contraseñas (30%) y ataques de caballos de troya (29%).

En línea con lo anterior, el Informe Global de Riesgos del Foro Económico Mundial, destaca que los ciberataques y las violaciones de datos se encuentran entre las principales amenazas globales, tanto para el sector privado como para el público. Además, el cumplimiento de normativas cada vez más estrictas, como el Reglamento General de Protección de Datos (GDPR) en Europa y otras leyes locales, obliga a las empresas a implementar medidas de seguridad más robustas para proteger la privacidad de los datos personales (Foro Económico Mundial, 2022).

Por su parte, según el Informe Global sobre Ciberseguridad (Hays, 2024), la importancia de los esfuerzos coordinados en ciberseguridad por parte de los países ha aumentado significativamente: con 5,400 millones de personas conectadas a internet, incluso las poblaciones no conectadas se ven afectadas por los rápidos avances tecnológicos, la adopción de la inteligencia artificial y la digitalización.

En el entorno actual, la seguridad de la información ha evolucionado más allá del ámbito tecnológico, convirtiéndose en un componente estratégico dentro de las organizaciones. La creciente sofisticación de las amenazas cibernéticas y las exigencias normativas demandan un enfoque integral y transversal, en el que todas las áreas sean responsables de la gestión de riesgos y la protección de los activos digitales. Tanto en el sector público como en el privado, la implementación de controles técnicos efectivos, el fortalecimiento de la capacitación continua y un enfoque proactivo en ciberseguridad son elementos esenciales para reducir vulnerabilidades y mejorar la resiliencia organizacional.

En este contexto, la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con ISO/IEC 27001:2022, proporciona un marco estructurado para garantizar la confidencialidad, integridad y disponibilidad de la información. Asimismo, fortalecer la resiliencia cibernética y la capacidad de respuesta ante incidentes es clave para minimizar el impacto de amenazas emergentes. Finalmente, el desarrollo de una cultura organizacional de seguridad permite mitigar riesgos y asegurar la continuidad del negocio, fomentando una postura de ciberseguridad robusta y adaptable a un entorno digital en constante evolución.

A pesar de la existencia de estándares internacionales en ciberseguridad, muchas

organizaciones aún no cuentan con políticas de seguridad adecuadas o bien, su implementación es incompleta o ineficiente. Esto deja a las empresas vulnerables a amenazas internas y externas, exponiéndolas a pérdidas significativas de información sensible y de recursos. La carencia de una cultura organizacional que priorice la seguridad de la información, junto con la falta de concienciación de los empleados, agrava el problema, ya que muchas veces las violaciones de seguridad son resultado de errores humanos.

Las amenazas cibernéticas para las empresas son uno de los principales riesgos a los que se enfrentan hoy en día debido al incremento del uso de la tecnología y la dependencia de sistemas informáticos y datos digitales. Estas amenazas pueden comprometer la seguridad de los datos, interrumpir las operaciones, dañar la reputación de la empresa y provocar pérdidas financieras significativas. Estos eventos se ven potenciados en el ámbito de las microfinancieras, las cuales en muchas ocasiones no cuentan con estrategias bien definidas y mecanismos robustos para hacer frente a los ciberataques.

De acuerdo con el Diagnóstico Global de Ciberseguridad en las Instituciones Financieras de Microfinanzas (IMF) de América Latina y el Caribe, basado en el Cybersecurity Framework del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), la comparación entre IMF de países, así como en grupos de IMF con similares características, ofrece una perspectiva valiosa sobre la madurez de las funciones clave en el ámbito de la ciberseguridad, destacando que, Honduras tiene un nivel general de madurez en el marco del NIST que representa un puntaje promedio alcanzado para las IMF del 2,4 (en una escala de 1,0 al 5,0) lo que representa un bajo nivel de madurez en ciberseguridad a nivel de las microfinancieras (IMF Ciberseguridad, 2024).

En Latinoamérica el costo de violación de datos en las empresas representa un crecimiento significativo en pérdidas monetarias, se reporta que en el año 2022 se tuvo un promedio de $2.80 millones de dólares y que el año 2023 el costo promedio fue de aproximante de $3.69 millones de dólares, según el Data Breach Investigations Report 2024 (Verizon, 2024b).

Según el Informe de Investigación Global sobre la brecha de competencias en Ciberseguridad, el 87% de las organizaciones experimentó al menos una vulneración de seguridad durante el año, y más del 53% reportó pérdidas superiores a un millón de dólares debido a afectaciones en ingresos, sanciones regulatorias y otros costos asociados. Estos hallazgos

evidencian el impacto financiero significativo de las brechas de seguridad en el entorno empresarial global (Fortinet, 2024).

Según el informe Aproximación al Marco de Gobernanza de la Ciberseguridad (Centro Criptológico Nacional, 2022), una estrategia de ciberseguridad debe concebirse como un enfoque integral que trascienda el cumplimiento normativo:

> Más allá de establecer un marco rígido de cumplimiento y demandante de recursos, ofrece una hoja de ruta contrastada, metodológica y estructurada en fases, que, junto a las soluciones de seguridad disponibles, permite conocer, en primer término, la superficie de exposición a las amenazas, evaluar y tratar los riesgos y, además, justificar y poner en marcha un plan de mejora continua a corto, medio y largo plazo para la implementación de la seguridad en las organizaciones. (Centro Criptológico Nacional, 2022, p.5)

En este contexto, una estrategia de seguridad de la información y ciberseguridad se fundamenta en la implementación de controles diseñados para mitigar brechas, fortalecer la integridad, garantizar la disponibilidad y proteger la confidencialidad de la información en el ciberespacio. En esta línea, se establecen las siguientes normativas:

La ISO/IEC 27001 establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando un marco estructurado para la protección de activos de información y la mitigación de riesgos cibernéticos. Por su parte, la ISO/IEC 27032 define directrices estratégicas y operativas destinadas a fortalecer la postura de ciberseguridad en las organizaciones, abordando aspectos clave como la protección del ciberespacio, la gestión de amenazas y la cooperación entre actores involucrados en la seguridad digital.

Además, los controles y requisitos definidos en estas normativas se fundamentan en un enfoque de gestión de riesgos alineado con la ISO/IEC 27005, que proporciona metodologías específicas para la identificación, análisis y tratamiento de amenazas. Asimismo, el diseño del marco de ciberseguridad organizacional se complementa con las mejores prácticas establecidas en el Cybersecurity Framework del NIST, garantizando un enfoque integral que combina controles técnicos, procesos organizativos y estrategias de respuesta ante incidentes.

En el contexto centroamericano, las microfinancieras se han convertido en un blanco cada

vez más vulnerable frente a amenazas cibernéticas, especialmente debido a la acelerada digitalización posterior a la pandemia. De acuerdo con el Diagnóstico de la Situación Actual del Proyecto HO-L1202, Gobierno de Honduras; Banco Interamericano de Desarrollo & BID (2025), Honduras enfrentó alrededor de 1.8 millones de ciberataques durante el año 2023, lo que generó pérdidas económicas estimadas en 150 millones de dólares anuales. Aunque el informe no desagrega por sector, se advierte que sectores financieros, incluyendo a las microfinancieras, han sido recurrentemente afectados, particularmente por ataques de tipo ransomware, suplantación de identidad y accesos no autorizados. La Comisión Nacional de Bancos y Seguros (CNBS) ha reconocido esta vulnerabilidad al emitir normativas específicas para las instituciones supervisadas, lo que subraya la necesidad urgente de estrategias de ciberseguridad robustas en este sector.

En Honduras, las microfinancieras enfrentan importantes retos tales como: deficiencia en el diseño, desarrollo e implementación de políticas y procedimientos para la gestión integral de riesgos (liquidez, mercado, crediticio, operacional, legal); también debilidades en el fortalecimiento de la gestión crediticia: Políticas, procedimientos y tecnologías de información, (Falck & Ordóñez, 2009). Además, la implementación de estrategias actualizadas para reforzar los controles internos ante ataques y mantener una estructura de ciberseguridad adecuada a los cambios globalizados del mundo digital.

Las microfinancieras afiliadas a la Red de Microfinancieras de Honduras (REDMICROH), conformada por ocho entidades, operan como agentes financieros que, debido a su tamaño, no están sujetas a la regulación directa de la Comisión Nacional de Bancos y Seguros (CNBS). Sin embargo, estas instituciones forman parte de REDMICROH, una asociación que recopila y gestiona datos estadísticos y financieros de sus miembros, permitiendo un seguimiento estructurado de su impacto en el ecosistema financiero hondureño (Comisión Nacional de Bancos y Seguros, 2022).

Dentro de la Red de Microfinancieras de Honduras (REDMICROH) se encuentra la Microfinanciera PRISMA de Honduras S.A. (PRISMA), una entidad fundada en 2003 con el propósito de consolidar y expandir gradualmente sus operaciones en el mercado financiero hondureño. Su enfoque estratégico está dirigido a fortalecer su presencia en zonas donde ya opera, así como a identificar y desarrollar nuevos nichos de mercado potenciales. A pesar de no estar regulada por la Comisión Nacional de Bancos y Seguros (CNBS), PRISMA se encuentra afiliada

a REDMICROH, organismo que gestiona y mantiene información estadística sobre sus entidades asociadas.

Actualmente, PRISMA impulsa el fortalecimiento de su postura de ciberseguridad para mitigar riesgos cibernéticos internos y externos. La gestión eficaz de estas amenazas requiere un enfoque estratégico integral, en el que directivos, empleados, clientes y proveedores desempeñen un papel clave en la implementación de controles de seguridad, la protección de activos de información y el fortalecimiento de la resiliencia operativa ante escenarios de riesgo.

En este sentido, PRISMA debe adoptar una estrategia de ciberseguridad robusta, que defina controles efectivos, lineamientos claros y mecanismos de respuesta eficientes frente a incidentes. La integración de ISO/IEC 27001:2022 e ISO/IEC 27032:2023 proporciona un marco normativo esencial para reforzar la protección de los procesos críticos, mejorar la capacidad de respuesta ante amenazas emergentes y garantizar la continuidad operativa en un entorno digital dinámico.

## 1.3 DEFINICIÓN DEL PROBLEMA

### 1.3.1 ENUNCIADO DEL PROBLEMA

La Microfinanciera PRISMA enfrenta un reto significativo: la ausencia de una evaluación estructurada que determine su nivel de madurez en seguridad de la información, conforme a estándares y protocolos internacionales de ciberseguridad. La falta de este diagnóstico expone a la organización a riesgos cibernéticos y dificulta la implementación de una estrategia integral para mitigar sus vulnerabilidades.

Para garantizar la protección de la información y la continuidad operativa, es fundamental realizar un diagnóstico que permita definir controles y estrategias robustas, asegurando la confidencialidad, integridad y disponibilidad de los activos digitales. Sin un marco de control adecuado, la institución se expone a incidentes de seguridad que podrían comprometer su reputación y generar pérdidas financieras significativas.

Asimismo, es necesario establecer protocolos efectivos de detección, prevención y respuesta ante amenazas críticas, complementados con políticas de ciberseguridad bien definidas, que reduzcan el impacto de posibles eventos adversos y mitiguen las implicaciones operativas y legales derivadas de futuras brechas de seguridad.

### 1.3.2 FORMULACIÓN DEL PROBLEMA

La Microfinanciera PRISMA enfrenta el desafío inminente de desarrollar e implementar una estrategia de ciberseguridad adaptada a sus necesidades específicas. En un panorama donde los ciberataques son cada vez más sofisticados y recurrentes, resulta indispensable que la organización identifique y gestione de manera proactiva los riesgos que comprometen su operatividad.

Dicha estrategia debe ir más allá de la mera prevención de incidentes, integrando mecanismos que fortalezcan la resiliencia organizacional y la capacidad de respuesta ante amenazas futuras. La adopción de controles efectivos y protocolos estructurados es esencial para preservar la continuidad del negocio y la protección de los activos de información.

No abordar este problema de manera estratégica podría exponer gravemente la estabilidad operativa de PRISMA, generando no solo impactos financieros significativos, sino también afectaciones reputacionales que comprometan la confianza de clientes y socios comerciales en el mercado.

### 1.3.3 PREGUNTAS DE INVESTIGACIÓN

El diseño de una estrategia de ciberseguridad alineada con los estándares ISO/IEC 27001:2022 e ISO/IEC 27032:2023 requiere un enfoque metodológico que permita identificar los principales desafíos en la protección de la información dentro de la Microfinanciera PRISMA. Para ello, es fundamental formular preguntas de investigación que orienten el estudio hacia la evaluación del nivel de madurez en ciberseguridad, la identificación de riesgos críticos y la definición de controles adecuados.

Las preguntas planteadas abordan aspectos clave, como el cumplimiento normativo, la efectividad de los controles existentes y la capacidad de respuesta ante incidentes de seguridad. Asimismo, estructuran el análisis de los hallazgos y fundamentan la formulación de una estrategia integral que fortalezca la protección de los activos de información y reduzca la exposición a amenazas digitales.

#### 1.3.3.1. PREGUNTA PRINCIPAL

¿Cómo diseñar una estrategia de ciberseguridad adaptada a las necesidades de la Microfinanciera PRISMA que, basada en la evaluación de su nivel de madurez en ciberseguridad,

fortalezca la protección de los activos de información y garantice el cumplimiento de los estándares ISO/IEC 27001:2022 e ISO/IEC 27032:2023?

#### 1.3.3.2. PREGUNTAS SECUNDARIAS

1. ¿Cuál es el estado actual de la ciberseguridad en la Microfinanciera PRISMA en relación con los controles y procesos establecidos en las normas ISO/IEC 27001:2022 y 27032:2023?
2. ¿Qué nivel de madurez presenta la Microfinanciera PRISMA en el cumplimiento de los controles de ciberseguridad, según los criterios e indicadores definidos en las normas ISO/IEC 27001:2022 y 27032:2023?
3. ¿Qué estrategias y controles pueden diseñarse para fortalecer la protección de la información en PRISMA, dentro de un marco de ciberseguridad alineado con las normas ISO/IEC 27001:2022 y 27032:2023?

## 1.4 OBJETIVOS DE LA INVESTIGACIÓN

### 1.4.1 OBJETIVO GENERAL

Diseñar una estrategia de ciberseguridad para la Microfinanciera PRISMA, basada en un diagnóstico integral de su estado actual y una evaluación del nivel de madurez en el cumplimiento de controles, que permita establecer recomendaciones y medidas alineadas con las normas ISO/IEC 27001:2022 y 27032:2023.

### 1.4.2 OBJETIVOS ESPECÍFICOS

1. Diagnosticar el estado actual de la ciberseguridad en la Microfinanciera PRISMA, evaluando el grado de cumplimiento de sus controles y procesos conforme a los lineamientos de las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023.
2. Determinar el nivel de madurez en ciberseguridad que presenta PRISMA, mediante indicadores basados en estándares internacionales, con el propósito de identificar brechas, riesgos críticos y oportunidades de mejora.
3. Diseñar estrategias y controles específicos para el fortalecimiento de la protección de la información en PRISMA, estructurando una propuesta de ciberseguridad alineada con los marcos ISO/IEC 27001:2022 e ISO/IEC 27032:2023.

## 1.5 JUSTIFICACIÓN

En los últimos años, los ataques cibernéticos han aumentado exponencialmente a nivel global, afectando a empresas de todos los sectores; según (Harán, 2023) en el informe ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina, el 69% de las organizaciones de América Latina sufrió algún incidente de seguridad durante el último año. En tal sentido, los países con el mayor porcentaje de detecciones de códigos maliciosos en campañas de phishing son Ecuador 8%, seguido por Costa Rica 7,2%, Colombia 5,7%, Guatemala 5,2% y El Salvador 5,1%. En Honduras, diversas instituciones financieras han sido blanco de ataques de ransomware, fraudes electrónicos y filtraciones de datos que han comprometido información confidencial de clientes y generado pérdidas económicas significativas.

A pesar de este panorama de riesgo creciente, la Microfinanciera PRISMA no cuenta con un diagnóstico formal sobre su nivel de madurez en seguridad de la información, ni con una estrategia integral de ciberseguridad alineada con estándares internacionales. La ausencia de protocolos de detección, prevención y respuesta ante amenazas cibernéticas expone a la organización a brechas de seguridad, pérdida de datos sensibles, fraudes internos y posibles sanciones regulatorias. Además, la falta de una cultura de ciberseguridad y de capacitación del personal aumenta la vulnerabilidad ante ataques de ingeniería social y accesos no autorizados.

Para reducir la exposición a amenazas cibernéticas y garantizar la confidencialidad, integridad y disponibilidad de la información, es fundamental diseñar una estrategia de ciberseguridad que fortalezca la postura de seguridad de PRISMA. La adopción de controles alineados con las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023 permitirá establecer medidas de protección efectivas, mejorar el monitoreo de riesgos y optimizar los mecanismos de respuesta ante incidentes.

Esta investigación proporcionará a PRISMA un marco metodológico estructurado para evaluar su estado actual en seguridad de la información, identificando brechas y vulnerabilidades críticas. A partir de este diagnóstico, se formularán recomendaciones prácticas que permitirán a la microfinanciera reducir riesgos operativos, mejorar la confianza de sus clientes y cumplir con las normativas de protección de datos.

Además, los resultados de este estudio podrán ser replicables y escalables en otras microfinancieras del país, brindando una hoja de ruta adaptable para instituciones con

características y desafíos similares. De esta manera, la investigación no solo fortalecerá la ciberseguridad de PRISMA, sino que también contribuirá a la madurez digital del sector financiero en Honduras.

# CAPÍTULO II. MARCO TEÓRICO

## 2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

### 2.1.1 ESTADO ACTUAL DE LA CIBERSEGURIDAD A NIVEL GLOBAL Y REGIONAL

En el contexto global, la ciberseguridad se ha convertido en una prioridad estratégica para gobiernos y empresas debido al incremento de amenazas cibernéticas. Según Stallings, (2022), "las organizaciones deben adoptar un enfoque proactivo en la gestión de riesgos, implementando marcos normativos que permitan una protección efectiva de la información" (p. 45). La rápida digitalización ha generado nuevas superficies de ataque, impulsando la adopción de estándares internacionales como la ISO/IEC 27001:2022 y la ISO/IEC 27032:2023.

A nivel regional, América Latina enfrenta retos significativos en materia de ciberseguridad. Un informe de la Organización de Estados Americanos (OEA) (2023) señala que "más del 60% de las empresas en la región no cuentan con planes de respuesta ante incidentes de ciberseguridad, lo que las deja vulnerables a ataques de ransomware y robo de datos" (p. 12). En Honduras, la ciberseguridad aún es un desafío emergente, con esfuerzos gubernamentales liderados por la Dirección General de Regulación (DIGER) y otras entidades del sector financiero (Ramírez & Gómez, 2021).

El panorama actual de la ciberseguridad, tanto a nivel global como regional, evidencia la creciente necesidad de un enfoque integral para la gestión de riesgos cibernéticos. Si bien los avances en normativas y estándares han permitido un mejor control de los incidentes de seguridad, las constantes amenazas demuestran que la implementación de marcos como ISO/IEC 27001:2022 y 27032:2023 debe ir acompañada de estrategias de capacitación y concienciación. La falta de inversión en infraestructura de ciberseguridad en países en vías de desarrollo sigue siendo un obstáculo para alcanzar niveles óptimos de protección.

### 2.1.2 TENDENCIAS Y DESAFÍOS EN LA PROTECCIÓN DE DATOS FINANCIEROS

El sector financiero es uno de los más afectados por ciberataques, dada la sensibilidad de los datos que maneja. Según un estudio de Anderson & Moore (2022), "las amenazas dirigidas a instituciones financieras han evolucionado, pasando de ataques directos a bancos a sofisticadas

campañas de phishing y fraude digital" (p. 33). Las tendencias actuales incluyen el uso de inteligencia artificial para la detección de fraudes y la implementación de tecnologías de cifrado avanzadas para la protección de datos.

Uno de los principales desafíos es la creciente sofisticación de los ataques. De acuerdo con Pérez & Rodríguez (2023), "el auge del ransomware como servicio (RaaS) ha permitido que incluso ciberdelincuentes sin conocimientos avanzados lancen ataques devastadores contra empresas y entidades gubernamentales" (p. 67). Este fenómeno ha llevado a un aumento en la inversión en soluciones de ciberseguridad, particularmente en la adopción de marcos como Zero Trust y el fortalecimiento de la autenticación multifactor.

### 2.1.3 REGULACIONES Y NORMATIVAS VIGENTES EN HONDURAS SOBRE CIBERSEGURIDAD

En Honduras, la regulación en materia de ciberseguridad ha avanzado en los últimos años, aunque aún existen brechas significativas. La Ley de Protección de Datos Personales, que se encuentra en proceso de desarrollo, establece lineamientos generales para el resguardo de información, pero carece de un enfoque específico en ciberseguridad (López, 2021a). A nivel financiero, la Comisión Nacional de Bancos y Seguros (CNBS) ha implementado normativas de gestión de riesgos tecnológicos alineadas con estándares internacionales, aunque su cumplimiento es variable entre las entidades supervisadas (Mendoza & Castillo, 2022a).

Además, Honduras ha buscado alinearse con marcos globales a través de iniciativas lideradas por DIGER y el Banco Central de Honduras. Según un informe del Foro Económico Mundial (2023) "los países en vías de desarrollo enfrentan retos adicionales en la implementación de estrategias nacionales de ciberseguridad debido a limitaciones en infraestructura y capacidades técnicas" (p. 23). En este sentido, la adopción de normativas como la ISO/IEC 27001:2022 y 27032:2023 podría fortalecer la postura de ciberseguridad en el sector financiero hondureño.

En el contexto hondureño, la regulación en ciberseguridad ha mostrado avances, pero aún enfrenta retos en términos de aplicación y cumplimiento. La adopción de normativas internacionales es un paso positivo, pero su efectividad dependerá en gran medida de la supervisión y del compromiso de las entidades gubernamentales y del sector financiero. La falta de una cultura de seguridad digital y la escasez de profesionales especializados en ciberseguridad representan

desafíos adicionales que deben ser abordados para fortalecer la postura del país frente a amenazas emergentes.

## 2.2 MACROENTORNO Y MICROENTORNO

### 2.2.1 MACROENTORNO DE LA CIBERSEGURIDAD

#### 2.2.1.1 PERSPECTIVA GLOBAL

A nivel global, la ciberseguridad sigue siendo una de las principales preocupaciones de organizaciones e instituciones gubernamentales. Según el Informe Cost of a Data Breach de IBM Security (2024), el costo promedio de una brecha de seguridad ha alcanzado los 4.45 millones de dólares, representando un incremento del 15% en los últimos tres años. "La falta de medidas de ciberseguridad efectivas no solo genera pérdidas económicas, sino también un daño irreparable a la reputación y confianza de los clientes" (IBM Security, 2024, p. 23).

La norma ISO/IEC 27001:2022 ha sido ampliamente adoptada como un marco esencial para la gestión de la seguridad de la información en respuesta al aumento de ciberataques. Según el 2024 Data Breach Investigations Report de Verizon, 83% de los incidentes de seguridad involucran factores humanos, como errores de configuración o phishing (Verizon, 2024). Esto refuerza la importancia de estrategias de ciberseguridad que incluyan capacitación y concienciación en seguridad digital, tal como lo establece la ISO/IEC 27001:2022.

El Global Risks Report 2024 del World Economic Forum (WEF, 2024) señala que las amenazas cibernéticas han sido clasificadas como uno de los cinco mayores riesgos globales para la estabilidad económica y social en la próxima década. "El aumento en la sofisticación de los ataques, combinado con la falta de regulación efectiva en algunos países, representa un desafío crítico para la seguridad digital" (WEF, 2024, p. 12). Este informe destaca la necesidad de marcos normativos como la ISO/IEC 27032:2023, que enfatiza la ciberseguridad colaborativa y la gestión de incidentes a nivel global.

Además del aumento en la sofisticación de los ataques, las empresas están adoptando estrategias proactivas para mitigar riesgos. Según el 2024 Data Breach Investigations Report de Verizon, el 94% de los incidentes cibernéticos están vinculados con actores externos, destacando la importancia de fortalecer los sistemas de defensa perimetral (Verizon, 2024). En este sentido, la norma ISO/IEC 27001:2022 establece controles específicos para la detección temprana y la

respuesta a incidentes, lo que permite minimizar el impacto de las vulnerabilidades. Por otro lado, el Global Risks Report 2024 señala que los ciberataques dirigidos a infraestructuras críticas, como el sector financiero y de telecomunicaciones, han aumentado un 30% en los últimos dos años (WEF, 2024) . Esto refuerza la importancia de implementar normas internacionales como ISO/IEC 27032:2023, que se centran en la gestión de riesgos colaborativos entre entidades gubernamentales y privadas.

#### 2.2.1.2 PERSPECTIVA LATINOAMERICANA

En América Latina, la situación de la ciberseguridad presenta desafíos significativos debido al crecimiento acelerado de la digitalización y la falta de regulaciones homogéneas en la región. Según el Reporte de Ciberseguridad 2025 de eDigital Chile, el 75% de las empresas latinoamericanas no cuentan con una estrategia formal de ciberseguridad basada en estándares internacionales (eDigital Chile, 2025). "Las microfinancieras y pymes son los sectores más vulnerables, pues carecen de recursos y personal especializado para implementar normativas como ISO 27001" (eDigital Chile, 2025, p. 34).

El Informe Cost of a Data Breach de IBM (2024) también resalta que en Latinoamérica, el sector financiero es el más afectado por ataques cibernéticos, con un costo promedio de 3.5 millones de dólares por incidente. Esto ha llevado a países como México, Brasil y Argentina a fortalecer sus regulaciones, promoviendo el cumplimiento de normas como ISO/IEC 27001:2022 y 27032:2023 (IBM Security, 2024).

Por su parte, el 2024 Data Breach Investigations Report de Verizon identifica que en Latinoamérica, el ransomware representa el 25% de los ataques registrados, superando la media global del 24% (Verizon, 2024). Esta tendencia resalta la urgencia de aplicar estrategias de ciberseguridad preventivas y reactivas basadas en estándares internacionales.

En la región, los ataques a sistemas financieros han evolucionado con técnicas cada vez más avanzadas, afectando tanto a grandes corporaciones como a microfinancieras. El Cost of a Data Breach Report de (IBM Security, 2024) indica que el tiempo promedio para identificar y contener una brecha de datos en América Latina es de 265 días, superior a la media global de 212 días, lo que evidencia la necesidad de fortalecer los protocolos de seguridad basados en ISO/IEC 27001 (IBM Security, 2024). Adicionalmente, el Reporte de Ciberseguridad 2025 de eDigital Chile menciona que el 48% de las empresas en la región han sido víctimas de al menos un intento

de ataque en el último año, pero solo el 20% ha implementado medidas preventivas eficaces (eDigital Chile, 2025). Este rezago en la adopción de estrategias de ciberseguridad refuerza la importancia de contar con normativas como la ISO/IEC 27032:2023, que promueven un enfoque estructurado en la gestión de amenazas cibernéticas.

#### 2.2.1.3 PERSPECTIVA CENTROAMERICANA

En Centroamérica, la ciberseguridad aún enfrenta barreras importantes debido a la baja inversión tecnológica y la falta de legislación robusta en muchos países. Según el Global Risks Report 2024 del World Economic Forum, las economías emergentes en América Central tienen mayor riesgo de sufrir ciberataques debido a infraestructuras tecnológicas obsoletas y la limitada preparación de sus instituciones financieras (WEF, 2024).

El Reporte de Ciberseguridad 2025 de eDigital Chile indica que Honduras y El Salvador están entre los países más vulnerables a ataques cibernéticos en la región, con un aumento del 60% en intentos de fraude digital en el último año (eDigital Chile, 2025). Esto pone de manifiesto la necesidad de que el sector financiero adopte normas como ISO/IEC 27001:2022, las cuales pueden mejorar la gestión de riesgos y la protección de la información en las microfinancieras.

El Informe Cost of a Data Breach de IBM Security (2024)IBM también destaca que las empresas en países con regulaciones más laxas tardan hasta 30 días adicionales en identificar y contener un incidente de seguridad, lo que agrava las pérdidas económicas (IBM Security, 2024). En este contexto, la adopción de estándares internacionales se presenta como una estrategia clave para reducir la brecha en ciberseguridad en Centroamérica.

La ciberseguridad en Centroamérica sigue siendo un desafío crítico, principalmente por la falta de infraestructura y capacitación especializada. Según el Global Risks Report 2024, la región tiene un déficit del 65% en profesionales capacitados en ciberseguridad, lo que dificulta la implementación efectiva de estándares como ISO/IEC 27001:2022 (WEF, 2024). En este sentido, el Cost of a Data Breach Report de IBM Security (2024) advierte que el tiempo de respuesta ante incidentes en Centroamérica es hasta un 35% más largo que en mercados más desarrollados, lo que expone a las instituciones a mayores pérdidas económicas (IBM Security, 2024).

Por otro lado, el Reporte de Ciberseguridad 2025 de eDigital Chile destaca que Honduras y Guatemala han comenzado a fortalecer su legislación en seguridad digital, incorporando

elementos de la ISO/IEC 27032:2023 en sus regulaciones para mejorar la protección de infraestructuras críticas (eDigital Chile, 2025).

### 2.2.2 MICROENTORNO DE LA CIBERSEGURIDAD EN HONDURAS

#### 2.2.2.1 ESTADO ACTUAL DE LA CIBERSEGURIDAD EN HONDURAS

En Honduras, la ciberseguridad enfrenta desafíos estructurales derivados de la falta de normativas especializadas y la carencia de recursos para la implementación de medidas de protección en sectores críticos. Según el Reporte de Ciberseguridad en Honduras 2024 de la Dirección General de Regulación (DIGER, 2024), el 62% de las instituciones financieras han sido objeto de intentos de ataques cibernéticos, con el phishing y el ransomware como principales amenazas.

En esta misma línea, el informe Paso a Paso para una Política de Seguridad Integral en Honduras de IPANDETEC (2024) destaca que uno de los principales obstáculos para la adopción de normativas internacionales en el país es la falta de una estrategia clara de gobernanza digital, lo que impide la correcta aplicación de estándares como ISO/IEC 27001:2022 y 27032:2023.

Adicionalmente, el estudio La Brecha Existente en Ciberseguridad en Honduras Raudales Centeno (2017) identifica que la infraestructura digital de Honduras presenta una alta vulnerabilidad debido a la insuficiente inversión en tecnologías de protección. Según Raudales Centeno (2017), "Honduras ha avanzado en conectividad, pero carece de un enfoque integral para la gestión de riesgos cibernéticos, lo que expone a las empresas y al sector público a ciberamenazas de alto impacto" (p. 31). Esta situación sigue vigente en 2024, donde la mayoría de las organizaciones aún no han implementado medidas preventivas adecuadas.

El contexto normativo también representa un reto significativo. Según la Organización de Estados Americanos (OEA, 2024), Honduras sigue en proceso de consolidación de su Estrategia Nacional de Ciberseguridad, con avances limitados en la adopción de estándares internacionales. Esto se traduce en brechas de seguridad que impactan a sectores estratégicos como el financiero y el gubernamental, facilitando el incremento de ciberataques.

Uno de los desafíos más críticos en la ciberseguridad hondureña es la falta de una legislación específica que regule la protección de datos y los protocolos de respuesta ante incidentes cibernéticos. Según el informe Paso a Paso para una Política de Seguridad Integral en

Honduras de IPANDETEC (2024), Honduras aún no cuenta con una ley de protección de datos de alcance nacional, lo que deja a empresas y ciudadanos sin un marco legal claro para la gestión de incidentes de seguridad digital. Esta carencia dificulta la aplicación efectiva de normativas como ISO/IEC 27001:2022 y ISO/IEC 27032:2023, ya que no existen requisitos obligatorios que impulsen su adopción en las organizaciones (IPANDETEC, 2024). En contraste, países vecinos como Costa Rica y Panamá han desarrollado legislaciones más avanzadas en ciberseguridad, lo que les ha permitido reducir su exposición a ciberataques y fomentar una mayor confianza digital en sus sectores económicos.

#### 2.2.2.2 CIBERSEGURIDAD EN EL SECTOR FINANCIERO HONDUREÑO

El sector financiero, incluyendo bancos y microfinancieras, ha sido uno de los más afectados por los ciberataques en Honduras. Según el Reporte de Seguridad Financiera 2024 del Banco Central de Honduras (BCH, 2024), el 45% de las instituciones financieras ha experimentado intentos de fraude digital en el último año, con pérdidas estimadas en más de 20 millones de lempiras. Estas cifras reflejan la creciente sofisticación de las amenazas y la necesidad de implementar controles de seguridad basados en estándares internacionales.

La falta de capacitación y concienciación en ciberseguridad sigue siendo un problema en el sector financiero hondureño. Un estudio de la Universidad Nacional Autónoma de Honduras (UNAH, 2023) destaca que el 60% de los empleados del sector financiero no ha recibido formación en seguridad digital en los últimos dos años, lo que incrementa la probabilidad de que sean víctimas de ataques de ingeniería social. Como señala (López, 2022), "la educación en ciberseguridad es un componente clave para reducir la vulnerabilidad de las organizaciones ante amenazas emergentes" (p. 56).

Las microfinancieras en Honduras enfrentan desafíos significativos en la implementación de normativas de seguridad de la información. Según el Informe de Evaluación Mutua de la República de Honduras (GAFILAT, 2016), se constató que, aunque existen esfuerzos por implementar normas de seguridad, persisten limitaciones en recursos y capacitación que dificultan su adopción efectiva. El informe señala que "todas las normas de seguridad de información están siendo implementadas por sus funcionarios"; sin embargo, la falta de infraestructura adecuada y apoyo institucional limita su eficacia (GAFILAT, 2016, p. 247). Esta situación refleja la necesidad de fortalecer las capacidades técnicas y financieras de las microfinancieras para cumplir con

estándares internacionales como la ISO/IEC 27001.

A pesar de estos desafíos, algunas entidades financieras en Honduras han comenzado a tomar medidas para fortalecer su postura en ciberseguridad. Según el Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe de la Organización de los Estados Americanos (OEA, 2023), el 68% de las entidades bancarias en la región han adoptado las normas ISO 27001, lo que refleja un compromiso creciente con la seguridad de la información. Además, el informe destaca que "en el 72% de las entidades bancarias, la junta directiva recibe reportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital" (OEA, 2023, p. 8), lo que indica una mayor atención de la alta dirección hacia la ciberseguridad. Aunque no se dispone de datos específicos para Honduras, estas tendencias regionales sugieren que las instituciones financieras hondureñas están alineándose con las mejores prácticas en seguridad digital.

El impacto económico de los ciberataques en el sector financiero hondureño sigue en aumento. Según el estudio Microfinanzas en Honduras, las instituciones microfinancieras dependen en gran medida de sistemas digitales para la gestión de créditos y pagos, pero pocas han implementado estrategias de ciberseguridad robustas. En el contexto actual, este problema sigue sin resolverse, ya que muchas microfinancieras continúan operando con infraestructuras tecnológicas desactualizadas, lo que las hace más vulnerables a ataques cibernéticos (Sánchez, 2010).

#### 2.2.2.3 ESTRATEGIAS Y AVANCES EN LA IMPLEMENTACIÓN DE NORMATIVAS DE CIBERSEGURIDAD

La adopción de normativas internacionales como ISO/IEC 27001:2022 e ISO/IEC 27032:2023 en Honduras aún es incipiente, pero existen iniciativas que buscan fortalecer la seguridad digital en el país. Según el Plan Estratégico de Ciberseguridad 2025 de DIGER, se espera que para 2026 al menos el 50% de las instituciones gubernamentales y financieras adopten estándares internacionales en sus estrategias de seguridad de la información (DIGER, 2025).

Un estudio de la Facultad de Ingeniería de la UNAH revela que la falta de incentivos gubernamentales y la carencia de marcos regulatorios claros han sido factores que han retrasado la implementación de normativas como ISO/IEC 27001 en las empresas hondureñas (UNAH, 2023). Esto demuestra la necesidad de una mayor intervención estatal para promover la adopción de estándares de ciberseguridad en el país.

El sector privado también ha comenzado a jugar un papel clave en la promoción de buenas prácticas en ciberseguridad. Según el Informe sobre Seguridad Empresarial en Honduras 2024 de la Cámara de Comercio e Industria de Tegucigalpa, el 40% de las grandes empresas en el país han comenzado a implementar políticas de seguridad basadas en normativas internacionales, aunque su aplicación en pymes y microfinancieras sigue siendo limitada (CCIT, 2024). Por otro lado, la cooperación internacional está desempeñando un papel fundamental en la mejora de la ciberseguridad en Honduras. Según el Programa de Cooperación en Ciberseguridad para Centroamérica (PCCC, 2024), Honduras ha recibido apoyo de organismos como la OEA y el Banco Mundial para fortalecer sus capacidades en seguridad digital y mejorar la implementación de estándares internacionales en entidades gubernamentales y privadas (PCCC, 2024).

En términos de adopción de normativas internacionales, Honduras aún enfrenta dificultades en la implementación de marcos de ciberseguridad a nivel gubernamental y privado. Según el informe La Brecha Existente en Ciberseguridad en Honduras, uno de los principales problemas es la falta de una estrategia nacional con plazos y objetivos concretos para la adopción de estándares internacionales. Raudales Centeno (2017) advierte que, "sin una estructura regulatoria clara, las empresas y entidades gubernamentales no tienen incentivos para cumplir con estándares como ISO/IEC 27001, dejando a Honduras rezagado en seguridad digital" (p. 39). A pesar de estos desafíos, el Programa de Cooperación en Ciberseguridad para Centroamérica (PCCC, 2024) ha iniciado capacitaciones y programas de financiamiento para ayudar a las organizaciones hondureñas a implementar medidas de protección alineadas con las mejores prácticas internacionales, lo que representa un paso positivo para mejorar la seguridad digital en el país.

### 2.2.3 ANÁLISIS FODA DE PRISMA EN TÉRMINOS DE CIBERSEGURIDAD

El análisis FODA permite evaluar la posición actual de PRISMA en materia de ciberseguridad y establecer estrategias para mitigar riesgos. Esta herramienta revela una combinación de elementos que influyen en la resiliencia de la institución frente a amenazas digitales. Desde una perspectiva experta en seguridad informática, se pueden extraer conclusiones críticas sobre los factores internos y externos que condicionan la postura de seguridad de la organización.


**Figura 1. FODA de PRISMA de Honduras en relación con Ciberseguridad**

Fuente: Elaboración Propia

#### 2.2.3.1 FORTALEZAS Y OPORTUNIDADES: BASES PARA UNA ESTRATEGIA DE SEGURIDAD SOSTENIBLE

Las fortalezas identificadas, como la adopción inicial de normativas internacionales y el compromiso de la alta dirección, representan un punto de partida positivo. No obstante, según la literatura en gestión de riesgos cibernéticos, la simple implementación de marcos regulatorios no garantiza una postura robusta en ciberseguridad (Stallings, 2022). La existencia de sistemas básicos de protección es un elemento esencial, pero insuficiente si no se complementa con un enfoque holístico que abarque tecnología, procesos y capacitación.

Desde la óptica de un especialista en seguridad, las oportunidades reflejan un entorno propicio para el crecimiento y la mejora. La implementación de ISO/IEC 27001:2022 y 27032:2023 permite estandarizar procesos de gestión de riesgos y respuesta a incidentes, lo que incrementa la madurez en ciberseguridad (Mendoza & Castillo, 2022). Asimismo, la expansión del sector Fintech en Honduras puede facilitar la adopción de herramientas tecnológicas avanzadas, incluyendo inteligencia artificial y análisis de comportamiento para la detección de fraudes. Sin embargo, la clave radica en la capacidad de la organización para aprovechar estas oportunidades de manera efectiva y estructurada.

#### 2.2.3.2 DEBILIDADES Y AMENAZAS: RIESGOS LATENTES EN UN ENTORNO VULNERABLE

Uno de los aspectos más críticos del análisis es la falta de una cultura organizacional enfocada en ciberseguridad. Según Anderson & Moore (2022), más del 80% de las brechas de seguridad en el sector financiero están vinculadas al error humano o a fallas en los procedimientos internos. La ausencia de programas de capacitación periódica no solo expone a PRISMA a incidentes de phishing o malware, sino que también limita su capacidad de respuesta ante ciberataques avanzados.

La dependencia de proveedores externos con controles de seguridad poco estrictos es otra debilidad que debe ser abordada con urgencia. En un ecosistema financiero donde los servicios de TI son cada vez más tercerizados, la gestión de riesgos en la cadena de suministro es fundamental (Foro Económico Mundial, 2023). Un proveedor que no cumpla con estándares adecuados puede convertirse en un punto de entrada para actores malintencionados, facilitando ataques como el supply chain attack o ataque a la cadena de suministro.

Las amenazas identificadas en el análisis FODA reflejan una tendencia global en la evolución del cibercrimen, caracterizada por la creciente sofisticación de los ataques y la diversificación de vectores de compromiso. En el contexto de América Latina, las instituciones financieras han emergido como objetivos prioritarios para actores maliciosos, dado el valor estratégico de los activos digitales y la acelerada transformación digital del sector (OEA, 2023). Entre las principales tácticas observadas se encuentran el uso de ransomware dirigido, ataques a la cadena de suministro, compromiso de credenciales mediante ingeniería social avanzada y explotación de vulnerabilidades en infraestructuras críticas.

En este sentido, PRISMA debe adoptar un enfoque proactivo y basado en inteligencia de amenazas, priorizando el monitoreo continuo del panorama de riesgos y la implementación de estrategias de detección, respuesta y resiliencia adaptativa. Solo a través de una arquitectura de seguridad dinámica y centrada en la mitigación de riesgos en tiempo real, PRISMA podrá reducir su superficie de ataque y aumentar su capacidad de recuperación frente a incidentes cibernéticos avanzados.

## 2.3 TEORÍAS DE SUSTENTO

### 2.3.1 TEORÍA GENERAL DE SISTEMAS: APLICACIÓN AL DISEÑO DE ESTRATEGIAS DE CIBERSEGURIDAD

La Teoría General de Sistemas (TGS), propuesta por Ludwig Von Bertalanffy en 1968, establece que los sistemas están compuestos por elementos interdependientes que interactúan entre sí para alcanzar un objetivo común (Von Bertalanffy, 1968). En el contexto de la ciberseguridad, esta teoría permite comprender la seguridad informática como un sistema complejo donde la infraestructura tecnológica, los procesos organizacionales y los usuarios deben operar de manera coordinada para garantizar la protección de la información.

Según Whitman & Mattord (2022), "una estrategia de ciberseguridad efectiva debe adoptar un enfoque sistémico que abarque tanto la prevención como la respuesta a incidentes" (p. 56). Esto implica diseñar políticas de seguridad basadas en la interconexión de sus elementos clave, como la protección de datos, la gestión de riesgos y la respuesta a incidentes.

Desde una perspectiva aplicada, el uso de la TGS en la ciberseguridad permite modelar arquitecturas de defensa en capas, donde cada componente contribuye al fortalecimiento del

sistema global. Tal como señalan Stallings & Brown (2021), “la implementación de controles de seguridad en niveles múltiples aumenta la resiliencia organizacional frente a ataques cibernéticos” (p. 73). En el caso de la Microfinanciera PRISMA, la adopción de esta perspectiva facilitaría la integración de tecnologías y procesos que garanticen una seguridad robusta y sostenible.

### 2.3.2 GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN: MODELOS Y METODOLOGÍAS RELEVANTES

La gestión de riesgos en seguridad de la información se basa en la identificación, evaluación y mitigación de amenazas potenciales que podrían comprometer la confidencialidad, integridad y disponibilidad de los datos. Modelos como el ISO/IEC 31000:2018 y el marco de gestión de riesgos NIST 800-39 han sido ampliamente adoptados para evaluar y mitigar riesgos cibernéticos en entornos financieros (NIST, 2020).

Según Peltier (2022), “la gestión de riesgos es un proceso continuo que debe adaptarse a la evolución de las amenazas y las vulnerabilidades tecnológicas” (p. 89). En el caso de la Microfinanciera PRISMA, la adopción de una metodología estructurada como OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) podría proporcionar una visión integral de los riesgos específicos de la organización, permitiendo diseñar estrategias de mitigación más eficaces.

Por otro lado, el enfoque de Análisis de Impacto en el Negocio (BIA, por sus siglas en inglés) resulta esencial para determinar la criticidad de los activos digitales y establecer prioridades en la gestión de incidentes. Como indican Tipton & Krause (2022), “un plan de gestión de riesgos sin una evaluación del impacto en el negocio puede generar respuestas ineficaces ante incidentes de seguridad” (p. 104).

### 2.3.3 ENFOQUE BASADO EN NORMAS INTERNACIONALES: BENEFICIOS Y APLICACIONES EN LA GESTIÓN DE TI

Las normas internacionales como la ISO/IEC 27001:2022 y la ISO/IEC 27032:2023 proporcionan un marco estructurado para la implementación de medidas de seguridad de la información. Estas normas establecen directrices para la gestión de riesgos, el establecimiento de controles de seguridad y la mejora continua en la protección de activos digitales (ISO, 2022).

De acuerdo con Calder & Watkins (2022), “la implementación de estándares internacionales mejora la gobernanza de la seguridad de la información y refuerza la confianza en la organización” (p. 132). Para una institución financiera como PRISMA, la adopción de estas normativas permitiría alinear sus procesos con mejores prácticas globales y fortalecer su postura de ciberseguridad.

Además, estudios recientes han demostrado que la certificación en ISO/IEC 27001 no solo mejora la seguridad, sino que también ofrece ventajas competitivas en el mercado. Un análisis realizado por Von Solms & Van Niekerk (2022) concluyó que “las organizaciones certificadas en ISO/IEC 27001 experimentan una reducción significativa en incidentes de seguridad y un aumento en la percepción de confiabilidad por parte de clientes y socios” (p. 67).

En el caso de PRISMA, la implementación de estos estándares no solo contribuiría a la seguridad interna, sino que también facilitaría el cumplimiento de regulaciones locales y fortalecería su reputación en el sector financiero.

### 2.3.4 CIBER RESILIENCIA Y CONTINUIDAD DEL NEGOCIO: ESTRATEGIAS PARA ENFRENTAR INCIDENTES DE SEGURIDAD

El concepto de ciber resiliencia se ha convertido en un pilar fundamental en la gestión de seguridad de la información. La ciber resiliencia se define como la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse ante incidentes cibernéticos (Linkov et al., 2022). A diferencia de los enfoques tradicionales de ciberseguridad, la ciber resiliencia enfatiza la preparación y la recuperación rápida ante ataques.

Según Bodeau & Graubart (2021), “las estrategias de ciber resiliencia deben incluir planes de respuesta ante incidentes, redundancia en la infraestructura crítica y simulaciones periódicas de ciberataques” (p. 89). En este sentido, la implementación de un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés) resulta esencial para mitigar el impacto de incidentes y garantizar la operatividad de la Microfinanciera PRISMA.

La incorporación de estrategias de respaldo y recuperación de datos es otro aspecto clave en la continuidad del negocio. Según un estudio de Castellanos et al. (2022), “las organizaciones que implementan copias de seguridad automatizadas y mecanismos de recuperación en la nube reducen significativamente el tiempo de recuperación tras un ataque” (p. 118).

Desde la perspectiva de PRISMA, la combinación de ciber resiliencia y continuidad del negocio permitiría fortalecer su capacidad de respuesta ante amenazas emergentes, asegurando la estabilidad operativa y protegiendo los datos sensibles de sus clientes.

## 2.4 CIBERSEGURIDAD: CONCEPTOS FUNDAMENTALES

### 2.4.1 DEFINICIÓN DE CIBERSEGURIDAD Y SU IMPORTANCIA EN LAS ORGANIZACIONES FINANCIERAS

La ciberseguridad se refiere a la práctica de proteger sistemas, redes y programas de ataques digitales que buscan acceder, alterar o destruir información sensible, extorsionar a los usuarios o interrumpir procesos empresariales. En el contexto de las organizaciones financieras, la ciberseguridad es crucial debido a la naturaleza confidencial y valiosa de los datos manejados, así como al potencial impacto económico de los ciberataques. Según el Fondo Monetario Internacional (FMI) (2024), los ataques dirigidos a compañías financieras representan casi una quinta parte del total, siendo los bancos las entidades más expuestas.

### 2.4.2 DIFERENCIAS ENTRE SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Aunque los términos seguridad de la información, seguridad informática y ciberseguridad suelen utilizarse indistintamente, presentan diferencias sutiles:

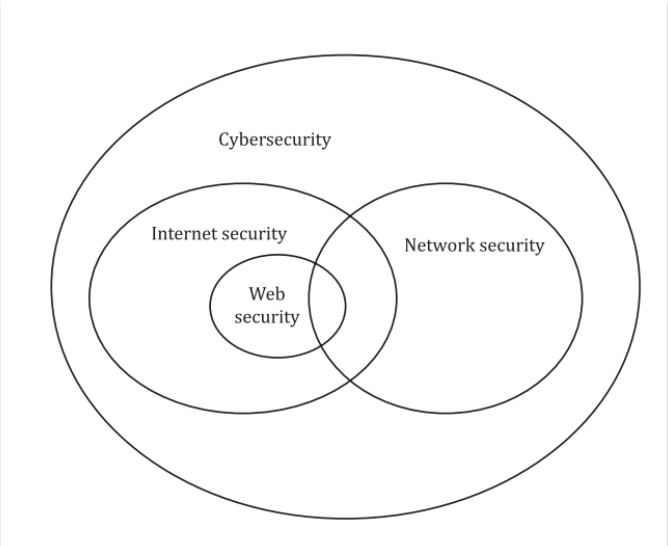


**Figura 2. Relación entre la Seguridad de Internet, Web, Red y Cibernética**

Fuente: (ISO & IEC, 2022)

- Seguridad de la información: Se enfoca en la protección de los datos, independientemente del formato (físico o digital). Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información (ISO, 2022).
- Seguridad informática: Se centra en la protección de los sistemas informáticos y los datos que procesan, abarcando hardware y software (Stallings & Brown, 2021).
- Ciberseguridad: Se dedica a la protección contra ataques que ocurren en el ciberespacio, es decir, en entornos digitales y redes interconectadas (Whitman & Mattord, 2022).

En el sector financiero, la ciberseguridad adquiere una relevancia particular debido a la creciente digitalización de los servicios y la sofisticación de las amenazas cibernéticas.

Distinguir entre seguridad de la información, seguridad informática y ciberseguridad es esencial para una gestión efectiva de los riesgos en el entorno digital. La Seguridad de la Información se refiere a la protección de los datos en cualquier forma, asegurando su confidencialidad, integridad y disponibilidad. Por otro lado, la Seguridad Informática se enfoca en salvaguardar los sistemas de información, incluyendo hardware y software, contra accesos no autorizados y daños. Finalmente, la Ciberseguridad se centra en proteger la información que reside en el ciberespacio, es decir, en entornos digitales y redes interconectadas.

Según Figueroa Suárez et al. (2017), "la seguridad informática atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales, mientras que la seguridad de la información integra toda la información independientemente del medio en el que esté" (p. 153).

No reconocer las diferencias y relaciones entre estos conceptos puede conducir a una gestión inadecuada de la seguridad, exponiendo a las organizaciones a múltiples riesgos. Una comprensión limitada puede resultar en la implementación de medidas de protección insuficientes o inapropiadas, dejando vulnerabilidades explotables por actores malintencionados. Además, la falta de claridad puede generar confusión en la asignación de responsabilidades y en la aplicación de políticas de seguridad, debilitando la postura defensiva de la organización.

Como señalan Rodríguez Zambrano & Moreno Tamayo (2024) "la ciberseguridad es un tema crucial en el siglo XXI, con diversos enfoques y desafíos planteados por los expertos" (p.

174). Por lo tanto, es imperativo que las organizaciones adopten un enfoque integral que abarque todos los aspectos de la seguridad de la información, informática y cibernética para mitigar eficazmente los riesgos asociados.

### 2.4.3 PRINCIPALES AMENAZAS Y VULNERABILIDADES EN EL SECTOR FINANCIERO

El sector financiero enfrenta diversas amenazas y vulnerabilidades en el ámbito de la ciberseguridad, entre las cuales destacan:

- Robo y manipulación de datos**:** Los ciberdelincuentes buscan acceder a información financiera sensible para cometer fraudes o extorsionar a las víctimas. La manipulación de datos puede generar desconfianza en los sistemas financieros y afectar la estabilidad económica. Según GlobalSign (2024), debido a la liquidez de las empresas financieras, el robo de datos puede resultar muy rentable para los ciberdelincuentes.
- Ataques a la cadena de suministro**:** Las instituciones financieras dependen de terceros y proveedores para diversos servicios. La falta de transparencia y controles de seguridad en estos socios puede introducir vulnerabilidades (GlobalSign, 2024).
- Tecnologías emergentes**:** La adopción de nuevas tecnologías, como la inteligencia artificial y el Internet de las Cosas (IoT), introduce riesgos adicionales debido a posibles vulnerabilidades y la falta de estándares de seguridad universales (NIST, 2020).
- Escasez de talento en ciberseguridad**:** Existe una demanda creciente de profesionales capacitados en ciberseguridad. La falta de personal especializado puede dejar a las instituciones financieras vulnerables a ataques, ya que no cuentan con los recursos humanos necesarios para implementar y mantener medidas de seguridad efectivas (Bodeau & Graubart, 2021).
- Ataques de malware**:** El uso de software malicioso para infiltrarse en sistemas financieros es una amenaza constante. Tipos específicos de malware, como la inyección SQL o el ransomware, se utilizan para comprometer la integridad y disponibilidad de los datos financieros (GlobalSign, 2024).

Para ilustrar la posición de las principales empresas en soluciones de ciberseguridad, se presenta el Cuadrante Mágico de Gartner para plataformas de protección de Endpoints.


**Figura 3. Cuadrante Mágico de Gartner para plataformas de Endpoint 2024**

Fuente: Skyhigh Security (2024)

Este cuadrante evalúa a los proveedores en función de su capacidad de ejecución y la integridad de su visión, proporcionando una perspectiva sobre las opciones disponibles para fortalecer la ciberseguridad en el sector financiero.

Reconocer y comprender las principales amenazas y vulnerabilidades en el sector financiero es esencial para garantizar la continuidad y estabilidad de las organizaciones en este ámbito. La creciente digitalización ha incrementado la exposición a ciberataques, los cuales pueden resultar en pérdidas financieras significativas y dañar la reputación corporativa. Según un estudio de Haruna et al. (2022), "las amenazas cibernéticas al sistema de pagos y bancario se han convertido en una amenaza mundial", lo que subraya la necesidad de inversiones deliberadas en tecnologías sofisticadas y medidas de seguridad para salvaguardar contra pérdidas financieras y brechas de información. Además, Javaheri et al. (2024) destacan que "la rápida evolución del

movimiento Smart-everything y los avances en inteligencia artificial han dado lugar a amenazas cibernéticas sofisticadas que los métodos tradicionales no pueden contrarrestar", enfatizando la urgencia de adoptar estrategias de defensa actualizadas en el sector financiero.

A pesar de estos riesgos evidentes, en ocasiones la alta dirección muestra reticencia a invertir en tecnología preventiva debido a una percepción limitada del retorno de inversión en ciberseguridad o una falta de comprensión profunda de las amenazas actuales. Esta desconexión puede deberse a una brecha generacional o a una cultura organizacional que no prioriza la seguridad digital. Como señalan Haruna et al. (2022), "la proliferación de delitos cibernéticos es una gran preocupación para las diversas partes interesadas en el sector bancario", lo que indica la necesidad de una mayor concienciación a nivel ejecutivo.

Por lo tanto, es imperativo que los departamentos de tecnología realicen análisis exhaustivos y presenten evidencias contundentes sobre la importancia de estas inversiones. Esto incluye demostrar cómo las amenazas cibernéticas pueden afectar directamente la operatividad y rentabilidad de la empresa, y cómo la implementación de medidas de seguridad adecuadas puede mitigar estos riesgos, asegurando la continuidad del negocio y protegiendo los activos financieros y la confianza de los clientes.

## 2.5 ESTRATEGIAS DE CIBERSEGURIDAD EN INSTITUCIONES FINANCIERAS

### 2.5.1 FACTORES CLAVE PARA EL DISEÑO DE ESTRATEGIAS DE CIBERSEGURIDAD EN MICROFINANCIERAS

El diseño de estrategias de ciberseguridad en microfinancieras requiere una combinación de factores que integren la gestión de riesgos, la implementación de tecnologías avanzadas y la concienciación organizacional. Según Stallings & Brown (2021), “una estrategia de ciberseguridad efectiva debe considerar no solo la protección de la infraestructura tecnológica, sino también la educación y capacitación de los usuarios” (p. 112). La seguridad en las microfinancieras debe estar alineada con estándares internacionales como ISO/IEC 27001:2022, asegurando una correcta gestión de riesgos y continuidad operativa.

Uno de los factores clave es la identificación de los activos críticos de información y la implementación de controles basados en riesgos. Calder & Watkins (2022) destacan que una estrategia efectiva debe incluir un enfoque basado en riesgo, donde se prioricen los activos más

vulnerables y valiosos de la organización. En el contexto de las microfinancieras, esto significa proteger los datos de los clientes, sistemas de transacciones y plataformas digitales que facilitan el acceso a servicios financieros.

Además, la adopción de herramientas de seguridad basadas en inteligencia artificial y machine learning es fundamental para la detección y mitigación de amenazas. Según Peltier (2022), "el uso de tecnologías predictivas permite reducir los tiempos de respuesta ante incidentes y mejorar la capacidad de detección de ataques cibernéticos" (p. 87). Las microfinancieras pueden aprovechar estas innovaciones para implementar sistemas de monitoreo en tiempo real y análisis de comportamiento de usuarios.

Finalmente, la ciberseguridad en microfinancieras debe incluir una sólida cultura organizacional orientada a la prevención de ataques. La falta de formación en ciberseguridad es una de las principales debilidades en este sector, lo que hace necesario establecer programas continuos de capacitación. Como señalan Whitman & Mattord (2022), las políticas de seguridad deben ir acompañadas de procesos de educación que involucren a todos los actores dentro de la organización, desde empleados hasta clientes y proveedores.

### 2.5.2 RETOS Y DESAFÍOS EN LA IMPLEMENTACIÓN DE SEGURIDAD EN MICROFINANZAS

Las microfinancieras enfrentan múltiples desafíos en la implementación de estrategias de ciberseguridad debido a la falta de recursos, la evolución constante de amenazas y la complejidad de la regulación. Según Anderson et al. (2023), "las instituciones financieras pequeñas tienen dificultades para asignar presupuestos adecuados para la ciberseguridad, lo que las convierte en objetivos atractivos para los ciberdelincuentes" (p. 92). La falta de inversión en tecnología y la ausencia de equipos especializados en seguridad informática representan barreras significativas.

Otro de los retos principales es la creciente sofisticación de los ataques cibernéticos dirigidos al sector financiero. Pérez & Rodríguez (2023) explican que el auge de técnicas como el ransomware y el phishing avanzado han incrementado los incidentes en entidades financieras con menor capacidad de defensa. Las microfinancieras, al manejar grandes volúmenes de datos personales y financieros, se convierten en blancos vulnerables ante estas amenazas.

Además, la falta de cumplimiento de normativas de seguridad es otro desafío importante. Según el Informe de la OEA sobre Ciberseguridad en América Latina (OEA) (2023), muchas microfinancieras aún no han adoptado estándares internacionales de ciberseguridad, lo que las deja expuestas a vulnerabilidades sistémicas. En Honduras, la adopción de regulaciones alineadas con la ISO/IEC 27032:2023 podría fortalecer la postura de seguridad de estas entidades.

Finalmente, el cambio cultural dentro de las microfinancieras es una barrera que debe abordarse para mejorar la seguridad digital. La resistencia a adoptar nuevas tecnologías y la falta de concienciación en ciberseguridad limitan la efectividad de las estrategias implementadas. De acuerdo con López (2022), "el éxito de cualquier estrategia de ciberseguridad radica en la transformación cultural y la adopción de una mentalidad de seguridad en todos los niveles organizativos" (p. 119).

### 2.5.3 MEJORES PRÁCTICAS EN LA PROTECCIÓN DE DATOS Y TRANSACCIONES FINANCIERAS

Para garantizar la seguridad de los datos y transacciones financieras en microfinancieras, es esencial adoptar mejores prácticas basadas en normativas internacionales y estrategias tecnológicas avanzadas. Según Mendoza & Castillo (2022), la implementación de medidas de cifrado, autenticación multifactor y segmentación de redes es fundamental para mitigar riesgos en el sector financiero. El uso de tecnologías como blockchain también ha demostrado ser efectivo para garantizar la integridad de las transacciones.

Una de las mejores prácticas es la adopción de una arquitectura Zero Trust, que asume que ninguna entidad dentro o fuera de la red es completamente confiable. Según un estudio de Gartner (2023), las instituciones financieras que han implementado Zero Trust han reducido significativamente los incidentes de acceso no autorizado y han mejorado la visibilidad de amenazas internas. En microfinanzas, esta estrategia puede aplicarse mediante la verificación continua de identidad y el monitoreo en tiempo real de accesos.

Otra recomendación clave es la implementación de sistemas de detección y respuesta ante incidentes de seguridad (SIEM, por sus siglas en inglés). Según Whitman & Mattord, (2022), "los sistemas SIEM permiten la correlación de eventos de seguridad, facilitando la identificación temprana de anomalías en las transacciones" (p. 145). Para las microfinancieras, el uso de estos sistemas podría mejorar la respuesta ante incidentes y reducir el impacto de ataques cibernéticos.

Por último, la adopción de estrategias de seguridad basadas en la nube ha ganado relevancia en la protección de datos financieros. Según Calder & Watkins (2022), las soluciones de seguridad en la nube ofrecen mayor flexibilidad, escalabilidad y eficiencia en comparación con los enfoques tradicionales. En este sentido, las microfinancieras pueden beneficiarse de plataformas en la nube que incluyen medidas de seguridad integradas, como cifrado de datos, monitoreo continuo y protección contra ataques DDoS.

**Tabla 1. Mejores prácticas en la protección de datos**

| Nombre de la práctica | Descripción de la práctica | Lo que se evita |
|---|---|---|
| Cifrado de Datos | Aplicación de algoritmos criptográficos para proteger datos en tránsito y en reposo. | Accesos no autorizados, robo de datos y espionaje. |
| Autenticación Multifactor (MFA) | Uso de múltiples factores de autenticación (contraseña, biometría, token) para validar accesos. | Suplantación de identidad y accesos fraudulentos. |
| Control de Accesos y Privilegios | Definición y restricción de permisos para garantizar que solo usuarios autorizados accedan a los datos. | Fugas de información y accesos indebidos. |
| Respaldo y Recuperación de Datos | Realización de copias de seguridad periódicas y pruebas de recuperación de datos. | Pérdida de datos por incidentes cibernéticos o fallos técnicos. |
| Monitoreo Continuo y Detección de Amenazas | Uso de herramientas SIEM para identificar y responder a amenazas en tiempo real. | Ataques de malware, ransomware y accesos sospechosos. |
| Actualización y Parches de Seguridad | Aplicación constante de actualizaciones y parches de seguridad en sistemas y software. | Explotación de vulnerabilidades por software obsoleto. |
| Seguridad en la Nube | Uso de proveedores de nube con altos estándares de seguridad, incluyendo cifrado y segmentación de redes. | Filtración de datos y accesos no autorizados a la nube. |
| Concienciación y Capacitación en Seguridad | Capacitación continua a empleados sobre buenas prácticas de seguridad y concienciación sobre amenazas. | Errores humanos que comprometan la seguridad de la organización. |
| Evaluaciones de Riesgo Periódicas | Análisis de riesgos regulares para identificar vulnerabilidades y definir estrategias de mitigación. | Falta de preparación ante incidentes de seguridad. |
| Implementación de una Política de Seguridad de Datos | Definición y aplicación de una política clara sobre el manejo, acceso y almacenamiento de datos. | Manejo inadecuado de datos, incumplimiento normativo y sanciones legales. |

Fuente: Adaptado de Mendoza & Castillo (2022), Gartner (2023), Whitman & Mattord (2022), Calder & Watkins (2022)

## 2.6 NORMAS ISO/IEC 27001:2022 Y 27032:2023 EN CIBERSEGURIDAD

### 2.6.1 ISO/IEC 27001:2022

#### 2.6.1.1 OBJETIVO Y ALCANCE DE LA NORMA

La norma ISO/IEC 27001:2022 es un estándar internacional diseñado para la gestión de la seguridad de la información en organizaciones de cualquier tamaño y sector. Su principal objetivo es establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la confidencialidad, integridad y disponibilidad de los datos (ISO, ).

Según Calder & Watkins (2022), "ISO/IEC 27001:2022 proporciona un marco sistemático para gestionar los riesgos de seguridad de la información, asegurando que las empresas adopten una estrategia proactiva en la protección de sus activos digitales" (p. 45). Su alcance abarca desde la gestión de riesgos hasta la implementación de controles de seguridad específicos para proteger los sistemas y la información.

Además, la norma tiene un enfoque basado en la evaluación de riesgos, permitiendo a las organizaciones personalizar su SGSI de acuerdo con sus necesidades particulares y la naturaleza de sus operaciones. Según López (2022), "la flexibilidad del SGSI bajo ISO/IEC 27001:2022 permite su aplicación en distintos entornos, desde instituciones financieras hasta empresas tecnológicas" (p. 67).

#### 2.6.1.2 TRIADA DE SEGURIDAD DE LA INFORMACIÓN

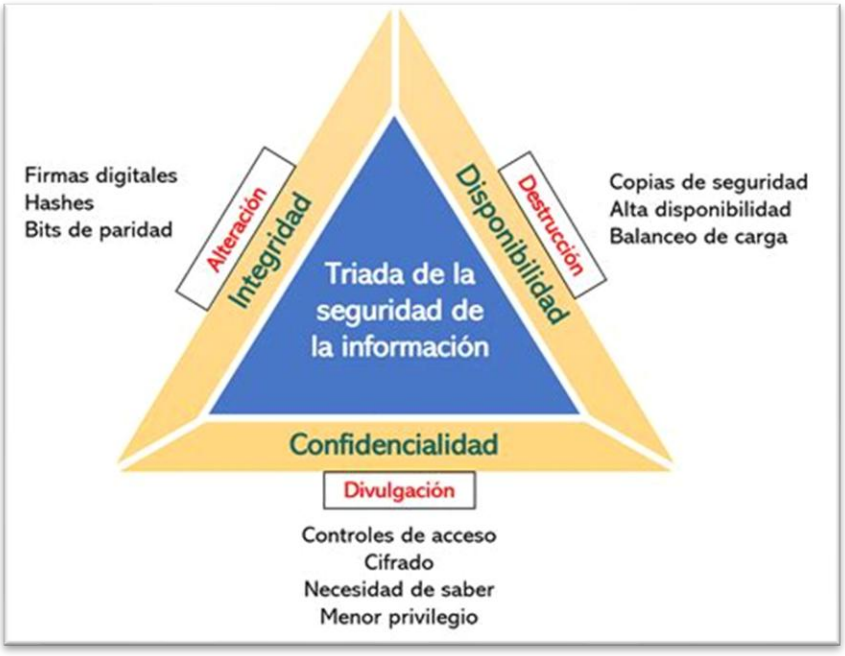


**Figura 4. Triada de la Seguridad de la Información: ¿Cómo y qué?**

Fuente: Adaptado de Calder & Watkins (2022)

La tríada de la seguridad de la información, según la norma ISO/IEC 27001, se fundamenta en tres pilares esenciales: confidencialidad, integridad y disponibilidad. Estos principios son cruciales para garantizar la protección adecuada de los datos en cualquier organización.

1. Confidencialidad: Este principio asegura que la información sea accesible únicamente para personas autorizadas, evitando divulgaciones no permitidas. La confidencialidad se mantiene mediante controles de acceso estrictos y mecanismos de autenticación robustos, garantizando que solo individuos con permisos adecuados puedan acceder a datos sensibles. Según la ISO/IEC 27001, "la confidencialidad implica que la información no esté disponible o divulgada a individuos, entidades o procesos no autorizados" (ISO, 2022).
2. Integridad: Se refiere a la exactitud y completitud de la información, asegurando que los datos no sean alterados de manera no autorizada. La integridad protege contra modificaciones indebidas, ya sean accidentales o malintencionadas, y se implementa mediante controles como sumas de verificación, firmas digitales y registros de auditoría. La ISO/IEC 27001 define la integridad como "la salvaguarda de la exactitud y completitud de los activos" (ISO, 2022).
3. Disponibilidad: Este componente garantiza que la información esté accesible y utilizable cuando se requiera por las personas autorizadas. La disponibilidad se logra mediante la implementación de infraestructuras resilientes, planes de recuperación ante desastres y medidas de redundancia que aseguren el acceso continuo a los datos. La norma ISO/IEC 27001 señala que la disponibilidad es "la accesibilidad y usabilidad de la información y los sistemas en el momento que se requiera" (ISO, 2022).

Es imperativo que la alta dirección comprenda y valore estos tres pilares, ya que su entendimiento es fundamental para el desarrollo e implementación efectiva de políticas de seguridad de la información. La falta de conocimiento en estos conceptos puede conducir a decisiones que pongan en riesgo la protección de los datos, afectando la reputación y operatividad de la organización.

Como indican Calder & Watkins (2022), "la implicación de la alta dirección es crucial para establecer una cultura de seguridad que promueva la confidencialidad, integridad y disponibilidad de la información" (p. 34). Además, un liderazgo informado puede asignar recursos adecuados y

priorizar iniciativas que fortalezcan la postura de seguridad de la empresa, alineando las estrategias de protección de datos con los objetivos corporativos.

#### 2.6.1.3 PRINCIPIOS Y REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El SGSI de ISO/IEC 27001:2022 se basa en principios clave, como la gestión del riesgo, la mejora continua y el cumplimiento de requisitos legales y normativos. Para su implementación, las organizaciones deben seguir un conjunto de requisitos fundamentales, que incluyen:

1. Análisis y evaluación de riesgos: Identificación de amenazas y vulnerabilidades para mitigar posibles impactos (ISO, 2022).
2. Políticas de seguridad de la información: Definición de principios y directrices para proteger los activos digitales (Whitman & Mattord, 2022).
3. Controles de acceso y autenticación: Establecimiento de mecanismos que restringen el acceso a la información según roles y privilegios (T. R. Peltier, 2022).
4. Monitoreo y auditoría de seguridad: Implementación de sistemas de supervisión para detectar y responder a incidentes (Calder & Watkins, 2022).
5. Capacitación y concienciación: Formación continua a empleados para reducir el riesgo de ataques por error humano (Mendoza & Castillo, 2022).

#### 2.6.1.4 CAMBIOS CLAVE RESPECTO A LA VERSIÓN 2013

La versión ISO/IEC 27001:2022 introduce varias actualizaciones respecto a la versión 2013, enfocándose en la adaptación a las nuevas amenazas cibernéticas y la evolución tecnológica. Según el International Organization for Standardization (ISO, 2022), los cambios principales incluyen:

- Revisión y simplificación de los controles de seguridad: Se han agrupado y reducido los controles de 114 a 93, mejorando su organización y aplicabilidad.
- Incorporación de nuevos controles de ciberseguridad: Se incluyen estrategias como inteligencia de amenazas, seguridad en la nube y prevención de fuga de datos.
- Mayor énfasis en la resiliencia y continuidad del negocio: Se promueve la capacidad de recuperación ante ciberataques y desastres tecnológicos.


**Figura 5. Distribución de Controles ISO/IEC 27001:2022**

Fuente: (ISO & IEC, 2022)

Según Calder & Watkins (2022), "la nueva versión de ISO/IEC 27001 refuerza la importancia de la resiliencia organizacional, permitiendo que las empresas enfrenten amenazas emergentes con una estrategia estructurada" (p. 78).

**Tabla 2. Comparación ISO/IEC 27001:2013 vs 2022**

| Aspecto | ISO/IEC 27001:2013 | ISO/IEC 27001:2022 |
|---|---|---|
| Contexto de la Organización y Partes Interesadas | Se introduce la necesidad de entender el contexto de la organización y las expectativas de las partes interesadas. | Se profundiza en este entendimiento, exigiendo un análisis más exhaustivo del entorno externo e interno, incluyendo la cadena de suministro y partes interesadas relevantes. |
| Liderazgo y Compromiso | Se enfatiza la importancia del liderazgo y el compromiso con el SGSI. | Se refuerza este enfoque, promoviendo un mayor compromiso de la alta dirección en la integración de los requisitos de seguridad de la información en los procesos empresariales generales. |
| Enfoque Basado en Riesgos | Se introduce un enfoque sistemático para gestionar riesgos de seguridad de la información. | Se presenta una metodología más detallada para la evaluación y gestión de riesgos, alineándola más estrechamente con otras normas de sistemas de gestión. |
| Controles de Seguridad de la Información | Se proporciona un conjunto de 114 controles en el Anexo A, agrupados en 14 dominios. | Se reorganizan los controles (ahora 93, reagrupados en 4 temas en lugar de 14 dominios) y se actualizan para reflejar amenazas emergentes, tecnologías en evolución y nuevas prácticas empresariales. |
| Operación del SGSI | Se enfoca en la necesidad de implementar y operar el SGSI de manera coherente y predecible. | Se introduce una mayor flexibilidad en la operación del SGSI, permitiendo una adaptación más ágil a los cambios en el contexto de seguridad de la información. |

| Aspecto | ISO/IEC 27001:2013 | ISO/IEC 27001:2022 |
|---|---|---|
| Evaluación del Desempeño | Se establecen requisitos para la monitorización, medición, análisis y evaluación del SGSI. | Se refuerzan estos requisitos, alentando una evaluación más profunda del desempeño y efectividad del SGSI y promoviendo una mejora continua más dinámica y adaptativa. |
| Gestión del Cambio | Se define, pero no se profundiza en la gestión del cambio. | Se pone un mayor énfasis en la gestión del cambio, reconociendo la necesidad de adaptar y modificar el SGSI de manera proactiva ante cambios internos y externos. |

Fuente: Adaptado de Calder & Watkins (2022)

#### 2.6.1.5 IMPLEMENTACIÓN DE CONTROLES Y GESTIÓN DEL RIESGO EN CIBERSEGURIDAD

La implementación de la ISO/IEC 27001:2022 requiere la adopción de controles de seguridad alineados con la gestión de riesgos de la organización. Entre los controles más relevantes destacan:

- Criptografía y protección de datos: Uso de técnicas avanzadas para cifrar y resguardar información sensible (ISO, 2022).
- Autenticación multifactor (MFA): Implementación de medidas de acceso seguro para prevenir accesos no autorizados Whitman & Mattord (2022).
- Resiliencia ante ciberataques: Desarrollo de planes de respuesta a incidentes y continuidad operativa (Mendoza & Castillo, 2022).

### 2.6.2 ISO/IEC 27032:2023

#### 2.6.2.1 ENFOQUE ACTUALIZADO EN CIBERSEGURIDAD Y COOPERACIÓN ENTRE PARTES INTERESADAS

La norma ISO/IEC 27032:2023 proporciona un enfoque integral de la ciberseguridad, fomentando la colaboración entre sectores públicos, privados y comunidades digitales. Según Peltier (2022), “ISO/IEC 27032:2023 no solo establece lineamientos técnicos, sino que promueve la cooperación entre gobiernos, empresas y usuarios para fortalecer la seguridad cibernética” (p. 89).

Esta norma se centra en la gestión de amenazas en el ciberespacio, abordando aspectos como seguridad en redes sociales, protección contra ataques avanzados y cibercrimen (ISO, 2022).

#### 2.6.2.2 PROTECCIÓN CONTRA ATAQUES CIBERNÉTICOS AVANZADOS

ISO/IEC 27032:2023 enfatiza la prevención y respuesta ante ataques cibernéticos avanzados, tales como:

- Ataques de ransomware: Estrategias para detectar y mitigar secuestros de datos digitales.
- Suplantación de identidad (phishing y spear phishing): Controles de seguridad para identificar intentos de fraude en correos electrónicos y redes sociales.
- Amenazas persistentes avanzadas (APT): Implementación de inteligencia de amenazas para detectar ataques dirigidos.

Según Mendoza & Castillo (2022), "la adopción de ISO/IEC 27032:2023 permite a las organizaciones anticiparse a amenazas sofisticadas mediante un enfoque coordinado de gestión de ciberseguridad" (p. 134).

#### 2.6.2.3 FORTALECIMIENTO DE LA GOBERNANZA EN CIBERSEGURIDAD Y GESTIÓN DE INCIDENTES

Uno de los pilares de la ISO/IEC 27032:2023 es el fortalecimiento de la gobernanza en ciberseguridad. Esta norma establece la necesidad de estructuras de gobernanza bien definidas, promoviendo:

- Roles y responsabilidades claras en seguridad digital.
- Procesos de gestión de incidentes y respuesta rápida.
- Uso de marcos regulatorios y normativos para el cumplimiento de seguridad.

Según Whitman & Mattord (2022), "el fortalecimiento de la gobernanza permite a las organizaciones mejorar su capacidad de respuesta ante amenazas cibernéticas y reducir el impacto de los incidentes" (p. 155).

## 2.7 CONTEXTO DE LA MICROFINANCIERA PRISMA, HONDURAS

### 2.7.1 RESEÑA HISTÓRICA

PRISMA Microfinance Inc. con sede en la ciudad de Boston, Massachusetts, USA, constituye PRISMA Honduras S. A., el 8 de noviembre de 2003 con el objetivo de ingresar al

mercado hondureño de las microfinanzas como un nuevo oferente de crédito e inicia operaciones en Julio 2006. PRISMA surge de la iniciativa de inversionistas privados de los Estados Unidos, con el deseo de contribuir al combate de la pobreza en la región de Centro y Sur América bajo la filosofía que las microfinanzas solo pueden ser sostenibles si son rentables, motivo por el cual se constituyen como una Sociedad Anónima con fines de lucro y opera legalmente en Honduras bajo la figura legal de prestamista no bancario.

El programa de microcrédito se orientó al financiamiento de la micro y pequeña empresa y a mejoras de vivienda social, buscando llegar a las periferias urbanas y comunidades rurales más pobres.

El capital humano de la organización está integrado por 74 colaboradores de los cuales el 37% son oficiales de crédito y el 40% son mujeres.

Microfinanciera PRISMA de Honduras atiende preferentemente en la periferia urbana a personas viviendo en zonas de riesgo social, pequeños emprendedores y en la zona rural a pequeños productores agropecuarios, comerciantes y otros a través de sus agencias, en donde causan un mayor impacto ambiental, calidad de vida y el nivel de ingresos de las familias.

La microfinanciera tiene diez oficinas atendiendo las zonas centro sur, norte y oriente; ofreciendo servicios de crédito en seis departamentos (Francisco Morazán, Comayagua, El Paraíso, Choluteca, Valle, Olancho).

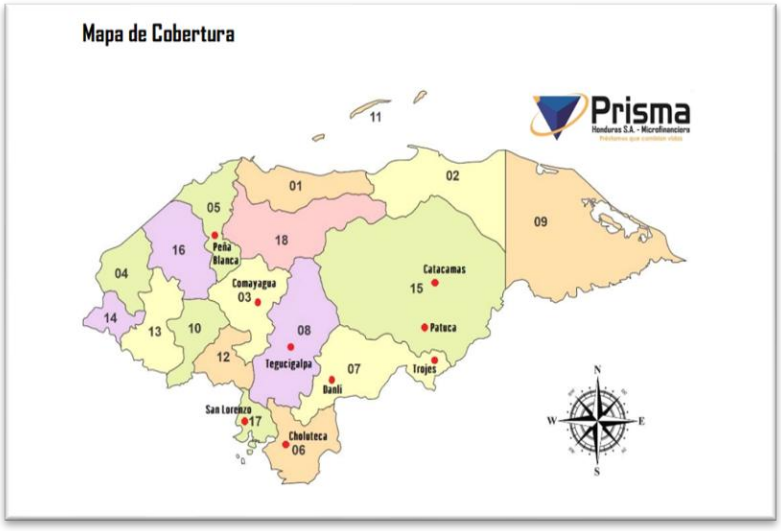


**Figura 6. Mapa de Cobertura PRISMA de Honduras**

Fuente: PRISMA Honduras S.A. (2022)

La organización se propone en estos cinco años expandir sus operaciones y cobertura hacia otras zonas como El Progreso, Santa Bárbara y La Esperanza, mediante la apertura de agencias y/o puntos de servicio de bajo costo, con una estructura organizacional que enfatiza en la conformación de un equipo operacional sólido para el logro de sus objetivos.

### 2.7.2 MARCO LEGAL PRISMA

Microfinanciera PRISMA de Honduras tiene como objetivo intermediar recursos propios y provenientes de financiamiento local e internacional y está autorizada para realizar toda clase de actividades lícitas orientadas a la intermediación y prestación de productos y servicios financieros. La duración de la sociedad es por tiempo ilimitado.

### 2.7.3 MANDATO INSTITUCIONAL

Microfinanciera PRISMA de Honduras opera en el sector de las microfinanzas ofreciendo productos y servicios financieros de calidad, para la sostenibilidad y crecimiento financiero de los clientes, empleados y socios.

### 2.7.4 VALORES INSTITUCIONALES

Promueven en cada acción, un conjunto de valores intangibles que son el reflejo e inspiración institucional:

- Compromiso
- Excelencia
- Integridad y Ética
- Responsabilidad
- Respeto
- Transparencia

### 2.7.5 VISIÓN

Ser una institución de microfinanzas a nivel nacional, que genere impacto económico, social y ambiental, con productos y servicios integrales, sostenibles e innovadores que cambien la calidad de vida de nuestros clientes, empleados y socios.

### 2.7.6 MISIÓN

Mejorar la calidad de vida de nuestros clientes, empleados y socios; a través de la oferta de productos y servicios financieros de calidad, con soluciones tecnológicas prácticas, bajo un esquema de rentabilidad económica, social y ambiental, promoviendo la inclusión financiera.

### 2.7.7 OBJETIVOS ESTRATÉGICOS

- Facilitar el acceso a préstamos, generar oportunidades de empleo y alcanzar indicadores de rentabilidad adecuados para la industria, devolviendo valor a los accionistas por su inversión en nuestra institución.
- Ofrecer productos y servicios financieros rentables y de calidad, desarrollados para atender las necesidades de nuestros clientes.
- Implementar herramientas tecnológicas que nos permitan reducir costos y alcanzar un mayor número de clientes, contribuyendo de esta forma a la inclusión financiera.
- Generar un impacto económico, social y ambiental.

### 2.7.8 PROPUESTA DE VALOR

Posicionar la imagen de Microfinanciera PRISMA de Honduras como una institución con solidez financiera, transparente y confiable que brinda fácil acceso y atención personalizada a sus clientes que demandan sus productos y servicios.

### 2.7.9 ANÁLISIS DEL ENTORNO DIGITAL Y TECNOLÓGICO DE PRISMA

#### 2.7.9.1 PRINCIPALES RIESGOS EN TÉRMINOS DE CIBERSEGURIDAD

Una auditoría reciente realizada en la Microfinanciera PRISMA reveló diversos riesgos en su entorno digital y tecnológico que afectan su postura de ciberseguridad. Entre los hallazgos más críticos se identificó el uso de servidores legacy, los cuales carecen de soporte técnico y actualizaciones de seguridad. Según López (2022), “los sistemas heredados representan un riesgo significativo, ya que son vulnerables a exploits y carecen de parches para amenazas recientes” (p. 112). La persistencia de estas infraestructuras obsoletas en PRISMA aumenta la posibilidad de ataques como el ransomware y la ejecución de código malicioso.

Otro riesgo fundamental identificado en la auditoría es la necesidad de licenciamiento en software crítico, lo que deja expuesta a la organización a vulnerabilidades en herramientas sin actualizaciones oficiales. Whitman & Mattord (2022) enfatizan que "el uso de software sin licenciamiento adecuado puede generar brechas de seguridad al carecer de soporte técnico y actualizaciones esenciales" (p. 78). En PRISMA, la falta de licenciamiento adecuado en sistemas operativos y aplicaciones financieras incrementa el riesgo de accesos no autorizados y pérdida de datos sensibles.

Finalmente, otro riesgo importante es la ausencia de un plan de continuidad del negocio ante incidentes cibernéticos. Según el Foro Económico Mundial (2023), "las organizaciones que carecen de planes de recuperación ante desastres son más susceptibles a interrupciones prolongadas tras un ciberataque" (p. 45). PRISMA no cuenta con procedimientos estructurados para la restauración de datos en caso de ataque, lo que pone en riesgo la operatividad del negocio y la confianza de sus clientes.

#### 2.7.9.2 PRINCIPALES VULNERABILIDADES EN TÉRMINOS DE CIBERSEGURIDAD EN PRISMA

La auditoría realizada también permitió identificar diversas vulnerabilidades en los sistemas tecnológicos de PRISMA. Una de las más críticas es la falta de un Directorio Activo (Active Directory) para la gestión centralizada de usuarios y permisos. Según Mendoza & Castillo (2022), "sin un Directorio Activo, las organizaciones tienen una gestión de credenciales descentralizada, lo que facilita ataques de escalamiento de privilegios y accesos no autorizados" (p. 134). La ausencia de esta herramienta en PRISMA aumenta el riesgo de fugas de información y dificulta la administración de accesos en la organización.

Otro aspecto vulnerable identificado es el no uso de servicios en la nube, lo que limita la escalabilidad y seguridad de los sistemas financieros. Calder & Watkins (2022) sostienen que "las soluciones en la nube ofrecen medidas avanzadas de seguridad, como cifrado de datos, autenticación multifactor y monitoreo continuo, lo que reduce la exposición a ataques" (p. 88). PRISMA continúa dependiendo de infraestructura on-premise, lo que incrementa la posibilidad de pérdida de datos en caso de fallos físicos o incidentes cibernéticos.

Finalmente, se identificó una falta de segmentación de redes, lo que facilita el movimiento lateral de atacantes dentro de la infraestructura de TI de PRISMA. Según Peltier (2022), "la

segmentación de redes minimiza la superficie de ataque al restringir el acceso entre distintos niveles del sistema, dificultando la propagación de malware y accesos no autorizados" (p. 67). La falta de estas medidas en PRISMA aumenta la vulnerabilidad de la organización ante ataques dirigidos y facilita la explotación de brechas de seguridad.

El análisis del entorno digital y tecnológico de PRISMA evidencia una necesidad urgente de fortalecer su estrategia de ciberseguridad. Los riesgos y vulnerabilidades identificados, como el uso de servidores legacy, la falta de licenciamiento, la ausencia de Directorio Activo y el no uso de la nube, reflejan una postura de seguridad débil que expone a la organización a amenazas avanzadas. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001:2022 permitiría mitigar estos riesgos y fortalecer la resiliencia digital de PRISMA.

## 2.8 MODELOS Y ENFOQUES PARA EL DISEÑO DE ESTRATEGIAS DE CIBERSEGURIDAD

### 2.8.1 MODELOS DE MADUREZ EN CIBERSEGURIDAD APLICABLES A MICROFINANCIERAS

Los modelos de madurez en ciberseguridad permiten a las organizaciones evaluar su nivel de preparación frente a amenazas digitales y establecer una hoja de ruta para la mejora continua en la gestión de seguridad. En el sector de las microfinancieras, donde los recursos son limitados, contar con un modelo de madurez adecuado es fundamental para priorizar inversiones y mitigar riesgos estratégicos (T. R. Peltier, 2022).

Uno de los modelos más utilizados es el Cybersecurity Capability Maturity Model (C2M2), desarrollado por el Departamento de Energía de EE.UU., el cual proporciona una evaluación estructurada de las capacidades de ciberseguridad. Según López (2022), "el modelo C2M2 ayuda a las organizaciones a determinar sus fortalezas y debilidades en ciberseguridad, proporcionando un marco progresivo de mejora" (p. 89). Para las microfinancieras, este modelo permite identificar las brechas de seguridad y definir estrategias adaptadas a su contexto.

Otro modelo relevante es el Cybersecurity Maturity Model Certification (CMMC), promovido por el Departamento de Defensa de EE.UU., el cual establece niveles de madurez basados en la implementación de controles de seguridad. Calder & Watkins (2022) afirman que

“el CMMC representa un enfoque escalonado que facilita a las empresas establecer medidas progresivas de seguridad sin requerir una transformación abrupta” (p. 73). Para PRISMA, la adopción de un modelo de madurez estructurado facilitaría la optimización de su postura de seguridad a lo largo del tiempo.

Finalmente, la aplicación del Information Security Maturity Model (ISMM) permite a las organizaciones determinar su nivel de madurez en seguridad de la información de acuerdo con criterios alineados con ISO/IEC 27001. Este modelo, según Mendoza & Castillo (2022), “permite una transición gradual desde niveles básicos de ciberseguridad hasta una estrategia robusta y resiliente” (p. 114). En el contexto de PRISMA, la adopción de ISMM ayudaría a consolidar un enfoque basado en riesgos para la mejora continua de la seguridad digital.

### 2.8.2 METODOLOGÍAS PARA LA EVALUACIÓN Y MITIGACIÓN DE RIESGOS

La evaluación y mitigación de riesgos en ciberseguridad es un componente esencial para las microfinancieras, ya que les permite anticiparse a posibles amenazas y establecer controles adecuados para minimizar impactos operativos y financieros (Whitman & Mattord, 2022).

Una metodología ampliamente utilizada es OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), desarrollada por el Instituto de Ingeniería de Software de Carnegie Mellon. Según Peltier (2022), “OCTAVE proporciona un enfoque estructurado para identificar vulnerabilidades y priorizar riesgos con base en el impacto organizacional” (p. 92). Su implementación en PRISMA permitiría evaluar el impacto de amenazas como ransomware, phishing y accesos no autorizados.

Otra metodología clave es FAIR (Factor Analysis of Information Risk), la cual permite cuantificar los riesgos cibernéticos en términos económicos. Mendoza & Castillo (2022) argumentan que “FAIR permite traducir el impacto de los riesgos cibernéticos en métricas financieras, facilitando la toma de decisiones estratégicas para la inversión en seguridad” (p. 128). Su adopción en PRISMA ayudaría a justificar presupuestos en ciberseguridad con base en análisis de costo-beneficio.

Además, el NIST Risk Management Framework (RMF) proporciona un marco integral para la identificación, evaluación y mitigación de riesgos, alineado con estándares de seguridad globales. Según López (2022), “el RMF facilita la integración de la ciberseguridad en los procesos

de negocio, asegurando que los riesgos se gestionen de manera proactiva" (p. 104). Para PRISMA, este enfoque contribuiría a establecer procesos de seguridad más estructurados y alineados con normas internacionales.

### 2.8.3 FRAMEWORKS COMPLEMENTARIOS (NIST, COBIT, CIS CONTROLS)

El diseño de estrategias de ciberseguridad en microfinancieras no solo requiere la aplicación de normativas como ISO/IEC 27001, sino también el uso de frameworks complementarios que refuercen las medidas de seguridad. Entre los más relevantes se encuentran NIST, COBIT y CIS Controls.

El NIST Cybersecurity Framework (CSF) proporciona un marco flexible basado en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar. Según Calder & Watkins (2022), "el NIST CSF ayuda a las organizaciones a establecer una estrategia de ciberseguridad escalable y alineada con mejores prácticas internacionales" (p. 138). PRISMA podría beneficiarse de este modelo al estructurar su programa de seguridad en torno a estas funciones clave.

Por otro lado, COBIT (Control Objectives for Information and Related Technologies) es un marco de gobierno de TI que permite a las empresas alinear su seguridad con los objetivos de negocio. Whitman & Mattord (2022) explican que "COBIT proporciona un enfoque centrado en la gobernanza y control de la seguridad de la información, facilitando el cumplimiento normativo y la gestión eficiente de riesgos" (p. 117). La implementación de COBIT en PRISMA contribuiría a mejorar la supervisión y control de sus procesos de seguridad.

Finalmente, CIS Controls (Center for Internet Security) establece un conjunto de controles críticos que permiten reducir la superficie de ataque y mejorar la postura de seguridad. Según López (2022), "los CIS Controls proporcionan medidas prácticas y priorizadas para fortalecer la seguridad organizacional de manera efectiva" (p. 90). Para PRISMA, la aplicación de estos controles ayudaría a reducir vulnerabilidades técnicas y operativas.

### 2.8.4 CMMI EN CIBERSEGURIDAD

El Capability Maturity Model Integration (CMMI) es un modelo de madurez ampliamente utilizado en la industria de TI para evaluar y mejorar procesos organizacionales, incluyendo la ciberseguridad. Según Mendoza & Castillo (2022), "el CMMI permite a las organizaciones

mejorar su capacidad de gestión de seguridad mediante un enfoque basado en niveles de madurez" (p. 142).

El CMMI se divide en cinco niveles: Inicial, Gestionado, Definido, Cuantitativamente Gestionado y Optimizado. Su aplicación en PRISMA permitiría estructurar un enfoque de seguridad escalonado, pasando de un modelo reactivo a uno proactivo. Según Peltier (2022), "las organizaciones que implementan CMMI en seguridad logran mayor eficiencia en la identificación y mitigación de riesgos" (p. 76).

Además, el CMMI facilita la integración con otros marcos de ciberseguridad, como ISO/IEC 27001, NIST y COBIT, permitiendo a PRISMA optimizar sus controles de seguridad en función de su nivel de madurez. Como destaca López (2022), "la sinergia entre CMMI y frameworks de seguridad proporciona una base sólida para la mejora continua de la ciberseguridad" (p. 99).

## 2.9 INTEGRACIÓN DE LAS NORMAS ISO/IEC 27001 Y 27032 EN LA ESTRATEGIA DE CIBERSEGURIDAD

### 2.9.1 BENEFICIOS DE LA ADOPCIÓN DE UN ENFOQUE BASADO EN NORMAS INTERNACIONALES

La integración de ISO/IEC 27001:2022 e ISO/IEC 27032:2023 en la estrategia de ciberseguridad de una organización permite fortalecer su postura de seguridad mediante un enfoque estructurado y reconocido internacionalmente. La adopción de estas normas ofrece múltiples beneficios, incluyendo una mejor gestión del riesgo, cumplimiento normativo y fortalecimiento de la resiliencia organizacional (Von Solms & Van Niekerk, 2022).

Uno de los principales beneficios es la gestión sistemática de la seguridad de la información. La norma ISO/IEC 27001 establece un Sistema de Gestión de Seguridad de la Información (SGSI) que permite identificar, evaluar y mitigar riesgos de manera continua. Según (Calder & Watkins, 2022), "la implementación de un SGSI conforme a ISO/IEC 27001 proporciona un marco estructurado que facilita la protección de los activos digitales y la mejora de la gobernanza en seguridad" (p. 54).

Otro beneficio clave es el cumplimiento regulatorio y la alineación con estándares internacionales. Las microfinancieras, como PRISMA, operan en un entorno con regulaciones de

seguridad en evolución. La adopción de ISO/IEC 27032, centrada en la ciberseguridad, permite cumplir con marcos legales y mejorar la confianza de clientes y socios comerciales (Ahmad et al., 2022). Como indican Peltier & Sherwood (2023), "la integración de normas ISO no solo protege a las organizaciones contra amenazas emergentes, sino que también refuerza su reputación y credibilidad en el mercado" (p. 78).

Además, la combinación de ISO/IEC 27001 y 27032 permite fortalecer la ciber resiliencia organizacional, asegurando que la empresa pueda responder y recuperarse de incidentes cibernéticos con mayor eficiencia (Tipton & Krause, 2022). Esto es fundamental en el sector financiero, donde la disrupción de servicios digitales puede generar pérdidas económicas significativas.

### 2.9.2 IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD SEGÚN LAS NORMAS ISO

La implementación de controles de seguridad alineados con ISO/IEC 27001 y 27032 es crucial para garantizar una gestión eficaz de la ciberseguridad en PRISMA. Estos controles abarcan desde la protección de datos hasta la gestión de accesos y la respuesta a incidentes.

Uno de los controles fundamentales en ISO/IEC 27001:2022 es la gestión de acceso y autenticación, que busca restringir el acceso a la información únicamente a usuarios autorizados. Según Whitman & Mattord (2022), "la aplicación de controles de acceso en múltiples capas, como la autenticación multifactor, reduce significativamente el riesgo de accesos no autorizados" (p. 132). PRISMA debe adoptar mecanismos de autenticación fuerte y políticas de privilegios mínimos para fortalecer su seguridad.

Otro control clave es la gestión de incidentes de seguridad, que permite a la organización detectar, responder y recuperarse ante ataques cibernéticos. La norma ISO/IEC 27032 enfatiza la coordinación entre partes interesadas en la gestión de incidentes (Ahmad et al., 2022). Según (López, 2022), "una respuesta efectiva ante incidentes depende de la capacidad de la organización para aplicar procesos estructurados que minimicen el impacto de las amenazas" (p. 98).

Además, la norma recomienda la protección de datos mediante cifrado avanzado, garantizando que la información sensible esté resguardada contra accesos no autorizados. En

PRISMA, la implementación de cifrado de extremo a extremo y almacenamiento seguro en la nube contribuiría a mitigar vulnerabilidades críticas en sus sistemas financieros.

### 2.9.3 EVALUACIÓN DE CUMPLIMIENTO Y MEJORA CONTINUA EN PRISMA

Para garantizar la efectividad de la integración de ISO/IEC 27001 y 27032, PRISMA debe adoptar un enfoque de evaluación de cumplimiento y mejora continua en su estrategia de ciberseguridad. Esto implica la implementación de auditorías periódicas, revisión de políticas y adaptación a nuevas amenazas.

Uno de los métodos más efectivos para evaluar el cumplimiento es la auditoría interna del SGSI, que permite identificar brechas en la aplicación de controles de seguridad. Según Calder & Watkins (2022), "las auditorías internas proporcionan una visión detallada del estado de la seguridad de la información, permitiendo tomar decisiones basadas en datos" (p. 142). PRISMA debe establecer revisiones programadas para garantizar que sus políticas y procedimientos estén alineados con los requisitos de ISO/IEC 27001.

Además, la adopción de un enfoque basado en la mejora continua es esencial para adaptarse a la evolución de las amenazas cibernéticas. La norma ISO/IEC 27032 enfatiza la necesidad de actualizar regularmente las estrategias de ciberseguridad y fomentar una cultura organizacional de seguridad (Tipton & Krause, 2022). Como afirman López & Rodríguez (2023), "la ciberseguridad no es un estado estático, sino un proceso dinámico que requiere innovación constante y ajuste a nuevas vulnerabilidades" (p. 89).

Finalmente, PRISMA debe evaluar la efectividad de sus estrategias mediante pruebas de penetración y ejercicios de simulación de incidentes. Estas prácticas, alineadas con ISO/IEC 27032, permiten anticipar escenarios de ataque y fortalecer la capacidad de respuesta de la organización. Según Ahmad et al. (2022), "las pruebas de ciberseguridad permiten identificar debilidades antes de que sean explotadas, garantizando un entorno más seguro y resiliente" (p. 75).

## 2.10 MARCO LEGAL

### 2.10.1 MARCO LEGAL INTERNACIONAL PARA LA IMPLEMENTACIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD

Implementar una estrategia de ciberseguridad efectiva implica considerar un marco legal que establezca normas, directrices y acuerdos internacionales. Este marco puede variar entre

regiones y sectores, pero existen algunos tratados y convenios internacionales que son fundamentales en la construcción de políticas de ciberseguridad. A continuación, se describen algunos de los marcos legales internacionales más relevantes para implementar estrategias de ciberseguridad:

**Tabla 3. Marcos legales internacionales para implementar estrategias de ciberseguridad**

| Convenio | Contenido | Relevancia |
|---|---|---|
| Convenio de Budapest sobre Cibercrimen (2001) | También conocido como el "Convenio de Budapest", este tratado es el primer instrumento internacional que establece un marco legal para la lucha contra el cibercrimen. Promueve la cooperación entre los Estados miembros para la prevención y el control del crimen informático . | Establece directrices sobre la legislación nacional, la cooperación internacional y la capacitación en la lucha contra el cibercrimen. Facilita la investigación y el enjuiciamiento de delitos cibernéticos. |
| Reglamento General de Protección de Datos (GDPR) | Este reglamento de la Unión Europea se centra en la protección de datos personales y la privacidad de los ciudadanos de la UE. Aunque no es estrictamente un marco de ciberseguridad, establece normas sobre cómo manejar y proteger datos sensibles. | Obliga a las organizaciones a implementar medidas de seguridad adecuadas para proteger los datos personales, lo que incluye la gestión de incidentes de seguridad y la notificación de brechas de datos. |
| Marco de Ciberseguridad del Consejo de Europa | Este marco incluye diversas recomendaciones y políticas sobre ciberseguridad, diseñadas para fortalecer la capacidad de los Estados para prevenir y responder a los ciber incidentes. | Proporciona directrices para la elaboración de políticas nacionales de ciberseguridad y fomenta la cooperación entre los Estados miembros del Consejo de Europa. |
| Estrategia de Ciberseguridad de la OTAN | La Organización del Tratado del Atlántico Norte (OTAN) ha desarrollado una estrategia de ciberseguridad que busca mejorar la defensa cibernética de sus miembros y proteger la infraestructura crítica. | Promueve la cooperación en defensa cibernética y la resiliencia de las infraestructuras críticas a través de alianzas y acuerdos internacionales. |
| Acuerdo de París sobre Ciberseguridad | Este acuerdo se centra en la creación de un espacio cibernético seguro y accesible, promoviendo la cooperación internacional en ciberseguridad. | Establece directrices para la colaboración entre países en la gestión de riesgos cibernéticos y la prevención de incidentes. |
| Normas ISO/IEC 27001 e ISO/IEC 27032 | Estas normas internacionales proporcionan un marco para la gestión de la seguridad de la información (ISO/IEC 27001) y la ciberseguridad (ISO/IEC 27032). Aunque no son leyes, son ampliamente reconocidas y utilizadas en todo el mundo. | Ayudan a las organizaciones a establecer políticas y procedimientos efectivos de seguridad, alineándose con los requisitos legales y regulatorios. |
| Directrices del Grupo de Acción Financiera Internacional (GAFI) | El GAFI proporciona directrices para combatir el lavado de dinero y el financiamiento del terrorismo, que incluyen aspectos relacionados con la seguridad cibernética. | Establece estándares sobre cómo las instituciones financieras deben gestionar los riesgos asociados con el cibercrimen. |

Fuente: Adaptado de Participación estratégica en ciberseguridad (2021)

### 2.10.2 MARCO LEGAL EN HONDURAS PARA LA IMPLEMENTACIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD

La implementación de una estrategia de ciberseguridad en Honduras, basada en las normas ISO/IEC 27001 e ISO/IEC 27032, requiere un marco legal que promueva la protección de la información y la infraestructura crítica, así como la prevención y respuesta ante ciber incidentes. A continuación, se presenta un análisis del marco legal existente en Honduras que respalda la ciberseguridad y su alineación con las normas internacionales.

Honduras ha desarrollado un marco legal que aborda la ciberseguridad y la protección de datos, aunque aún se encuentra en proceso de consolidación. Algunos de los principales elementos incluyen:

**Tabla 4. Marco legal en Honduras para la ciberseguridad**

| Ley | Contenido | Relevancia |
|---|---|---|
| Ley de Protección de Datos Personales | Aún en proceso de desarrollo, esta ley establece normas para la recolección, almacenamiento, uso y transferencia de datos personales. Busca garantizar la privacidad de los ciudadanos y establece responsabilidades para las entidades que manejan datos personales. | Facilita la implementación de medidas de seguridad adecuadas para proteger la información personal, alineándose con los principios de la norma ISO/IEC 27001. |
| Ley sobre Cibercrimen | Aún en proceso de desarrollo, se busca establecer un marco legal para prevenir, investigar y sancionar delitos cibernéticos en Honduras. Esta ley pretende regular las actividades delictivas en el ciberespacio y promover la cooperación internacional en la lucha contra el cibercrimen. | La creación de esta ley es fundamental para abordar la problemática del cibercrimen, apoyando la implementación de prácticas recomendadas en ciberseguridad. |
| Ley de Telecomunicaciones | Regula el uso de telecomunicaciones en el país y establece directrices para la seguridad en las redes de telecomunicaciones. | Establece responsabilidades para los proveedores de servicios en la protección de sus infraestructuras y la información de los usuarios, alineándose con las exigencias de la norma ISO/IEC 27032. |
| Normas para la Gestión de Tecnologías de Información y Comunicaciones en Instituciones del Sistema Financiero Resolución No.1301/22-11-200 | Regula la administración de las tecnologías de información y comunicaciones utilizadas por las instituciones del sistema financiero; asimismo, regula los servicios financieros y operaciones realizadas por medio de redes electrónicas de uso externo e interno. | Ley de la Comisión Nacional de Bancos y Seguros, corresponde a este ente supervisor dictar las normas prudenciales que se requieran para la revisión, verificación, control, vigilancia y fiscalización de las instituciones supervisadas, para lo cual se basará en la legislación vigente, en acuerdos y prácticas |

| Ley | Contenido | Relevancia |
|---|---|---|
| | | internacionales. |
| Norma para la Administración de Tecnologías de Información y Comunicaciones TIC para las cooperativas de Ahorro y Crédito. Acuerdo Número 002-15-12-2022. | Establece los lineamientos para la gestión del riesgo tecnológico y continuidad de las operaciones de las Tecnologías de la información. | Basada en identificar, evaluar, mitigar, monitorear y comunicar los riesgos que surgen de las tecnologías de la información. |

Fuente: Elaboración Propia

Las normas ISO/IEC 27001 e ISO/IEC 27032 proporcionan directrices para la gestión de la seguridad de la información y la ciberseguridad. Aunque no son leyes, su implementación puede estar respaldada por el marco legal nacional. A continuación se detalla su relación:

**Tabla 5. Normas ISO/IEC para gestión de seguridad de la información y ciberseguridad**

| Ley | Contenido | Relación con el marco legal |
|---|---|---|
| ISO/IEC 27001 | Proporciona un marco para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). | Las leyes de protección de datos y cibercrimen pueden requerir que las organizaciones implementen controles de seguridad adecuados, que son fundamentales en la norma ISO/IEC 27001. Esto ayuda a las organizaciones a cumplir con los requisitos legales y normativos. |
| ISO/IEC 27032 | Se centra en la ciberseguridad y las mejores prácticas para proteger las infraestructuras y la información en el ciberespacio. | Fomenta un enfoque proactivo para la ciberseguridad, promoviendo la colaboración entre diferentes partes interesadas, lo que es crucial en la legislación sobre cibercrimen y la protección de datos. |

Fuente: Elaboración Propia

# CAPÍTULO III. METODOLOGÍA

## 3.1 CONGRUENCIA METODOLÓGICA

Este apartado del estudio muestra de manera clara la relación lógica entre el problema de investigación, los objetivos generales y específicos, así como las distintas variables, garantizando una secuencia estructurada y coherente. Estos elementos se organizan y presentan a través de una matriz metodológica.

### 3.1.1 MATRIZ METODOLÓGICA

Rivas Tovar (2017) señala que "la matriz metodológica es el instrumento científico que permite hacer congruente y coherente el proceso de la medición de variables independientes, creando un marco de comparación racional y ordenada para la construcción de un cuestionario" (p. 221). En este sentido, facilita el análisis e interpretación de la operatividad teórica de la investigación, al sistematizar los elementos clave: problema, objetivos, variables y su respectiva operacionalización.

La Tabla 6 presenta la matriz metodológica utilizada en esta tesis, detallando la relación entre las variables de estudio, las dimensiones analizadas y los indicadores o ítems seleccionados. Así, la matriz metodológica no solo constituye un eje articulador de la investigación, sino que también garantiza la validez y fiabilidad de los hallazgos obtenidos, facilitando el análisis comparativo y la formulación de recomendaciones fundamentadas.

### 3.1.2 ESQUEMA DE VARIABLES DE ESTUDIO

En este apartado se expone un diagrama sagital, en la Figura 7, la cual ilustra la relación causal entre las variables independientes y la variable dependiente. Un diagrama sagital es una representación gráfica en la que se organizan las variables de estudio a lo largo de un eje, permitiendo evidenciar la secuencia y la relación causal entre las variables independientes y dependientes. Este tipo de diagrama facilita la comprensión de la dirección del efecto o influencia entre dichas variables, al ordenarlas de forma lineal o secuencial (Hernández Sampieri, 2018).

**Tabla 6. Matriz Metodológica**

| Título de la investigación | Objetivos de Investigación | | Variables | Dimensiones | Ítems |
|---|---|---|---|---|---|
| | General | Específicos | | | |
| **DISEÑO DE UNA ESTRATEGIA DE CIBERSEGURIDAD BASADA EN LAS NORMAS ISO/IEC 27001:2022 Y 27032:2023. CASO: MICROFINANCIERA PRISMA DE HONDURAS, 2025** | Diseñar una estrategia de ciberseguridad para la microfinanciera PRISMA, basada en un diagnóstico integral de su estado actual y una evaluación del nivel de madurez en el cumplimiento de controles, que permita establecer recomendaciones y medidas alineadas con las normas ISO/IEC 27001:2022 y 27032:2023. | Diagnosticar el estado actual de la ciberseguridad en la Microfinanciera PRISMA, evaluando el grado de cumplimiento de sus controles y procesos conforme a los lineamientos de las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023. | Estado actual de la ciberseguridad | Cumplimiento normativo | Nivel de cumplimiento de los requisitos de ISO/IEC 27001:2022. |
| | | | | | Nivel de cumplimiento de las recomendaciones de ISO/IEC 27032:2023. |
| | | | | Controles implementados | Existencia y efectividad de controles organizativos, de personas, físicos y tecnológicos. |
| | | | | | Aplicación de medidas de protección para prevenir ciberataques. |
| | | | | Fortalezas en seguridad | Identificación de activos críticos y su protección. |
| | | | | | Capacidad de detección y respuesta ante incidentes de seguridad. |
| | | | | Brechas en seguridad | Evaluación de medidas actuales contra ciberamenazas. |
| | | | | | Detección de brechas en procedimientos y políticas de seguridad. |
| | | Determinar el nivel de madurez en ciberseguridad que presenta PRISMA, mediante indicadores basados en estándares internacionales, con el propósito de identificar brechas, riesgos críticos y oportunidades de mejora. | Nivel de madurez en ciberseguridad | Cumplimiento de controles | Nivel de cumplimiento de los controles definidos en ISO/IEC 27001:2022. |
| | | | | Capacidad de respuesta | Capacidad de detección y respuesta ante incidentes de ciberseguridad. |
| | | | | Mejora continua | Estrategias implementadas para la mejora continua en ciberseguridad. |
| | | | | | Existencia de procesos de revisión y actualización de controles de seguridad. |

| Título de la investigación | Objetivos de Investigación | | Variables | Dimensiones | Ítems |
|---|---|---|---|---|---|
| | General | Específicos | | | |
| | | Diseñar estrategias y controles específicos para el fortalecimiento de la protección de la información en PRISMA, estructurando una propuesta de ciberseguridad alineada con los marcos ISO/IEC 27001:2022 e ISO/IEC 27032:2023. | Estrategia de ciberseguridad diseñada | Enfoque normativo | Alineación con controles de ISO/IEC 27001:2022. |
| | | | | | Inclusión de lineamientos de ISO/IEC 27032:2023. |
| | | | | | Compatibilidad con marcos como NIST y CNBS 025-2022. |
| | | | | Diseño de controles estratégicos | Controles definidos por dominio (organizativos, tecnológicos, físicos y de personas). |
| | | | | | Priorización de controles según análisis de riesgos y madurez. |
| | | | | | Relación directa entre brechas identificadas y controles propuestos. |
| | | | | Gestión del riesgo | Controles asociados a vulnerabilidades críticas. |
| | | | | | Medidas de mitigación para amenazas identificadas. |
| | | | | | Evaluación del impacto de los controles propuestos. |
| | | | | Sostenibilidad y mejora continua | Inclusión de un plan de monitoreo y auditoría. |
| | | | | | Propuesta de procedimientos de respuesta y recuperación. |
| | | | | | Indicadores para medir la efectividad de los controles. |

Fuente: Elaboración Propia

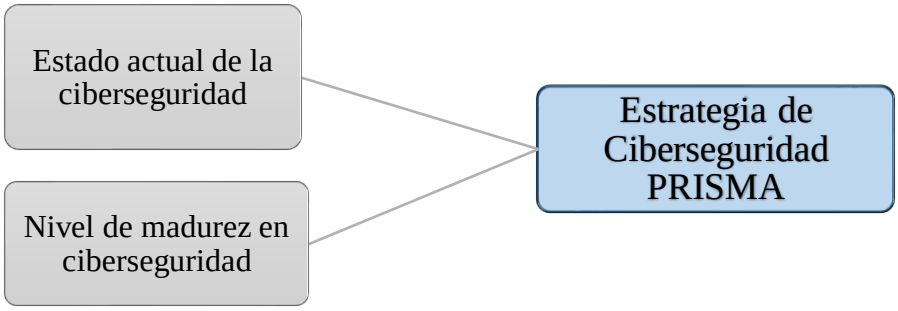


**Figura 7. Diagrama Sagital de las variables de investigación**

Fuente: Elaboración Propia

### 3.1.3 OPERACIONALIZACIÓN DE LAS VARIABLES

Este apartado presenta una descripción detallada de las variables del estudio, incluyendo su definición, método de medición, dimensiones e ítems, con el propósito de proporcionar un esquema claro y estructurado que permita visualizar la operacionalización de las variables dependientes e independientes, información que se encuentra la Tabla 7.

**Tabla 7. Operacionalización de las variables**

| Variable | Definición Conceptual | Definición Operacional | Dimensiones | Ítems |
|---|---|---|---|---|
| Estado actual de la ciberseguridad | El estado actual de la ciberseguridad se refiere al nivel presente de implementación y eficacia de las políticas, procedimientos y controles de seguridad cibernética dentro de una organización. Según el Marco de Ciberseguridad del NIST (NIST, 2024), las organizaciones pueden desarrollar perfiles que describen su estado actual en estas áreas, permitiendo comparar su situación presente con los objetivos de seguridad deseados y facilitando la implementación de controles adecuados para gestionar los riesgos de ciberseguridad. | El estado actual de la ciberseguridad en la microfinanciera PRISMA será medido a través de un análisis estructurado basado en la matriz de evaluación de cumplimiento y madurez, considerando los requisitos y controles establecidos en las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023. | Cumplimiento normativo | Nivel de cumplimiento de los requisitos de ISO/IEC 27001:2022. |
| | | | | Nivel de cumplimiento de las recomendaciones de ISO/IEC 27032:2023. |
| | | | Controles implementados | Existencia y efectividad de controles organizativos, de personas, físicos y tecnológicos. |
| | | | | Aplicación de medidas de protección para prevenir ciberataques. |
| | | | Fortalezas en seguridad | Identificación de activos críticos y su protección. |
| | | | | Capacidad de detección y respuesta ante incidentes de seguridad. |
| | | | Brechas en seguridad | Evaluación de medidas actuales contra ciberamenazas. |
| | | | | Detección de brechas en procedimientos y políticas de seguridad. |
| Nivel de madurez en ciberseguridad | Según el CMMI Institute (2018), el nivel de madurez en ciberseguridad se define como el grado de desarrollo, formalización y optimización de los procesos, controles y estrategias de seguridad de la información dentro de una organización. Basado en el Modelo de Madurez Integrado de Capacidades (CMMI), este nivel refleja la capacidad de la entidad para identificar, gestionar y mejorar continuamente su postura de ciberseguridad, asegurando la protección de sus activos digitales frente a amenazas cibernéticas. | El nivel de madurez en ciberseguridad en la microfinanciera PRISMA será medido a través de un modelo de evaluación basado en el marco CMMI, complementado con los controles establecidos en ISO/IEC 27001:2022 e ISO/IEC 27032:2023. | Cumplimiento de controles | Nivel de cumplimiento de los controles definidos en ISO/IEC 27001:2022. |
| | | | Capacidad de respuesta | Capacidad de detección y respuesta ante incidentes de ciberseguridad. |
| | | | Mejora continua | Estrategias implementadas para la mejora continua en ciberseguridad. |
| | | | | Existencia de procesos de revisión y actualización de controles de seguridad. |

| Variable | Definición Conceptual | Definición Operacional | Dimensiones | Ítems |
|---|---|---|---|---|
| Estrategia de ciberseguridad diseñada | La estrategia de ciberseguridad es un plan estructurado que establece prioridades, objetivos, políticas y controles específicos para proteger los activos digitales de una organización, reducir riesgos y garantizar la continuidad operativa. Según la ISO/IEC 27032:2023, una estrategia de ciberseguridad debe contemplar la identificación, protección, detección, respuesta y recuperación ante amenazas cibernéticas, con enfoque en la colaboración entre múltiples actores (ISO & IEC, 2022b). Además, el NIST (2020) plantea que una estrategia efectiva está alineada con los objetivos del negocio, basada en la gestión de riesgos, y adaptada a la naturaleza de las amenazas emergentes. | La estrategia de ciberseguridad diseñada para la Microfinanciera PRISMA es el resultado de un proceso estructurado basado en el diagnóstico de madurez, análisis de riesgos, brechas identificadas y cumplimiento con las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023. Esta estrategia incorpora controles organizativos, físicos, tecnológicos y de personas, alineados al marco NIST, con planes específicos para monitoreo, respuesta a incidentes, recuperación y mejora continua. | Estructura del plan de ciberseguridad. | Existencia de un plan estructurado con objetivos, fases y componentes claros. |
| | | | Controles definidos por dominio (organización, personas, físicos, tecnológicos). | Integración de controles específicos por dominio (organizativo, personas, físico, tecnológico). |
| | | | | Correspondencia entre los controles propuestos y los hallazgos del diagnóstico. |
| | | | Alineación normativa (ISO/IEC 27001:2022, ISO/IEC 27032:2023, NIST CSF). | Coherencia con estándares ISO/IEC 27001:2022, ISO/IEC 27032:2023 y principios NIST. |
| | | | Sostenibilidad y mejora continua. | Consideración de indicadores de monitoreo, auditoría y resiliencia. |
| | | | | Inclusión de procesos de revisión y mejora continua. |

Fuente: Elaboración Propia

### 3.1.4 HIPÓTESIS

Debido al enfoque descriptivo y mixto de esta investigación, orientado a evaluar y diagnosticar el estado actual de la ciberseguridad en PRISMA, no se formulan hipótesis. En su lugar, se emplean preguntas de investigación, ya que no se busca probar relaciones causales ni realizar inferencias estadísticas, sino describir y analizar cómo la organización se alinea con los estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27032:2023.

Hernández Sampieri (2018) establece que "los estudios descriptivos tienen como objetivo detallar características y elementos de un fenómeno, sin requerir necesariamente la elaboración o comprobación de hipótesis específicas". En consecuencia, las razones metodológicas para la no formulación de hipótesis son:

**Tabla 8. Fundamentos metodológicos ausencia de hipótesis**

| Aspecto Metodológico | Descripción y Justificación |
|---|---|
| **Enfoque de la Investigación** | Enfoque mixto, combinando técnicas cualitativas y cuantitativas. Se centra en describir, analizar y diagnosticar la situación actual de la seguridad de la información en PRISMA. No busca establecer relaciones causa-efecto. |
| **Técnicas de Recolección de Datos** | Aplicación de la herramienta MASS (Modelo de Evaluación de Sistemas de Seguridad de la Información) y una matriz de Diagnóstico de Seguridad Global basada en ISO/IEC 27001:2022, para identificar patrones, analizar cumplimiento normativo y evaluar niveles de madurez. |
| **Estructura Analítica del Estudio** | Se estructura mediante preguntas de investigación, que guían el análisis y permiten identificar niveles de cumplimiento de controles, detectar vulnerabilidades y diseñar estrategias para optimizar la ciberseguridad en PRISMA. |
| **Fundamentación Normativa** | Basado en marcos normativos internacionales (ISO/IEC 27001:2022, ISO/IEC 27032:2023), utilizados como criterios de referencia para evaluar la seguridad de la información, por lo que no requiere validar teorías mediante hipótesis causales. |

Fuente: Elaboración Propia

## 3.2 ENFOQUE Y MÉTODOS

### 3.2.1 ENFOQUE

El presente estudio adopta un enfoque mixto de investigación, integrando técnicas tanto cualitativas como cuantitativas, con el objetivo de abordar de manera integral el fenómeno investigado: el diseño de una estrategia de ciberseguridad para la Microfinanciera PRISMA. Esta combinación metodológica permite capturar tanto la profundidad contextual del problema como

la evidencia empírica necesaria para sustentar las decisiones estratégicas.

La elección del enfoque mixto se justifica por la naturaleza del problema: por un lado, es necesario recolectar y analizar datos cualitativos mediante entrevistas semiestructuradas a actores clave de la organización, a fin de comprender percepciones, brechas operativas y prácticas informales relacionadas con la gestión de la seguridad de la información. Por otro lado, se aplican instrumentos estructurados, como la matriz de Diagnóstico de Seguridad Global, basada en normas ISO/IEC 27001:2022 y 27032:2023, lo cual proporciona evidencia cuantitativa sobre el estado actual de los controles implementados en la organización.

El enfoque mixto resulta especialmente útil para triangular los hallazgos entre distintas fuentes, fortalecer la validez del diagnóstico y estructurar una propuesta de estrategia de ciberseguridad alineada tanto con el contexto organizacional como con los estándares internacionales. Este enfoque no solo permite una mayor profundidad analítica, sino también la generación de recomendaciones prácticas basadas en evidencia medible y contextualizada.

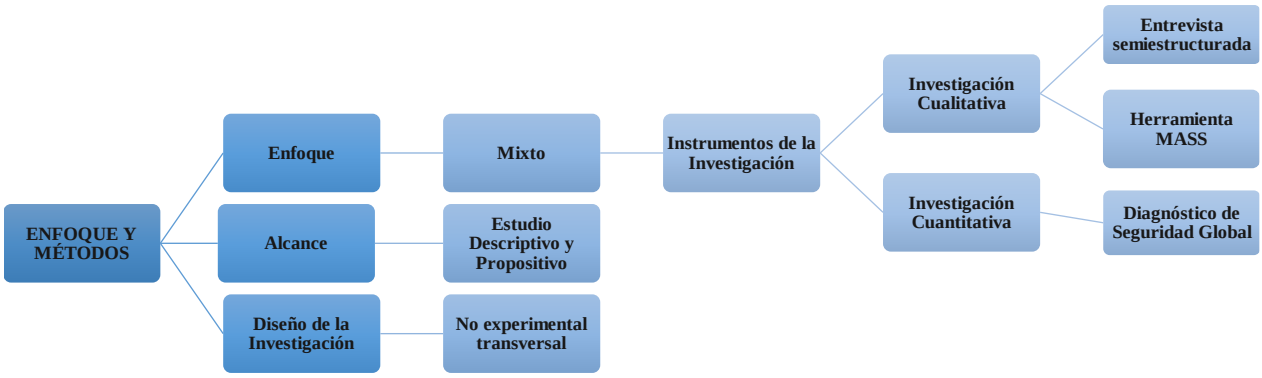


**Figura 8. Enfoque y Métodos**

Fuente: Elaboración Propia

### 3.2.2 ALCANCE

El alcance que presenta este estudio es descriptivo ya que se busca identificar y analizar el estado actual de la ciberseguridad en PRISMA, sus amenazas, vulnerabilidades y los controles aplicados; y así poder esbozar los resultados de las variables que se estudian para dar respuestas a las preguntas de investigación. También se puede considerar propositivo, ya que además de describir la situación actual, la investigación propone una estrategia de ciberseguridad basada en las normas ISO/IEC 27001 y 27032.

Los estudios descriptivos pretenden especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, miden o recolectan datos y reportan información sobre diversos conceptos, variables, aspectos, dimensiones o componentes del fenómeno o problema a investigar (Hernández Sampieri, 2018).

Según Hernández Sampieri (2018) los estudios propositivos se centran en diseñar, proponer o sugerir soluciones a un problema identificado, en lugar de solo describirlo o analizarlo. En este tipo de estudios, el investigador no solo examina la situación actual, sino que también ofrece alternativas de acción, estrategias o propuestas de intervención fundamentadas en el conocimiento disponible. El propósito principal es generar un impacto práctico, proponiendo soluciones aplicables y útiles para resolver los problemas investigados.

### 3.2.3 DISEÑO

El diseño de la investigación será no experimental y transversal, ya que no se manipularán directamente las variables. En su lugar, se recopilará información a través de la aplicación de instrumentos cualitativos y cuantitativos. Este estudio se llevará a cabo en un período determinado, con el propósito de analizar el estado actual de la ciberseguridad y desarrollar una estrategia alineada con las necesidades específicas de la organización y las mejores prácticas del sector.

Este enfoque metodológico se caracteriza por la ausencia de manipulación deliberada de las variables. Es decir, no se introducen cambios intencionales en las variables independientes para evaluar su impacto en otras variables, sino que el estudio se basa en la observación y análisis de su comportamiento en condiciones reales (Hernández Sampieri, 2018).

## 3.3 DISEÑO DE LA INVESTIGACIÓN

Dado el enfoque mixto y el carácter descriptivo de la investigación, se emplea un diseño no experimental de tipo transversal, lo que posibilita la recopilación de datos en un único momento para obtener una visión precisa de la situación actual. Esta metodología facilita la identificación de oportunidades de mejora y la formulación de una estrategia alineada con estándares internacionales. A partir de este diseño, se definen aspectos clave como la población y muestra de estudio, las técnicas e instrumentos de recolección de datos, así como las fuentes de información que respaldan el análisis. Todo ello con el objetivo de garantizar la rigurosidad y validez de los hallazgos, proporcionando insumos sólidos para la formulación de una estrategia alineada con estándares internacionales.

### 3.3.1 POBLACIÓN

La población de este estudio está conformada por los 74 colaboradores de la Microfinanciera PRISMA, quienes desempeñan diversas funciones dentro de la organización. Esta población incluye tanto personal operativo como administrativo, distribuidos en áreas clave. La inclusión de todos los colaboradores en la población general permite considerar el contexto organizacional en el que se desarrolla la ciberseguridad, abarcando los diferentes niveles de interacción con los sistemas de información y los procesos de seguridad implementados.

Sin embargo, para el análisis específico de la seguridad de la información, se ha definido una población objetivo, compuesta por los colaboradores que tienen un rol clave en la gestión, supervisión y operación de los sistemas tecnológicos, así como en la aplicación de controles de seguridad y cumplimiento normativo. Esta población delimitada incluye a las áreas de Tecnología, Auditoría Interna, Cumplimiento y Riesgos, Finanzas, Riesgo de Crédito, Gerencia de Negocios y Atención al Cliente, ya que sus funciones implican el acceso a datos sensibles, la administración de controles de seguridad o la supervisión del cumplimiento de políticas de ciberseguridad. Esta delimitación permite focalizar el estudio en los actores más relevantes, asegurando que los hallazgos reflejen de manera precisa el estado de la seguridad de la información en la organización.

### 3.3.2 MUESTRA

Un estudio carecería de validez si no se dispone de datos suficientes y representativos para el análisis. Por ello, es fundamental establecer criterios de inclusión y exclusión bien definidos,

que permitan garantizar la pertinencia y representatividad de la muestra, asegurando así la rigurosidad metodológica y la coherencia en los resultados obtenidos (Hernández Sampieri, 2018).

Los criterios de inclusión y exclusión a considerar para la selección de la muestra se presentan a continuación:

**Tabla 9. Criterios de Inclusión y Exclusión**

| Criterios de Inclusión | Criterios de Exclusión |
|---|---|
| **Empleados en agencias con más de seis meses de operación:** Solo se incluirán a los empleados que laboran en agencias que han estado operando por más de seis meses, asegurando que estén familiarizados con los procesos operativos y las medidas de seguridad implementadas en dichas agencias. | **Empleados en agencias con menos de seis meses de operación:** Se excluirán a los empleados que laboran en agencias que han estado operando por menos de seis meses, ya que es probable que no tengan suficiente conocimiento sobre los procesos operativos y los controles de seguridad implementados en esas agencias. |
| **Antigüedad mínima de seis meses en la organización**, garantizando que los participantes tengan suficiente conocimiento sobre los procesos internos y controles de seguridad implementados**.** | **Colaboradores con menos de seis meses en la empresa,** ya que podrían no tener un conocimiento profundo de los controles de seguridad implementados. |
| **Colaboradores involucrados en la gestión y aplicación de controles de seguridad, abarcando las siguientes áreas:**<br><br>**Administrativos/Organizativos:** Personal de alta dirección, cumplimiento, auditoría interna y gestión de riesgos, quienes supervisan la implementación de políticas de seguridad**.**<br><br>**Personas:** Recursos Humanos y áreas encargadas de la gestión del personal, formación en seguridad y concienciación sobre ciberseguridad**.**<br><br>**Físicos:** Personal responsable de la infraestructura física y seguridad perimetral, incluyendo control de accesos y videovigilancia**.**<br><br>**Tecnológicos:** Equipos de TI y ciberseguridad, encargados de la gestión de sistemas, redes, protección de datos y respuesta ante incidentes. | **Personal sin relación directa o indirecta con la seguridad de la información**, incluyendo áreas operativas o administrativas sin acceso a sistemas de información, datos críticos o responsabilidades en la gestión de seguridad. |
| **Personal con acceso y responsabilidad sobre datos sensibles,** incluyendo colaboradores que manipulan información financiera, registros de clientes o infraestructura crítica de la microfinanciera. | **Colaboradores de áreas exclusivamente operativas**, como personal de servicio general, mensajería o asistencia, cuyo rol no implica interacción con controles de seguridad de la información. |

Fuente: Elaboración Propia

Para garantizar una evaluación precisa y representativa del nivel de madurez de los controles de seguridad en la Microfinanciera PRISMA, se ha definido una muestra estratégica, considerando los distintos niveles organizacionales y sus respectivas funciones dentro de la institución, como se ilustra en la Figura 9.

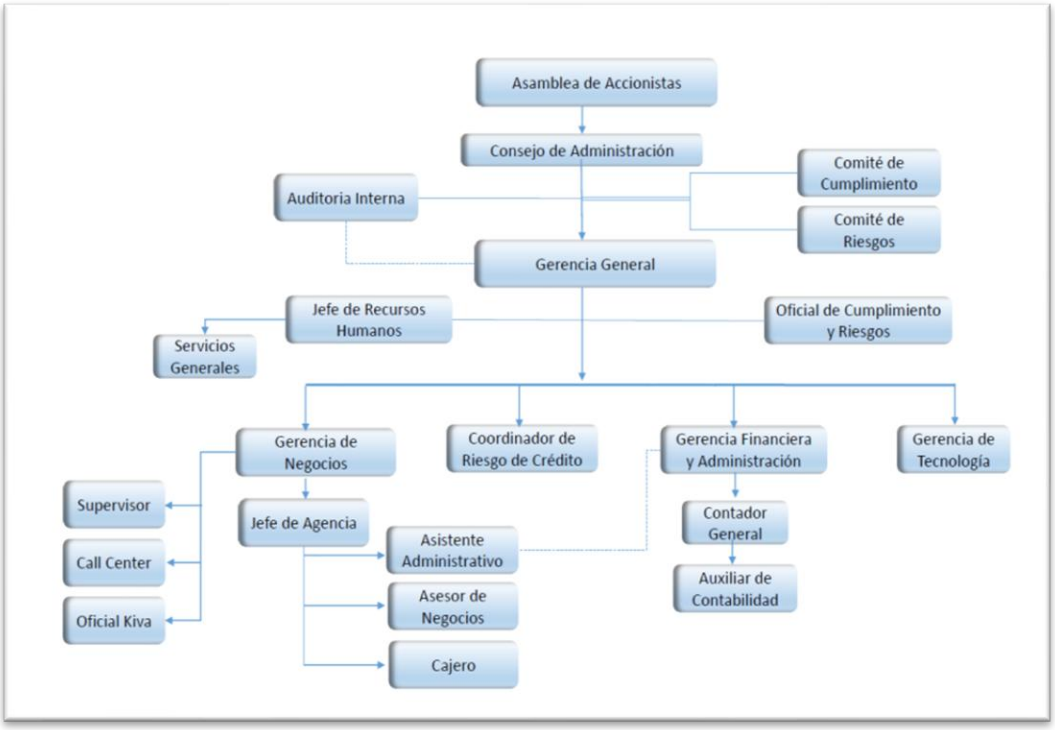


**Figura 9. Estructura Organizacional de PRISMA**

Fuente: Plan Estratégico 2022-2026 PRISMA (2022)

Para asegurar que la muestra seleccionada refleje con precisión la realidad de la seguridad de la información en PRISMA, se llevó a cabo un proceso de selección basado en criterios de inclusión y exclusión previamente definidos. Inicialmente, la población total estaba conformada por los 74 colaboradores de la microfinanciera, quienes desempeñan diversas funciones dentro de la organización. No obstante, no todos los colaboradores tienen la misma interacción con los sistemas de información ni la misma responsabilidad en la gestión de la ciberseguridad.

Por esta razón, se estableció una población objetivo, incluyendo únicamente a los colaboradores con roles clave en Tecnología, Auditoría Interna, Cumplimiento y Riesgos, Finanzas, Riesgo de Crédito, Gerencia de Negocios y Atención al Cliente. Posteriormente, se aplicaron criterios de inclusión como una antigüedad mínima de seis meses en la organización,

garantizando que los participantes tengan conocimiento suficiente sobre los procesos internos y controles de seguridad implementados. Asimismo, se consideraron aquellos colaboradores directamente involucrados en la gestión y aplicación de controles de seguridad, abarcando aspectos administrativos/organizativos, de gestión de personal, seguridad física y tecnológica.

De manera complementaria, se establecieron criterios de exclusión para evitar la incorporación de participantes cuyo rol no esté vinculado con la seguridad de la información. Se excluyeron colaboradores con menos de seis meses en la empresa, ya que podrían no tener conocimiento profundo de los controles de seguridad implementados, así como personal de áreas operativas o administrativas sin acceso a sistemas críticos ni responsabilidad en la gestión de seguridad, como servicios generales o mensajería.

Finalmente, tras la aplicación de estos criterios, se definió una muestra final de 8 colaboradores, quienes cumplen con los requisitos establecidos y pueden aportar información relevante para la evaluación del estado de la ciberseguridad en PRISMA. En la Figura 10 se presenta el proceso de selección mediante un diagrama en forma de embudo (funnel), el cual ilustra la reducción progresiva de la población hasta la conformación de la muestra de estudio.

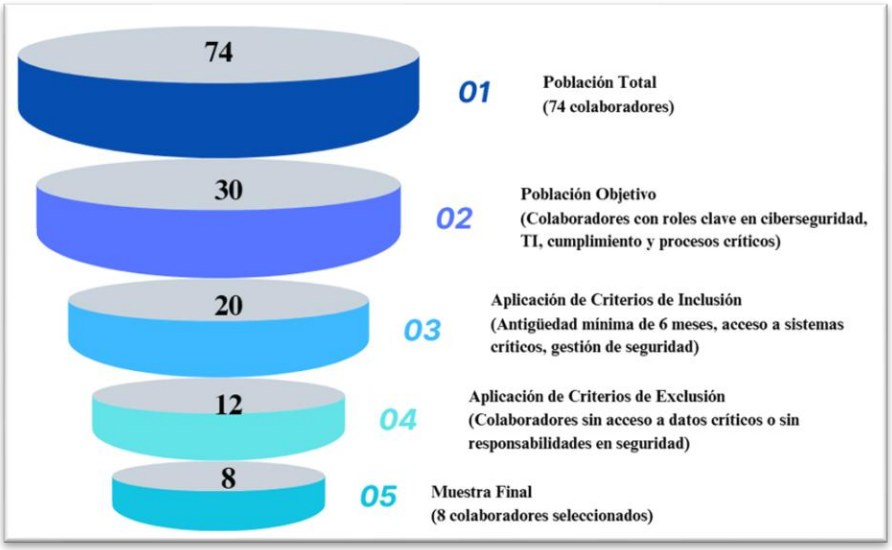


**Figura 10. Funnel proceso de selección de la muestra**

Fuente: Elaboración Propia

En la Tabla 10 se presenta la distribución de la muestra propuesta detallando los roles incluidos y la justificación de su participación en el estudio.

**Tabla 10. Muestra seleccionada**

| No. | Participante | Rol en la Organización | Criterios de Selección |
|---|---|---|---|
| **1** | **Gerente General** | Liderazgo estratégico y toma de decisiones en la organización | Acceso a datos sensibles y decisiones estratégicas |
| **2** | **Oficial de Cumplimiento y Riesgos** | Supervisión de normativas y riesgos organizacionales | Responsabilidad sobre normativas de seguridad y cumplimiento |
| **3** | **Jefe de Recursos Humanos** | Gestión de personal y cumplimiento de políticas de seguridad | Gestión de credenciales y accesos de empleados |
| **4** | **Gerente de Tecnología** | Administración de infraestructura tecnológica y ciberseguridad | Administración de sistemas críticos y seguridad TI |
| **5** | **Gerente Financiero – Administrativo** | Gestión financiera y auditoría de seguridad | Control sobre datos financieros y transacciones |
| **6** | **Gerente de Negocios** | Desarrollo de estrategias comerciales y de negocio | Interacción con clientes y administración de datos sensibles |
| **7** | **Auditor Interno** | Auditoría y control interno de procesos | Control y revisión de cumplimiento de normativas internas |
| **8** | **Jefe de Agencia** | Supervisión de operaciones en sucursales | Gestión de equipos de trabajo y aplicación de seguridad operativa |

Fuente: Elaboración Propia

### 3.3.3 TÉCNICAS DE MUESTREO

Este estudio utiliza un muestreo no probabilístico por criterio o intencional, en el cual la selección de los participantes responde a su conocimiento especializado y experiencia en ciberseguridad dentro de la Microfinanciera PRISMA. Esta estrategia permite centrar el análisis en los colaboradores que desempeñan funciones clave en la gestión, supervisión e implementación de controles de seguridad de la información, asegurando que los datos recopilados reflejen con precisión los procesos y prácticas de ciberseguridad en la organización.

En este caso, la muestra está conformada por 8 colaboradores, seleccionados con base en criterios predefinidos que incluyen responsabilidades estratégicas en seguridad de la información, gestión de TI, cumplimiento normativo y administración de procesos críticos. Este enfoque cualitativo y estratégico no busca una representación estadística de la población total, sino la obtención de información relevante para el diagnóstico y evaluación del nivel de madurez en ciberseguridad. Aunque la muestra es reducida, su composición es significativa, ya que cada participante aporta una perspectiva clave para el análisis, permitiendo una comprensión profunda

del estado de la seguridad de la información en PRISMA.

## 3.4 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

Tras definir el diseño del estudio y determinar a los participantes, el siguiente paso consiste en estructurar el proceso de recolección de datos, seleccionando las técnicas más apropiadas según la naturaleza del problema, las características de la información requerida y la metodología adoptada. La recopilación de estos datos es un componente esencial, ya que permitirá obtener evidencia empírica para analizar el fenómeno en estudio y responder de manera fundamentada a la pregunta de investigación (Monroy & Nava, 2018).

Las técnicas de investigación constituyen el conjunto de herramientas y procedimientos utilizados para la aplicación del método científico en la recopilación y análisis de datos. Si bien el método se refiere a la estructura general que orienta el proceso investigativo a través de etapas sistemáticas y replicables, aplicables a diversas disciplinas, la técnica abarca los instrumentos específicos empleados para obtener información relevante (Monroy & Nava, 2018). Dado que esta investigación adopta un enfoque mixto, se integran técnicas cualitativas y cuantitativas, permitiendo una comprensión más amplia y profunda del fenómeno estudiado.

### 3.4.1 TÉCNICAS

#### 3.4.1.1 TÉCNICAS CUALITATIVAS

Las técnicas cualitativas utilizadas en el estudio permiten explorar las percepciones, conocimientos y experiencias de los participantes en torno a los controles de seguridad implementados. A través de este análisis, se identifican factores organizacionales, procedimentales y tecnológicos que inciden en la gestión de la ciberseguridad, además permitirán contrastar y validar los datos cuantitativos obtenidos mediante la aplicación de otros instrumentos.

#### 3.4.1.2 TÉCNICAS CUANTITATIVAS

Las técnicas cuantitativas seleccionadas permiten medir y evaluar de manera objetiva el nivel de madurez de la ciberseguridad en la microfinanciera, a partir de indicadores y métricas específicas alineadas con los estándares ISO/IEC 27001:2022 e ISO/IEC 27032:2023.

### 3.4.2 INSTRUMENTOS

Para la recopilación de datos en esta investigación, se han aplicado tres instrumentos complementarios cada uno diseñado para abordar distintos aspectos del estudio desde una perspectiva cualitativa y cuantitativa:

- Guía de entrevista semiestructurada.
- Cuestionario estructurado, basado en la herramienta de MASS ((Maturity Assessment for Security Survey) de LAC4.
- Diagnóstico de Seguridad Global, basado en los estándares ISO/IEC 27001:2022.

La guía de entrevista semiestructurada (Instrumento Cualitativo), cuyo guion se encuentra en el Anexo 1, fue aplicada a 6 colaboradores de la Microfinanciera PRISMA, seleccionados por su rol en la seguridad de la información, gestión de TI y administración de riesgos. Su objetivo fue obtener una visión detallada de las prácticas y percepciones organizacionales en materia de ciberseguridad y, validar los datos cuantitativos recopilados.

La herramienta MASS puede considerarse más cualitativa que cuantitativa, ya que se basa en un cuestionario que evalúa prácticas, procesos y controles en materia de seguridad de la información mediante preguntas estructuradas, las cuales son principalmente descriptivas y analíticas. El objetivo es identificar áreas de vulnerabilidad, riesgos, y la madurez de las políticas de seguridad dentro de una organización. Algunas de las respuestas pueden traducirse a una escala numérica para facilitar la comparación o el análisis de la madurez en seguridad, el enfoque principal es obtener una comprensión profunda de las prácticas actuales a través de la evaluación cualitativa (LAC4, 2025).

La herramienta MASS, una plataforma de autoevaluación de la seguridad de la información diseñada para medir la madurez de los procesos de seguridad de una organización permitió medir el nivel de madurez en materia de ciberseguridad de PRISMA e identificar áreas de mejora, sirviendo de base para elaborar planes concretos de acción.

En esencia, MASS califica qué tan desarrollados y consistentes están los procesos y controles de seguridad, indicando si se siguen las mejores prácticas de la industria en cada dominio evaluado. Esta plataforma está inspirada en la matriz CMMI (Capability Maturity Model Integration), un marco ampliamente utilizado que describe las mejores prácticas para evaluar y

mejorar la madurez de los procesos organizacionales (Solutions, 2025).

El modelo CMMI provee una estructura de niveles de madurez que van desde procesos iniciales o ad hoc hasta procesos optimizados y en mejora continua. Siguiendo este enfoque, MASS realiza una evaluación cualitativa de la madurez de los procesos de seguridad de la información, examinando la existencia de políticas, la formalización de procedimientos, la medición de su efectividad y la mejora continua de los mismos. Además, la herramienta se basa en estándares internacionales reconocidos, incorporando recomendaciones de las Normas de Seguridad de la Información de Estonia, del informe ENISA Threat Landscape 2022 y los objetivos de control de la norma ISO/IEC 27002:2022 (LAC4, 2025). Esto asegura que la evaluación esté alineada con prácticas de seguridad de vanguardia y requerimientos globales.

**Tabla 11. Escala de Evaluación de MASS**

| Nivel de Madurez | Valor | Descripción |
|---|---|---|
| **Iniciado** | **<0.75** | No se han implementado buenas prácticas de seguridad.<br>No se han reconocido los riesgos.<br>La alta dirección no ha tomado iniciativa en seguridad.<br>Las actividades de seguridad son esporádicas e impulsadas desde niveles operativos sin estrategia clara. |
| **Definido** | **≥0.75 y <1.5** | Se inician procesos y actividades, pero de manera ad hoc.<br>Existen documentos de seguridad, pero están parcialmente desactualizados o no reflejan la realidad operativa. |
| **Básico** | **≥1.5 y <2.25** | Se han establecido prácticas documentadas y se planifican recursos para seguridad.<br>Existen asignaciones de funciones y responsabilidades claras.<br>Aún no se ha logrado la regularidad en la ejecución de actividades de seguridad. |
| **Estándar** | **>2.25** | Las políticas y principios organizacionales son claros y estandarizados.<br>Las actividades de seguridad son monitoreadas y rastreadas regularmente.<br>Se ha implementado un enfoque de mejora continua y monitoreo de excepciones. |

Fuente: (LAC4, 2025)

El Diagnóstico de Seguridad Global (Instrumento Cuantitativo y Cualitativo) permite evaluar la implementación y eficacia de los controles de seguridad en PRISMA, se diseñó alineada con las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023. Esta matriz facilitó el análisis del cumplimiento de 93 controles de seguridad, distribuidos en las siguientes categorías: 37 controles organizativos, 8 controles relacionados con el factor humano, 14 controles físicos y 34 controles tecnológicos.

Los objetivos de esta matriz de evaluación son:

- Medir el nivel de madurez de la ciberseguridad en la organización.
- Evaluar el grado de cumplimiento de los controles establecidos en los estándares ISO 27001 e ISO 27032.
- Identificar brechas de seguridad y oportunidades de mejora en los procesos internos.

Este instrumento combina indicadores cualitativos y cuantitativos, proporcionando un diagnóstico estructurado y basado en evidencia sobre la gestión de la seguridad de la información en PRISMA. Para su correcta aplicación, se han definido criterios específicos de evaluación, organizados en columnas que detallan aspectos clave de cada control analizado. A continuación, se presenta la descripción de cada una de las columnas de la matriz de evaluación:

**Tabla 12. Descripción del Diagnóstico de Seguridad Global**

| Columna de la matriz | Descripción |
|---|---|
| **Métrica** | Define el indicador o parámetro específico que se utilizará para evaluar el rendimiento o la eficacia del control, en este caso corresponde a los requisitos de la norma ISO/IEC 27001. |
| **Control** | Especifica el mecanismo o procedimiento de seguridad a analizar, conforme a los estándares y buenas prácticas (por ejemplo, ISO/IEC 27001 o 27032). Identifica el elemento concreto que protege contra riesgos o vulnerabilidades específicas. |
| **Propósito** | Explica la razón de ser del control evaluado, detallando cómo contribuye a mitigar riesgos, salvaguardar activos y asegurar la continuidad operativa. Establece la justificación y los objetivos estratégicos que motivan su implementación. |
| **Capítulo** | Indica la sección o apartado del estándar o marco normativo en el que se encuentra definido el control, facilitando la trazabilidad y la vinculación directa con los requisitos normativos. |
| **Madur_Desc** | Abreviatura de “Descripción de la Madurez”. Proporciona una valoración cualitativa del nivel de implementación y evolución del control, describiendo su grado de integración, formalización y mejora continua dentro del SGSI. |
| **Valor** | Asigna una puntuación numérica que cuantifica el nivel de madurez del control. Este valor facilita el análisis comparativo y global del SGSI, permitiendo el seguimiento de la evolución en el tiempo. |
| **Aspecto_Clave** | Resalta los elementos críticos o factores determinantes que inciden en la eficacia del control. Identifica aquellos aspectos cuya optimización tendría un impacto significativo en la postura de seguridad de la organización. |

Fuente: adaptado de UNSTA (2023)

### 3.4.3 VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS

Para garantizar la rigurosidad metodológica de la investigación, es fundamental evaluar la validez y confiabilidad de los instrumentos aplicados. Estos aspectos aseguran que los datos recopilados sean precisos, consistentes y representativos del fenómeno en estudio.

La validez se refiere a la capacidad de los instrumentos para medir con precisión las variables planteadas en el estudio. En esta investigación, se aplicaron estrategias para garantizar la validez de ambos instrumentos:

- La entrevista se deriva del Diagnóstico de Seguridad Global, además, se diseñó con base en modelos de madurez en ciberseguridad y en normativas ISO/IEC 27001 y 27032, garantizando que las preguntas aborden dimensiones clave del fenómeno analizado.
- El Diagnóstico de Seguridad Global se diseñó con referencia a estándares internacionales (ISO/IEC 27001:2022 e ISO/IEC 27032:2023) y fue sometido a validación por pares, incluyendo expertos en gestión de seguridad de la información. Los resultados obtenidos a través de la matriz se comparan con indicadores de referencia establecidos en modelos de madurez reconocidos, como CMMI y NIST CSF, para evaluar su precisión en la medición.
- La validez de la herramienta MASS se respalda en su fundamentación sobre marcos normativos ampliamente reconocidos como ISO/IEC 27002:2022, el modelo CMMI y el ENISA Threat Landscape. Su diseño por dominios permite evaluar integralmente prácticas de ciberseguridad, alineadas con estándares internacionales. Esta alineación garantiza que los resultados obtenidos midan de forma precisa el nivel de madurez de los controles y procesos de seguridad de la información en la organización evaluada.

La confiabilidad mide la consistencia y estabilidad de los instrumentos a lo largo del tiempo y en diferentes condiciones. Se aplicaron los siguientes métodos para evaluar la confiabilidad de los datos recopilados:

- Se entrevistó a diferentes actores clave dentro de la organización (TI, seguridad de la información, cumplimiento y gestión de riesgos) para comparar respuestas y detectar patrones consistentes.
- Se realizó una aplicación preliminar de la matriz de diagnóstico con un grupo reducido de colaboradores para evaluar su claridad, funcionalidad y coherencia en la recolección de datos.
- La matriz de diagnóstico fue evaluada por especialistas en seguridad de la información y metodología de investigación, asegurando su solidez técnica.
- La confiabilidad de MASS se aseguró mediante la aplicación uniforme del instrumento a colaboradores estratégicos, seleccionados por su conocimiento técnico y su rol en la gestión de seguridad. Los resultados obtenidos mostraron consistencia entre respuestas similares y fueron verificados mediante triangulación con entrevistas semiestructuradas y revisión documental.

El análisis de esta investigación en la Microfinanciera PRISMA requiere la evaluación de diversas variables que permitan medir su nivel de madurez y cumplimiento con normativas internacionales. Estas variables se han clasificado en cualitativas y cuantitativas, asegurando un enfoque integral que combine la interpretación descriptiva con mediciones objetivas.

A continuación, se detallan las variables del Diagnóstico de Seguridad Global, seleccionadas para el análisis:

**Tabla 13. Variables de la Matriz seleccionadas para el análisis**

| Variable | Tipo de Variable | Justificación |
|---|---|---|
| Nivel de Madurez | Cualitativa | Describe el nivel de implementación y optimización del control de manera narrativa. |
| Valor | Cuantitativa | Asigna una puntuación numérica al nivel de madurez del control. |
| Aspecto clave | Cualitativa | Resalta factores críticos para la seguridad sin datos numéricos. |

Fuente: Elaboración Propia

La evaluación en la Microfinanciera PRISMA se basa en un Modelo de Madurez de Procesos, alineado con el enfoque de CMMI (Capability Maturity Model Integration). Este modelo permite determinar el grado de desarrollo e implementación de los controles de seguridad mediante

una escala de seis niveles de madurez, lo que proporciona una visión estructurada y medible del estado actual. El modelo aplicado establece seis grados de madurez, cada uno asociado a un valor porcentual que refleja el nivel de implementación y control del proceso evaluado.

**Tabla 14. Grados de madurez según CMMI**

| Nivel de Madurez | Grado | Valor | Descripción | Aspecto Clave |
|---|---|---|---|---|
| **N/A - No Aplica** | **N/A** | **NA** | No aplica al ámbito de estudio / Organización | N/A |
| **0 – Inexistente** | **0** | **0%** | No se realiza ningún aspecto de la actividad. | Sin Acciones |
| **1 – Inicial** | **1** | **5%** | Estado donde el éxito de las actividades se basa, la mayoría de las veces, en el esfuerzo personal. Los procesos son desorganizados, totalmente reactivos y los roles y responsabilidades están mal o poco definidos. | Esfuerzo Personal |
| **2 – Gestionado** | **2** | **15%** | Se normalizan las buenas prácticas en base a la experiencia y el método. Están definidos los productos a realizar, y los hitos para su revisión. Las definiciones no aplican a nivel corporativo, ni existe normalización. | Buenas Prácticas |
| **3 – Definido** | **3** | **60%** | La Organización entera participa en el proceso. Existen métodos y templates bien definidos y documentados. Existen normativas y procedimientos aprobados que regulan la actividad. Los correspondientes actores han sido formados. | Procedimientos |
| **4 – Cuantitativo** | **4** | **85%** | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. | Indicadores |
| **5 – Optimizado** | **5** | **100%** | En base a criterios cuantitativos, se pueden determinar las desviaciones más comunes y optimizar los procesos. En lo sucesivo, se reducirán costos gracias a la reducción de problemas y a la continua revisión de los procesos. | Mejora Continua |

Fuente: Adaptado de CMMI Institute (2018)

La estructuración y análisis de los datos recopilados a través del Diagnóstico de Seguridad Global permite una evaluación objetiva y detallada del estado actual de la seguridad de la información en PRISMA. La combinación de variables cualitativas y cuantitativas en este instrumento facilita la obtención de un diagnóstico integral, proporcionando una base sólida para la formulación de estrategias de fortalecimiento en ciberseguridad alineadas con las mejores prácticas y estándares internacionales.

Los resultados obtenidos a partir de la aplicación de la guía de entrevista semiestructurada y del Diagnóstico de Seguridad Global permitirán no solo determinar el nivel de madurez de la seguridad de la información en la organización, sino también compararlo con estándares internacionales y segmentos similares a nivel global. Este análisis contribuirá a la identificación de brechas y oportunidades de mejora, facilitando la toma de decisiones estratégicas para fortalecer

la resiliencia cibernética de PRISMA.

## 3.5 FUENTES DE INFORMACIÓN

Este apartado describe las principales fuentes de recopilación de datos empleadas en el proceso de investigación. Estas fuentes se dividen en dos categorías: primarias y secundarias. Las fuentes primarias incluyen aquellos medios de los que se obtiene información de primera mano o en los que se originan los datos, como personas, registros históricos de empresas e instituciones, entre otros. En contraste, las fuentes secundarias corresponden a aquellas que proporcionan información relevante sobre el tema, pero sin ser el origen directo de los datos, como libros y diversas fuentes en internet.

### 3.5.1 FUENTES PRIMARIAS

Las fuentes primarias utilizadas en esta investigación provienen directamente de los actores clave de la Microfinanciera PRISMA, lo que permitió obtener información contextualizada, confiable y alineada con la realidad operativa de la organización. Este enfoque, coherente con el diseño metodológico mixto, combinó la recolección de datos cualitativos y cuantitativos para lograr una comprensión integral del estado de la ciberseguridad institucional.

Para este propósito, se utilizaron tres instrumentos fundamentales:

Guía de entrevista semiestructurada (instrumento cualitativo): aplicada a seis colaboradores estratégicos con funciones vinculadas a TI, gestión de riesgos y seguridad de la información. Esta herramienta permitió captar percepciones, experiencias y prácticas organizacionales en torno a la seguridad de la información. Además, facilitó la triangulación y validación de los hallazgos cuantitativos.

Diagnóstico de Seguridad Global: instrumento híbrido basado en las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023. Evaluó 93 controles distribuidos en los dominios organizativos, de personas, físicos y tecnológicos. Este diagnóstico incluyó variables cualitativas (nivel de madurez, aspectos clave) y cuantitativas (valor numérico por control), lo que facilitó la elaboración de matrices de riesgo y madurez, generando insumos sólidos para el diseño de la estrategia de ciberseguridad.

Herramienta MASS (Maturity Assessment for Security Survey): instrumento de evaluación

cualitativo-cuantitativo desarrollado por LAC4, alineado con modelos de madurez como CMMI e ISO/IEC 27002:2022. Fue utilizada para medir el nivel de madurez de los controles de seguridad de la información en PRISMA, a través de la categorización de prácticas organizacionales en diferentes niveles (iniciado, definido, básico y estándar). Este instrumento generó datos estructurados para diagnosticar brechas de ciberseguridad y priorizar acciones correctivas.

### 3.5.2 FUENTES SECUNDARIAS

Este estudio se basa exclusivamente en fuentes primarias, ya que la información relevante para el análisis fue obtenida directamente a través de la aplicación de instrumentos de recolección de datos a la muestra seleccionada. No se recurrió a fuentes secundarias, como informes previos, bases de datos externas o literatura académica específica sobre la organización, debido a la naturaleza del estudio, el cual busca evaluar el estado actual de la ciberseguridad en PRISMA a partir de la percepción y experiencia de los colaboradores involucrados en su gestión. Esta decisión garantiza que los hallazgos reflejen de manera precisa y actualizada la realidad de la organización, sin depender de análisis previos que podrían no ajustarse al contexto específico de la investigación.

La Figura 11 muestra las características básicas de los datos recopilados en la investigación y que serán presentados para su análisis, conclusiones y recomendaciones.

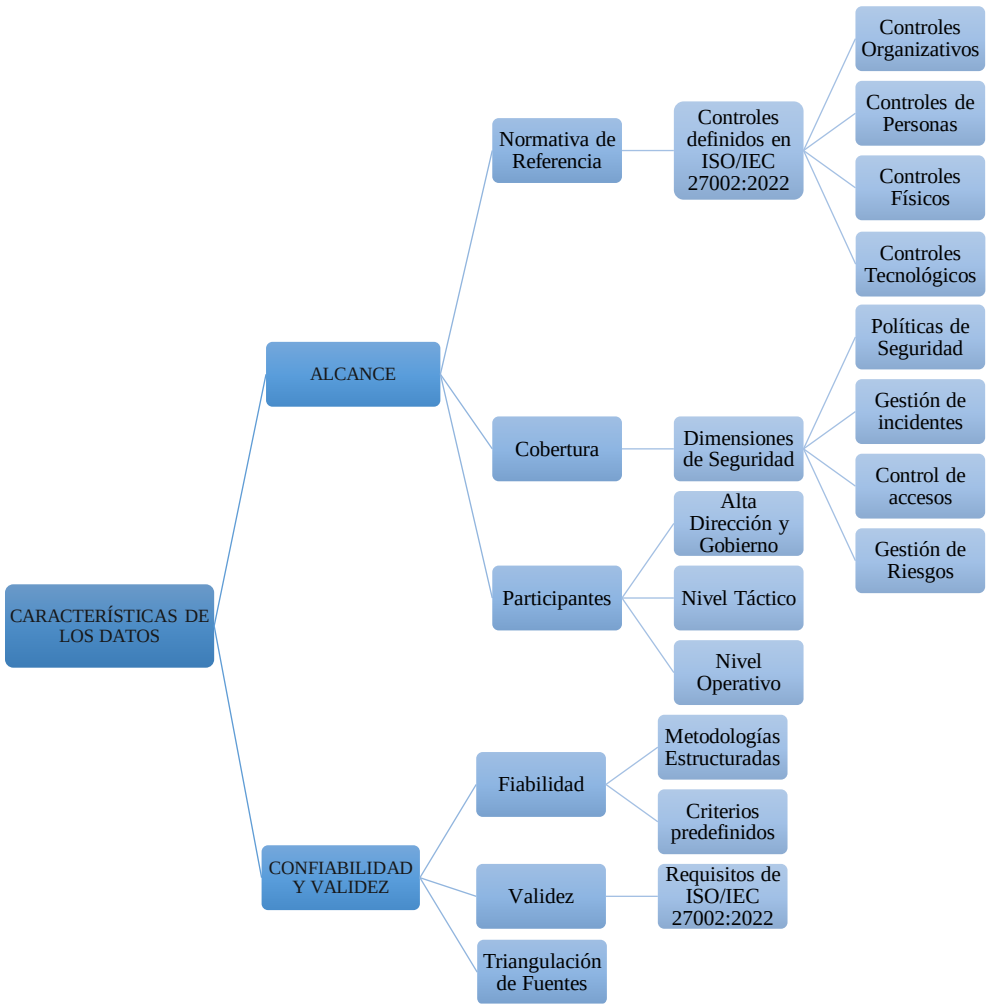


**Figura 11. Características básicas de los datos recopilados**

Fuente: Elaboración Propia

# CAPÍTULO IV. RESULTADOS Y ANÁLISIS

Este capítulo presenta los resultados de la evaluación de los controles y dominios de ciberseguridad en la Microfinanciera PRISMA, aplicando herramientas de diagnóstico de seguridad de la información para determinar su nivel de madurez en ciberseguridad. Los hallazgos obtenidos servirán como base para el diseño de una estrategia integral de ciberseguridad alineada con los estándares internacionales, permitiendo la mitigación de riesgos y el fortalecimiento de la postura de seguridad de la organización.

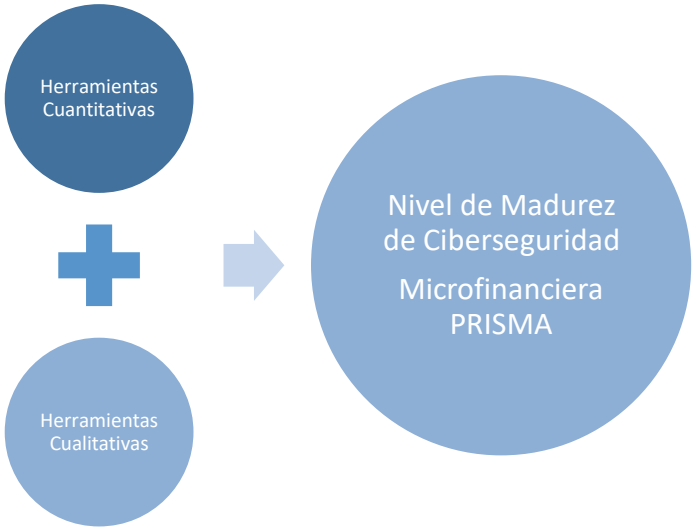


**Figura 12. Enfoque Mixto – Identificación nivel de madurez de ciberseguridad**

Fuente: Elaboración Propia

Para garantizar un análisis efectivo de los resultados, se emplearon herramientas especializadas y entrevistas semiestructuradas, complementadas con representaciones visuales como gráficos, esquemas y tablas. Estos elementos facilitaron la interpretación de los hallazgos y su alineación con estándares y marcos de referencia internacionales en ciberseguridad.

## 4.1 ANÁLISIS EXPLORATORIO DE DATOS (EDA)

Este apartado presenta el Análisis Exploratorio de Datos (EDA) realizado para evaluar los controles y dominios de ciberseguridad en la Microfinanciera PRISMA. El EDA constituye una fase preliminar esencial que permite examinar, visualizar y resumir los datos recopilados antes de aplicar análisis más avanzados. Según González Támara (2017), esta etapa tiene como propósito

identificar patrones, tendencias, relaciones y anomalías mediante herramientas de estadística descriptiva y visualización gráfica. En el contexto de esta investigación, el EDA es fundamental para detectar inconsistencias, validar la integridad de los datos y responder preguntas clave sobre el nivel de madurez en ciberseguridad de la organización

El Análisis Exploratorio de Datos es un paso fundamental en la investigación, ya que proporciona una visión detallada del estado actual de la ciberseguridad en PRISMA. A través de técnicas estadísticas y visualización de datos, se busca responder preguntas clave como:

- ¿Cuáles son los dominios con mayor y menor nivel de cumplimiento en los controles de seguridad?
- ¿Existen valores atípicos que podrían indicar riesgos críticos o inconsistencias en la gestión de la seguridad?
- ¿Qué relaciones pueden encontrarse entre la efectividad de los controles y el nivel de riesgo identificado?

Para responder a estas interrogantes, se emplean herramientas como histogramas, diagramas de dispersión, diagramas de caja y bigotes y matrices de correlación, las cuales facilitan la identificación de tendencias, la variabilidad en los datos y las asociaciones entre variables. Asimismo, se analiza la posible existencia de datos faltantes o sesgos en la recolección de información, factores que podrían influir en la interpretación de los resultados.

El resultado de este análisis exploratorio servirá como base para evaluar el nivel de madurez de la seguridad de la información en PRISMA, proporcionando información clave para la formulación de estrategias que optimicen la gestión de ciberseguridad en la entidad.

### 4.1.1 DESCRIPCIÓN GENERAL DEL CONJUNTO DE DATOS

La evaluación se realizó mediante una metodología integral que combinó cuestionarios estructurados y entrevistas semiestructuradas, recopilando datos cuantitativos y cualitativos sobre el cumplimiento y la efectividad de los controles de seguridad en PRISMA.

Para el análisis de los datos se empleó la librería Pandas de Python, utilizando funciones como df. describe () para obtener estadísticas descriptivas (medias, medianas, cuartiles, etc.) y df.info () para verificar la estructura del conjunto de datos, incluyendo tipos de variables y la

presencia de valores nulos.

```
# Datos actualizados
data = {
    "Nivel de Madurez": ["Inexistente", "Inicial", "Gestionado", "Definido", "Cuantitativo", "Optimizado"],
    "Controles Organizativos": [8, 13, 10, 6, 0, 0],
    "Controles Tecnologicos": [0, 4, 4, 15, 9, 1],
     "Controles Fisicos": [0, 0, 2, 4, 8, 0],
    "Controles Personas": [0, 3, 2, 1, 0, 2]

}

# Crear DataFrame
df = pd.DataFrame(data)

# Cálculo de estadísticos
estadisticas = df.iloc[:, 1:].describe().T
rangos = df.iloc[:, 1:].max() - df.iloc[:, 1:].min()
frecuencias = df.iloc[:, 1:].sum()
mediana = df.iloc[:, 1:].median()
primer_cuartil = df.iloc[:, 1:].quantile(0.25)
tercer_cuartil = df.iloc[:, 1:].quantile(0.75)
desviacion = df.iloc[:, 1:].std()
varianza = df.iloc[:, 1:].var()
coef_var = desviacion / estadisticas["mean"]
sesgo = df.iloc[:, 1:].skew()
curtosis = df.iloc[:, 1:].kurt()
```

**Figura 13. Cálculos estadísticos**

Fuente: Elaboración Propia

Esta combinación de instrumentos permitió una visión holística del estado de la ciberseguridad, integrando datos comparables de los cuestionarios con el contexto detallado aportado por las entrevistas.

La evaluación se llevó a cabo mediante una metodología integral que combinó diferentes técnicas para analizar la seguridad de la información en la organización. En particular, se utilizaron:

Cuestionarios Semiestructurado y formularios estandarizados que permitieron recopilar información cuantitativa y cualitativa sobre el cumplimiento de políticas y la efectividad de los controles de seguridad existentes.

Entrevistas al personal: Se desarrolló un cuestionario de 20 preguntas orientados a las Reuniones dirigidas con empleados clave para profundizar en aspectos específicos, aclarar respuestas de los cuestionarios y obtener perspectivas directas sobre cómo se aplican los controles de seguridad en la práctica.

#### 4.1.1.1 MUESTRA Y CONJUNTO DE DATOS

La población del estudio estuvo conformada por los 74 colaboradores de la Microfinanciera PRISMA, quienes fueron segmentados estratégicamente según su perfil de puesto y nivel de

involucramiento en la gestión de la seguridad de la información. A partir de esta población, se seleccionó una muestra compuesta por 8 participantes clave, quienes participaron en la aplicación de herramientas como la Measurement Application for Self-assessing Security (MASS). Adicionalmente, se realizaron entrevistas a 6 autoridades de agencias, excluyendo aquellas que tenían menos de seis meses de operación al momento de la evaluación. El propósito principal de la herramienta MASS fue proporcionar retroalimentación sobre el estado de la seguridad en la organización y facilitar una autoevaluación estructurada. Las Tablas 15 y 16 presentan la distribución de la muestra y los 93 controles evaluados en los cuatro dominios definidos, conforme a los estándares ISO/IEC 27001:2022.

**Tabla 15. Tamaño de la Muestra**

| | Controles ISO 27002 | Herramienta MASS | Entrevistas |
|---|---|---|---|
| **No. Colaboradores PRISMA** | **8** | **8** | **6** |

Fuente: Elaboración Propia

Asimismo, para la aplicación de las entrevistas, se seleccionaron las máximas autoridades de cada agencia de PRISMA establecida en el país. Se excluyeron aquellas agencias con menos de seis meses de operación, asegurando que los participantes contaran con el conocimiento y la experiencia necesarios para proporcionar información relevante sobre la gestión de la seguridad de la información en sus respectivas unidades.

**Tabla 16. Participantes por control evaluado**

| Participante | Cantidad de controles evaluados |
|---|---|
| Auditor Interno | 1 |
| Gerente Financiero - Administrativo | 2 |
| Gerente General | 6 |
| Gerente de Negocios | 2 |
| Gerente de Tecnología | 53 |
| Jefe de Agencia | 7 |
| Jefe de Recursos Humanos | 7 |
| Oficial de Cumplimiento y Riesgos | 15 |
| **Total de controles** | **93** |

Fuente: Elaboración Propia

El conjunto de datos analizado proviene de la evaluación de 93 controles de seguridad

implementados en la Microfinanciera PRISMA, obtenidos mediante la aplicación de los instrumentos de recolección estructurados. Estos controles están diseñados para evaluar integralmente la postura de seguridad de la organización. Además, su diseño y aplicación están alineados con estándares internacionales reconocidos, como la ISO/IEC 27001:2022 y las directrices del National Institute of Standards and Technology (NIST), garantizando un enfoque basado en mejores prácticas y principios de gestión de riesgos.

Los datos para evaluar se componen de variables que permiten analizar la implementación y efectividad de los controles. A continuación, se describen las principales columnas incluidas en el análisis:

**Tabla 17. Descripción del conjunto de datos**

| Categoría del elemento | Elemento del conjunto de datos | Descripción |
|---|---|---|
| Identificación del Control | MT (Métrica) | Número de identificación del control dentro del marco de evaluación. |
| | Métrica | Nombre asignado al control evaluado |
| | Control | Descripción detallada del control de seguridad. |
| | Propósito | Razón de existencia del control y su impacto en la organización. |
| Clasificación del Control | Capítulo | Categoría a la que pertenece el control dentro del marco de seguridad (Ejemplo: Controles Organizativos, Controles Técnicos, Seguridad Física, etc.). |
| Tipo de Control | Preventivo | Control diseñado para evitar incidentes de seguridad. |
| | Detectivo | Control orientado a la identificación de eventos o incidentes. |
| | Correctivo | Control destinado a la mitigación y recuperación después de un incidente. |
| Impacto en Principios de Seguridad | Confidencialidad | Indica si el control protege el acceso a la información para evitar divulgaciones no autorizadas. |
| | Integridad | Evalúa si el control asegura que la información y los sistemas no sean alterados de forma indebida. |
| | Disponibilidad | Mide si el control garantiza que la información y los sistemas estén disponibles cuando sean requeridos. |
| Categoría del Control | Identificación | Controles destinados a la identificación de usuarios y dispositivos. |
| | Protección | Controles enfocados en la seguridad de activos y datos. |
| | Detección | Controles que permiten identificar incidentes y amenazas. |
| | Respuesta | Controles relacionados con la gestión de incidentes. |
| | Recuperación | Controles para la restauración de operaciones tras un incidente. |
| Evaluación de Madurez y Cumplimiento | Madur_Desc (Nivel de Madurez) | Evaluación del control en función de la madurez de su implementación (Inicial, Repetible, Definido, Gestionado, Optimizado). |
| | Valor | Puntuación asignada al control en función de su nivel de cumplimiento. |

| Categoría del elemento | Elemento del conjunto de datos | Descripción |
|---|---|---|
| Responsabilidad y Gestión | Aspecto Clave | Observaciones sobre el estado actual del control dentro de la organización. |
| | Responsable | Cargo dentro de la organización que tiene la responsabilidad de asegurar la implementación del control (Gerente General, Gerente de Tecnología, Auditor Interno, Oficial de Cumplimiento y Riesgos). |

Fuente: Elaboración Propia

La estructura de este análisis permite una evaluación integral y sistemática del estado de la ciberseguridad en PRISMA, facilitando la identificación de brechas, niveles de madurez y oportunidades de mejora en la organización. A través del análisis exploratorio de datos, se busca:

- Detectar tendencias en la implementación y efectividad de los controles de seguridad.
- Examinar la distribución del nivel de madurez en función de las distintas categorías evaluadas.
- Analizar la relación entre variables clave de seguridad, identificando patrones y correlaciones relevantes.
- Determinar las áreas críticas que presentan mayores deficiencias en seguridad de la información, priorizando acciones correctivas.

#### 4.1.1.2 VARIABLES ANALIZADAS (CUANTITATIVAS Y CUALITATIVAS)

Para el análisis se utilizó la herramienta de Diagnóstico de Seguridad de la Información o Matriz de Evaluación, basada en la evaluación estructurada de cuatro dominios clave, con el propósito de determinar el nivel de gestión de los 93 controles de seguridad.

En este proceso, se identificaron tres tipos de variables para garantizar un análisis preciso:

- Variables cuantitativas nominales (Variable 1): Utilizadas para clasificar a los participantes en las entrevistas, permitiendo su segmentación según características específicas orientadas a alta gerencia, donde se puede ver en Tabla 16.

**Tabla 18. Variables analizadas del Diagnóstico de Seguridad Global**

| Variable 1 | Variable 2 | Variable 3 | | | | |
|---|---|---|---|---|---|---|
| | Nivel de Madurez | Controles Organizativos | Controles Personas | Controles Físicos | Controles Tecnológicos | |
| Perfil de puesto | No Aplica | 0 | 0 | 0 | 1 | **1** |
| | Existente | 8 | 0 | 0 | 0 | **8** |
| | Inicial | 12 | 3 | 0 | 4 | **19** |
| | Gestionado | 11 | 2 | 2 | 4 | **19** |
| | Definido | 6 | 1 | 4 | 15 | **26** |
| | Cuantitativo | 0 | 0 | 8 | 9 | **17** |
| | Optimizado | 0 | 2 | 0 | 1 | **3** |
| | | **37** | **8** | **14** | **34** | **93** |

Fuente: Elaboración Propia

- Variables cualitativas ordinales (Variable 2): Aplicadas en la evaluación del nivel de madurez de los controles de seguridad, de acuerdo con la escala del modelo CMMI, que establece un orden progresivo en el desarrollo de proceso aplicando la herramienta MASS.

**Tabla 19. Variables Analizadas de la Herramienta MASS**

| Dimensión | Descripción |
|---|---|
| ISMS | Gestión de accesos, políticas de personal, capacitación en seguridad |
| CON | Administración de red, hardware, nube y teletrabajo |
| ORP | Gestión de accesos, políticas de personal, capacitación en seguridad |
| OPS | Administración de red, hardware, nube y teletrabajo |
| DER | Forense digital, preparación ante emergencias, ejercicios de prueba |
| NET | Configuración, segmentación, monitoreo de red |
| INF | Infraestructura física, Edificios, cableado, puestos móviles |
| APP | Software en suscripciones, logs, actualizaciones automáticas |
| SYS | Servidores, laptops, medios extraíbles, virtualización |

Fuente: Elaboración Propia

- Variables ordinales (Variable 3): Utilizadas para realizar la encuesta a los Jefes de Agencias, basados en el nivel de conocer el comportamiento concientización que tienen los usuarios y las capacidades de la Microfinanciera Prisma en identificar, detectar, proteger, responder y recuperar ante un incidente de ciberseguridad que afecte la

operatividad de la organización.

**Tabla 20. Variables analizadas del Diagnóstico Global de Seguridad**

| Nivel de Madurez | ISO 27032 | Controles Organizativos | Controles Personas | Controles Físicos | Controles Tecnológicos |
|---|---|---|---|---|---|
| Concienciación y formación | IDENTIFICAR | | x | | |
| Protección y buenas prácticas en temas de seguridad de la información | PROTEGER | | | | x |
| Respuesta individual ante una vulnerabilidad o amenaza que pueda considerarse un riesgo de la operatividad de la Microfinanciera | DETECTAR | x | | | |
| Comunicación de riesgos y responsabilidades | RESPONDER | x | | | |
| Confianza en la preparación de la organización para poder mantener la continuidad de las operaciones de la organización | RECUPERAR | | | x | |

Fuente: Elaboración Propia

#### 4.1.1.3 CARACTERÍSTICAS BÁSICAS DE LOS DATOS – ESTADÍSTICA DESCRIPTIVA

El análisis de estadísticas descriptivas permite identificar características clave de los datos, como rangos, promedios y frecuencias, facilitando la comprensión de su distribución. En este caso, se utilizaron las librerías de Pandas de Python para procesar y evaluar todas las variables relevantes, lo que proporciona una visión estructurada de la información. Este enfoque permite a la organización optimizar la gestión de los controles de seguridad, focalizando sus esfuerzos en mejorar los niveles de madurez y fortaleciendo su postura en ciberseguridad.

A continuación, se presenta un análisis cuantitativo basado en los datos de la Tabla 17, aplicando técnicas estadísticas descriptivas para medir los siguientes elementos clave:

- Distribución de frecuencias: Evaluación del nivel de madurez en cada dominio de control.
- Medidas de tendencia central: Cálculo de la media para identificar el valor representativo de cada conjunto de datos.
- Medidas de variabilidad: Análisis del rango, desviación estándar y varianza,

proporcionando información sobre la dispersión y consistencia de los datos.

A través del entorno de desarrollo Jupyter Notebook, se extrajeron las características estadísticas de los datos por dominio importando los datos desde un archivo CSV, mediante la biblioteca Pandas, numpy, matplotlib y scipy, realizando el cálculo.

**Tabla 21. Variables Cuantitativas (Medición de Impacto y Cumplimiento)**

| Valores Estadísticos | Controles Organizativos | Controles Tecnológicos | Controles Físicos | Controles Personas |
|---|---|---|---|---|
| Valor mínimo | 6.17 | 5.50 | 2.33 | 1.33 |
| Primer Cuartil | 5.31 | 5.61 | 3.20 | 1.21 |
| Máximo Valor | 13.00 | 15.00 | 8.00 | 3.00 |
| Mediana | 7.00 | 4.00 | 1.00 | 1.50 |
| Primer Cuartil | 1.50 | 1.75 | 0.00 | 0.25 |
| Tercer Cuartil | 9.50 | 7.75 | 3.50 | 2.00 |
| Desviación Estándar | 5.31 | 5.61 | 3.20 | 1.21 |
| Q1 | 1.50 | 1.75 | 0.00 | 0.25 |
| Q2 | 7.00 | 4.00 | 1.00 | 1.50 |
| Q3 | 9.50 | 7.75 | 3.50 | 2.00 |
| Varianza | 28.17 | 31.50 | 10.27 | 1.47 |

Fuente: Elaboración Propia

Se realizó un análisis de frecuencias para identificar y priorizar los riesgos asociados a la gestión de los controles de seguridad, siguiendo las directrices de ISO/IEC 27002. Los resultados se presentan clasificados por nivel de madurez, permitiendo una evaluación estructurada de cada categoría dentro de los dominios analizados.

**Tabla 22. Frecuencia por grado de madurez**

| Grado de Madurez | Frecuencia |
|---|---|
| Inexistente | 8 |
| Inicial | 19 |
| Gestionado | 19 |
| Definido | 26 |

| Grado de Madurez | Frecuencia |
|---|---|
| Cuantitativo | 17 |
| Optimizado | 3 |

Fuente: Elaboración Propia

El análisis de frecuencia permite estimar que la mayoría de los controles evaluados se encuentran en un nivel de implementación Intermedio. Sin embargo, los resultados también evidencian la presencia de áreas críticas dentro de la microfinanciera que requieren mejoras sustanciales para alcanzar niveles óptimos de madurez en seguridad de la información.

La presencia de controles en niveles de madurez bajos (Inexistente, con 8 controles, e Inicial, con 19 controles) correspondientes al 29% de los controles evaluados, evidencia brechas significativas que incrementan la exposición de la microfinanciera a riesgos y vulnerabilidades críticas. Estos resultados subrayan la necesidad de intervenciones estratégicas, enfocadas en la implementación de metodologías sistemáticas para la evaluación cuantitativa de la eficacia de los controles, así como en el desarrollo de mecanismos robustos de mejora continua, que permitan elevar el nivel de madurez en la gestión de la seguridad de la información.

### 4.1.2 LIMPIEZA Y PREPARACIÓN DE LOS DATOS

Para garantizar la calidad y fiabilidad del conjunto de datos utilizado en esta investigación, se llevó a cabo un proceso exhaustivo de limpieza y preparación de datos, por lo que aplicando la librería de panda, me realizó una separación por conjunto de datos según su tipo.

DataFrame limpio:

| | Tema | Métrica | Valor |
|---|---|---|---|
| 0 | Controles Organizativos | 5.1 - Políticas de SI | 5.0 |
| 1 | Controles Organizativos | 5.2 - Roles y responsabilidades de la SI | 0.0 |
| 2 | Controles Organizativos | 5.3 - Segregación de tareas | 5.0 |
| 3 | Controles Organizativos | 5.4 - Responsabilidades de la dirección | 5.0 |
| 4 | Controles Organizativos | 5.5 - Contacto con autoridades | 5.0 |
| ... | ... | ... | ... |
| 85 | Controles Tecnologicos | 8.27 - Principios de ingeniería y arquitectura... | 60.0 |
| 86 | Controles Tecnologicos | 8.28 - Codificación segura | 5.0 |
| 87 | Controles Tecnologicos | 8.29 - Pruebas de seguridad y aceptación en de... | 60.0 |
| 88 | Controles Tecnologicos | 8.30 - Desarrollo subcontratado | 15.0 |
| 89 | Controles Tecnologicos | 8.31 - Separación de entornos de desarrollo, p... | 100.0 |

**Figura 14. Limpieza y preparación de los datos**

Fuente: Elaboración Propia

#### 4.1.2.1 DETECCIÓN Y MANEJO DE VALORES FALTANTES

Para identificar la presencia de valores faltantes en el conjunto de datos, se utilizó Python y la función **isnull().sum(),** que permitió calcular el número de datos ausentes en cada variable, obteniendo los siguientes resultados:

- Se identificaron valores faltantes en variables que representan controles inexistentes. Como parte del análisis, se verificó que en estos casos no era necesario imputar valores, ya que los datos en blanco poseen un significado específico dentro del contexto del estudio y reflejan la ausencia de ciertos controles.
- Se detectó un valor faltante en la variable "Valor", correspondiente a un control clasificado como "No Aplica". Esto indica que la ausencia de datos es intencional, dado que dicho control no está alineado con la estructura organizacional. Esta metodología es coherente con el enfoque del diagnóstico donde ciertos controles pueden no ser aplicables dependiendo del contexto evaluado.

```python
# Crear el DataFrame a partir de la lista
df = pd.DataFrame(data, columns=["Tema", "Métrica", "Valor"])

# Limpiar la columna "Valor": eliminar el símbolo de porcentaje y reemplazar "N/A" por NaN
df["Valor"] = df["Valor"].str.replace("%", "").replace("N/A", np.nan)
df["Valor"] = pd.to_numeric(df["Valor"], errors="coerce")

# Detección de valores faltantes en cada columna
missing_counts = df.isnull().sum()
print("Conteo de valores faltantes en cada columna:")
print(missing_counts)

# Eliminamos filas con valores nulos
df_clean = df.dropna()

# Mostrar el DataFrame limpio
print("\nDataFrame limpio:")
display(df_clean)
```

```
Conteo de valores faltantes en cada columna:
Tema       0
Métrica    0
Valor      1
dtype: int64
```

**Figura 15. Valores Faltantes**

Fuente: Elaboración Propia

#### 4.1.2.2 IDENTIFICACIÓN Y TRATAMIENTO DE VALORES ATÍPICOS (OUTLIERS)

Durante el proceso de validación y limpieza de datos, se llevó a cabo un análisis para detectar valores atípicos (outliers) que pudieran afectar la interpretación de los resultados. La presencia de valores extremos puede distorsionar la evaluación de los niveles de madurez en seguridad de la información, por lo que es fundamental su identificación y tratamiento.

En este análisis, no se encontraron valores atípicos en el conjunto de datos, lo que confirma la consistencia y homogeneidad de la información recopilada. Esto garantiza que los resultados obtenidos reflejan fielmente la realidad de la organización, sin la necesidad de ajustes adicionales para la corrección o eliminación de datos anómalos.

#### 4.1.2.3 NORMALIZACIÓN O ESTANDARIZACIÓN DE LOS DATOS

En vista de que los valores numéricos dentro del conjunto de datos no presentan escalas dispares ni valores atípicos significativos, no se consideró necesario aplicar técnicas de normalización o estandarización. Esto garantiza que los datos se analicen en su forma original, preservando la estructura real de las mediciones y evitando posibles distorsiones en el análisis

posterior.

Con estos pasos completados, el conjunto de datos se encuentra en óptimas condiciones para continuar con el análisis exploratorio y la evaluación de los controles de seguridad de la información en la Microfinanciera PRISMA.

### 4.1.3 VISUALIZACIÓN DE DATOS

Para complementar el análisis exploratorio, se realizó una visualización de los datos con el objetivo de identificar tendencias, patrones y relaciones clave dentro del conjunto de controles de seguridad evaluados en la Microfinanciera PRISMA.

La representación gráfica de la información permite una mejor comprensión de la distribución de los controles, su clasificación en los distintos capítulos de seguridad, así como su nivel de madurez. Mediante gráficos exploratorios como histogramas, diagramas de caja y bigote, gráficos de dispersión y gráficos de barras, se lograron extraer hallazgos relevantes que enriquecen el estudio.

#### 4.1.3.1 USO DE GRÁFICOS EXPLORATORIOS

A continuación, se interpretan los datos obtenidos por cada uno de los controles de dominio:

a) Controles Organizativos

El histograma de los controles organizativos nos presenta la distribución de las frecuencias de los diferentes niveles de gestión de cada uno de los controles evaluados:

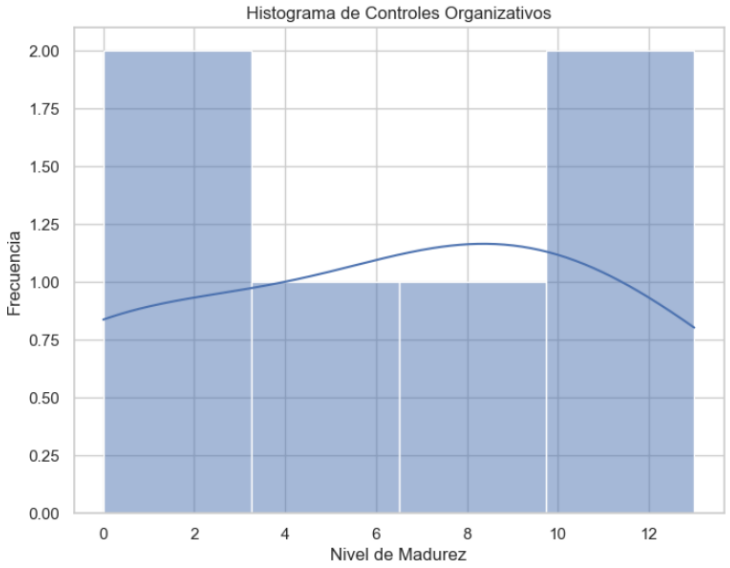


**Figura 16. Histograma - Controles Organizativos**

Fuente: Elaboración Propia

Los resultados obtenidos, representan que la mayoría de los controles organizativos se encuentran en los niveles de gestión inicial, y como se puede observar los valores de las categorías inferiores, indican que hay procesos que existen, pero en los que no se ha podido alcanzar los niveles de desarrollo y de estandarización para reducir los riesgos de este dominio.

Para la obtención de los datos cabe destacar la interpretación de cada variable de la investigación por lo que se interpretarán los valores de la tendencia central y el conjunto de datos de los resultados de la evaluación del dominio organizativo.

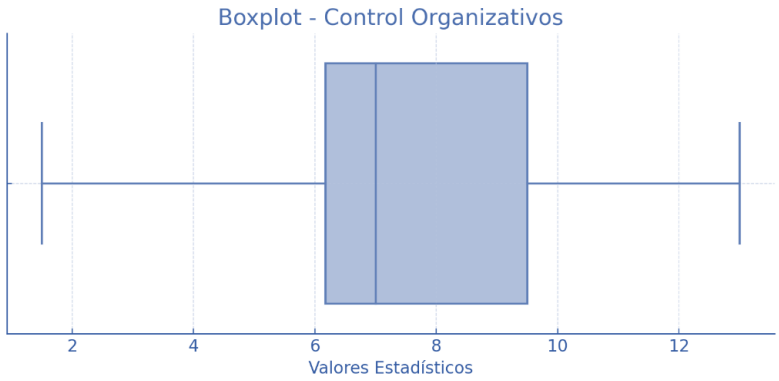


**Figura 17. Caja y Bigote - Controles Organizativos**

Fuente: Elaboración Propia

En los hallazgos estadísticos se puede identificar una alta dispersión, indicando en este dominio unas inconsistencias de gestión en implementación de controles en las diferentes áreas, pero hay otros elementos que son los que podemos destacar.

- Se identificó la media en alrededor de entre los valores 7 y 8, que se pueden identificar como los controles gestionados.
- Los valores identificados entre los valores de rango mínimo y rango máximo, nos indica que existen varios controles con una implementación muy básica y no se han gestionado de la forma adecuada.
- Se identifica que a nivel cuantitativo y optimizado no se encuentran en la escala por lo que es importante comprender que se requiere mejorar la implementación de los controles.

b) Controles Tecnológicos

A continuación, se presenta el análisis de los datos obtenidos de la evaluación de las 34 preguntas del dominio de Controles Tecnológicos. La curva nos representa la tendencia general facilitando la interpretación de la distribución de los datos.

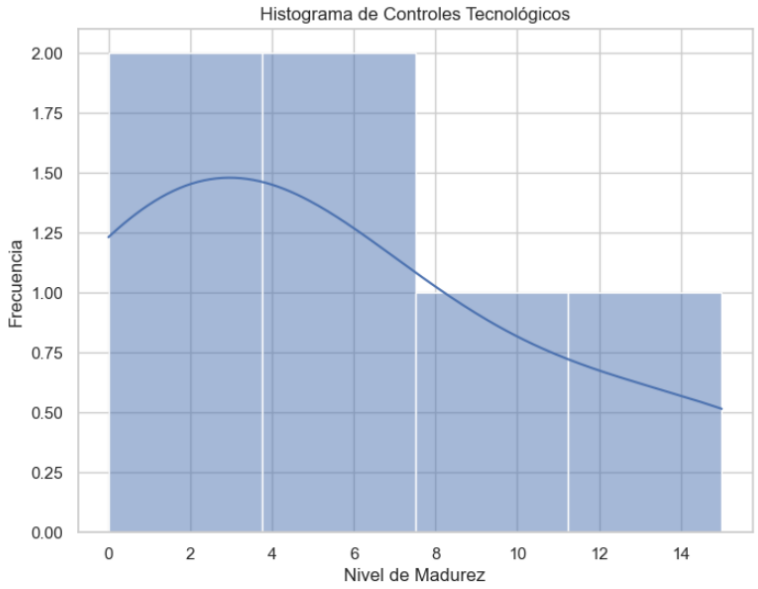


**Figura 18. Histograma - Controles Tecnológicos**

Fuente: Elaboración Propia

En los hallazgos se puede identificar que existe una frecuencia alta en la que la mayoría de los controles tecnológicos están gestionados entre las fases iniciales y definidas del nivel de madurez, por lo que establece que la Microfinanciera PRISMA debe enfocarse para realizar en la mejora de la gestión de esos controles.

En los niveles de tendencia entre los rangos medios se identifica que la falta de planificación, o de un área de seguridad de la información permitan mejorar o robustecer de forma progresiva a niveles de madurez optimizados.

La coexistencia del sector mayoritario en los niveles bajos y el subconjunto de niveles altos evidencia una varianza significativa, lo que representa diferencias en cuanto a los recursos disponibles que pueda tener la Microfinanciera PRISMA, asimismo como una cultura organizacional alineada a la estrategia de seguridad de la información.

Para el siguiente elemento se procedió a representar un gráfico del resumen estadístico e identificar los valores percentiles y valores atípicos, así como la tendencia central de los datos evaluados:

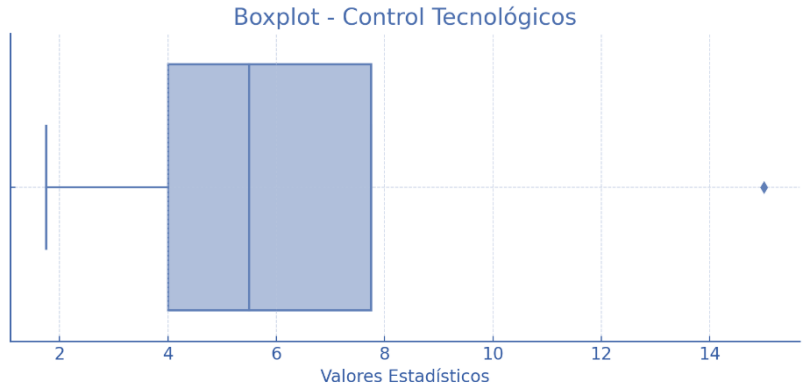


**Figura 19. Caja y Bigote - Controles Tecnológicos**

Fuente: Elaboración Propia

Como se observa la mayor parte se concentra entre 4 y 8 con una mediana cercana a 6, lo que confirma que la mayoría de los controles se encuentra en un rango medio de los niveles de madurez en este dominio, Se puede observar un valor atípico alrededor de 14, lo que indica que solamente un control se encuentra en un nivel de madurez optimizado en comparación al resto.

El límite inferior con el valor 2 representa que estos controles necesitan un mayor nivel de

atención considerando que se encuentra en la etapa inicial y que se deben definir planes de acción para la mejora de estos.

c) Controles de Personas

Para garantizar que el factor humano dentro de la organización contribuya a la protección de la información y gestión de los riesgos de ciberseguridad.

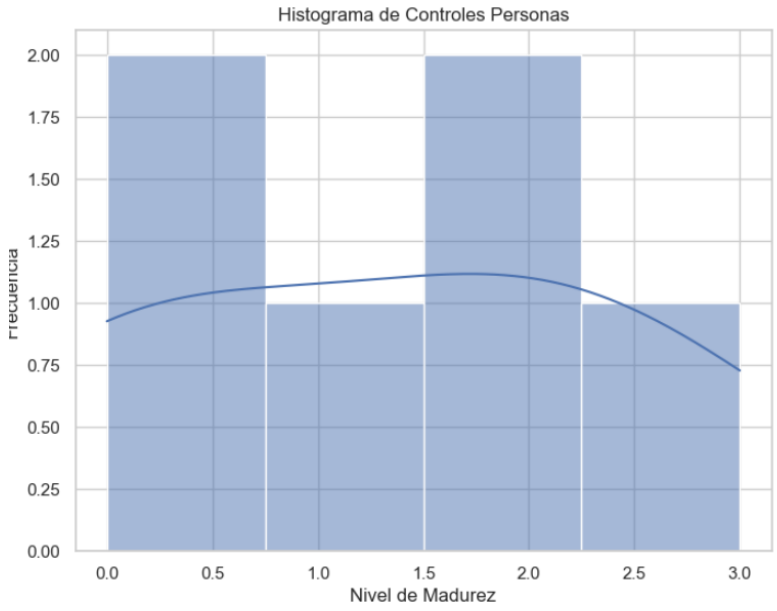


**Figura 20. Histograma - Controles de Personas**

Fuente: Elaboración Propia

Los hallazgos que se identificaron de forma estadística, se revela una distribución multimodal, con los picos en niveles muy básicos de madurez y un segmento intermedio.

A simple vista, el Histograma de Controles de Personas muestra que la mayoría de los controles se concentran entre los niveles 0.0 y 1.5 de madurez, con una menor presencia en los niveles más altos (por encima de 2.5). Esto sugiere que, si bien algunos controles relacionados con el factor humano alcanzan un estadio inicial o parcialmente gestionado, todavía hay pocos controles ubicados en etapas más avanzadas o cercanas a la definición y optimización.

En términos prácticos, esta distribución indica la necesidad de reforzar las políticas de concienciación y capacitación, así como de documentar formalmente los procesos relativos al personal (por ejemplo, gestión de accesos, procedimientos disciplinarios, definición clara de roles

y responsabilidades). Al avanzar estos controles hacia niveles de madurez más altos, se reducirán las brechas que podrían exponer a la microfinanciera a riesgos derivados de errores humanos o procesos de seguridad incompletos.

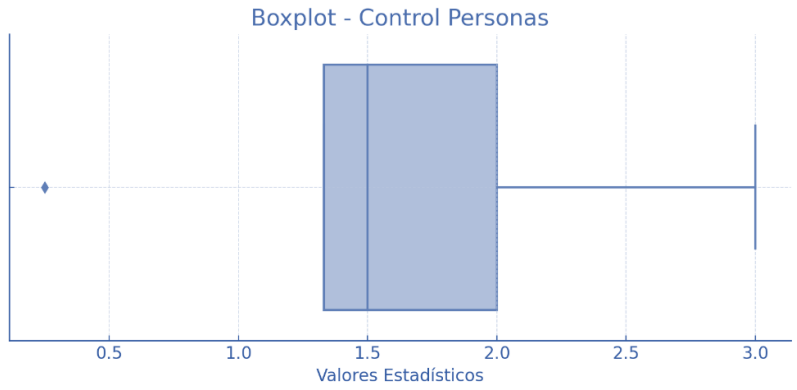


**Figura 21. Caja y Bigote - Controles de Personas**

Fuente: Elaboración Propia

El boxplot de Controles de Personas evidencia que la mediana de los valores se sitúa alrededor de 1.5, señalando un nivel de madurez mayormente inicial o parcialmente gestionado para la mayoría de los controles del dominio. El rango intercuartílico (IQR) se extiende aproximadamente de 1.2 a 1.9, lo que confirma cierta consistencia en esa franja intermedia de madurez; sin embargo, se observa un valor atípico cercano a 0, indicando la ausencia o nula formalización de, al menos, un control esencial.

Adicionalmente, se aprecia un extremo que alcanza el nivel 3.0, lo que sugiere que algunos controles presentan un grado de madurez más avanzado o definido/optimizado. Esta disparidad refleja la heterogeneidad en la gestión de la seguridad del factor humano: mientras la mayoría de los controles muestran un grado mínimo de implementación, se encuentran casos extremos tanto de baja como de alta madurez. Como consecuencia, se recomienda establecer políticas y procedimientos consistentes para los controles con menor madurez, a la vez que se consolidan las buenas prácticas en aquellos con mayor nivel, con el fin de unificar e incrementar el nivel de madurez de toda la dimensión “Personas”.

d) Controles Físicos

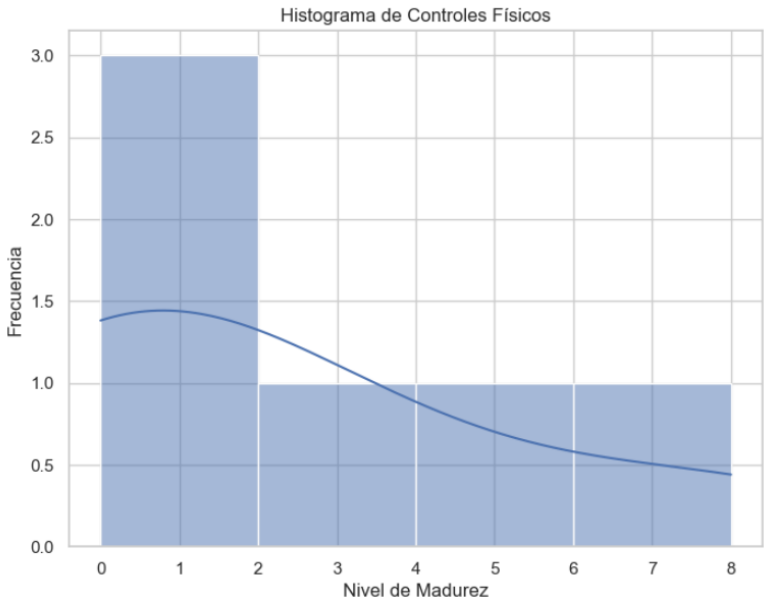


**Figura 22. Histograma - Controles Físicos**

Fuente: Elaboración Propia

A partir de este Histograma de Controles Físicos, se observa que la mayor concentración de valores se sitúa entre los niveles de madurez 0 y 2, señalando que la mayoría de estos controles permanece en estadios iniciales o parciales de implementación. La frecuencia decrece progresivamente hacia los niveles superiores, lo que indica que pocos controles físicos alcanzan una madurez avanzada.

En la práctica, esto sugiere que, si bien se han establecido ciertas medidas básicas (por ejemplo, protecciones perimetrales o controles de acceso), la formalización y el monitoreo continuo de estos controles todavía no están plenamente consolidados. Algunas áreas podrían contar con políticas de seguridad definidas, mientras que otras podrían requerir refuerzos adicionales, como el monitoreo de instalaciones, la protección de equipos sensibles o la aplicación de protocolos específicos frente a amenazas físicas y ambientales.

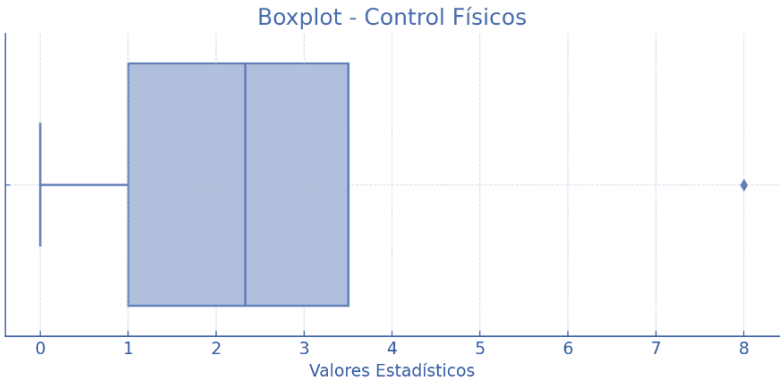


**Figura 23. Caja y Bigote - Controles Físicos**

Fuente: Elaboración Propia

En este boxplot de Controles Físicos, se observa que la mayoría de los valores se concentran entre 1 y 3, reflejando un nivel de madurez bajo a intermedio para la mayoría de los controles de seguridad física. La mediana, situada cerca de 2, indica que la mayor parte de estos controles cuenta con cierto grado de implementación, aunque no llega a un estándar avanzado ni plenamente optimizado.

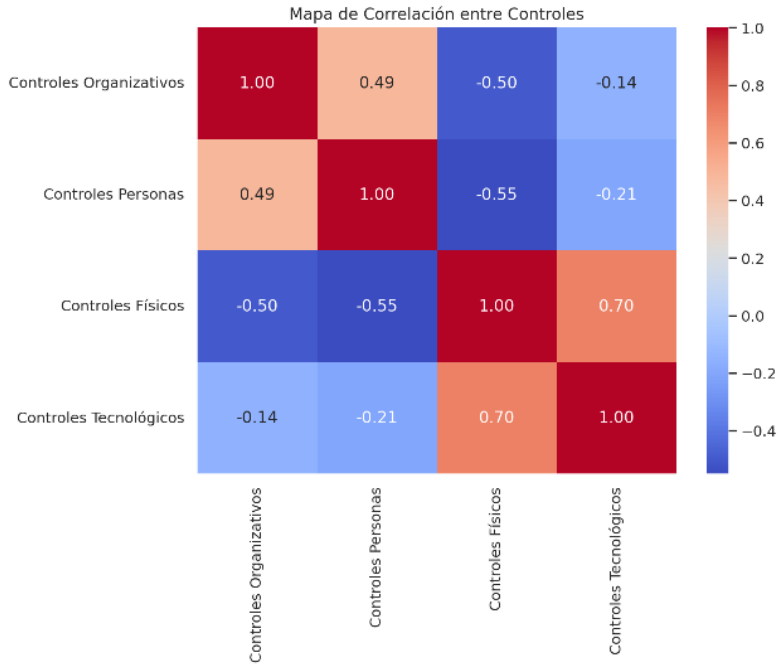


**Figura 24. Mapa de Correlación entre Controles**

Fuente: Elaboración Propia

Este mapa de correlación muestra la relación entre los niveles de madurez de los controles organizativos, de personas, físicos y tecnológicos:

Correlaciones positivas: Entre Controles Organizativos y Controles de Personas (0.49): Sugiere que, a medida que mejoran las políticas y procedimientos organizativos (definición de roles, responsabilidades, capacitaciones), también aumenta la madurez relacionada con el factor humano, reflejando cierto sincronismo entre la gestión corporativa y el desarrollo del personal.

Entre Controles Físicos y Controles Tecnológicos (0.70): Indica una fuerte asociación: al implementarse medidas de seguridad física más robustas (protección de equipos, perímetros, instalaciones), se observan avances en la adopción de soluciones tecnológicas (monitoreo, cifrado, sistemas de detección) o viceversa.

Correlaciones negativas: Controles Organizativos y Controles Físicos (-0.50): Un avance en la formalización de políticas y procedimientos organizativos no necesariamente se traduce en mejoras en seguridad física, o podría indicar que la atención y recursos se focalizan en lo organizativo, dejando en segundo plano los controles de infraestructura.

Controles de Personas y Controles Físicos (-0.55): Del mismo modo, un mayor enfoque en capacitación y concienciación del personal parece no estar directamente asociado a mejoras en el ámbito físico, lo que revela desconexión o falta de integración entre la formación de los colaboradores y la seguridad de las instalaciones.

Controles de Personas y Controles Tecnológicos (-0.21): La gestión del factor humano podría no estar alineada con la adopción de medidas tecnológicas, lo que sugiere la necesidad de coordinar la formación y las políticas de uso con el despliegue de soluciones técnicas.

En conjunto, este mapa de correlación evidencia que fortalecer la seguridad física a menudo se acompaña de avances en los controles tecnológicos, mientras que las iniciativas organizativas y de personas guardan cierta sintonía mutua pero no siempre se traducen en mejoras tangibles en lo físico-tecnológico. Para incrementar la eficacia global, se recomienda integrar las estrategias de cada dominio, asegurando que la protección física y la adopción de herramientas tecnológicas vayan de la mano con políticas organizativas y una cultura de seguridad sólida en el factor humano.

## 4.2 RESULTADOS DEL DIAGNOSTICO GLOBAL DE LA MATRIZ DE EVALUACION DE SEGURIDAD ISO/IEC 27002:2022

El presente análisis se fundamenta en la evaluación del nivel de cumplimiento de los controles de seguridad en la Microfinanciera PRISMA, con el objetivo de determinar su madurez en seguridad de la información.

### 4.2.1 PRESENTACIÓN DE DATOS

Para garantizar un análisis estructurado y preciso, esta sección presenta los datos obtenidos en la evaluación de los controles de seguridad en la Microfinanciera PRISMA, alineados con la norma ISO/IEC 27002:2022. La organización y visualización de estos datos permiten una interpretación clara del nivel de madurez en seguridad de la información, facilitando la identificación de fortalezas y brechas en la gestión de los controles implementados.

La presentación de datos se realiza mediante tablas y gráficos estadísticos, los cuales reflejan la distribución de los niveles de madurez por dominio de control. Este enfoque proporciona una base sólida para el análisis cuantitativo y cualitativo, asegurando una evaluación objetiva que respalde la toma de decisiones estratégicas en ciberseguridad y gestión de riesgos.

#### 4.2.1.1 EVALUACIÓN DEL DOMINIO DE LOS CONTROLES ORGANIZATIVOS

La norma ISO/IEC 27002:2022 establece un marco de referencia para la implementación y gestión de controles de seguridad de la información, proporcionando directrices para fortalecer un Sistema de Gestión de Seguridad de la Información (SGSI). En este análisis, se evaluó el cumplimiento de los controles organizativos, permitiendo identificar fortalezas, brechas y oportunidades de mejora dentro de la Microfinanciera PRISMA.

El dominio de Controles Organizativos abarca aspectos clave relacionados con la gobernanza de la seguridad de la información, incluyendo la definición de políticas, gestión de riesgos, asignación de responsabilidades y cumplimiento normativo. La evaluación realizada permitió clasificar los controles en diferentes niveles de madurez, reflejando el grado de implementación dentro de la organización.

En esta fase del estudio, se analizaron un total de 37 controles organizativos, evaluando su

nivel de cumplimiento en los ámbitos estratégico, táctico y de supervisión. Los resultados obtenidos proporcionan una visión clara del grado de madurez en la gestión de seguridad organizativa, facilitando la toma de decisiones para fortalecer la postura de seguridad de la información en PRISMA.

**Tabla 23. Nivel de Madurez Dominio Controles Organizativos**

| Descripción de Controles | Controles No Gestionados (Inexistentes) | Controles Iniciales | Controles Gestionados | Controles Definidos |
|---|---|---|---|---|
| 5.2 - Roles y responsabilidades de la SI | 0% | | | |
| 5.7 - Inteligencia de amenazas | | | | |
| 5.8 - SI en la gestión de proyectos | | | | |
| 5.12 - Clasificación de la información | | | | |
| 5.13 - Etiquetado de información | | | | |
| 5.14 - Transferencia de información | | | | |
| 5.23 - SI para el uso de servicios en la nube | | | | |
| 5.33 - Protección de registros | | | | |
| | | | | |
| 5.3 - Segregación de tareas | | 5% | | |
| 5.4 - Responsabilidades de la dirección | | | | |
| 5.5 - Contacto con autoridades | | | | |
| 5.6 - Contacto con grupos de interés especial | | | | |
| 5.15 - Control de acceso | | | | |
| 5.16 - Gestión de identidad | | | | |
| 5.17 - Información de autenticación | | | | |
| 5.18 - Derechos de acceso | | | | |
| 5.24 - Planificación y preparación para la gestión de incidentes de SI | | | | |
| 5.32 - Derechos de propiedad intelectual | | | | |
| 5.34 - Privacidad y protección de la información de identificación personal (PII) | | | | |
| 5.35 - Revisión independiente de SI | | | | |
| | | | | |
| 5.1 - Políticas de SI | | | 15% | |
| 5.9 - Inventario de información y activos asociados | | | | |
| 5.10 - Uso de la información y activos asociados | | | | |
| 5.11 - Devolución de activos | | | | |
| 5.26 - Respuesta a incidentes de SI | | | | |
| 5.27 - Aprendizaje de los incidentes de SI | | | | |
| 5.28 - Recolección de evidencia | | | | |
| 5.29 - SI durante una disrupción | | | | |

| Descripción de Controles | Controles No Gestionados (Inexistentes) | Controles Iniciales | Controles Gestionados | Controles Definidos |
|---|---|---|---|---|
| 5.31 - Identificación de requisitos legales, estatutarios, reglamentarios y contractuales | | | | |
| 5.36 - Cumplimiento de políticas y estándares de SI | | | | |
| 5.37 - Procedimientos operativos documentados | | | | |
| | | | | |
| 5.19 - SI en las relaciones con los proveedores | | | | |
| 5.20 - Abordar la SI en acuerdos con proveedores | | | | |
| 5.21 - Gestión de la SI en la cadena de suministro de las TIC | | | | |
| 5.22 - Seguimiento, revisión y gestión de cambios de servicios de proveedores | | | | **60%** |
| 5.25 - Evaluación y decisión sobre eventos de SI | | | | |
| 5.30 - Preparación de las TIC para la continuidad de negocio | | | | |

Fuente: Elaboración Propia

Los controles evaluados representan los siguientes hallazgos:

**Tabla 24. Hallazgos Dominio Controles Organizativos**

| Nivel de Madurez | Grado | Valor | Descripción | Total Controles |
|---|---|---|---|---|
| **0 - Inexistente** | **0** | **0%** | Varios controles críticos se encuentran en un nivel de No Gestionado o Inexistente, lo que indica una falta de formalización y supervisión en aspectos clave de la gobernanza de la seguridad de la información. Entre las principales deficiencias identificadas se encuentran la ausencia de políticas documentadas, debilidades en la gestión de riesgos, falta de asignación clara de responsabilidades y deficiencias en el cumplimiento normativo. | **8** |
| **1 – Inicial** | **1** | **5%** | Varios controles se encuentran en un nivel Inicial, indicando que, aunque existen, carecen de formalización y monitoreo efectivo. Entre ellos destacan la segregación de tareas, responsabilidades de la dirección, gestión de identidad, control de acceso y preparación para incidentes de seguridad, lo que refleja brechas en la administración de privilegios, cumplimiento normativo y gestión de riesgos. Además, la protección de información personal y la revisión independiente de seguridad requieren fortalecimiento. | **12** |

| Nivel de Madurez | Grado | Valor | Descripción | Total Controles |
|---|---|---|---|---|
| **2 – Gestionado** | **2** | **15%** | Varios controles se encuentran en un nivel Gestionado, lo que indica que han sido implementados de manera estructurada y cuentan con supervisión, aunque aún pueden optimizarse. Entre ellos destacan las políticas de seguridad de la información, inventario y uso de activos, respuesta a incidentes y cumplimiento normativo, reflejando un marco sólido de gobernanza. Asimismo, la recolección de evidencia, continuidad de la seguridad durante disrupciones y cumplimiento de estándares demuestran una gestión efectiva. | **11** |
| **3 – Definido** | **3** | **60%** | Varios controles se encuentran en un nivel Definido, lo que significa que están formalmente documentados y estandarizados dentro de la organización. Destacan la gestión de seguridad en relaciones con proveedores, acuerdos y cadena de suministro TIC, asegurando un enfoque estructurado en la gestión de terceros. Además, la gestión de cambios en servicios de proveedores, evaluación de eventos de seguridad y preparación de TIC para la continuidad del negocio reflejan un alto grado de alineación con las mejores prácticas. | **6** |

Fuente: Elaboración Propia

#### 4.2.1.2 EVALUACIÓN DEL DOMINIO DE LOS CONTROLES DE PERSONAS

El dominio de Controles de Personas en la ISO/IEC 27002:2022 abarca las medidas necesarias para garantizar que el factor humano dentro de la organización contribuya a la protección de la información y la gestión de riesgos de ciberseguridad. Este dominio evalúa la concienciación, capacitación, asignación de responsabilidades y control de acceso del personal, asegurando que las políticas y procedimientos sean comprendidos y aplicados en todos los niveles organizacionales.

A continuación, se presentan los resultados de la evaluación en este dominio, clasificando los controles según su nivel de madurez y analizando las fortalezas, brechas y oportunidades de mejora en la gestión de la seguridad de la información a nivel humano:

**Tabla 25. Nivel de Madurez Dominio Controles de Personas**

| Descripción de Controles | Controles Iniciales | Controles Gestionados | Controles Definidos | Controles Optimizados |
|---|---|---|---|---|
| 6.4 - Proceso disciplinario | 5% | | | |
| 6.5 - Responsabilidades tras la desvinculación o cambio de empleo | | | | |
| 6.7 - Trabajo remoto | | | | |
| | | | | |

| Descripción de Controles | Controles Iniciales | Controles Gestionados | Controles Definidos | Controles Optimizados |
|---|---|---|---|---|
| 6.8 - Reporte de eventos de SI | | 15% | | |
| 6.1 - Verificación de antecedentes (screening) | | | | |
| | | | | |
| 6.3 - Concientización, educación y entrenamiento en SI | | | 60% | |
| | | | | |
| 6.2 - Términos y condiciones de empleo | | | | 100% |
| 6.6 - Acuerdos de confidencialidad o no divulgación | | | | |

Fuente: Elaboración Propia

Los controles evaluados representan los siguientes hallazgos:

**Tabla 26. Hallazgos Dominio Controles de Personas**

| Nivel de Madurez | Grado | Valor | Descripción | Total Controles |
|---|---|---|---|---|
| **1 – Inicial** | **1** | **5%** | Los controles relacionados con la gestión disciplinaria, responsabilidades tras la desvinculación o cambio de empleo, y trabajo remoto se encuentran en un nivel Inicial. Esto indica que, si bien existen lineamientos en estas áreas, aún carecen de formalización, monitoreo y aplicación consistente. | **3** |
| **2 – Gestionado** | **2** | **15%** | Los controles de reporte de eventos de seguridad de la información y verificación de antecedentes del personal se encuentran en un nivel Gestionado. Esto significa que han sido implementados de manera estructurada y cuentan con procedimientos establecidos, aunque aún pueden optimizarse. | **2** |
| **3 – Definido** | **3** | **60%** | El control sobre concientización, educación y entrenamiento en seguridad de la información se encuentra en un nivel Definido, lo que indica que la organización ha establecido un programa formal de capacitación en ciberseguridad, con lineamientos documentados y aplicados de manera estructurada. | **1** |
| **5 – Optimizado** | **5** | **100%** | El control sobre acuerdos de confidencialidad o no divulgación se encuentra en un nivel Optimizado, lo que indica que la organización no solo ha implementado estos acuerdos de manera formal y consistente, sino que también mantiene un proceso de mejora continua para su aplicación y cumplimiento. | **2** |

Fuente: Elaboración Propia

### 4.2.1.3 EVALUACIÓN DEL DOMINIO DE LOS CONTROLES FÍSICOS

El dominio de Controles Físicos en la ISO/IEC 27002:2022 abarca las medidas de seguridad diseñadas para proteger los activos de información contra accesos no autorizados, daños o interrupciones causadas por factores físicos o ambientales. Estos controles incluyen la gestión

de accesos a instalaciones, protección de equipos y prevención de riesgos relacionados con infraestructura crítica.

A continuación, se presentan los resultados de la evaluación en este dominio, clasificando los controles según su nivel de madurez, destacando fortalezas, brechas y oportunidades de mejora para fortalecer la seguridad física en la organización.

**Tabla 27. Nivel de Madurez Dominio Controles Físicos**

| Descripción de Controles | Controles Gestionados | Controles Definidos | Controles Cuantitativos |
|---|---|---|---|
| 7.7 - Escritorio despejado y pantalla limpia | **15%** | | |
| 7.9 - Seguridad de los activos fuera de las instalaciones | | | |
| 7.1 - Perímetro de seguridad física | | **60%** | |
| 7.4 - Monitoreo de seguridad física | | | |
| 7.10 - Medios de almacenamiento | | | |
| 7.11 - Instalaciones de soporte | | | |
| 7.2 - Ingresos físicos | | | **85%** |
| 7.3 - Asegurar oficinas, salas e instalaciones | | | |
| 7.5 - Protección contra amenazas físicas y ambientales | | | |
| 7.6 - Trabajo en áreas seguras | | | |
| 7.8 - Ubicación y protección de equipos | | | |
| 7.12 - Seguridad del cableado | | | |
| 7.13 - Mantenimiento de equipos | | | |
| 7.14 – Eliminación segura o reutilización de equipos | | | |

Fuente: Elaboración Propia

Los controles evaluados representan los siguientes hallazgos:

**Tabla 28. Hallazgos Dominio Controles Físicos**

| Nivel de Madurez | Grado | Valor | Descripción | Total Controles |
|---|---|---|---|---|
| **2 – Gestionado** | **2** | **15%** | Los controles sobre escritorio despejado y pantalla limpia y seguridad de los activos fuera de las instalaciones se encuentran en un nivel Gestionado, lo que significa que la organización ha establecido procedimientos formales para su cumplimiento y monitoreo. | **2** |
| **3 – Definido** | **3** | **60%** | Los controles perímetro de seguridad física, monitoreo de seguridad, gestión de medios de almacenamiento e instalaciones de soporte se encuentran en un nivel Definido, lo que refleja la existencia de políticas documentadas y procesos estructurados para su gestión. | **4** |

| Nivel de Madurez | Grado | Valor | Descripción | Total Controles |
|---|---|---|---|---|
| **4- Cuantitativo** | **5** | **100%** | Los controles ingresos físicos, aseguramiento de oficinas e instalaciones, protección contra amenazas físicas y ambientales, trabajo en áreas seguras, ubicación y protección de equipos, seguridad del cableado, mantenimiento de equipos y eliminación segura o reutilización de equipos se encuentran en un nivel Cuantitativo. Esto indica que la organización ha implementado mecanismos de medición y monitoreo para evaluar la efectividad de estos controles en tiempo real, permitiendo una gestión basada en métricas y datos verificables. | **8** |

Fuente: Elaboración Propia

#### 4.2.1.4 EVALUACIÓN DEL DOMINIO DE LOS CONTROLES TECNOLÓGICOS

El dominio de Controles Tecnológicos en la ISO/IEC 27002:2022 abarca la implementación de medidas de seguridad en sistemas, redes y aplicaciones para proteger la integridad, disponibilidad y confidencialidad de la información. Estos controles incluyen la gestión de accesos, protección contra amenazas, monitoreo de sistemas y aplicación de mecanismos criptográficos.

A continuación, se presentan los resultados de la evaluación en este dominio, organizados según su nivel de madurez, destacando fortalezas, brechas y oportunidades de mejora para fortalecer la seguridad tecnológica en la organización.

**Tabla 29. Nivel de Madurez Dominio Controles Tecnológicos**

| Descripción de Controles | Controles Iniciales | Controles Gestionados | Controles Definidos | Controles Cuantitativos | Controles Optimizados |
|---|---|---|---|---|---|
| 8.4 - Acceso al código fuente | **5%** | | | | |
| 8.5 - Autenticación segura | | | | | |
| 8.25 - Seguridad en el ciclo de vida de desarrollo | | | | | |
| 8.28 - Codificación segura | | | | | |
| | | | | | |
| 8.14 - Redundancia en instalaciones de procesamiento de información | | **15%** | | | |
| 8.15 - Registros (logs) | | | | | |
| 8.24 - Uso de criptografía | | | | | |
| 8.30 - Desarrollo subcontratado | | | | | |
| | | | | | |
| 8.7 - Protección contra malware | | | **60%** | | |
| 8.8 - Gestión de vulnerabilidades técnicas | | | | | |

| Descripción de Controles | Controles Iniciales | Controles Gestionados | Controles Definidos | Controles Cuantitativos | Controles Optimizados |
|---|---|---|---|---|---|
| 8.9 - Gestión de configuración | | | | | |
| 8.10 - Eliminación de información | | | | | |
| 8.11 - Enmascaramiento de datos | | | | | |
| 8.12 - Prevención de fuga de datos | | | | | |
| 8.13 - Copia de seguridad de la información | | | | | |
| 8.16 - Monitoreo de actividades | | | | | |
| 8.18 - Uso de programas utilitarios privilegiados | | | | | |
| 8.26 - Requisitos de seguridad de aplicaciones | | | | | |
| 8.27 - Principios de ingeniería y arquitectura de sistemas seguros | | | | | |
| 8.29 - Pruebas de seguridad y aceptación en desarrollo | | | | | |
| 8.32 - Gestión del cambio | | | | | |
| 8.33 - Protección de la información de las pruebas | | | | | |
| 8.34 - Protección de los sistemas de información durante las pruebas de auditoría | | | | | |
| | | | | | |
| 8.1 - Dispositivos de usuario (endpoint) | | | | | |
| 8.2 - Derechos de acceso privilegiado | | | | | |
| 8.3 - Restricción de acceso a la información | | | | | |
| 8.6 - Gestión de capacidad | | | | | |
| 8.19 - Instalación de software en sistemas operacionales | | | | **85%** | |
| 8.20 - Seguridad en redes | | | | | |
| 8.21 - Seguridad de los servicios de red | | | | | |
| 8.22 - Segregación en redes | | | | | |
| 8.23 - Filtrado web | | | | | |
| | | | | | |
| 8.31 - Separación de entornos de desarrollo, prueba y producción | | | | | **100%** |

Fuente: Elaboración Propia

Los controles evaluados representan los siguientes hallazgos:

**Tabla 30. Hallazgos Dominio Controles Tecnológicos**

| Nivel de Madurez | Grado | Valor | Descripción | Total Controles |
|---|---|---|---|---|
| **1 – Inicial** | **1** | **5%** | La gestión deficiente del acceso al código fuente representa un riesgo significativo de manipulación indebida o exposición no autorizada, mientras que la falta de autenticación segura incrementa la vulnerabilidad ante accesos no legítimos. Además, la seguridad en el ciclo de vida de desarrollo y la codificación segura requieren mejoras para mitigar riesgos en la creación y despliegue de software. | **4** |
| **2 – Gestionado** | **2** | **15%** | La existencia de infraestructura redundante mejora la resiliencia ante fallos, mientras que la gestión de logs permite un registro adecuado de eventos para auditoría y detección de incidentes. Asimismo, el uso de criptografía garantiza la protección de datos, aunque su efectividad depende de una correcta gestión de claves. En cuanto al desarrollo subcontratado, se han establecido procesos de control, pero requieren mayor supervisión para alinear la seguridad del software con los estándares internos. | **4** |
| **3 – Definido** | **3** | **60%** | La protección contra malware, gestión de vulnerabilidades, monitoreo de actividades y prevención de fuga de datos, refleja un enfoque estructurado en la detección y mitigación de amenazas cibernéticas. Asimismo, la copia de seguridad, eliminación de información y enmascaramiento de datos garantizan la integridad y confidencialidad de la información. En el ámbito del desarrollo seguro, se han formalizado los requisitos de seguridad en aplicaciones, pruebas de seguridad y gestión del cambio, alineando la seguridad con el ciclo de vida del software. | **15** |
| **4 - Cuantitativo** | **4** | **85%** | El control de dispositivos de usuario y acceso privilegiado minimiza el riesgo de compromisos internos, mientras que la seguridad y segregación de redes fortalece la protección contra accesos no autorizados y ataques externos. Además, la gestión de capacidad y control de instalación de software garantizan la estabilidad operativa y reducen vulnerabilidades en los sistemas. | **9** |
| **5 – Optimizado** | **5** | **100%** | Se mantiene una separación técnica y organizativa clara entre los diferentes entornos. Existen políticas formalizadas y procedimientos estandarizados para gestionar los accesos, cambios y despliegues en cada entorno. Se ha implementado una automatización de pruebas y despliegues que minimiza errores humanos. La organización realiza auditorías periódicas y controles preventivos para asegurar que no se comprometan los datos ni los sistemas en producción. Se aplican lecciones aprendidas y mejora continua para afinar este proceso en cada nuevo proyecto o iteración tecnológica. | **1** |

Fuente: Elaboración Propia

## 4.3 SÍNTESIS DE HALLAZGOS

La siguiente gráfica ilustra el nivel de cumplimiento de la Microfinanciera PRISMA en cuatro dominios de seguridad definidos por la norma ISO/IEC 27022:2022: Controles Físicos,

Controles Tecnológicos, Controles de Personas y Controles Organizativos. Este resumen permite identificar fortalezas y áreas de mejora en la protección de la información, sirviendo como base para priorizar acciones y reforzar la estrategia de seguridad de la institución.

La gráfica muestra los siguientes niveles de cumplimiento en cuatro dominios clave:

- Controles Físicos (67.86%): Es el porcentaje más elevado de la evaluación, cercano al 68%.

Incluye la protección de la infraestructura de PRISMA, como el control de acceso a oficinas y áreas de TI, la utilización de sistemas de videovigilancia, cerraduras especializadas y medidas preventivas contra intrusiones.

Un cumplimiento alto en este dominio refleja la prioridad que la Microfinanciera PRISMA otorga a la salvaguarda física de sus activos, reduciendo considerablemente los riesgos de pérdidas o daños intencionados.

- Controles Tecnológicos (55.91%)

Ocupan el segundo lugar con aproximadamente 56% de cumplimiento.

Este dominio comprende la adopción de soluciones tecnológicas de seguridad, tales como firewalls, antivirus, cifrado, sistemas de detección de intrusos y configuraciones seguras en servidores y dispositivos.

Aunque el porcentaje es aceptable, todavía existe margen de mejora para robustecer la infraestructura tecnológica, implementar actualizaciones oportunas y reforzar las políticas de seguridad en entornos digitales.

- Controles de Personas (38.13%)

Con alrededor del 38%, se ubican en el tercer lugar.

Abarcan las medidas enfocadas en la gestión del factor humano, como la capacitación continua, la asignación clara de roles y responsabilidades, la sensibilización en políticas de seguridad y la verificación de antecedentes laborales.

Este resultado indica que PRISMA necesita intensificar la formación y concientización de su personal, promoviendo una cultura de seguridad en todos los niveles de la organización.

- Controles Organizativos (15.54%)

Presentan el nivel más bajo de cumplimiento, cercano al 15.5%.

Implican la implementación de estrategias, políticas y procedimientos formales a nivel institucional, así como la definición de un modelo de gobernanza de la seguridad de la información.

Dado que estos controles sirven como base para que el resto de las medidas funcionen de forma sostenible y coordinada, su refuerzo resulta prioritario para Microfinanciera PRISMA.

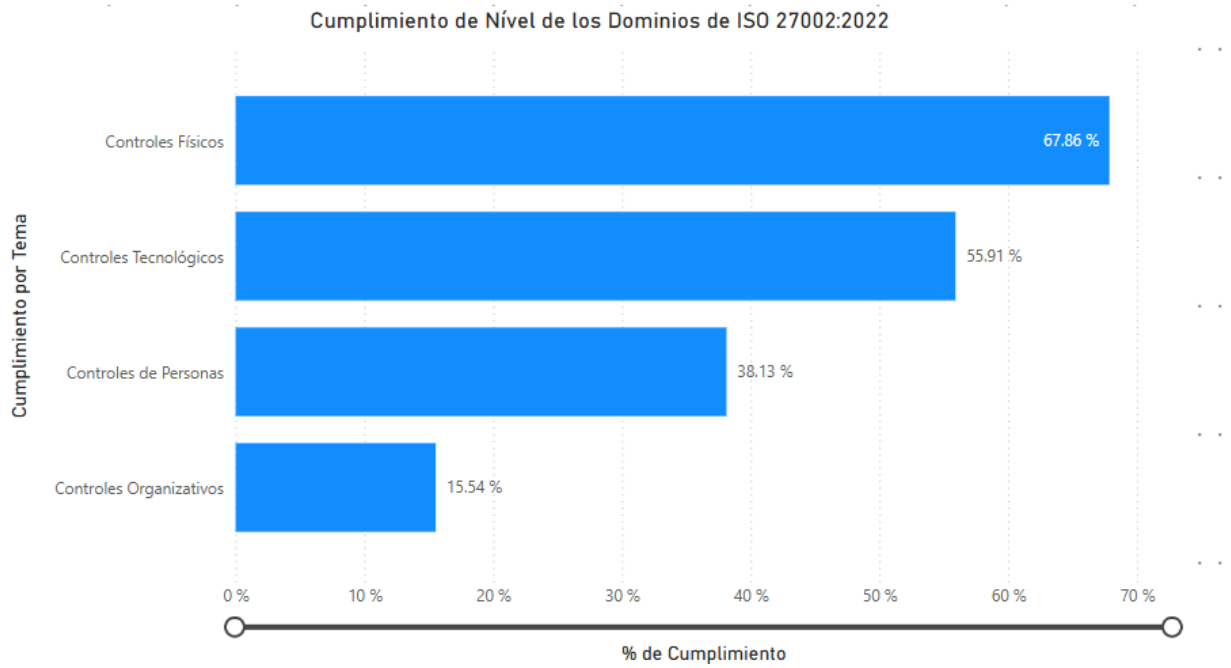


**Figura 25. Nivel de Madurez por Dominio**

Fuente: Elaboración Propia

La aplicación de esta metodología y el uso de MASS proporcionaron una visión estructurada sobre la capacidad de la organización en la gestión de la seguridad de la información. Los resultados permitieron ubicar a la organización en un nivel de madurez determinado, mostrando con claridad cuáles son sus fortalezas en seguridad y qué aspectos requieren atención. En particular, el análisis identificó áreas de mejora específicas – por ejemplo, políticas que necesitan actualización, controles que podrían fortalecerse o procesos que carecen de documentación – y ofreció oportunidades de optimización para elevar el nivel de seguridad.

Gracias a la evaluación, la organización cuenta ahora con un diagnóstico claro de su postura de seguridad. Este diagnóstico sirve como hoja de ruta para priorizar iniciativas de mejora, ya sea

mediante la implementación de nuevas medidas de seguridad, la capacitación del personal, la actualización de procedimientos o la adopción de mejores prácticas internacionales.

En resumen, la metodología integral combinada con la herramienta MASS no solo evaluó el cumplimiento actual de los controles de seguridad, sino que también orientó a la organización hacia la mejora continua de su sistema de gestión de seguridad de la información.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

**1)** En cumplimiento del primer objetivo, se concluye que el estado actual de la ciberseguridad en PRISMA presenta brechas relevantes en múltiples dominios de control. De los 93 controles evaluados, un total de 31 controles (33.3%) se encuentran en niveles bajos de madurez:

- 8 controles (8.6%) están en estado "Existente", reflejando prácticas mínimas sin documentación formal.
- 19 controles (20.4%) están en estado "Inicial", caracterizado por acciones reactivas y no estandarizadas.
- 4 controles (4.3%) no se han gestionado o no aplican en el entorno actual.

La mayor concentración de controles en estados bajos se observa en el dominio organizativo, con 12 controles en nivel Inicial y 8 en nivel Existente, lo que representa el 54% de los controles organizativos (20 de 37). En el dominio tecnológico, 12 de los 34 controles (35.2%) también se encuentran en estados bajos, especialmente en autenticación, gestión de identidades, control de acceso y contacto con autoridades.

Estos resultados indican que más de un tercio de los controles evaluados requieren atención inmediata, sobre todo en la definición de políticas, gestión documental, gobierno de la seguridad y control de acceso a la información.

**2)** En relación con el segundo objetivo, se determinó que PRISMA mantiene un nivel de madurez general entre los niveles "Inicial" y "Gestionado", con 45 controles (48.4%) ubicados en estos dos niveles medios:

- 19 controles (20.4%) en nivel "Gestionado".
- 26 controles (28%) en nivel "Definido".

Los dominios tecnológicos y físicos son los que presentan los mayores avances. Por ejemplo, en el dominio tecnológico, 15 controles (44.1%) alcanzaron el nivel "Definido", mientras

que 9 controles (26.4%) se encuentran en niveles “Cuantitativo” u “Optimizado”.

En contraste, el dominio de Personas, que abarca aspectos como formación, verificación de antecedentes, procesos disciplinarios y acuerdos de confidencialidad, presenta una madurez general baja, con 3 de 8 controles (37.5%) en niveles Inicial o Existente y solo 1 control (12.5%) en nivel Definido. Este hallazgo sugiere debilidades en la cultura organizacional de seguridad y en la preparación del talento humano para enfrentar amenazas cibernéticas.

**3)** Los hallazgos del estudio evidencian que la Microfinanciera PRISMA requiere una estrategia de ciberseguridad estructurada para abordar las brechas críticas identificadas, especialmente en los dominios organizativo y tecnológico, donde más del 33% de los controles evaluados presentan baja madurez. Se constató la necesidad de integrar funciones clave como identificación, protección, detección, respuesta y recuperación, alineadas con ISO/IEC 27001:2022, ISO/IEC 27032:2023 y el marco NIST CSF. Asimismo, el análisis determinó que el diseño de dicha estrategia debe contemplar fases operativas, indicadores de desempeño, una matriz RACI clara y mecanismos de mejora continua, garantizando su sostenibilidad y pertinencia institucional.

## 5.2 RECOMENDACIONES

**1)** Con base en los hallazgos que indican que 33.3% de los controles evaluados se encuentran en niveles bajos (No Gestionado, Existente e Inicial), se recomienda la formulación e implementación de una estrategia integral de ciberseguridad, que aborde las brechas identificadas en los dominios organizativos, de personas, físicos y tecnológicos. Esta estrategia debe estructurarse en fases, tomando como referencia el marco NIST CSF, e incluir medidas de protección, detección, respuesta y recuperación, alineadas con ISO/IEC 27001:2022 y 27032:2023. El enfoque progresivo facilitará a PRISMA pasar de un estado reactivo a un modelo preventivo, proactivo y resiliente ante amenazas cibernéticas.

**2)** El 54% de los controles organizativos se encuentra en niveles bajos de madurez (20 de 37), lo que refleja una débil gobernanza de la seguridad de la información. Se recomienda que PRISMA priorice la implementación de políticas institucionales, asignación de roles y responsabilidades claras, así como la gestión documental de procesos relacionados con riesgos, clasificación de activos, gestión de proyectos y seguridad en la nube. Este fortalecimiento permitirá

estructurar un entorno organizacional más robusto, base indispensable para el resto de las acciones de ciberseguridad.

**3)** Se recomienda que la Microfinanciera PRISMA proceda con el diseño formal de una estrategia integral de ciberseguridad, tomando como base los resultados del diagnóstico de madurez y las brechas detectadas en los controles organizativos y tecnológicos. Esta estrategia debe estructurarse bajo los lineamientos de los marcos ISO/IEC 27001:2022, ISO/IEC 27032:2023 y NIST CSF, e incluir un plan por fases que contemple capacidades de monitoreo, mecanismos efectivos de respuesta a incidentes y protocolos de continuidad operativa. Además, se sugiere establecer indicadores cuantificables para evaluar el avance y la eficacia de las acciones, así como una matriz RACI que defina con claridad las responsabilidades de cada actor involucrado, asegurando una implementación ordenada, escalable y sostenible en el tiempo.

# CAPÍTULO VI. APLICABILIDAD

## 6.1 NOMBRE DE LA PROPUESTA

Diseño de una Estrategia de Ciberseguridad para la Microfinanciera PRISMA: Enfoque Basado en Normas ISO/IEC 27001:2022 y 27032:2023.

## 6.2 JUSTIFICACIÓN DE LA PROPUESTA

El sector MIPYME representa uno de los pilares fundamentales para el desarrollo económico y social de Honduras, aportando más del 70% del empleo y contribuyendo significativamente al dinamismo del mercado local. Sin embargo, muchas micro, pequeñas y medianas empresas enfrentan desafíos estructurales en materia de administración, formalización, financiamiento e incorporación de tecnologías digitales, lo que limita su sostenibilidad y capacidad de adaptación en un entorno altamente digitalizado y expuesto a crecientes amenazas cibernéticas.

Dentro de este ecosistema, el sector microfinanciero hondureño, conformado por 19 instituciones activas según la Red de Microfinanzas de Honduras REDCAMIF (2023), ha tenido un papel clave en la inclusión financiera de sectores vulnerables. Este sector se compone de Instituciones Microfinancieras (IMFs), OPDFs, cooperativas y entidades especializadas como los Sistemas de Financiamiento Alternativo Rural (SIFAR). No obstante, la mayoría de estas organizaciones carece de una cultura de ciberseguridad formal y de mecanismos estructurados para prevenir, detectar y responder ante amenazas informáticas.

La Microfinanciera PRISMA se posiciona en este contexto como una entidad clave, enfocada en facilitar el acceso a microcréditos y soluciones de vivienda social, operando principalmente en comunidades rurales y urbanas de bajos ingresos. Esta labor implica la gestión de datos altamente sensibles, personales, financieros y operacionales, lo cual la convierte en un objetivo atractivo para actores del cibercrimen.

Un ciberataque exitoso podría tener impactos financieros significativos para PRISMA. Por ejemplo, una filtración de datos o un ataque tipo ransomware podría generar:

- Pérdidas operativas por suspensión de servicios durante varios días.
- Pérdidas reputacionales, disminución de confianza y reducción de la cartera de clientes.

- Costos de recuperación e inversión en forense digital, que podrían superar los $25,000 USD, según benchmarks regionales del BID (2023).
- Potenciales sanciones o exclusiones de futuras líneas de financiamiento internacional, especialmente si no se demuestra cumplimiento con buenas prácticas de seguridad.

A pesar de estos riesgos, PRISMA no se encuentra bajo regulación directa de la CNBS en materia de ciberseguridad, y opera bajo un modelo de autorregulación, lo que incrementa su nivel de exposición. La ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI), sumada a la carencia de roles definidos, controles formales y planes de continuidad, la posicionan como una institución vulnerable ante incidentes cibernéticos.

El diagnóstico realizado como parte de esta investigación, basado en la herramienta MASS y en el análisis de 93 controles de seguridad según ISO/IEC 27001:2022 y 27032:2023, evidenció que el 33.3% de los controles se encuentra en niveles de madurez bajos (Inexistente o Inicial). Asimismo, solo el 3% alcanza niveles optimizados, lo cual muestra que las prácticas actuales no garantizan la protección integral de los activos digitales.

En este contexto, la presente propuesta titulada “Diseño de una Estrategia de Ciberseguridad para la Microfinanciera PRISMA: Enfoque Basado en Normas ISO/IEC 27001:2022 y 27032:2023” surge como una respuesta estratégica a la necesidad urgente de robustecer su postura de seguridad. Su objetivo es proporcionar un plan estructurado que permita establecer controles organizativos, técnicos y humanos orientados a la gestión de riesgos, continuidad operativa, respuesta a incidentes y fortalecimiento de la resiliencia institucional.

Al adoptar esta estrategia, PRISMA podrá avanzar hacia un modelo de seguridad proactivo, basado en estándares reconocidos, con una visión integral de la ciberseguridad como factor habilitador de su sostenibilidad y competitividad.

## 6.3 ALCANCE DE LA PROPUESTA

La presente propuesta tiene como alcance el diseño de una Estrategia Integral de Ciberseguridad para la Microfinanciera PRISMA, basada en los resultados del diagnóstico del estado actual de la seguridad de la información y el análisis del nivel de madurez en el cumplimiento de controles, conforme a los lineamientos de las normas ISO/IEC 27001:2022 e

ISO/IEC 27032:2023.

El enfoque planteado abarca únicamente la formulación del plan estratégico y no contempla la implementación ni evaluación de los controles propuestos, debido a los límites temporales y metodológicos del estudio. El alcance de la propuesta está delimitado por varios factores estructurales de la organización:

- La disponibilidad limitada de recursos humanos especializados en ciberseguridad, lo cual condiciona la aplicabilidad inmediata de ciertas acciones.
- La ausencia de una unidad interna dedicada exclusivamente a la gestión de seguridad de la información, lo que obliga a plantear estrategias progresivas y adaptadas a la estructura actual.
- Restricciones presupuestarias propias del modelo operativo de las instituciones microfinancieras de pequeño y mediano tamaño.
- La condición de autorregulación bajo la que opera PRISMA, al no estar sujeta a supervisión directa de un ente regulador en temas de ciberseguridad, lo cual limita el marco de cumplimiento obligatorio y exige el fortalecimiento voluntario de buenas prácticas.

A pesar de estas limitaciones, el diseño de esta estrategia proporciona a PRISMA una hoja de ruta sólida y adaptable para transitar hacia una postura de seguridad más robusta, alineada con estándares internacionales y contextualizada a su realidad operativa. El marco temporal estimado para la ejecución del plan es el año 2025, permitiendo a la institución programar sus acciones de acuerdo con su disponibilidad de recursos y prioridades estratégicas.

### 6.3.1 OBJETIVO GENERAL

Diseñar la Estrategia Integral de Ciberseguridad para la Microfinanciera PRISMA, basada en el diagnóstico del estado actual de su seguridad de la información y el análisis del nivel de madurez en el cumplimiento de controles de ciberseguridad, con el fin de fortalecer la protección de sus activos digitales, garantizar la continuidad operativa y mejorar el cumplimiento de los estándares ISO/IEC 27001:2022 e ISO/IEC 27032:2023, para el año 2025.

### 6.3.2 OBJETIVOS ESPECÍFICOS

1. Evaluar los factores que afectan la protección de la información en la microfinanciera PRISMA.
2. Diseñar estrategias para fortalecer la seguridad de la información, optimizando la gestión de riesgos, la gobernanza y la capacitación del talento humano.
3. Definir un plan de fortalecimiento tecnológico y operativo, alineado con ISO/IEC 27001:2022 e ISO/IEC 27032:2023, para mejorar la prevención y respuesta ante amenazas cibernéticas.

## 6.4 DESCRIPCIÓN Y DESARROLLO

### 6.4.1 DESCRIPCIÓN

El diseño de una estrategia de ciberseguridad efectiva requiere un enfoque estructurado y alineado con las mejores prácticas internacionales. En este contexto, se ha adoptado el NIST Cybersecurity Framework (CSF) como referencia metodológica para el desarrollo de la Estrategia Integral de Ciberseguridad para la microfinanciera PRISMA, garantizando un enfoque holístico basado en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar.

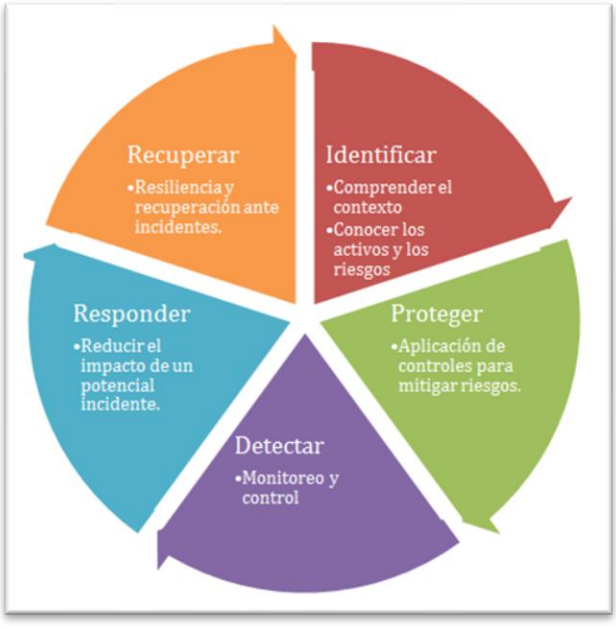


**Figura 26. Niveles de Implementación del NIST Cybersecurity Framework (CSF)**

Fuente: Herrera (2020)

Adaptar este esquema del NIST Cybersecurity Framework (CSF) a la realidad de PRISMA es una forma poderosa de ejemplificar cómo la estrategia propuesta se traduce en acciones concretas para la organización. A continuación se presenta cómo se puede contextualizar cada función del NIST CSF con casos aplicados a PRISMA:

**Tabla 31. Adaptación del Marco NIST CSF al contexto de PRISMA**

| Función NIST | Aplicación práctica en PRISMA |
|---|---|
| **Identificar** | Realizar un inventario completo de activos de información (servidores, bases de datos de clientes, sistemas core de crédito), identificar usuarios con privilegios, y mapear los riesgos tecnológicos. Por ejemplo, clasificar los datos sensibles de clientes rurales que acceden a microcréditos y determinar vulnerabilidades asociadas al acceso remoto. |
| **Proteger** | Establecer controles de acceso robustos y segmentación de redes internas. Implementar políticas de uso de dispositivos móviles para el personal de agencias, y realizar capacitaciones periódicas sobre buenas prácticas de seguridad. Ejemplo: aplicación de autenticación multifactor (MFA) para el sistema de gestión crediticia. |
| **Detectar** | Implementar sistemas básicos de monitoreo de red, alertas de comportamiento anómalo y registro de eventos (logs) de accesos no autorizados. Ejemplo: detectar actividad fuera de horario en cuentas con acceso a bases de datos de clientes. |
| **Responder** | Crear un procedimiento de respuesta ante incidentes que incluya la notificación inmediata a los equipos responsables, aislamiento de sistemas afectados y comunicación a partes interesadas. Ejemplo: definir el rol del gerente de agencia en caso de sospecha de fuga de información vía USB. |
| **Recuperar** | Desarrollar un plan de continuidad de negocio (BCP) y respaldo periódico de la base de datos de operaciones financieras. Ejemplo: mantener copias cifradas y fuera de línea del sistema central de créditos que puedan restaurarse en caso de ransomware. |

Fuente: Elaboración propia

Con el fin de facilitar la comprensión global del proceso metodológico propuesto y visualizar la secuencia lógica del diseño de la estrategia, se presenta a continuación el Mapa de Ruta Estratégico, que resume las cinco fases desarrolladas en el capítulo. Este roadmap sirve como guía estructurada para el fortalecimiento progresivo de la ciberseguridad institucional en PRISMA, considerando los principios del ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar) y los lineamientos del marco NIST CSF.

Cada fase está orientada a cubrir una función crítica en la gestión de la ciberseguridad: desde el diagnóstico inicial, pasando por la definición y priorización de controles, hasta la capacidad de detectar, responder y recuperarse ante incidentes.

Este mapa de ruta no solo establece las bases para el diseño de la estrategia de ciberseguridad, sino que ofrece una orientación táctica para futuras fases de implementación y

evaluación, una vez que la estrategia sea adoptada formalmente por la organización.

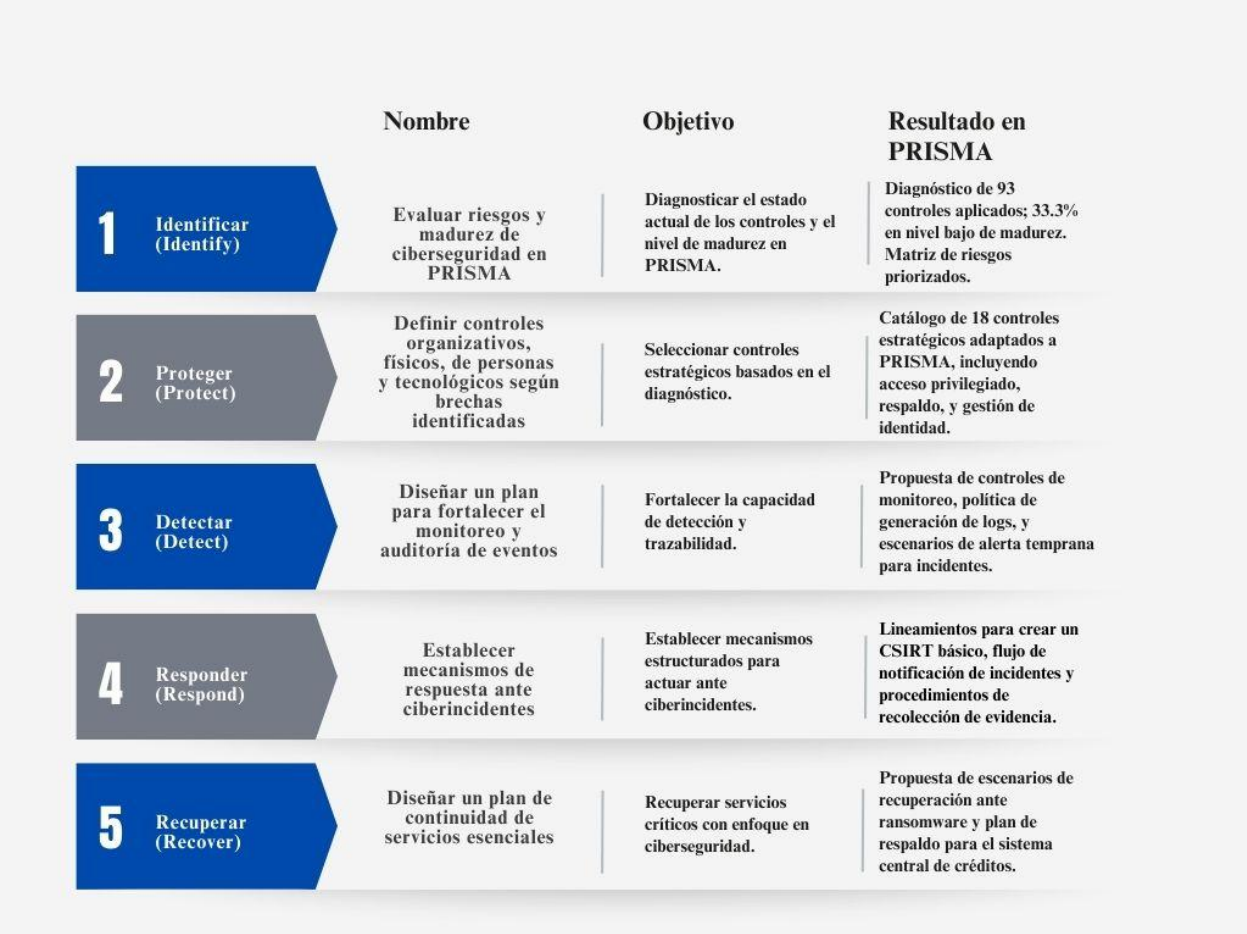


**Figura 27. Mapa de Ruta Estratégico**

Fuente: Elaboración Propia

Con el objetivo de evidenciar la coherencia entre el marco conceptual y la aplicación práctica de la estrategia de ciberseguridad propuesta para PRISMA, se presenta a continuación un esquema teórico–operativo que complementa la secuencia de fases mostrada en la figura anterior. Este esquema establece de manera explícita cómo cada una de las cinco funciones del marco NIST (Identificar, Proteger, Detectar, Responder y Recuperar) se fundamenta en modelos internacionales y normativas vigentes, tales como las normas ISO/IEC 27001:2022, ISO/IEC 27032:2023, el Modelo de Madurez de Ciberseguridad de Oxford (CMMI), y recomendaciones regionales del BID y la OEA. Esta integración garantiza que las acciones desarrolladas estén alineadas con mejores prácticas internacionales, adaptadas a la realidad de las microfinancieras en

el contexto centroamericano.

**Tabla 32. Esquema Teórico–Operativo de la Propuesta de Estrategia de Ciberseguridad**

| Fase | Nombre (Función NIST) | Objetivo operativo en PRISMA | Fundamentación teórica / normativa | Aplicación específica |
|---|---|---|---|---|
| 1 | Identificar (Identify) | Evaluar riesgos y nivel de madurez en ciberseguridad. | - ISO/IEC 27001:2022<br>- Modelo de Madurez CMMI (Oxford)<br>- Herramienta MASS | Aplicación del cuestionario MASS para evaluar 93 controles en 4 dominios. Segmentación de la muestra según roles clave. |
| 2 | Proteger (Protect) | Definir controles organizativos, físicos, humanos y tecnológicos. | - ISO/IEC 27001:2022<br>- ISO/IEC 27032:2023 | Priorización de controles organizativos, de personas, físicos y tecnológicos según criticidad y cumplimiento. |
| 3 | Detectar (Detect) | Fortalecer la capacidad de monitoreo y trazabilidad de eventos. | - ISO/IEC 27001:2022<br>- Marco NIST CSF | Inclusión de controles relacionados con trazabilidad, registros de eventos y detección temprana. |
| 4 | Responder (Respond) | Establecer mecanismos de actuación ante ciberincidentes. | - ISO/IEC 27001:2022<br>- Marco NIST CSF | Recomendaciones para establecer un protocolo básico de actuación y comunicación frente a incidentes. |
| 5 | Recuperar (Recover) | Diseñar un plan de continuidad y recuperación de servicios. | - ISO/IEC 27001:2022<br>- Marco NIST CSF | Sugerencias para un plan de recuperación de servicios esenciales ante interrupciones. |

Fuente: Elaboración Propia

### 6.4.2 DESARROLLO

#### 6.4.2.1 EVALUAR RIESGOS Y MADUREZ DE CIBERSEGURIDAD

En la primera fase, se realiza la evaluación de la ciberseguridad en la microfinanciera PRISMA la cual ha permitido identificar fortalezas, debilidades y brechas de seguridad en sus procesos, sistemas y controles. Este diagnóstico se basa en el análisis de madurez realizado mediante la herramienta MASS y en la identificación de riesgos alineada a los marcos normativos ISO/IEC 27001:2022 e ISO/IEC 27032:2023. A partir de estos resultados, se presenta la matriz de identificación de riesgos de PRISMA, la cual permite visualizar los riesgos críticos, por dominio evaluado y su nivel de impacto en la organización.

La evaluación de madurez permitió clasificar los controles en los siguientes niveles:

**Tabla 33. Niveles de Madurez Por Dominio**

| Dominio de Control | Nivel Predominante de Madurez |
|---|---|
| Controles Organizativos | Inicial – Gestionado |
| Controles de Personas | No Gestionado – Inicial |
| Controles Físicos | Definido – Cuantitativo |
| Controles Tecnológicos | Inicial – Gestionado |

Fuente: Elaboración Propia

A continuación se presentan las tablas que contienen los diagnósticos de los niveles de riesgos por dominio evaluado durante el estudio:

El diagnóstico se inicia con el dominio de controles organizativos, en tal sentido, se considera que la seguridad de la información debe partir desde una base sólida de gobernanza. En este dominio se presentan los controles que buscan establecer políticas claras, roles definidos, estructuras de decisión efectivas y un marco de cumplimiento alineado a las normas internacionales. Estos controles están orientados a cerrar las brechas detectadas en cuanto a planificación estratégica, gestión de proyectos, clasificación de la información y supervisión de terceros.

**Tabla 34. Diagnóstico Riesgos Dominio de Controles Organizativos**

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| O-01 | Ausencia de definición de roles y responsabilidades en SI | Alta | Alto | Crítico | Establecer una estructura formal con roles y responsabilidades en un SGSI alineado a ISO 27001 |
| O-02 | Desconocimiento de amenazas emergentes por falta de inteligencia de amenazas | Alta | Alto | Crítico | Implementar procesos de recolección, análisis y respuesta a inteligencia de amenazas |
| O-03 | Exclusión de requisitos de seguridad en la gestión de proyectos institucionales | Alta | Alto | Crítico | Integrar criterios de seguridad de la información desde la planificación de proyectos |
| O-04 | Divulgación o tratamiento inadecuado de información sensible por falta de clasificación | Alta | Alto | Crítico | Diseñar e implementar un esquema de clasificación de la información según criticidad |
| O-05 | Riesgos de integridad y confidencialidad por etiquetado incorrecto o inexistente | Alta | Medio | Alto | Establecer procedimientos para el etiquetado físico y digital de la información |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| O-06 | Filtración de datos en la transferencia de información no segura | Alta | Alto | Crítico | Aplicar cifrado, uso de canales seguros y control de acceso en procesos de transmisión |
| O-07 | Riesgos en la adopción de servicios en la nube sin criterios de seguridad | Alta | Alto | Crítico | Establecer una política de uso de servicios cloud con evaluación de proveedores y controles técnicos |
| O-08 | Pérdida, modificación o acceso no autorizado a registros institucionales | Alta | Alto | Crítico | Implementar controles de acceso, respaldo y protección de la integridad de los registros |
| O-09 | Inadecuada segregación de funciones que compromete la confidencialidad o integridad | Alta | Alto | Crítico | Definir claramente funciones y restricciones de acceso por rol |
| O-10 | Falta de involucramiento de la alta dirección en la gobernanza de SI | Media | Alto | Alto | Establecer comités de SI y mecanismos de supervisión ejecutiva |
| O-11 | Pérdida de capacidad de respuesta ante incidentes legales o regulatorios | Media | Alto | Alto | Establecer protocolos de contacto con autoridades e instituciones clave |
| O-12 | Desconexión con actores clave del sector en temas de seguridad | Media | Medio | Medio | Establecer relaciones con grupos de interés, ISACs o foros de ciberseguridad |
| O-13 | Acceso no controlado a sistemas críticos | Alta | Alto | Crítico | Establecer controles de acceso basados en roles y revisiones periódicas |
| O-14 | Gestión deficiente de identidades y cuentas inactivas | Alta | Alto | Crítico | Aplicar principios de gestión de identidad y acceso (IAM) |
| O-15 | Contraseñas inseguras y mal manejo de credenciales | Alta | Alto | Crítico | Establecer autenticación robusta y capacitación al usuario |
| O-16 | Accesos privilegiados sin control ni auditoría | Alta | Alto | Crítico | Aplicar el principio de menor privilegio y monitoreo de accesos privilegiados |
| O-17 | Baja preparación para gestionar incidentes de seguridad | Alta | Alto | Crítico | Diseñar un plan de respuesta a incidentes y capacitar a los equipos clave |
| O-18 | Riesgos legales por uso inadecuado de propiedad intelectual | Media | Medio | Medio | Establecer políticas claras sobre propiedad intelectual y su uso interno |
| O-19 | Incumplimiento de normativas de protección de datos personales (PII) | Alta | Alto | Crítico | Diseñar e implementar una política de privacidad y protección de datos personales |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| O-20 | Ausencia de auditorías independientes sobre el SGSI | Media | Alto | Alto | Establecer auditorías internas y externas regulares de la seguridad de la información |
| O-21 | Políticas de SI no difundidas o actualizadas regularmente | Media | Medio | Medio | Asegurar revisión periódica y divulgación de las políticas a todos los colaboradores |
| O-22 | Inventario de activos incompleto o desactualizado | Media | Medio | Medio | Establecer procesos automatizados de descubrimiento y actualización de activos |
| O-23 | Uso inadecuado o no autorizado de activos de información | Media | Alto | Alto | Establecer lineamientos claros de uso aceptable y controles de monitoreo |
| O-24 | Falta de control en la devolución de activos al finalizar la relación laboral | Media | Alto | Alto | Implementar checklist de salida e inventario digital asignado por usuario |
| O-25 | Respuesta a incidentes sin integración con políticas ni documentación | Media | Medio | Medio | Alinear los procedimientos de respuesta a incidentes con el SGSI y capacitar a los equipos |
| O-26 | Lecciones no documentadas ni incorporadas tras incidentes previos | Media | Medio | Medio | Documentar, analizar y comunicar aprendizajes para prevención de recurrencias |
| O-27 | Recolección de evidencia inadecuada ante incidentes de seguridad | Media | Alto | Alto | Establecer procedimientos forenses y cadena de custodia en recolección de evidencia |
| O-28 | Disrupción de operaciones críticas sin planes definidos de continuidad | Media | Alto | Alto | Desarrollar planes de continuidad de negocio con enfoque en SI y pruebas regulares |
| O-29 | Desconocimiento de requisitos legales y contractuales aplicables | Media | Medio | Medio | Mantener matriz de requisitos actualizada y divulgada entre responsables clave |
| O-30 | Incumplimiento de políticas internas y estándares de SI | Media | Medio | Medio | Establecer monitoreo del cumplimiento y sistema de consecuencias documentado |
| O-31 | Ausencia de procedimientos operativos documentados | Media | Alto | Alto | Elaborar procedimientos por área que incluyan aspectos de seguridad de la información |
| O-32 | Exposición a riesgos de terceros por falta de controles en relaciones con proveedores | Media | Alto | Alto | Establecer requisitos de seguridad en contratos y procesos de evaluación periódica de proveedores |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| O-33 | Omisión de cláusulas específicas de seguridad en acuerdos con terceros | Media | Alto | Alto | Incorporar cláusulas de SI obligatorias en todos los acuerdos de servicios tercerizados |
| O-34 | Vulnerabilidades en la cadena de suministro TIC sin supervisión | Media | Alto | Alto | Aplicar criterios de evaluación de riesgos y monitoreo a proveedores de TIC |
| O-35 | Cambios no controlados en servicios tercerizados que afectan la SI | Media | Alto | Alto | Establecer un proceso formal de gestión de cambios con visibilidad de seguridad |
| O-36 | Evaluación inadecuada de eventos de seguridad que afecta la respuesta | Media | Medio | Medio | Establecer comité de análisis de eventos con métricas y lecciones aprendidas |
| O-37 | Falta de preparación tecnológica ante interrupciones operativas | Media | Alto | Alto | Implementar redundancias tecnológicas y pruebas de recuperación |

Fuente: Elaboración Propia

El factor humano sigue siendo uno de los vectores más críticos en ciberseguridad. Esta sección agrupa los controles orientados a la gestión del personal, incluyendo la verificación de antecedentes, acuerdos de confidencialidad, programas de capacitación continua y el tratamiento disciplinario de incidentes. Estos controles buscan fortalecer la cultura organizacional en torno a la protección de la información y reducir los errores humanos que puedan comprometer la seguridad.

**Tabla 35. Diagnóstico Riesgos Dominio de Controles de Personas**

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| P-01 | Ausencia de procedimientos disciplinarios claros ante violaciones de seguridad | Alta | Alto | Crítico | Establecer y difundir una política disciplinaria formal por incidentes de SI |
| P-02 | Falta de revocación oportuna de accesos tras desvinculación o cambio de funciones | Alta | Alto | Crítico | Implementar un proceso formal de salida y reasignación de roles con checklist de seguridad |
| P-03 | Riesgos de seguridad en entornos de trabajo remoto mal gestionados | Alta | Alto | Crítico | Definir políticas de teletrabajo seguras, uso de VPN, cifrado de datos y controles de acceso |
| P-04 | Omisión o demora en el reporte de eventos de seguridad por parte del personal | Media | Alto | Alto | Establecer una cultura de reporte, canales seguros y capacitación continua |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| P-05 | Contratación de personal sin verificación previa de antecedentes relevantes | Media | Alto | Alto | Establecer procedimientos de screening laboral previo al ingreso al puesto |
| P-06 | Bajo nivel de concientización en SI a pesar de esfuerzos iniciales | Media | Medio | Medio | Fortalecer el programa de capacitación continua en SI con enfoque en riesgos actuales y simulacros prácticos |
| P-07 | Inadecuada formalización de los términos y condiciones laborales en temas de seguridad | Baja | Medio | Bajo | Mantener actualizados los contratos laborales con cláusulas de seguridad específicas |
| P-08 | Riesgos legales y reputacionales por falta de acuerdos de confidencialidad firmados | Baja | Alto | Medio | Garantizar la firma y renovación periódica de NDAs para todo el personal y terceros |

Fuente: Elaboración Propia

Este conjunto de controles se enfoca en garantizar la seguridad del entorno físico donde residen los activos de información. Se incluyen mecanismos para restringir accesos no autorizados, monitorear espacios sensibles y asegurar el manejo correcto de equipos y medios. La implementación de estos controles es fundamental para mitigar amenazas ambientales, intrusiones físicas y pérdida de activos.

**Tabla 36. Diagnóstico Riesgos Dominio de Controles Físicos**

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| F-01 | Exposición de información sensible por incumplimiento del protocolo de escritorio limpio | Media | Alto | Alto | Reforzar las políticas de escritorio despejado y realizar auditorías internas frecuentes |
| F-02 | Robo, pérdida o uso indebido de activos fuera de las instalaciones | Media | Alto | Alto | Establecer controles de registro y autorización para uso externo de dispositivos, y aplicar cifrado y rastreo |
| F-03 | Acceso físico no autorizado a instalaciones críticas por debilidad en el perímetro | Media | Alto | Alto | Mejorar las medidas perimetrales (barreras, vigilancia, control de accesos) |
| F-04 | Falta de evidencia ante eventos de seguridad por deficiencias en el monitoreo físico | Media | Alto | Alto | Ampliar la cobertura de videovigilancia y establecer retención segura de registros |
| F-05 | Exposición de información por almacenamiento inadecuado de medios | Media | Alto | Alto | Establecer procedimientos de custodia, cifrado y |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| | | | | | destrucción segura de medios |
| F-06 | Interrupciones operativas por fallos en instalaciones de soporte (electricidad, HVAC, etc.) | Media | Alto | Alto | Realizar mantenimiento preventivo y establecer redundancia en sistemas críticos |
| F-07 | Ingreso físico no controlado a zonas sensibles | Baja | Alto | Medio | Utilizar sistemas de autenticación de acceso y monitoreo de entradas/salidas |
| F-08 | Acceso físico indebido a oficinas o salas críticas | Baja | Alto | Medio | Establecer controles de acceso biométricos o con tarjetas RFID en zonas restringidas |
| F-09 | Daños por amenazas físicas y ambientales (incendios, inundaciones, etc.) | Media | Alto | Alto | Implementar controles de protección ambiental (sensores, extinguidores, UPS) |
| F-10 | Riesgos operativos por deficiencias en las áreas seguras | Baja | Alto | Medio | Realizar auditorías regulares sobre las condiciones de seguridad de estas zonas |
| F-11 | Pérdida o manipulación de equipos mal ubicados o sin protección adecuada | Media | Medio | Medio | Reubicar activos críticos en ubicaciones seguras y limitar su acceso físico |
| F-12 | Interrupción de servicios por fallas en el cableado inseguro o expuesto | Media | Medio | Medio | Canalizar y etiquetar el cableado según estándares de buenas prácticas |
| F-13 | Daños a la infraestructura por falta de mantenimiento preventivo | Baja | Alto | Medio | Establecer un plan de mantenimiento programado con evidencias documentadas |
| F-14 | Filtración de datos por eliminación insegura o reutilización de equipos | Media | Alto | Alto | Aplicar procedimientos de borrado seguro, desmagnetización y destrucción física |

Fuente: Elaboración Propia

Los controles tecnológicos evaluados están enfocados en salvaguardar la infraestructura digital de la organización. Se abordan áreas clave como la gestión de vulnerabilidades, autenticación segura, segmentación de red, desarrollo seguro y protección contra fugas de información. Su adecuada implementación permitirá reducir significativamente el riesgo de ciberataques, mejorar la resiliencia tecnológica y asegurar la continuidad operativa.

**Tabla 37. Diagnóstico Riesgos Dominio de Controles Tecnológicos**

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| T-01 | Acceso no autorizado o manipulación del código fuente por falta de controles | Alta | Alto | Crítico | Establecer controles de acceso al repositorio y trazabilidad de cambios |
| T-02 | Vulnerabilidades por ausencia de mecanismos de autenticación robustos | Alta | Alto | Crítico | Implementar MFA, políticas de contraseñas seguras y sesiones controladas |
| T-03 | Brechas de seguridad por no incorporar controles en el ciclo de desarrollo | Alta | Alto | Crítico | Integrar actividades de revisión de seguridad desde la fase de diseño (DevSecOps) |
| T-04 | Fallos en las aplicaciones por uso de prácticas de codificación insegura | Alta | Alto | Crítico | Aplicar estándares de codificación segura como OWASP y capacitar a los desarrolladores |
| T-05 | Interrupción de servicios críticos por falta de redundancia | Media | Alto | Alto | Implementar arquitecturas con tolerancia a fallos y planes de contingencia |
| T-06 | Falta de trazabilidad de eventos por registros incompletos o no protegidos | Media | Alto | Alto | Asegurar la generación, almacenamiento y monitoreo seguro de logs |
| T-07 | Exposición de datos sensibles por uso inadecuado de criptografía | Media | Alto | Alto | Aplicar algoritmos de cifrado robustos, gestión de llaves y protocolos seguros |
| T-08 | Vulnerabilidades en software desarrollado por terceros sin revisión de seguridad | Media | Alto | Alto | Establecer requisitos de seguridad en contratos y pruebas a desarrollos externos |
| T-09 | Infección de sistemas por malware no detectado | Media | Alto | Alto | Mantener soluciones antimalware actualizadas y realizar escaneos periódicos |
| T-10 | Explotación de vulnerabilidades técnicas por falta de gestión | Media | Alto | Alto | Implementar un programa continuo de gestión de parches y escaneos de vulnerabilidades |
| T-11 | Alteración o configuración insegura de sistemas | Media | Alto | Alto | Establecer controles de configuración segura y revisiones periódicas |
| T-12 | Recuperación incompleta o errónea por eliminación inadecuada de información | Media | Medio | Medio | Aplicar procedimientos documentados de eliminación y respaldo |
| T-13 | Exposición de datos sensibles por falta de enmascaramiento | Media | Alto | Alto | Aplicar enmascaramiento de datos en ambientes de prueba y desarrollo |
| T-14 | Filtración de datos por ausencia de mecanismos de prevención | Media | Alto | Alto | Implementar soluciones DLP (Data Loss Prevention) |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| T-15 | Pérdida de información por fallas en respaldos | Media | Alto | Alto | Establecer políticas de copia de seguridad y pruebas de restauración |
| T-16 | Actividades no autorizadas por falta de monitoreo de sistemas | Media | Alto | Alto | Implementar herramientas de monitoreo continuo y SIEM |
| T-17 | Uso indebido de programas utilitarios con privilegios elevados | Media | Alto | Alto | Limitar y monitorear el uso de utilitarios críticos mediante control de accesos |
| T-18 | Requisitos de seguridad no considerados en el diseño de aplicaciones | Media | Medio | Medio | Integrar validaciones de seguridad en el ciclo de vida de desarrollo |
| T-19 | Arquitectura de sistemas sin principios de seguridad desde el diseño | Media | Medio | Medio | Aplicar principios de "security by design" y arquitectura de referencia |
| T-20 | Aplicaciones sin pruebas de seguridad ni validación previa a despliegue | Media | Alto | Alto | Incluir pruebas de seguridad como parte del proceso de QA |
| T-21 | Cambios no controlados que generan vulnerabilidades | Media | Alto | Alto | Establecer controles de gestión del cambio con aprobaciones y auditorías |
| T-22 | Filtración de información en ambientes de prueba | Media | Medio | Medio | Aplicar aislamiento de entornos y sanitización de datos de prueba |
| T-23 | Exposición de datos o sistemas durante auditorías o pruebas externas | Baja | Medio | Bajo | Definir controles de acceso y protocolos durante procesos de auditoría |
| T-24 | Exposición de endpoints sin protección adecuada | Media | Alto | Alto | Aplicar soluciones de EDR y hardening de dispositivos de usuario |
| T-25 | Elevación de privilegios no controlada | Media | Alto | Alto | Implementar revisiones periódicas y segregación de privilegios por roles |
| T-26 | Acceso no autorizado a información crítica | Media | Alto | Alto | Aplicar controles de acceso basado en roles (RBAC) y revisiones de permisos |
| T-27 | Degradación de rendimiento por falta de planificación de capacidad | Media | Medio | Medio | Establecer monitoreo de capacidad y umbrales críticos para escalar |
| T-28 | Instalación de software no autorizado o inseguro | Media | Alto | Alto | Restringir instalaciones mediante políticas de aplicación y listas blancas |
| T-29 | Riesgos en la infraestructura por falta de seguridad en redes | Media | Alto | Alto | Segmentar redes, aplicar firewalls y protocolos de comunicación seguros |
| T-30 | Vulnerabilidades en los servicios de red expuestos | Media | Alto | Alto | Aplicar pruebas de penetración y monitoreo constante de servicios |
| T-31 | Ausencia de separación entre redes críticas y redes de usuario | Media | Alto | Alto | Implementar VLANs, firewalls internos y control de tráfico |

| ID | Riesgo Identificado | Probabilidad | Impacto | Nivel de Riesgo | Medida de Mitigación |
|---|---|---|---|---|---|
| T-32 | Acceso a contenidos maliciosos por falta de filtrado web | Media | Medio | Medio | Establecer filtros web y políticas de navegación corporativa |

Fuente: Elaboración Propia

Tras el análisis de madurez de ciberseguridad mediante la herramienta MASS y la matriz alineada con ISO/IEC 27001:2022 e ISO/IEC 27032:2023, se validaron los resultados con actores clave internos. Se organizaron sesiones con alta dirección, jefaturas y personal estratégico, donde se socializaron hallazgos, se ajustaron interpretaciones y se validaron los riesgos identificados. Esta validación participativa permitió identificar controles omitidos y aseguró la aceptación institucional del diagnóstico, consolidando así una base sólida para el diseño de la estrategia de ciberseguridad.

#### 6.4.2.2 DEFINIR CONTROLES ORGANIZATIVOS, DE PERSONAS, FÍSICOS Y TECNOLÓGICOS

El objetivo de esta fase es establecer y definir los controles organizativos, físicos, de personas y tecnológicos requeridos para elevar el nivel de madurez de la ciberseguridad en PRISMA, alineándolos con las brechas identificadas en la fase diagnóstica y con los lineamientos establecidos en las normas ISO/IEC 27001:2022, ISO/IEC 27002:2022 y el marco NIST CSF.

Con base en los resultados del diagnóstico de madurez y la matriz de diagnóstico de riesgos elaborada en la fase anterior, esta etapa se centra en la selección y definición de los controles necesarios para reducir vulnerabilidades críticas, mitigar los riesgos priorizados y fortalecer integralmente la postura de seguridad de la información de la organización.

La propuesta de controles se estructura en cuatro dimensiones clave, con enfoque multidominio: controles organizativos, controles físicos, controles de personas y controles tecnológicos.

Los criterios para la definición y selección de los controles son:

**Tabla 38. Criterios para la selección de controles**

| Criterio de selección del control | Descripción |
|---|---|
| 1. Nivel de Madurez Actual | Se priorizan controles que en el diagnóstico aparecen en niveles bajos de madurez: |

| Criterio de selección del control | Descripción |
|---|---|
| | • No gestionado<br>• Inicial<br>• Gestionado, pero con impacto alto o interdependencias críticas.<br>El objetivo es atender primero las brechas más significativas para elevar la postura de seguridad general de PRISMA. |
| 2. Riesgo Asociado (según la matriz de riesgos) | Se seleccionan controles que:<br>• Mitiguen riesgos críticos o altos detectados en la matriz.<br>• Se relacionen con vulnerabilidades frecuentes: acceso no autorizado, falta de clasificación, codificación insegura, etc. |
| 3. Alineación con los Marcos ISO/IEC 27002:2022 y NIST CSF | Todos los controles están referenciados a dominios normativos establecidos y tienen trazabilidad directa con:<br>• Los dominios 5 al 8 de ISO/IEC 27002:2022.<br>• Las funciones de NIST: Identificar, Proteger, Detectar, Responder y Recuperar. |
| 4. Viabilidad e impacto estratégico | Se seleccionan controles que pueden ser implementados o reforzados por PRISMA en un plazo corto a mediano, considerando:<br>• Recurso humano existente.<br>• Recursos tecnológicos disponibles.<br>• Factibilidad en el contexto de una microfinanciera. |

Fuente: Elaboración Propia

El resultado de esta fase es una lista estructurada y priorizada de controles recomendados, clasificados por dominio, acompañada de una descripción funcional, su nivel de madurez actual y su alineación con los controles de la norma ISO/IEC 27002:2022.

**Tabla 39. Controles recomendados para la estrategia**

| Dominio | Control Sugerido | Referencia ISO/IEC 27002:2022 | Nivel de Madurez Actual |
|---|---|---|---|
| Organizativo | Definición formal de roles y responsabilidades de SI | 5.2 | No gestionado |
| Organizativo | Implementación de un programa de inteligencia de amenazas | 5.7 | No gestionado |
| Organizativo | Clasificación y etiquetado de la información crítica | 5.12 / 5.13 | No gestionado |
| Organizativo | Integración de SI en la gestión de proyectos institucionales | 5.8 | No gestionado |
| Organizativo | Establecimiento de un comité de gobernanza de SI | 5.4 | Inicial |

| Dominio | Control Sugerido | Referencia ISO/IEC 27002:2022 | Nivel de Madurez Actual |
|---|---|---|---|
| Personas | Verificación de antecedentes del personal con acceso a información sensible | 6.1 | Gestionado |
| Personas | Formalización de acuerdos de confidencialidad y no divulgación | 6.6 | Optimizado |
| Personas | Programa continuo de concientización y capacitación en SI | 6.3 | Definido |
| Personas | Gestión del proceso disciplinario frente a incumplimientos de seguridad | 6.4 | Inicial |
| Físico | Control de acceso físico a instalaciones críticas | 7.1 / 7.2 | Gestionado |
| Físico | Monitoreo mediante sistemas de videovigilancia | 7.4 | Definido |
| Físico | Política de escritorio limpio y protección de medios | 7.7 / 7.10 | Gestionado |
| Físico | Eliminación segura y reutilización de equipos | 7.14 | Cuantitativo |
| Tecnológico | Gestión de vulnerabilidades técnicas (escaneo y parches) | 8.8 | Definido |
| Tecnológico | Autenticación multifactor (MFA) en sistemas críticos | 8.5 | Inicial |
| Tecnológico | Segmentación de red y control de tráfico | 8.22 | Cuantitativo |
| Tecnológico | Prevención de fuga de datos (DLP) | 8.12 | Definido |
| Tecnológico | Aplicación de pruebas de seguridad en el ciclo de desarrollo | 8.29 | Definido |

Fuente: Elaboración Propia

A continuación se presenta la matriz de priorización de controles por dominio, donde se combinan los factores de: nivel de madurez actual, impacto en la seguridad, viabilidad de implementación. Esto permite establecer un enfoque táctico para definir qué controles implementar primero.

**Tabla 40. Matriz de Priorización de Controles por Dominio**

| Dominio | Control Sugerido | Nivel de Madurez Actual | Impacto en la Seguridad | Viabilidad de Implementación | Prioridad Estimada |
|---|---|---|---|---|---|
| Organizativo | Definición de roles y responsabilidades | No gestionado | Alto | Alta | Alta |
| Organizativo | Inteligencia de amenazas | No gestionado | Alto | Media | Alta |
| Organizativo | Clasificación y etiquetado de información | No gestionado | Alto | Media | Alta |

| Dominio | Control Sugerido | Nivel de Madurez Actual | Impacto en la Seguridad | Viabilidad de Implementación | Prioridad Estimada |
|---|---|---|---|---|---|
| Organizativo | SI en la gestión de proyectos | No gestionado | Alto | Media | Alta |
| Organizativo | Comité de gobernanza de SI | Inicial | Medio | Alta | Media |
| Físico | Control de acceso físico | Gestionado | Alto | Alta | Alta |
| Físico | Monitoreo de videovigilancia | Definido | Medio | Alta | Media |
| Físico | Política de escritorio limpio | Gestionado | Medio | Alta | Media |
| Físico | Eliminación segura de equipos | Cuantitativo | Medio | Alta | Media |
| Personas | Verificación de antecedentes | Gestionado | Alto | Alta | Alta |
| Personas | Acuerdos de confidencialidad | Optimizado | Alto | Alta | Media |
| Personas | Capacitación en seguridad | Definido | Alto | Alta | Alta |
| Personas | Proceso disciplinario en SI | Inicial | Medio | Media | Media |
| Tecnológico | Gestión de vulnerabilidades | Definido | Alto | Media | Alta |
| Tecnológico | Autenticación multifactor (MFA) | Inicial | Alto | Alta | Alta |
| Tecnológico | Segmentación de red | Cuantitativo | Alto | Media | Media |
| Tecnológico | Prevención de fuga de datos (DLP) | Definido | Alto | Media | Alta |
| Tecnológico | Pruebas de seguridad en desarrollo | Definido | Medio | Media | Media |

Fuente: Elaboración Propia

#### 6.4.2.3 DISEÑAR UN PLAN PARA INCREMENTAR LAS CAPACIDADES DE MONITOREO Y AUDITORÍA

El objetivo de esta fase es diseñar un plan estructurado que permita fortalecer las capacidades de monitoreo continuo, recolección de registros (logs) y auditoría de eventos relacionados con la seguridad de la información, con el fin de mejorar la capacidad de detección temprana de amenazas y garantizar la trazabilidad de los incidentes.

En el marco del ciclo de ciberseguridad, la función "Detectar" del NIST Cybersecurity

Framework (CSF) establece la necesidad de contar con mecanismos eficaces para identificar anomalías y eventos de seguridad en tiempo real. Esta fase se centra en la planificación de capacidades que le permitan a PRISMA mantener visibilidad sobre su infraestructura tecnológica, usuarios y procesos críticos.

El resultado esperado de esta fase es un conjunto de recomendaciones estratégicas y operativas para implementar capacidades de monitoreo y auditoría, que incluyan la identificación de herramientas, roles clave, procedimientos de revisión y lineamientos para asegurar la trazabilidad, detección y análisis de eventos de seguridad.

**Tabla 41. Controles y Acciones Estratégicas para Monitoreo y Auditoría**

| Área de Enfoque | Control Sugerido | Acción Estratégica Propuesta | Prioridad (según diagnóstico) | Dominio ISO/IEC 27002:2022 |
|---|---|---|---|---|
| Gestión de registros (logs) | 8.15 - Registros (logs) | Establecer una política de retención y revisión de logs para sistemas críticos. | Alta | 8.15 |
| Análisis y correlación de eventos | SIEM - Integración de eventos de seguridad | Seleccionar e implementar una herramienta de SIEM adaptada al tamaño y recursos de PRISMA. | Alta | 8.16 / 5.25 |
| Auditoría interna de seguridad | 5.35 - Revisión independiente de SI | Diseñar un plan anual de auditorías internas con criterios basados en riesgos. | Media | 5.35 |
| Alertas y respuesta temprana | Configuración de umbrales de alerta e indicadores clave | Configurar alertas automáticas para accesos inusuales, fallos de autenticación o movimientos de datos sensibles. | Media | 5.24 / 8.16 |
| Supervisión del cumplimiento de controles | Monitoreo del cumplimiento de políticas y estándares de SI | Aplicar revisiones mensuales del cumplimiento de controles con métricas de desempeño y evidencia documental. | Media | 5.36 / 5.37 |

Fuente: Elaboración Propia

A continuación, se presenta la tabla de entregables correspondientes a la fase de fortalecimiento de capacidades de monitoreo y auditoría. Cada uno de estos documentos y acciones estratégicas responde a los requerimientos identificados en la fase diagnóstica.

**Tabla 42. Entregables de la Fase de Monitoreo y Auditoría**

| Nombre del Entregable | Propósito | Norma Relacionada |
|---|---|---|
| Política de Gestión de Registros de Seguridad (Logs) | Establecer reglas para la generación, retención y revisión de registros de seguridad. | ISO/IEC 27002:2022 - 8.15 |
| Plan de Implementación de Herramienta de Monitoreo (SIEM) | Guiar la selección e implementación de una solución de monitoreo centralizado. | ISO/IEC 27002:2022 - 8.16 / 5.25 |

| Nombre del Entregable | Propósito | Norma Relacionada |
|---|---|---|
| Procedimiento de Auditoría Interna de Seguridad de la Información | Definir el protocolo de auditoría interna orientado a los controles de SI. | ISO/IEC 27002:2022 - 5.35 |
| Matriz de Umbrales de Alerta y Eventos Críticos | Establecer eventos críticos, umbrales de alerta y criterios de respuesta. | ISO/IEC 27002:2022 - 5.24 / 8.16 |
| Programa de Revisión de Cumplimiento de Controles de Seguridad | Monitorear periódicamente el cumplimiento de los controles definidos en la estrategia. | ISO/IEC 27002:2022 - 5.36 / 5.37 |

Fuente: Elaboración Propia

Dado el nivel de madurez actual de PRISMA y sus limitaciones presupuestarias y técnicas, se propone un enfoque escalonado para fortalecer las capacidades de monitoreo, partiendo de soluciones open-source o de bajo costo que permitan una implementación inicial eficiente, con posibilidad de escalar a soluciones más robustas en fases futuras. Entre las herramientas recomendadas se encuentra Wazuh, una plataforma de código abierto que permite monitoreo en tiempo real, análisis de logs, detección de intrusiones (HIDS) y generación de alertas, lo cual resulta altamente funcional para entornos financieros de tamaño mediano con limitaciones de infraestructura.

Asimismo, se sugiere evaluar ELK Stack (Elasticsearch, Logstash, Kibana) para el procesamiento y visualización de eventos de seguridad, así como Graylog, por su facilidad de implementación en infraestructuras híbridas y su enfoque en auditoría y cumplimiento. En una etapa posterior, y en caso de contar con mayor disponibilidad de recursos, se podría considerar el análisis de soluciones SIEM comerciales como Splunk, IBM QRadar o AlienVault, que ofrecen mayor automatización, correlación avanzada de eventos y capacidades integradas de respuesta a incidentes. La selección de herramientas debe realizarse considerando la escalabilidad, facilidad de uso, soporte técnico disponible y alineación con los controles definidos en la estrategia.

#### 6.4.2.4 ESTABLECER UN PLAN DE RESPUESTA A INCIDENTES

El objetivo de esta fase es desarrollar un plan para fortalecer las capacidades de PRISMA en la detección, contención, análisis, comunicación y recuperación ante incidentes de ciberseguridad, garantizando una respuesta ágil y eficiente alineada con las mejores prácticas internacionales.

Esta etapa busca dotar a la microfinanciera de un marco formal para responder a incidentes de seguridad de la información, contemplando desde la preparación del personal y procedimientos,

hasta la coordinación con actores internos y externos, en cumplimiento con los controles de las normas ISO/IEC 27002:2022 (especialmente la sección 5.24 al 5.28) y la función "Responder" del NIST CSF.

El resultado esperado de esta fase es un plan de respuesta a incidentes de ciberseguridad documentado, validado con las necesidades específicas de PRISMA, que pueda ser activado ante eventos críticos para minimizar daños, preservar evidencia y restablecer la normalidad operativa en el menor tiempo posible.

**Tabla 43. Componentes del Plan de Respuesta a Incidentes**

| Componente del Plan | Acción Clave | Norma Relacionada |
|---|---|---|
| Identificación de incidentes y clasificación por criticidad | Establecer una taxonomía de incidentes y niveles de severidad para PRISMA. | ISO/IEC 27002:2022 - 5.24 |
| Definición de roles y responsabilidades | Asignar responsabilidades claras en un equipo de respuesta (CSIRT) institucional. | ISO/IEC 27002:2022 - 5.4 / 5.26 |
| Procedimiento de análisis y contención | Establecer protocolos de análisis de impacto y medidas inmediatas de contención. | ISO/IEC 27002:2022 - 5.25 |
| Canales de comunicación y escalamiento | Definir líneas de reporte interno y externo, incluyendo notificación a entes regulatorios. | ISO/IEC 27002:2022 - 5.26 |
| Gestión de evidencia digital | Estandarizar la preservación de evidencia digital conforme a cadena de custodia. | ISO/IEC 27002:2022 - 5.28 |
| Recuperación de servicios críticos | Definir pasos para restaurar operaciones priorizando servicios críticos. | ISO/IEC 27002:2022 - 5.29 |
| Documentación y retroalimentación | Establecer una fase de revisión post-incidente con plan de mejora. | ISO/IEC 27002:2022 - 5.27 |

Fuente: Elaboración Propia

A continuación, se detallan los entregables definidos para la fase de respuesta a incidentes de ciberseguridad. Cada uno de estos productos estratégicos busca formalizar y operacionalizar la gestión de incidentes dentro de PRISMA, permitiendo una reacción rápida, organizada y conforme a estándares internacionales.

**Tabla 44. Entregables de la Fase de Respuesta a Incidentes**

| Nombre del Entregable | Propósito | Norma Relacionada |
|---|---|---|
| Plan de Respuesta a Incidentes de Ciberseguridad (PRI) | Establecer un marco institucional para actuar ante eventos de seguridad de la información. | ISO/IEC 27002:2022 - 5.24 / 5.25 / 5.26 |
| Manual del Equipo de Respuesta a Incidentes (CSIRT) | Definir funciones, estructura, responsabilidades y flujo operativo del equipo de respuesta. | ISO/IEC 27002:2022 - 5.26 |
| Formato de Registro y Clasificación de Incidentes | Estandarizar el registro, categorización y seguimiento de incidentes de ciberseguridad. | ISO/IEC 27002:2022 - 5.25 |

| Nombre del Entregable | Propósito | Norma Relacionada |
|---|---|---|
| Procedimiento de Gestión de Evidencia Digital | Asegurar la trazabilidad y custodia de la evidencia recopilada durante un incidente. | ISO/IEC 27002:2022 - 5.28 |
| Informe de Lecciones Aprendidas Post-Incidente | Documentar hallazgos clave y generar retroalimentación para fortalecer controles futuros. | ISO/IEC 27002:2022 - 5.27 |

Fuente: Elaboración Propia

#### 6.4.2.5 DISEÑAR UN PLAN DE RECUPERACIÓN Y CONTINUIDAD OPERATIVA EN CIBERSEGURIDAD

El objetivo de esta fase es diseñar un conjunto de acciones, procedimientos y lineamientos que permitan restablecer los servicios críticos de la microfinanciera PRISMA tras un incidente de ciberseguridad, garantizando la continuidad operativa, la recuperación de datos y el cumplimiento regulatorio.

La función "Recover" del NIST CSF busca asegurar que las organizaciones puedan recuperarse eficazmente tras un incidente, minimizando el impacto en las operaciones, protegiendo su reputación y asegurando la integridad de sus activos digitales.

Estas medidas permitirán que PRISMA asegure una recuperación estructurada y rápida, alineada a las buenas prácticas definidas en la norma ISO/IEC 27002:2022 (especialmente los controles 5.29, 5.30 y 8.13) y los principios de continuidad del negocio.

El resultado esperado es un plan de recuperación y continuidad operativa en ciberseguridad adaptado al entorno y capacidades de PRISMA, que integre procedimientos, responsables, prioridades y medios técnicos necesarios para restablecer los servicios esenciales ante un incidente disruptivo.

**Tabla 45. Componentes del Plan de Recuperación y Continuidad**

| Componente del Plan | Acción Clave | Norma Relacionada |
|---|---|---|
| Identificación de procesos y servicios críticos | Realizar un inventario actualizado de los procesos críticos y sistemas esenciales para la operación. | ISO/IEC 27002:2022 - 5.29 |
| Estrategia de respaldo y restauración de información | Establecer una política de respaldo con frecuencia, ubicación segura y validación de restauración. | ISO/IEC 27002:2022 - 8.13 |
| Procedimientos de recuperación escalonada | Definir una hoja de ruta técnica para la recuperación de servicios priorizados por impacto. | ISO/IEC 27002:2022 - 5.30 |

| Componente del Plan | Acción Clave | Norma Relacionada |
|---|---|---|
| Actualización del Plan de Continuidad del Negocio (BCP) | Revisar e incorporar amenazas cibernéticas al plan general de continuidad operativa. | ISO/IEC 27002:2022 - 5.30 / 8.29 |
| Simulación de escenarios de recuperación (ciberdrills) | Planificar y ejecutar pruebas simuladas de recuperación ante ataques o pérdidas de datos. | ISO/IEC 27002:2022 - 5.30 |
| Definición de roles post-incidente | Establecer un equipo responsable del restablecimiento funcional y la comunicación post-incidente. | ISO/IEC 27002:2022 - 5.26 / 5.27 |

Fuente: Elaboración Propia

A continuación, se detallan los entregables claves asociados a la fase de recuperación y continuidad operativa en ciberseguridad. Estos productos estratégicos tienen como finalidad garantizar que la microfinanciera PRISMA esté preparada para restablecer sus servicios esenciales de manera ordenada y eficaz ante un incidente cibernético.

**Tabla 46. Entregables de la Fase de Recuperación y Continuidad**

| Nombre del Entregable | Propósito | Norma Relacionada |
|---|---|---|
| Plan de Recuperación ante Incidentes Cibernéticos (PRIC) | Establecer las directrices y procedimientos para restaurar operaciones tras un incidente cibernético. | ISO/IEC 27002:2022 - 5.29 / 5.30 |
| Matriz de Procesos Críticos y RTO/RPO definidos | Identificar procesos críticos y definir tiempos máximos aceptables de recuperación. | ISO/IEC 27002:2022 - 5.30 |
| Política de Respaldo y Restauración de Información | Normar la frecuencia, tipo, ubicación y validación de respaldos de información clave. | ISO/IEC 27002:2022 - 8.13 |
| Procedimiento de Recuperación Escalonada de Servicios | Detallar los pasos técnicos y prioridades para recuperar los servicios según criticidad. | ISO/IEC 27002:2022 - 5.30 |
| Informe de Simulación de Recuperación (Ciberdrill) | Documentar los resultados y lecciones aprendidas de simulaciones de recuperación organizacional. | ISO/IEC 27002:2022 - 5.30 / 5.27 |

Fuente: Elaboración Propia

## 6.5 ALINEACIÓN CON LA NORMATIVA NACIONAL DE LA CNBS

Aunque actualmente la Microfinanciera PRISMA no se encuentra bajo supervisión directa de la Comisión Nacional de Bancos y Seguros (CNBS), es relevante destacar que la estrategia de ciberseguridad propuesta se encuentra alineada con los principios establecidos en la Resolución CNBS No. 025/2022: Normas para la Gestión de Tecnologías de la Información y la Seguridad de la Información.

Este instrumento normativo nacional establece disposiciones aplicables a las instituciones financieras reguladas, orientadas a fortalecer la gobernanza de las tecnologías, la gestión de riesgos

tecnológicos y cibernéticos, la protección de datos, la continuidad del negocio y la respuesta ante incidentes de seguridad. A pesar de no ser de cumplimiento obligatorio para PRISMA, su adopción voluntaria representa una oportunidad estratégica para robustecer el cumplimiento futuro, mejorar la percepción institucional ante socios financieros y preparar a la organización para una eventual supervisión formal.

La propuesta desarrollada en este capítulo retoma elementos clave de la resolución, como:

- La necesidad de establecer roles y responsabilidades claras en TI y Seguridad de la Información.
- La implementación de procesos de gestión de incidentes, continuidad operativa y control de accesos.
- El fortalecimiento del monitoreo, auditoría y evaluación del cumplimiento interno.
- La formalización de políticas de seguridad y protección de datos sensibles.

De este modo, se refuerza la coherencia normativa entre el diseño estratégico propuesto y las exigencias regulatorias nacionales, facilitando su futura aplicabilidad en entornos supervisados y posicionando a PRISMA como una entidad con visión de madurez organizacional y sostenibilidad tecnológica.

El plan de diseño de la estrategia de ciberseguridad para PRISMA no solo se alinea con los estándares internacionales ISO/IEC 27001:2022, ISO/IEC 27032:2023 y NIST CSF, sino que también guarda coherencia operativa con los lineamientos establecidos por la CNBS en su normativa nacional. A continuación, se muestra la relación entre cada fase del plan y los componentes relevantes de la Resolución 025/2022:

**Tabla 47. Correspondencia Operativa Plan y Resolución CNBS No. 025/2022**

| Fase del Plan Diseñado | Requisitos Asociados en CNBS 025/2022 |
|---|---|
| Fase 1: Evaluación de riesgos y madurez de ciberseguridad | Art. 13 y 14: Requieren una evaluación formal del riesgo tecnológico y cibernético, así como la adopción de metodologías para su identificación, análisis y mitigación. |
| Fase 2: Definición de controles estratégicos | Art. 9, 15 y 16: Obligación de establecer políticas, roles, medidas de control y segregación de funciones para garantizar la protección de los activos de información. |

| Fase del Plan Diseñado | Requisitos Asociados en CNBS 025/2022 |
|---|---|
| Fase 3: Diseño del plan de monitoreo y auditoría | Art. 17, 20 y 23: Establecen la necesidad de implementar monitoreo continuo, gestión de eventos e incidentes, así como auditorías internas de los controles implementados. |
| Fase 4: Diseño del plan de respuesta a incidentes | Art. 21 y 22: Requieren que las instituciones cuenten con un plan formal de respuesta a incidentes de seguridad, con roles definidos, flujos de reporte y recuperación. |
| Fase 5: Diseño del plan de recuperación y continuidad | Art. 24 y 25: Establecen que las entidades deben contar con planes de continuidad de negocio y recuperación ante desastres, incorporando riesgos cibernéticos y TI. |

Fuente: Elaboración Propia

## 6.6 MEDIDAS DE CONTROL

### 6.6.1 INDICADORES

A fin de asegurar la trazabilidad, coherencia técnica y validez metodológica del proceso de formulación del plan para el diseño de la estrategia de ciberseguridad en PRISMA, se establecieron medidas de control asociadas a cada una de las fases estratégicas desarrolladas. Estas medidas no están orientadas a evaluar la implementación, sino a verificar que cada fase del plan se haya construido con rigor técnico, alineación normativa y en correspondencia directa con los hallazgos del diagnóstico.

Para tal fin, se definieron indicadores específicos de verificación, que permiten evidenciar el cumplimiento de los objetivos metodológicos en cada etapa del diseño. La siguiente tabla resume las medidas de control aplicadas y sus respectivos indicadores de logro, los cuales servirán como referencia para futuros procesos de implementación, seguimiento o auditoría del plan estratégico.

**Tabla 48. Medidas de Control con Indicadores por Fase del Plan**

| Fase del Plan Diseñado | Medida de Control Aplicada | Indicadores |
|---|---|---|
| Fase 1: Evaluación de riesgos y madurez de ciberseguridad | Validación del diagnóstico mediante el uso estructurado de la herramienta MASS, matriz de evaluación de la madurez, triangulación con entrevistas. | Cobertura del 100% de los dominios evaluados con MASS. Logro de una reducción proyectada de riesgos críticos ≥ 50% para implementación en 6 meses. |
| Fase 2: Definición de controles estratégicos | Coherencia entre los resultados del diagnóstico y los controles seleccionados. Verificación de alineación con ISO/IEC 27002:2022 por dominio. | Definición de al menos 18 controles estratégicos priorizados con base en brechas identificadas. 100% alineados con dominios ISO/IEC 27002:2022. |

| Fase del Plan Diseñado | Medida de Control Aplicada | Indicadores |
|---|---|---|
| Fase 3: Diseño del plan de monitoreo y auditoría | Revisión técnica de los controles propuestos, consistencia en la priorización y correspondencia con las brechas detectadas en monitoreo, trazabilidad y registros. | Diseño de al menos 5 controles de monitoreo implementables. |
| Fase 4: Diseño del plan de respuesta a incidentes | Revisión del modelo de respuesta propuesto (PRI), su alineación con los controles normativos y la claridad en los roles y procedimientos definidos. | Documento PRI validado con roles definidos y al menos 3 escenarios de incidente modelados. Expectativa de reducción de impacto operativo ≥ 40% una vez implementado. |
| Fase 5: Diseño del plan de recuperación y continuidad | Evaluación de la lógica de los componentes propuestos (respaldo, restauración, ciberdrills o ejercicio de ciberseguridad) y validación de su correspondencia con los hallazgos del diagnóstico. | Plan de respaldo formalizado con al menos 2 mecanismos redundantes. Expectativa de recuperación de servicios críticos en ≤ 8 horas para escenarios de disrupción severa. |

Fuente: Elaboración Propia

### 6.6.2 PLAN DE SEGUIMIENTO Y CONTROL

La siguiente matriz RACI define de forma estructurada los roles y niveles de responsabilidad asignados para cada una de las fases del plan estratégico de ciberseguridad diseñado para la Microfinanciera PRISMA. Esta herramienta facilita la gestión de la estrategia al clarificar quién debe ejecutar (Responsable), aprobar (Aprobador), ser consultado (Consultado) y mantenerse informado (Informado) en cada actividad clave. La matriz se ha desarrollado con base en las mejores prácticas de gobernanza y seguridad, promoviendo la transparencia, trazabilidad y eficiencia en la implementación del plan.

**Tabla 49. Matriz RACI**

| Fase del Plan Diseñado | Actividad Principal | Responsable (R) | Aprobador (A) | Consultado (C) | Informado (I) |
|---|---|---|---|---|---|
| Fase 1: Evaluación de riesgos y madurez de ciberseguridad | Aplicación del diagnóstico MASS y matriz ISO/IEC 27001:2022 | Área de TI / Seguridad de la Información | Alta Dirección | Jefaturas de Agencias / Auditores | Toda la organización |
| | Validación del diagnóstico con actores clave | Líder del proyecto | Alta Dirección | Comité de Seguridad | Colaboradores involucrados |
| Fase 2: Definición de controles estratégicos | Priorización y selección de controles | Líder del proyecto/ Consultor Externo | Comité de Seguridad | TI, Auditoría, Cumplimiento | Alta Dirección |

| Fase del Plan Diseñado | Actividad Principal | Responsable (R) | Aprobador (A) | Consultado (C) | Informado (I) |
|---|---|---|---|---|---|
| | Alineación normativa ISO/IEC 27002:2022 | Consultor de Seguridad | Líder del proyecto | Comité de Seguridad | TI y Cumplimiento |
| Fase 3: Diseño del plan de monitoreo y auditoría | Selección de herramientas de monitoreo (SIEM, logs) | Área de TI | Líder del proyecto | Auditor Interno | Comité de Seguridad |
| | Definición de umbrales de alertas y reportes | Seguridad de la Información | Líder del proyecto | TI y Cumplimiento | Alta Dirección |
| Fase 4: Diseño del plan de respuesta a incidentes (PRI) | Estructuración del PRI (roles, fases, flujos) | Líder del Proyecto / Coordinador de Incidentes | Comité de Seguridad | TI / Legal / Comunicaciones | Toda la organización |
| | Simulacros de respuesta (ciberdrills) | Seguridad de la Información | Líder del proyecto | Recursos Humanos / TI | Alta Dirección |
| Fase 5: Diseño del plan de recuperación y continuidad | Definición de políticas de respaldo, restauración y contingencia | Área de TI | Comité de Seguridad | Auditoría / Cumplimiento | Alta Dirección |
| | Elaboración del plan de continuidad (BCP) | Coordinador de Continuidad | Comité de Seguridad | Dirección General / Riesgos | Toda la organización |

Fuente: Elaboración Propia

Dado que PRISMA es una microfinanciera con una operación nacional distribuida (10 agencias) y un total de 74 empleados, la estructura del área de Seguridad de la Información debe ser funcional, eficiente y escalable, evitando el sobredimensionamiento, pero cumpliendo con los requerimientos clave establecidos en la matriz RACI del plan de ciberseguridad.

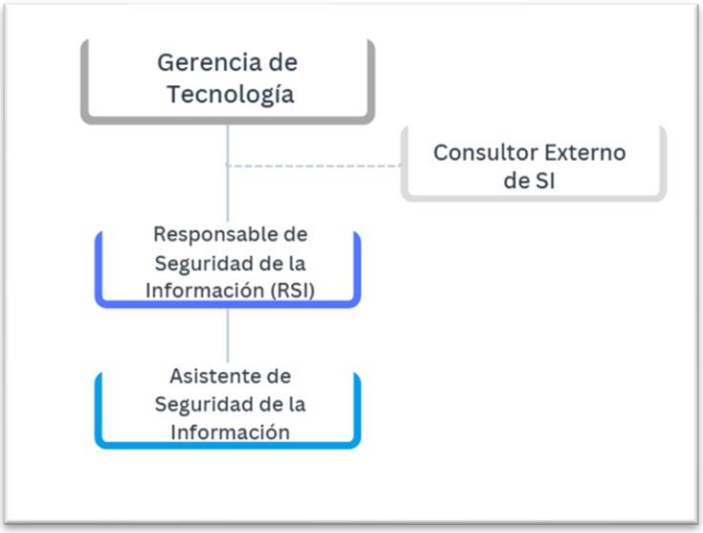


**Figura 28. Estructura sugerida Área de Seguridad de Información PRISMA**

Fuente: Elaboración Propia

La estructura sugerida para el Área de Seguridad de la Información en PRISMA es:

1. Responsable de Seguridad de la Información (RSI):

Reporta a la Gerencia de Tecnología y tiene relación directa con la Alta Dirección y el Comité de Seguridad. Es el líder del área y encargado de la planificación, control y mejora continua del programa de ciberseguridad.

2. Asistente de Seguridad de la Información (rol operativo):

Apoya al RSI en actividades diarias, como:

- Seguimiento de alertas.
- Apoyo en controles técnicos básicos.
- Coordinación de simulacros y campañas de concientización.

3. Comité de Seguridad de la Información (estructura de gobernanza):

No forma parte del área, pero trabaja en conjunto. Está formado por representantes de:

- Alta Dirección.
- TI.

- Auditoría Interna.
- Cumplimiento.

Este comité valida decisiones estratégicas y revisa reportes de incidentes o riesgos.


**Figura 29. Comité Seguridad de la Información PRISMA**

Fuente: Elaboración Propia

4. Roles transversales (por función, no por jerarquía directa):

No pertenecen al área, pero tienen funciones relevantes en seguridad:

- Coordinador de Continuidad: apoyo en temas de BCP/DRP.
- Auditor Interno: evaluaciones de cumplimiento de controles.
- TI (Infraestructura y Soporte): implementación de controles técnicos y gestión de incidentes.
- Recursos Humanos: en concientización, simulacros y control de accesos.

Los beneficios de esta estructura para PRISMA son:

- Ligera y rentable, adecuada para su tamaño.
- Cumple con los roles definidos en la matriz RACI.
- Escalable, puede crecer en roles según se fortalezca la estrategia de ciberseguridad.

## 6.7 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

### 6.7.1 CRONOGRAMA

Con el objetivo de garantizar una adecuada planificación y gestión del estudio para el diseño de la estrategia de ciberseguridad en la Microfinanciera PRISMA, se elaboró una estimación de tiempos basada en la técnica PERT (Program Evaluation and Review Technique). Esta técnica permite calcular una duración estimada más realista para cada actividad, combinando tres escenarios posibles: el optimista (O), el más probable (P) y el pesimista (M).

La tabla a continuación presenta las principales actividades del estudio, junto con sus respectivas estimaciones de duración, la identificación de aquellas que forman parte de la ruta crítica —es decir, aquellas que determinan la duración total del proyecto— y la duración esperada calculada para cada una. Este análisis facilita la priorización de tareas y la optimización de recursos para cumplir con los plazos establecidos en el cronograma general de ejecución.

**Tabla 50. Estimación de duración y ruta crítica**

| Actividad | O | P | M | Ruta Crítica | Duración Estimada (semanas) |
|---|---|---|---|---|---|
| A - Definición del Alcance e Investigación | 2 | 3 | 4 | Sí | 3 |
| B - Recolección de Información | 1 | 2 | 3 | No | 2 |
| C - Evaluación del Nivel de Madurez | 5 | 6 | 8 | Sí | 6.16667 |
| D - Diseño del Plan de Acción | 3 | 4 | 5 | No | 4 |
| E - Desarrollo del Manual Estratégico | 7 | 8 | 9 | Sí | 8 |
| F - Validación y Presentación Final | 2 | 3 | 4 | No | 3 |

Fuente: Elaboración propia

Para representar gráficamente la secuencia lógica, duración estimada y relaciones de dependencia entre las actividades que conforman el estudio de diseño de la estrategia de ciberseguridad en la Microfinanciera PRISMA, se elaboró un diagrama PERT (Program Evaluation and Review Technique).

El diagrama incluye seis actividades principales, ordenadas de forma cronológica, con su respectiva duración estimada en semanas. Estas estimaciones se derivan de un promedio

ponderado basado en los tiempos optimistas (O), más probables (P) y pesimistas (M), calculados mediante la fórmula de PERT:

$$\text{Duración Estimada (TE)} = \frac{O + 4P + M}{6}$$

Las actividades marcadas en color rojo dentro del diagrama PERT representan la ruta crítica del proyecto (A → C → E), la cual define la duración mínima total del estudio en aproximadamente 17.5 semanas. Cualquier retraso en estas tareas afectará directamente la fecha de finalización del proyecto.

Por su parte, las actividades en color azul representan tareas no críticas que pueden manejarse con mayor flexibilidad en el calendario, sin que ello implique un impacto directo en el plazo global, siempre y cuando no excedan su margen de holgura.

El diagrama PERT no solo permitió establecer las dependencias entre tareas, sino también priorizar recursos y tomar decisiones informadas para la asignación eficiente del tiempo y del equipo involucrado. En consecuencia, esta visualización es clave para una adecuada gestión del cronograma del estudio, permitiendo monitorear el progreso de cada fase y anticipar cuellos de botella o retrasos.

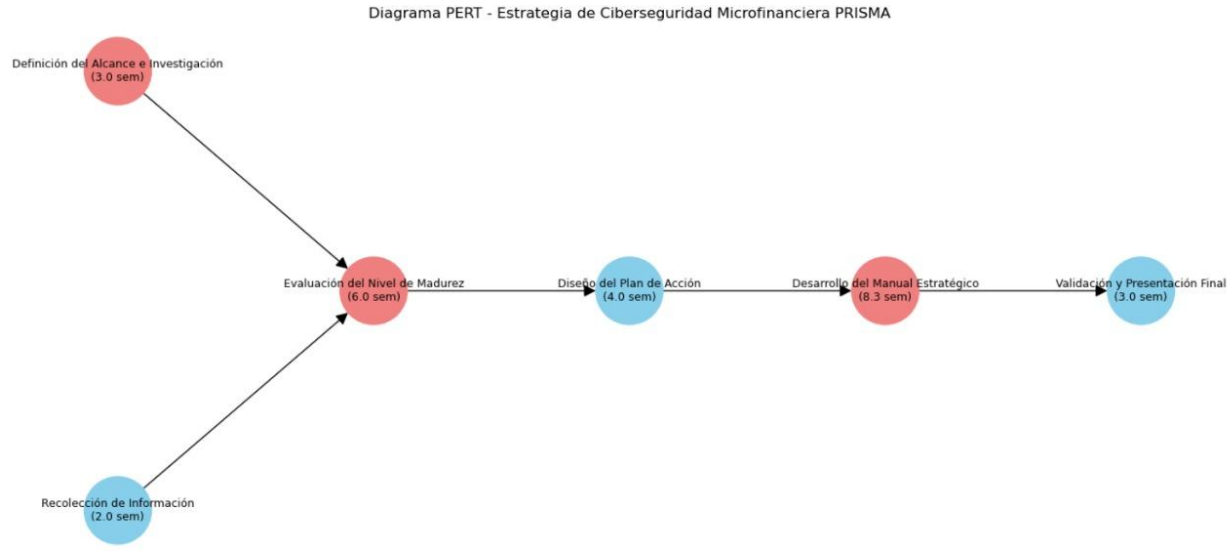


**Figura 30. Diagrama de PERT del proyecto**

Fuente: Elaboración propia

El siguiente diagrama de Gantt representa la planificación temporal del proyecto, cuyo

inicio está programado para el 24 de enero de 2025 y una duración total de 17.5 semanas. En él se detallan las actividades principales, sus tiempos estimados y su secuencia lógica, permitiendo visualizar claramente el flujo de trabajo, así como las tareas que conforman la ruta crítica, es decir, aquellas cuya ejecución en tiempo y forma es esencial para no retrasar la entrega final del proyecto. El cronograma ha sido elaborado con el objetivo de facilitar el seguimiento, control y gestión eficiente del proyecto en cada una de sus fases.

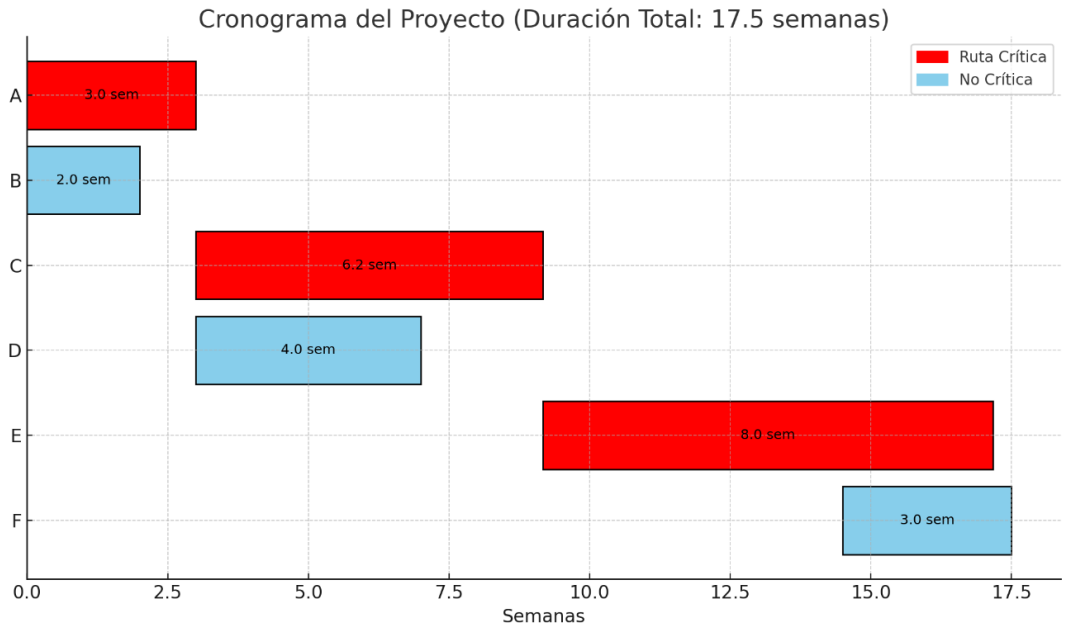


**Figura 31. Diagrama de Gantt del Proyecto**

Fuente: Elaboración propia

A continuación se presenta la tabla que detalla la distribución de fechas para cada una de las actividades del proyecto, calculadas a partir de la fecha de inicio establecida: 24 de enero de 2025. Esta tabla permite identificar con claridad el tiempo de ejecución asignado a cada fase, así como su inicio y finalización estimada, lo cual facilita la planificación y el monitoreo del avance del proyecto.

**Tabla 51. Distribución de actividades del proyecto**

| Actividad | Descripción | Inicio | Fin | Ruta Crítica |
|---|---|---|---|---|
| A | Definición del Alcance e Investigación | 24-ene-25 | 14-feb-25 | Sí |
| B | Recolección de Información | 24-ene-25 | 7-feb-25 | No |

| Actividad | Descripción | Inicio | Fin | Ruta Crítica |
|---|---|---|---|---|
| C | Evaluación del Nivel de Madurez | 14-feb-25 | 29-mar-25 | Sí |
| D | Diseño del Plan de Acción | 14-feb-25 | 14-mar-25 | No |
| E | Desarrollo del Manual Estratégico | 29-mar-25 | 24-may-25 | Sí |
| F | Validación y Presentación Final | 5-may-25 | 26-may-25 | No |

Fuente: Elaboración propia

### 6.7.2 PRESUPUESTO

Como parte del proceso de planificación estratégica para el diseño de la estrategia de ciberseguridad de la Microfinanciera PRISMA, se realizó un análisis integrado de costos basado en la metodología PERT, incorporando no solo la duración estimada de las actividades, sino también los tipos y montos de recursos requeridos para su ejecución.

Este modelo proporciona una visión integral del esfuerzo económico y técnico necesario para llevar a cabo el estudio, estimando un total de USD $19,000, de los cuales el 52% corresponde al desarrollo del manual estratégico, y el 31% a la evaluación del nivel de madurez.

Además, permite identificar las actividades de mayor peso financiero dentro de la ruta crítica (A → C → E), lo que facilita la asignación eficiente de recursos, así como la elaboración de escenarios de ajuste presupuestario ante contingencias.

Este enfoque garantiza una planificación metodológica robusta, con base en tiempos realistas y un presupuesto alineado con las fases clave del proyecto.

**Tabla 52. Presupuesto estimado**

| | Actividad | O | P | M | Ruta Crítica | Tipo Costo | Costo (USD) | Duración Estimada (semanas) |
|---|---|---|---|---|---|---|---|---|
| 0 | A - Definición del Alcance e Investigación | 2 | 3 | 4 | Sí | Recursos humanos | 500 | 3.000000 |
| 1 | B - Recolección de Información | 1 | 2 | 3 | No | Herramientas | 1000 | 2.000000 |
| 2 | C - Evaluación del Nivel de Madurez | 5 | 6 | 8 | Sí | Consultoría | 6000 | 6.166667 |
| 3 | D - Diseño del Plan de Acción | 3 | 4 | 5 | No | Recursos humanos | 500 | 4.000000 |
| 4 | E - Desarrollo del Manual Estratégico | 7 | 8 | 9 | Sí | Herramientas + Recursos | 10000 | 8.000000 |
| 5 | F - Validación y Presentación Final | 2 | 3 | 4 | No | Recursos humanos | 1000 | 3.000000 |

Cálculo PERT con Costos por Tipo (USD)

Fuente: Elaboración propia

## 6.8 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

La matriz de concordancia metodológica representa una herramienta fundamental para verificar la coherencia interna de esta investigación. Su propósito es evidenciar la correspondencia lógica entre los distintos componentes estructurales del estudio, asegurando que el título, los objetivos, las variables, la fundamentación teórica, las técnicas empleadas, los resultados obtenidos y la propuesta final se encuentren debidamente articulados.

A través de esta matriz, se demuestra cómo cada uno de los objetivos específicos dio lugar a una estrategia metodológica particular, sustentada teóricamente y aplicada mediante instrumentos específicos, cuya implementación generó hallazgos relevantes que sirvieron de base para la formulación de conclusiones y la construcción de una propuesta concreta. Asimismo, se refleja cómo la estrategia de ciberseguridad diseñada para la microfinanciera PRISMA responde directamente al diagnóstico obtenido y se alinea con las normas internacionales ISO/IEC 27001:2022 y 27032:2023.

Esta estructura integradora permite validar la solidez científica del trabajo, garantizar su trazabilidad lógica y ofrecer evidencia de que la propuesta se deriva directamente del análisis riguroso de la realidad institucional diagnosticada.

**Tabla 53. Concordancia de la investigación con la propuesta**

| Capítulo I | | | Capítulo II | Capítulo III | | | Capítulo V | Capítulo VI | |
|---|---|---|---|---|---|---|---|---|---|
| **Título de la Investigación** | **Objetivo General** | **Objetivos Específicos** | **Teorías/Metodologías de sustento** | **Variables** | **Poblaciones** | **Técnicas** | **Conclusiones** | **Nombre de la propuesta** | **Objetivos de la propuesta** |
| Diseño de una estrategia de ciberseguridad basada en las normas ISO/IEC 27001:2022 y 27032:2023. Caso: Microfinanciera PRISMA de Honduras, 2025 | Diseñar una estrategia de ciberseguridad para la Microfinanciera PRISMA, basada en un diagnóstico integral de su estado actual y una evaluación del nivel de madurez en el cumplimiento de controles, que permita establecer recomendaciones y medidas alineadas con las normas | 1. Diagnosticar el estado actual de la ciberseguridad en la Microfinanciera PRISMA, evaluando el grado de cumplimiento de sus controles y procesos conforme a los lineamientos de las normas ISO/IEC 27001:2022 e ISO/IEC 27032:2023.<br>2. Determinar el nivel de madurez en ciberseguridad que presenta PRISMA, mediante indicadores | Teoría General de Sistemas.<br>Gestión de Riesgos en Seguridad de la Información.<br>Enfoque Basado en Normas Internacionales.<br>Ciber Resiliencia y Continuidad del Negocio. | Estado actual de la ciberseguridad.<br>Nivel de madurez en ciberseguridad.<br>Estrategia de ciberseguridad diseñada | **Población Total:** 74 colaboradores de PRISMA.<br>**Población Objetivo:** 30 colaboradores con roles claves en ciberseguridad.<br>**Criterios de Inclusión:** 20 colaboradores con antigüedad mínima de 6 meses, acceso a sistemas críticos, gestión de seguridad.<br>**Criterios de exclusión:** 12 colaboradores sin acceso a datos críticos. | <u>Cualitativa:</u> Entrevista semiestructurada a Jefes de Agencias.<br>Cuestionario estructurado basado en la herramienta de MASS ((Maturity Assessment for Security Survey) de LAC4.<br><u>Cuantitativa:</u> Diagnóstico de Seguridad Global.<br>El análisis exploratorio de datos (EDA) y el uso de Pandas/Jupyter | **1)** En cumplimiento del primer objetivo, se concluye que el estado actual de la ciberseguridad en PRISMA presenta brechas relevantes en múltiples dominios de control. De los 93 controles evaluados, un total de 31 controles (33.3%) se encuentran en niveles bajos de madurez.<br>**2)** En relación con el segundo objetivo, se determinó que PRISMA mantiene un nivel de madurez general entre los niveles “Inicial” y “Gestionado”, con 45 controles (48.4%) ubicados en dos | Diseño de una Estrategia de Ciberseguridad para la Microfinanciera PRISMA: Enfoque Basado en Normas ISO/IEC 27001:2022 y 27032:2023. | Evaluar los factores que afectan la protección de la información en la microfinanciera PRISMA.<br>Diseñar estrategias para fortalecer la seguridad de la información, optimizando la gestión de riesgos, la gobernanza y la capacitación del talento humano.<br>Definir un plan de fortalecimiento tecnológico y operativo, alineado con ISO/IEC 27001:2022 e ISO/IEC 27032:2023, para mejorar la |

| Capítulo I | | | Capítulo II | Capítulo III | | | Capítulo V | Capítulo VI | |
|---|---|---|---|---|---|---|---|---|---|
| **Título de la Investigación** | **Objetivo General** | **Objetivos Específicos** | **Teorías/Metodologías de sustento** | **Variables** | **Poblaciones** | **Técnicas** | **Conclusiones** | **Nombre de la propuesta** | **Objetivos de la propuesta** |
| | ISO/IEC 27001:2022 y 27032:2023. | basados en estándares internacionales, con el propósito de identificar brechas, riesgos críticos y oportunidades de mejora.<br><br>3. Diseñar estrategias y controles específicos para el fortalecimiento de la protección de la información en PRISMA, estructurando una propuesta de ciberseguridad alineada con los marcos ISO/IEC 27001:2022 e ISO/IEC 27032:2023. | | | **Muestra Final:** 8 colaboradores seleccionados. | fueron parte del enfoque cuantitativo. | niveles medios.<br>**3)**. Los hallazgos del estudio evidencian que la Microfinanciera PRISMA requiere una estrategia de ciberseguridad estructurada para abordar las brechas críticas identificadas, especialmente en los dominios organizativo y tecnológico, donde más del 33% de los controles evaluados presentan baja madurez. Se constató la necesidad de integrar funciones clave como identificación, protección, detección, respuesta y recuperación, alineadas con ISO/IEC 27001:2022, | | prevención y respuesta ante amenazas cibernéticas. |

| Capítulo I | | | Capítulo II | Capítulo III | | | Capítulo V | Capítulo VI | |
|---|---|---|---|---|---|---|---|---|---|
| **Título de la Investigación** | **Objetivo General** | **Objetivos Específicos** | **Teorías/Metodologías de sustento** | **Variables** | **Poblaciones** | **Técnicas** | **Conclusiones** | **Nombre de la propuesta** | **Objetivos de la propuesta** |
| | | | | | | | ISO/IEC 27032:2023 y el marco NIST CSF. Asimismo, el análisis determinó que el diseño de dicha estrategia debe contemplar fases operativas, indicadores de desempeño, una matriz RACI clara y mecanismos de mejora continua, garantizando su sostenibilidad y pertinencia institucional. | | |

Fuente: Elaboración Propia

# REFERENCIAS BIBLIOGRÁFICAS


Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2022). Journal of Information Security. *Cyber Security Risk Management Frameworks in Financial Institutions: A Comparative Study*, *18*(2), 72-88.

Anderson, R., & Moore, T. (2022). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3.ª ed.). Wiley.

Anderson, R., Moore, T., & Clayton, R. (2023). *The Economics of Information Security*. Cambridge University Press.

BCH. (2024). *Reporte de Seguridad Financiera 2024*. https://www.bch.hn/estadisticas-y-publicaciones-economicas/estabilidad-financiera/informe-de-estabilidad-financiera-%28ief%29

BID. (2023). *Ciberseguridad: Riesgos, políticas y capacidades en América Latina y el Caribe*. BID y Organización de los Estados Americanos (OEA). https://publications.iadb.org/es/ciberseguridad-en-america-latina-y-el-caribe

Bodeau, D., & Graubart, R. (2021). *Cyber Resilience: A Conceptual Framework for Assessment and Design*. MITRE Corporation. https://www.mitre.org/publications/technical-papers/cyber-resilience-a-conceptual-framework-for-assessment-and-design

Calder, A., & Watkins, S. (2022). *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002* (8.ª ed.). IT Governance Publishing.

Castellanos, P., Ramírez, J., & Pineda, L. (2022). *Resilient IT Systems: Data Recovery and Business Continuity in Financial Institutions*. Springer.

CCIT. (2024). *Informe sobre Seguridad Empresarial en Honduras 2024*. https://www.ccit.hn

Centro Criptológico Nacional. (2022). *Aproximación al Marco de Gobernanza de la Ciberseguridad*. https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-

publicos/

CMMI Institute. (2018). *CMMI for Development, Version 2.0*. Carnegie Mellon University. https://www.isaca.org/enterprise/cmmi

Comisión Nacional de Bancos y Seguros. (2022). *Reporte de Inclusión Financiera 2022*. https://www.cnbs.gob.hn/inclusion-financiera/wp-content/uploads/2023/05/Reporte-de-Inclusion-Financiera-2022.pdf

DIGER. (2024). *Reporte de Ciberseguridad en Honduras 2024*. https://diger.gob.hn/reporte-ciberseguridad-2024

DIGER. (2025). *Plan Estratégico de Ciberseguridad 2025*. https://www.diger.gob.hn

eDigital Chile. (2025). *Reporte de Ciberseguridad 2025*. https://enteldigital.cl/reporte-ciberseguridad

European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. Publications Office. https://data.europa.eu/doi/10.2824/764318

Falck, M., & Ordóñez, B. (2009). *Microfinanzas en Honduras: Realidad y retos para la definición de políticas*. CEPAL. https://www.cepal.org/es/publicaciones/5202-microfinanzas-honduras

Figueroa Suárez, J. A., Rodríguez Andrade, R. F., Bone Obando, C. C., & Saltos Gómez, J. A. (2017). Polo del Conocimiento. *La seguridad informática y la seguridad de la información*, *2*(12), 145-155.

Fondo Monetario Internacional (FMI). (2024). *Rising Cyber Threats Pose Serious Concerns for Financial Stability*. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Foro Económico Mundial. (2022). *Informe de Riesgos Globales 2022*. https://www.weforum.org/reports/global-risks-report-2022

Foro Económico Mundial. (2023). *Global Cybersecurity Outlook 2023*. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2023

Fortinet. (2024). *Informe de investigación global sobre la brecha de competencias en ciberseguridad*. Fortinet. https://www.fortinet.com/lat/resources/reports/cybersecurity-skills-gap

GAFILAT. (2016). *Informe de Evaluación Mutua de la República de Honduras*. https://biblioteca.gafilat.org/wp-content/uploads/2024/07/IEMHonduras-CuartaRonda.pdf

Gartner. (2023). *Zero Trust Strategy in Financial Services: Key Insights*.

GlobalSign. (2024). *5 Security Threats Facing Financial Services Industry*. https://www.globalsign.com/en/blog/5-friday-5-security-threats-facing-financial-services-industry

Gobierno de Honduras; Banco Interamericano de Desarrollo, & BID. (2025). *Diagnóstico de la situación actual: Estrategia Nacional de Ciberseguridad* (No. Proyecto HO-L1202-Operación 4942/BL-HO). Gobierno de Honduras / Banco Interamericano de Desarrollo (BID).

González Támara, L. (2017). *Análisis exploratorio de datos. Una introducción a la estadística descriptiva y probabilidad*. https://www.utadeo.edu.co/es/publicacion/libro/editorial/235/analisis-exploratorio-de-datos-una-introduccion-la-estadistica-descriptiva-y-probabilidad

Harán, J. M. (2023). *ESET Security Report 2023: El panorama de la seguridad en las empresas de América Latina*. https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). *Defending against cybersecurity threats to the payments and banking system* (No. arXiv:2212.12307). arXiv. https://arxiv.org/abs/2212.12307

Hays. (2024). *Informe Global sobre Ciberseguridad 2024*. https://www.hays.com.co/informes-destacados/ciberseguridad

Hernández Sampieri, R. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* (2018.ª ed.). McGraw-Hill Interamericana Editores, S.A. de C. V.

Herrera, H. (2020). *Que es el marco de ciberseguridad del NIST - Cyber security Framework. Para que sirve y como empezar.* https://www.hectorherrera.net/2020/07/que-es-el-marco-de-ciberseguridad-del.html

IBM Security. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report

IMF Ciberseguridad. (2024). *Evaluación de Ciberseguridad en Instituciones Financieras de Microfinanzas*. https://imfciberseguridad.com/#/results

IPANDETEC. (2024). *Paso a Paso para una Política de Seguridad Integral en Honduras*. https://ipandetec.org/publicaciones/paso-a-paso-para-una-politica-de-seguridad-integral-en-honduras

ISO, & IEC. (2022a). *ISO/IEC 27001:2022—Information Security Management Systems* (No. ISO/IEC 27001:2022). International Organization for Standardization. https://www.iso.org/standard/27001

ISO, & IEC. (2022b). *ISO/IEC 27032:2023—Cybersecurity Guidelines* (No. ISO/IEC 27032:2023). International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC).

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Expert Systems with Applications. *Cybersecurity Threats in FinTech: A Systematic Review*, *241*(122697). https://www.sciencedirect.com/science/article/pii/S0957417423031998

Kaspersky. (2024). *Kaspersky Security Bulletin 2024* (p. Securelist). https://securelist.com/ksb-2024/

LAC4. (2025). *Capacitación Para Fortalecimiento De Las Capacidades En Ciberseguridad Para Pymes*. LAC4. https://www.lac4.eu/es/event/capacitacion-para-fortalecimiento-de-las-capacidades-en-ciberseguridad-para-pymes/

Linkov, I., Kott, A., & Ferragut, E. (2022). *Cyber Resilience in Critical Infrastructure: Theory and Practice*. Springer.

López, J. A. (2021a). *Protección de datos personales y ciberseguridad en América Latina: Desafíos regulatorios*. Editorial Jurídica Iberoamericana.

López, J. A. (2021b). *Protección de datos personales y ciberseguridad en América Latina: Desafíos regulatorios*. Editorial Jurídica Iberoamericana.

López, J. A. (2022). Journal of Information Security. *Ciberseguridad y cultura organizacional en instituciones financieras*, *12*(3), 115-130.

López, J. A., & Rodríguez, M. A. (2023). Information Security Journal. *Cybersecurity Adaptation and Continuous Improvement Strategies in Organizations*, *29*(1), 77-91.

Mendoza, C., & Castillo, P. (2022a). Gestión de riesgos tecnológicos en el sector financiero: Aplicación de estándares internacionales. *Revista Latinoamericana de Seguridad Informática*, *9*(2), 45-62.

Mendoza, C., & Castillo, P. (2022b). Revista Latinoamericana de Seguridad Informática. *Gestión de riesgos tecnológicos en el sector financiero: Aplicación de estándares*, *9*(2), 45-62.

Monroy, M. de los Á., & Nava, N. (2018). *Metodología de la Investigación* (Grupo Editorial Éxodo).

NIST. (2020). *NIST Special Publication 800-39: Managing Information Security Risk*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-39/final

NIST, G. M. (2024). *The NIST Cybersecurity Framework 2.0* (No. NIST CSWP 29 spa; p. NIST CSWP 29 spa). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.spa

OEA. (2023). *Estado de la Ciberseguridad en América Latina: Retos y Oportunidades*. OEA. https://www.oas.org/es/sms/cicte/ciberseguridad

OEA. (2024). *Ciberseguridad en América Latina y el Caribe: Avances y desafíos*. https://www.oas.org/ext/es/seguridad/prog-ciber

Participación estratégica en ciberseguridad. (2021). *Guía para la elaboración de una estrategia nacional de ciberseguridad*. Unión Internacional de Telecomunicaciones (UIT). https://creativecommons.org/licenses/by-nc/3.0/igo/.

PCCC. (2024). *Iniciativas de fortalecimiento de la seguridad digital en Honduras*.

Peltier, T. R. (2022). *Information Security Risk Analysis*. Auerbach Publications.

Peltier, T., & Sherwood, J. (2023). *Information Security Policies and Strategies for Financial Institutions*. CRC Press.

Pérez, L., & Rodríguez, M. (2023). Journal of Financial Security. *Evolución de las ciberamenazas en la banca digital y estrategias de mitigación*, *12*(1), 55-78.

PRISMA Honduras S.A. (2022). *Plan Estratégico 2022-2026* (p. 43). PRISMA Honduras S.A.

Ramírez, F., & Gómez, R. (2021). Desarrollo de políticas de ciberseguridad en Honduras: Avances y desafíos. *Revista Centroamericana de Tecnología y Sociedad*, *5*(1), 30-49.

Raudales Centeno, C. (2017). *La Brecha Existente en Ciberseguridad en Honduras*. https://www.camjol.info/index.php/INNOVARE/article/view/5571

REDCAMIF. (2023). *Informe de desempeño del sector microfinanciero hondureño 2023*. REDCAMIF / RMH. https://redcamif.org

Rivas Tovar, L. A. (2017). *Elaboración de Tesis: Estructura y Metodología* (Primera). Trillas.

Rodríguez Zambrano, H. M., & Moreno Tamayo, C. H. (2024). Estudios y Perspectivas: Revista Científica y Académica. *Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática*, *4*(1), 159-178.

Sánchez, R. (2010). *Microfinanzas en Honduras*. CEPAL. https://repositorio.cepal.org/handle/11362/5202

Skyhigh Security. (2024). *2024 Gartner Magic Quadrant for Security Service Edge*.

https://www.skyhighsecurity.com/lp/2024-gartner-magic-quadrant-for-security-service-edge.html

Solutions, V. (2025). CMMI: Cumplimiento y certificaciones utilizando la herramienta de gestión de requisitos. *Visure Solutions*. https://visuresolutions.com/es/est%C3%A1ndares-de-salud/software-cmmi/

Stallings, W. (2022). *Cryptography and Network Security: Principles and Practice* (8.ª ed.). Pearson.

Stallings, W., & Brown, L. (2021). *Computer Security: Principles and Practice*. Pearson.

Tipton, H. F., & Krause, M. (2022). *Information Security Management Handbook, Volume 7*. Auerbach Publications.

UNAH. (2023). *Capacitación en ciberseguridad en el sector financiero hondureño*. https://www.unah.edu.hn

UNSTA. (2023). *Matriz Cuestionario ISO 27002:2022*. UNSTA Facultad de Ingeniería.

Verizon. (2024a). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Verizon. (2024b). *Data Breach Investigations Report 2024*. Verizon Communications. https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf

Von Bertalanffy, L. (1968). *General System Theory: Foundations, Development, Applications*. George Braziller.

Von Solms, B., & Van Niekerk, J. (2022). Journal of Cyber Risk Management. *Governance and Cybersecurity Standards in the Financial Sector*, *15*(3), 55-70.

WEF. (2024). *Global Risks Report 2024*. https://www.weforum.org/reports/global-risks-report-2024/

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.

# ANEXOS

## ANEXO 1. Guion de la entrevista semiestructurada.

### Controles Organizativos

***¿Ha recibido formación sobre seguridad en los últimos 12 meses?***

La mayoría de los empleados han recibido capacitación, pero algunos no recuerdan los conceptos clave ni las políticas específicas.

***¿Conoce la política de seguridad de PRISMA y sabe dónde consultarla?***

Aunque la mayoría sabe que existe, no todos recuerdan dónde encontrarla ni han revisado su contenido detalladamente.

***¿Sabe a quién reportar un incidente de seguridad?***

Un buen número de empleados conoce el procedimiento de reporte, pero aún hay confusión sobre a qué departamento acudir en casos específicos.

***¿Conoce las consecuencias de incumplir las políticas de seguridad?***

La mayoría está consciente de que existen sanciones, pero pocos pueden mencionar ejemplos concretos de medidas correctivas aplicadas.

***¿Recuerda algún caso de sanción por incumplimiento de seguridad?***

No todos recuerdan casos específicos, lo que sugiere una falta de divulgación sobre incidentes internos y lecciones aprendidas.

### Controles de Personas

***¿Podría explicar qué es información sensible y cómo debe protegerse?***

Hay un conocimiento general del concepto, pero no todos tienen claridad sobre qué información específica debe protegerse en su rol.

***¿Cómo actuaría ante un correo sospechoso solicitando credenciales?***

La mayoría lo reportaría o ignoraría, pero algunos aún podrían caer en ataques de phishing por desconocimiento o descuido.

***¿Siente que PRISMA promueve una cultura de seguridad?***

Se reconoce el esfuerzo de la empresa, pero se sugieren más ejercicios prácticos y campañas de concienciación.

***¿Qué recomendaciones daría para mejorar la seguridad?***

Los empleados sugieren mayor control en accesos y más formación interactiva con casos reales.

***¿Ha sido víctima o testigo de un intento de phishing, malware o ingeniería social?***

Algunos han recibido correos sospechosos, pero no todos han reportado los intentos de ataque.

**Controles Físicos**

***¿Está permitido el uso de dispositivos personales para acceder a información de PRISMA?***

Algunos empleados desconocen las restricciones, lo que indica la necesidad de reforzar la política de BYOD (Bring Your Own Device).

***¿Cómo almacena y protege la información confidencial?***

Aunque muchos la guardan en repositorios seguros, algunos la almacenan en sus escritorios o dispositivos personales sin cifrado.

***¿Qué medidas toma al trabajar fuera de la oficina?***

Algunos usan VPN y conexiones seguras, pero otros no verifican la seguridad de las redes a las que se conectan.

***¿Cómo maneja la eliminación de documentos físicos o digitales?***

Algunos siguen protocolos adecuados, pero hay empleados que eliminan información sin aplicar medidas de seguridad.

***¿Cómo gestiona sus credenciales de acceso?***

La mayoría usa contraseñas fuertes, pero algunos aún reutilizan claves en múltiples sistemas, lo que representa un riesgo.

**Controles Tecnológicos**

**¿Utiliza contraseñas fuertes y únicas para cada sistema?**

La mayoría lo hace, pero algunos reutilizan contraseñas o las anotan en lugares inseguros.

**¿Ha recibido directrices sobre autenticación multifactor (MFA)?**

MFA está implementado, pero algunos usuarios encuentran incómodo su uso y buscan formas de evitarlo.

**¿Con qué frecuencia actualiza sus dispositivos y aplicaciones?**

La mayoría lo hace cuando el sistema lo solicita, pero algunos posponen las actualizaciones, aumentando el riesgo de vulnerabilidades.

**¿Sabe qué hacer si su equipo es comprometido por malware?**

Algunos reportarían inmediatamente, pero no todos conocen el procedimiento exacto de respuesta ante incidentes.

**¿Conoce las mejores prácticas para la seguridad del correo corporativo?**

La mayoría evita abrir archivos sospechosos, pero no todos verifican los remitentes antes de interactuar con los correos recibidos.

## ANEXO 2. Ítems Diagnóstico de Seguridad Global

| **Grupo 5: Gestión y Organización de la Seguridad** | |
|---|---|
| Control | Pregunta |
| 5.1 - Políticas de SI | ¿Cuál es el estado actual de la política de seguridad de la información en PRISMA y qué medidas se han tomado para su aprobación, comunicación y revisión periódica? |
| 5.2 - Roles y responsabilidades de la SI | ¿Cómo se han definido y asignado las responsabilidades en materia de seguridad de la información en los diferentes niveles de la organización? |
| 5.3 - Segregación de tareas | ¿Qué estrategias han implementado para garantizar la separación de funciones y evitar conflictos de interés en los procesos críticos? |
| 5.4 - Responsabilidades de la dirección | ¿Cómo se asegura la alta dirección de que la seguridad de la información sea una prioridad en la estrategia organizacional? |
| 5.6 - Contacto con grupos de interés especial | ¿PRISMA participa en foros o asociaciones especializadas en seguridad de la información? ¿Cómo se utilizan estos espacios para mejorar la postura de seguridad? |
| 5.10 - Uso de la información y activos asociados | ¿Qué normas y procedimientos existen para regular el uso aceptable de la información y los activos asociados dentro de PRISMA? |
| 5.19 - SI en las relaciones con proveedores | ¿Cómo se integran los requisitos de seguridad de la información en la selección y gestión de proveedores? |
| 5.20 - Abordar la SI en acuerdos con proveedores | ¿Qué cláusulas de seguridad de la información se incluyen en los contratos con proveedores y cómo se asegura su cumplimiento? |
| 5.22 - Seguimiento, revisión y gestión de cambios de servicios de proveedores | ¿Cómo se monitorea y revisa el cumplimiento de las medidas de seguridad en los servicios de terceros? |
| 5.25 - Evaluación y decisión sobre eventos de SI | ¿Qué criterios se utilizan para evaluar y clasificar eventos de seguridad de la información? ¿Cómo se decide cuándo un evento debe tratarse como un incidente? |
| 5.30 - Preparación de las TIC para la continuidad de negocio | ¿Qué planes y estrategias han sido implementados para garantizar la continuidad de los servicios tecnológicos ante una interrupción crítica? |
| 5.31 - Identificación de requisitos legales, estatutarios, regulatorios y contractuales | ¿Cómo se asegura PRISMA de cumplir con los requisitos legales y regulatorios en materia de seguridad de la información? |
| 5.32 - Derechos de propiedad intelectual | ¿Qué políticas y controles existen para proteger la propiedad intelectual y la información confidencial de la organización? |

| | |
|---|---|
| 5.34 - Privacidad y protección de la información de identificación personal (PII) | ¿Qué medidas se han adoptado para garantizar la protección de los datos personales de clientes y empleados? |
| 5.36 - Cumplimiento de políticas y estándares de SI | ¿Cómo se mide y revisa el cumplimiento de las políticas y estándares de seguridad de la información dentro de PRISMA? |
| | |
| **Grupo 6: Seguridad en el Personal** | |
| Control | Pregunta |
| 6.6 - Acuerdos de confidencialidad o no divulgación | ¿Cómo se gestiona la firma y actualización de acuerdos de confidencialidad para empleados y terceros? ¿Se realizan revisiones periódicas de estos acuerdos? |
| | |
| **Grupo 7: Seguridad Física** | |
| Control | Pregunta |
| 7.1 - Perímetro de seguridad física | ¿Qué controles físicos se han implementado para proteger las instalaciones donde se maneja información crítica? |
| 7.2 - Ingresos físicos | ¿Cómo se controlan los accesos físicos a las instalaciones y qué mecanismos existen para evitar accesos no autorizados? |
| 7.3 - Asegurar oficinas, salas e instalaciones | ¿Qué medidas de seguridad física se aplican en las oficinas y espacios donde se almacenan datos sensibles? |
| 7.4 - Monitoreo de seguridad física | ¿Qué mecanismos de monitoreo y vigilancia existen para detectar y responder a amenazas físicas en las instalaciones? |
| 7.5 - Protección contra amenazas físicas y ambientales | ¿Qué estrategias se han implementado para mitigar riesgos físicos y ambientales que puedan afectar la infraestructura de la organización? |
| 7.6 - Trabajo en áreas seguras | ¿Qué procedimientos deben seguir los empleados que trabajan en áreas restringidas o de acceso controlado? |
| | |
| **Grupo 8: Operaciones y Controles Técnicos** | |
| Control | Pregunta |
| 8.31 - Separación de entornos de desarrollo, prueba y producción | ¿Cómo se asegura PRISMA de que los entornos de desarrollo, pruebas y producción estén adecuadamente separados y protegidos? |

## ANEXO 3. Ítems Herramienta MASS

### Tabla 54. Escala de Evaluación de Atributos - Herramienta MASS

| Color | Descripción del Nivel | Interpretación |
|---|---|---|
| **Rojo** | Aún no se ha hecho nada significativo para la situación descrita en el atributo. | Inexistente / No iniciado |
| **Naranja** | El atributo coincide parcialmente con la descripción de la situación, pero aún presenta deficiencias significativas. | Inicial |
| **Amarillo** | El atributo está razonablemente abordado con su organización, pero tiene algunas deficiencias. | Parcialmente implementado / Básico |
| **Verde** | El atributo es completamente verdadero en el contexto de su organización. | Alto nivel de cumplimiento / Optimizado |
| **Celeste** | No responde. | Sin respuesta / No evaluado |
| **Celeste** | No corresponde. | Atributo no aplicable |

Fuente: Adaptado de la herramienta MASS – (European Union Agency for Cybersecurity., 2022)

***ISMS - Gestión de seguridad***

Evaluación de la situación del establecimiento y desempeño del sistema de gestión de seguridad de la información de la organización, incluyendo la participación de la gerencia, la distribución de responsabilidades y la asignación de recursos y mapeo de activos

1. Las medidas de seguridad de la información y la documentación se han actualizado durante los últimos 3 años.

2. Se reconoce la necesidad de gestionar la seguridad de la información y tiene objetivos específicos.

3. El proceso de la gestión de seguridad de la información se inicia a nivel gerencial (decisión, protocolo)

4. Se han mapeado los procesos comerciales críticos y los activos relacionados.

5. Existe una política general de seguridad de la organización

6. Se asignan los roles y responsabilidades de la seguridad de la información

7. El plan de implementación de medidas de seguridad se documenta con fines de trazabilidad y comparabilidad.

8. Se han asignado recursos suficientes (dinero, personal, activos) para implementar el sistema de gestión de seguridad de la información.

9. El plan de implementación de seguridad de la información se actualiza en caso de cambios (nuevos procesos de negocio, componentes de TI, organización, amenazas, etc.) e incidentes.

10. La seguridad de la información está integrada en todos los procesos y los administradores de procesos (personas responsables designadas) supervisan la implementación de las medidas en sus procesos

11. Se realizan revisiones regulares de la gestión de la seguridad de la información (se mantienen protocolos)

12. Se han elaborado políticas de seguridad más detalladas en áreas más específicas (gestión de red, externalización de servicios, control de malware, copia de seguridad de datos, correo electrónico, uso de dispositivos móviles, gestión de firewalls).

***ORP - Organización y personal***

Evaluación de la situación de la gestión de la seguridad de la información, incluyendo reglas de uso de computadoras y otros dispositivos, política de personal, gestión de identidades y derechos de acceso y capacitación.

1. Se realiza formación introductoria sobre ciberseguridad.

2. Se evitan las soluciones ad hoc en la gestión del acceso.

3. Los roles de las responsabilidades definidas de la seguridad de la información son establecidas como reglas de respaldo, operación de medios, mantenimiento y trabajo de reparación, protección de datos y preparación.

4. Se asignan responsabilidades de seguridad para toda la información, procesos de negocio, aplicaciones y componentes de TI.

5. Los gerentes y gerentes de productos conocen las condiciones de la estructura legal, requerimientos y requerimientos protección relacionados con sus procesos de negocios y proveedores de servicios

6. Se establecen reglas de reemplazo temporal de empleados (incluyendo garantizar habilidades, canales de comunicación y acceso adecuado).

7. La política de personal se ocupa de la gestión de todo el ciclo de vida del empleado, incluida la gestión de accesos (nuevo empleado, salida, reemplazo, contratista externo)

8. Todos los empleados externos han firmado acuerdos de confidencialidad (Contracto externo)

9. Cuentas de usuarios son vinculadas a una persona en específico, los derechos de acceso son asignados de acuerdo con el rol del usuario y documentados como perfil de derechos.

10. Se ha establecido la calidad de la contraseña

11. Los empleados conocen a quien y qué canales dirigirse en caso de problema de la seguridad de la información o un incidente

12. Chequeos regulares aseguran que las cuentas de los usuarios estén actualizadas y que los grupos de usuarios y los permisos de perfiles se alineen con las tareas de los usuarios y los requerimientos de la seguridad de la información

13. Además de la formación introductoria en materia de seguridad, los empleados también reciben instrucciones en caso de cambios y con ejercicios regulares, al menos en lo referente al uso de contraseñas, control de exactitud de datos y fuentes, y procesamiento interno de la información

14. El acceso a todos los sistemas y servicios de TI está protegido mediante la identificación y autenticación de los usuarios (incluidos otros sistemas de TI).

15. Las contraseñas no se almacenan en texto simple en el sistema informático ni en la aplicación.

16. Las contraseñas de las cuentas de usuario y de sistema estándar del sistema informático o de la aplicación se han modificado lo antes posible. Las contraseñas predeterminadas se han sustituido por contraseñas suficientemente seguras y se han desactivado las cuentas innecesarias.

17. La organización tiene una visión general de las herramientas y sistemas utilizados (incluida la automatización industrial y el Internet de las cosas) y de los equipos a lo largo de su ciclo de vida.

18. Se utiliza un servicio de autenticación central con los procedimientos establecidos para la gestión de identidad y derechos de acceso.

19. Los usuarios son sometidos periódicamente a pruebas de concienciación sobre seguridad de la información, cuyo análisis de los resultados se tiene en cuenta en la elaboración del plan de formación en seguridad de la información.

20. Se han realizado análisis de riesgos y se ha coordinado con la gerencia las excepciones a la política de seguridad. Las excepciones se revisan periódicamente y se registra la necesidad de excepciones de forma reproducible.

***CON - Conceptos y metodologías***

Evaluación de la situación de los conceptos básicos de seguridad de la información de la organización aplicados a todas las demás áreas, incluidas las copias de seguridad, el archivo, el desarrollo, los principios de protección de datos personales, los procedimientos relacionados con la criptografía y la concienciación. Además, se revisan los acuerdos de intercambio de datos entre los socios con quienes se intercambian datos.

1. Se realiza copia de seguridad de los datos.

2. Se ha designado a la persona que desempeñará la función de especialista en protección de datos.

3. A la hora de elegir y utilizar herramientas criptográficas, en los estudios se controlan los algoritmos aprobados y las longitudes de clave (se sabe dónde verificar).

4. Se han realizado evaluaciones de impacto del tratamiento de datos personales, se han definido las medidas necesarias y se ha elaborado una política de privacidad.

5. Se han elaborado unas reglas de copia de seguridad de datos y un plan de copia de seguridad de datos que fijan la frecuencia, los períodos de retención y los principios de almacenamiento

6. Se determina qué información puede transmitirse a qué socios y a través de qué canales de intercambio de datos.

7. Se ha acordado con el desarrollador del software el cumplimiento de los requisitos de seguridad de la información, incluida la higiene de los datos de prueba.

8. Se ha establecido un procedimiento de almacenamiento y destrucción de datos que define, entre otras cosas, las condiciones de marcado y eliminación de datos y los períodos de conservación (incluidos los límites mínimos y máximos).

9. La restauración a partir de una copia de seguridad de datos se prueba periódicamente.

10. Los sistemas de respaldo están separados físicamente (por ej., ubicación diferente) y lógicamente (por ej., segmento de red/zona de firewall diferente) de las fuentes de datos (servidores).

11. Si se han realizado cambios críticos para la seguridad en las bibliotecas de software utilizadas en el software pedido o desarrollado en la organización, el desarrollador realiza los cambios necesarios en el software y entrega los parches correspondientes al cliente.

12. Se han mapeado los sistemas informáticos y las conexiones que utilizan criptografía

Información adicional

13. Para el intercambio regular de información con otras instituciones se han celebrado acuerdos que abordan, entre otras cosas, los requisitos de seguridad de la información de cada parte y la prueba de su cumplimiento.

14. Al utilizar copias de seguridad remotas, los datos contenidos en la copia de seguridad se cifran tanto en la ubicación de la copia de seguridad como durante la transferencia de datos. El acceso a las copias de seguridad se concede únicamente con autenticación segura. Se conoce la ubicación física de los datos.

15. En las aplicaciones web, se implementa la autenticación multifactor para la autenticación de usuarios.

***OPS - Operaciones***

Evaluación de la situación de la gestión de las operaciones de TI de la organización, independientemente de los componentes específicos de hardware, software o red. Esto incluye la gestión y documentación de los servicios en la nube y el trabajo remoto.

1. Se dispone de personal competente para realizar trabajos de administración del sistema

2. Se registran los eventos de seguridad de los sistemas y aplicaciones de TI

3. Se utilizan programas anti-malware

4. Se monitorean las necesidades de actualización y se verifican las actualizaciones antes de su implementación

5. Existen reglas y acuerdos sobre cómo se mantienen las herramientas de trabajo en el caso del trabajo remoto, incluida la actualización, el respaldo y una conexión segura durante el mantenimiento.

6. Se han acordado los términos del servicio para realizar mantenimiento remoto

7. Para los servicios externalizados se han pactado en los contratos normas que incluyen requisitos de seguridad y la supervisión de su cumplimiento.

8. La implementación del servicio en la nube se documenta con un análisis del cumplimiento de los requisitos de seguridad y una evaluación de impacto.

9. Antes de la subcontratación, se definen y documentan las reglas para garantizar la seguridad del proveedor de servicios (incluida la cadena de suministro).

10. Se mantienen actualizadas las reglas para la sustitución de los responsables de TI en una situación de emergencia (contactos, disponibilidad, acceso, calificaciones)

11. Las cuentas privilegiadas para mantenimiento informático son personales y solo se utilizan para operaciones administrativas. Las actividades realizadas con cuentas privilegiadas quedan registradas

12. Las actualizaciones se realizan periódicamente y las actualizaciones de seguridad se aplican lo antes posible después del lanzamiento y la prueba de la actualización de seguridad. Si la actualización no se instala, se documenta la decisión correspondiente.

13. La recopilación de registros tiene objetivos claros y las marcas de tiempo utilizadas en los registros se sincronizan para una revisión periódica de los registros

14. Se comprueba periódicamente la solidez de los mecanismos criptográficos y de las claves criptográficas utilizadas

15. Antes de la implementación del software, éste se aprueba mediante pruebas separadas del entorno de trabajo y el resultado/decisión se documenta

16. Los administradores de TI se capacitan en temas de seguridad de sistemas, servicios administrados y protocolos. Monitorean la información sobre vulnerabilidades de seguridad y actualizaciones de seguridad y reaccionan si es necesario.

17. Se supervisa y evalúa la gestión del cambio, y se considera y comunica a las partes su impacto en los procesos de negocio.

18. Una infraestructura de registro central está protegida contra el acceso no autorizado, se analizan los datos de registro y se emiten alertas en caso de inconsistencias.

19. Se ha elaborado y probado un plan de emergencia en caso de fallo de la gestión remota; el plan se revisa y actualiza periódicamente.

20. Las medidas de seguridad de los proveedores de servicios externos son evaluadas periódicamente por un auditor independiente.

21. Se elabora un plan de acción para abordar los riesgos específicos de la nube al utilizar este tipo de servicios. El plan de acción está actualizado y cumple con los términos de servicio tanto del proveedor de servicios en la nube como de la red.

***DER - Detección y reacción***

Evaluación de la situación de la gestión de incidentes de seguridad, actividades relacionadas (incluida la investigación forense de TI), auditorías y preparación para emergencias (incluidos ejercicios).

1. Si se informa de un incidente de seguridad, se responde siguiendo las reglas acordadas.

2. Se ha reconocido la obligación de auditoría de seguridad de la información y se ha designado al responsable.

3. Se ha creado una guía de primeras medidas en caso de un incidente de seguridad, que incluye, entre otras cosas, los roles de las personas y los canales de comunicación, así como la información de contacto y las responsabilidades de

las personas responsables (incluida la composición del grupo directivo y las condiciones para convocarlo)

4. Se ha creado una estrategia de escalada y un procedimiento de comunicación para eventos de seguridad más amplios (incluidos CERT nacionales, DPA (Autoridad de Protección de Datos) y Policía).

5. Se monitorean fuentes externas (incluidas las notificaciones CERT nacionales) para el análisis de información y la evaluación de riesgos (informes).

6. Se ha creado un canal para informar eventos de seguridad, y todos los eventos de seguridad se registran en el registro de eventos de seguridad

7. Los dispositivos afectados por incidentes de seguridad se aíslan para evitar la escalada de riesgos, se respaldan y se conservan como evidencia para un análisis posterior

8. Al reutilizar dispositivos afectados por un incidente de seguridad, se verifica la integridad de los datos respaldados, se cambian todas las contraseñas del dispositivo y se realizan pruebas de seguridad y funcionalidad (con el usuario).

9. Se realiza un seguimiento y análisis periódico de los registros, se implementan alarmas automáticas y se documentan los resultados de las inspecciones de los sistemas de detección (IDS, NIDS, etc.).

10. Las funciones de gestión de seguridad y gestión de incidentes tienen procedimientos uniformes para evaluar y clasificar incidentes de seguridad y otras interrupciones (por ejemplo, fallas de TI).

11. En la infraestructura de registro central también es posible analizar eventos de seguridad posteriormente (los registros se almacenan durante al menos un año)

12. Al documentar un incidente de seguridad, se registran todas las acciones realizadas junto con el tiempo de ejecución y se almacenan los datos de registro de los componentes afectados. Además, se elabora un informe del incidente de seguridad y se presenta al grupo destinatario o a la dirección con las modificaciones necesarias.

13. Se ha elaborado e implementado un plan para realizar auditorías periódicas internas y externas de seguridad de la información (incluidos los ejecutores designados) y se ha presentado para revisión de la gerencia como parte de la futura planificación presupuestaria para la seguridad de la información

14. Se analizan los resultados de la auditoría de seguridad de la información y se agregan las acciones necesarias al plan de implementación de seguridad de la información

15. Se ha creado un manual de emergencia que cubre los procesos críticos y se prueba periódicamente con los empleados

***APP - Applications***

Evaluación de la situación del software, groupware, servicios de directorio y gestión de software de suscripción, incluidas configuraciones seguras de actualizaciones, accesos basados en necesidades y registro.

1. A medida que se implementan las aplicaciones, se monitorean y restringen los permisos otorgados a las aplicaciones.

2. Sólo los administradores designados están autorizados a administrar aplicaciones, groupware y servicios de directorio.

3. Se implementa y utiliza software antimalware en los servidores de correo electrónico para detectar spam y contenido malicioso en correos electrónicos entrantes y salientes y

4. Se han establecido reglas para los servicios de directorio.

5. Se requiere autenticación para acceder a recursos de aplicaciones web no públicos (incluidas las aplicaciones web internas).

6. Una persona específica es responsable de administrar los nombres de dominio DNS de una organización.

7. Se han creado listas de requisitos (incluidos los requisitos de seguridad) para el software y las aplicaciones, que se prueban antes de su implementación.

8. El procesamiento de datos personales en un sistema de IA público está prohibido, o existe una evaluación de impacto positiva documentada para el procesamiento de datos personales con IA

9. Los navegadores web están actualizados en todos los dispositivos y utilizan una lista actualizada de certificados raíz (CA) confiables.

10. Antes de introducir la aplicación móvil, los derechos de acceso a la aplicación estaban restringidos únicamente a aquellos necesarios para el trabajo

11. Las aplicaciones web tienen acceso limitado a los archivos de un árbol de directorios específico (directorio raíz web). No se puede acceder a los recursos ubicados fuera del directorio web. Se han desactivado las funciones que proporcionan listados de directorios

12. Se utiliza una conexión segura (por ej., TLS) para la autenticación del usuario en los servicios y aplicaciones web

13. Cuando los datos se guardan en el servidor de archivos, se analizan en busca de malware

14. Los nombres de dominio de la organización se renuevan periódicamente y oportunamente

15. Las herramientas y los clientes de groupware (por ejemplo, Outlook, Office Suite, chats, calendarios, CRM) están preconfigurados para el usuario

16. Se ha capacitado a los usuarios para utilizar equipos de videoconferencia y garantizar que solo participen las partes acordadas.

17. Para proteger los documentos contra modificaciones durante el transporte (por ej., por correo electrónico), deberán estar firmados o sellados digitalmente

18. El acceso al servidor del servicio de directorio está restringido desde Internet.

19. Las actividades del servicio de directorio se controlan y registran, y los datos de registro se revisan periódicamente. Los registros se almacenan durante al menos un año.

20. La seguridad de las aplicaciones web y de los servidores se comprueba periódicamente mediante pruebas de penetración (por ej., durante cada auditoría).

21. A los usuarios se les asignan límites de volumen o cuotas en el servidor de archivos.

22. El dominio de espacios de nombres está claramente dividido en partes públicas e internas cuando se utiliza el mismo nombre de dominio

23. Los sistemas de bases de datos se revisan periódicamente. La revisión incluye al menos: estado de la documentación, configuración, medidas de seguridad, configuración de monitoreo, integridad de los componentes y anomalías detectadas en los registros.

24. Se advierte a los usuarios que no deben recibir correos electrónicos no solicitados de remitentes desconocidos, responder a dichos correos electrónicos y abrir enlaces y archivos adjuntos en los correos electrónicos

25. Los productos y servicios de software usados se incluyen en la lista de inventario y solo se pueden utilizar siguiendo las condiciones de la licencia

26. Los equipos de videoconferencia se gestionan y supervisan periódicamente

***SYS - Sistemas de TI***

Evaluación del estado de las soluciones de hardware y su gestión (incluida la configuración, la supervisión y la gestión), como servidores, computadoras, tabletas, teléfonos, medios de datos extraíbles y soluciones de virtualización

1. Sólo las personas autorizadas tienen acceso (físico y a través de la red) a los servidores

2. En los servidores se utiliza software de protección contra malware

3. Las impresoras y los dispositivos de impresión multifunción se colocan en un lugar visible para otros empleados y no permiten el acceso de invitados no acompañados.

4. Sólo los usuarios autorizados pueden utilizar los dispositivos de los clientes

5. Se documenta la configuración del software, los servicios y las cuentas del servidor

6. Para los equipos cliente, se ha decidido qué servicios en la nube se pueden utilizar y en qué medida

7. Sólo los administradores del sistema tienen derecho a acceder a los archivos del sistema de los servidores

8. El manual de seguridad de las computadoras cliente y los dispositivos inteligentes define las responsabilidades y los derechos de los administradores y usuarios del sistema, los principios relacionados con el acceso, los procedimientos de respaldo y la respuesta a eventos de seguridad.

9. Los usuarios se autentican en los servidores únicamente a través de cuentas de usuario personalizadas.

10. La comunicación de datos de los servidores virtuales está protegida mediante mecanismos de seguridad (por ej., cortafuegos) y la comunicación está supervisada.

11. La instalación automática de actualizaciones se activa en el sistema operativo y el software estándar del computador del cliente, que comprueba la disponibilidad de actualizaciones al menos diariamente.

12. Los dispositivos que no reciben actualizaciones de seguridad quedan fuera de uso o aislados en un segmento de red separado.

13. En todos los ordenadores portátiles está activado un firewall personal.

14. El acceso a la gestión de la configuración de las impresoras y dispositivos de impresión multifuncionales está restringido únicamente a los administradores.

15. El acceso de los dispositivos de Internet de las cosas (IoT) a la red interna está restringido, lo que permite el intercambio de datos solo con un sistema específico necesario (por ej., cámaras de vigilancia y sistema de gestión de edificios). El acceso hacia y desde otras redes (incluida Internet) está bloqueado.

16. A los empleados se les capacita sobre qué datos se pueden almacenar en soportes de datos extraíbles y bajo qué condiciones se permite retirarlos de la organización.

17. Existe la disposición a recibir datos cifrados en formato CDOC (incluido el intercambio de códigos de identificación personal o códigos de registro de la organización, garantizando la seguridad de los datos (malware, componentes activos, etc.) antes de utilizar los datos descifrados).

18. Antes de implementar un servidor, se elabora un plan de uso del servidor, en el que se definen el propósito de la implementación, los requisitos de hardware, la integración con otras aplicaciones (por ejemplo, servicios de directorio), el registro, la supervisión, la actualización de los componentes de TI y la organización de las copias de seguridad

19. Todos los servidores están conectados a un sistema de alimentación ininterrumpida (UPS) con suficiente capacidad y duración de batería, que se comprueba periódicamente.

20. En los servidores sólo se instalan los servicios necesarios para cumplir el propósito de un servidor

21. Se documentan las pruebas periódicas de seguridad del servidor

22. Todos los cambios de configuración del servidor y las acciones de seguridad se pueden rastrear mediante documentación (por ejemplo, registro automático).

23. La implementación del plan de recuperación ante desastres del servidor se practica periódicamente (protocolizado).

24. Los sistemas de monitorización informan inmediatamente al personal operativo cuando se superan los valores límite prescritos o cuando se producen averías

25. No se utilizan el micrófono ni la cámara de los ordenadores sin el consentimiento del usuario. Solo se conectan a los ordenadores los dispositivos autorizados. Los dispositivos habilitados están documentados

26. Las computadoras cliente están conectadas al sistema de monitoreo central

27. Para las computadoras de los clientes se ha creado una referencia de instalación. Durante la instalación, se clona

una instalación de referencia preconfigurada en el equipo del cliente. Una instalación de referencia incluye todos los cambios de configuración, actualizaciones y parches de seguridad, y se prueba y documenta previamente.

28. Las computadoras portátiles están encriptadas.

29. La configuración de seguridad de los equipos cliente se administra de forma centralizada; el usuario no puede cambiarla de forma independiente

30. El acceso desde dispositivos móviles a la intranet está encriptado a través de una red privada virtual (VPN).

31. Los nombres de los dispositivos no proporcionan información sobre la identidad del usuario y no contienen elementos que hagan referencia a la organización (por ej., teléfonos móviles).

32. Las interfaces de radio de los teléfonos móviles (por ej., WLAN o Bluetooth) se desactivan cuando no se necesitan o durante períodos de no uso.

***IND - TI Industrial***

Evaluación de la situación de la gestión segura (configuración y monitorización) y de la seguridad de ordenadores de control de máquinas y herramienta, sensores, robots, equipos de laboratorio y de diagnóstico, sistemas de almacén y otros sistemas informáticos industriales.

1. Se han mapeado los sistemas de control de operaciones y procesos y la automatización industrial, se ha asignado el responsable de ello y, si hay un socio de gestión externo, se ha firmado un contrato de servicios.

2. La infraestructura tecnológica operativa y la automatización industrial son parte de una política de seguridad integrada.

3. Se documentan los socios de intercambio de datos y las categorías de datos de los componentes de automatización industrial.

4. Se ha celebrado un contrato de servicios de soporte con el proveedor de los dispositivos industriales (por ejemplo, dispositivos robóticos).

5. Se especifica y documenta qué datos y eventos de los componentes de tecnología operativa y de automatización industrial se registran, durante cuánto tiempo se conservan los datos de registro y quién puede acceder a los registros.

6. Se han reemplazado las contraseñas predeterminadas de las tecnologías de operación industrial y se han sincronizado los relojes de todos los componentes

7. Se desactivan o desinstalan las interfaces, servicios y funciones innecesarios de la tecnología operativa y de los componentes de automatización industrial

8. El acceso de la automatización industrial a las interfaces de mantenimiento está limitado a personas autorizadas, está documentado y sigue el acuerdo central de gestión de derechos de acceso

9. Los componentes de automatización industrial están separados de los sistemas informáticos de la oficina y la comunicación de los componentes con otros componentes se basa en las necesidades y es lo mínima posible.

10. Al realizar el mantenimiento remoto de un dispositivo industrial (por ej., robótico), la persona que realiza el mantenimiento no puede acceder a otros sistemas o dispositivos de la organización.

11. Los componentes inteligentes y de hardware que pertenecen a los sistemas de automatización de seguridad y se utilizan junto con ellos no se utilizan para otros fines (incluido el uso personal) y están protegidos contra el acceso físico no autorizado

12. El mantenimiento remoto de la tecnología operativa se realiza únicamente desde las cuentas de usuario registradas en el servicio de directorio administrado de forma centralizada

13. Se realizan copias de seguridad periódicas de los programas de automatización industrial, de la configuración y de los datos, incluso antes y después de realizar cambios en el sistema

14. Los protocolos de comunicación de datos seguros protegen los datos de medición y control transmitidos a través

de redes públicas.

15. Los sensores se calibran periódicamente y la calibración queda documentada

16. Se definen los límites de valores de las variables de automatización de seguridad y se emite una alarma cuando se alcanza el límite

***NET - Redes y comunicación***

Evaluación de la situación de la red, componentes de la red, gestión de las comunicaciones telefónicas, puntualidad del proyecto de red informática, actualización periódica y se evitan soluciones obsoletas e inseguras (contraseñas predeterminadas y soluciones no soportadas por el fabricante)

1. Se asigna un rol específico para la administración de una red de computadoras

2. Se ha preparado un diagrama de red.

3. El diseño de la red y sus principios se han documentado y actualizado (incluido el diagrama de red y las descripciones de las subredes) en los últimos 3 años.

4. Hay instrucciones documentadas para administrar y operar dispositivos de red (incluidas las reglas del firewall).

5. Se ha elaborado una reglamentación sobre el uso de la red local inalámbrica que especifica a qué redes internas y externas y bajo qué condiciones se puede conectar el cliente de la red local inalámbrica.

6. La documentación se actualiza inmediatamente después de que se realizan los cambios en la red.

7. La red se encuentra segmentada en diferentes zonas de seguridad

8. Se han cambiado las contraseñas predeterminadas para todos los componentes de la red

9. Se realizan copias de seguridad de las soluciones de gestión de red (archivos de configuración, registros e informes de eventos)

10. La red interna sólo se puede acceder a través de un canal de comunicación seguro (VPN)

11. Se utiliza un mecanismo criptográfico actualizado para proteger las comunicaciones inalámbricas (por ejemplo, WPA3). Se bloquea el uso de protocolos de cifrado fáciles de descifrar, como WEP y WPA.

12. Todos los relojes de gestión de red y de los componentes de red relacionados están sincronizados y utilizan la misma zona horaria

13. Durante la inspección periódica y las pruebas de penetración de la gestión de red y de los componentes de red, se comprueba la actualidad de la documentación de gestión de red, el cumplimiento de la situación actual y los procedimientos reales, y se evalúa la sostenibilidad y la seguridad de la infraestructura de gestión de red (>1 protocolo de revisión por año).

14. Los eventos importantes relacionados con los componentes de red y las herramientas de gestión de red se notifican automáticamente al personal de TI responsable inmediatamente después del evento.

15. Se ha creado una subred (DMZ) que separa la red confiable de la que no lo es y aloja servidores proxy para permitir el acceso mutuo a servidores, servicios y aplicaciones accesibles desde Internet.

16. El software heredado está aislado en un segmento de red separado.

17. Se monitorean los componentes de la red y se almacenan los registros (al menos 1 año).

***INF - Infraestructura***

Evaluación de la situación de la gestión de la seguridad de edificios, salas, cableado, puestos de trabajo móviles, soluciones informáticas para vehículos y casas inteligentes. Se consideran el cumplimiento de los requisitos de seguridad contra incendios de los edificios, los requisitos especiales de seguridad y la ubicación en instalaciones de

las salas protegidas, así como la inclusión de infraestructuras inteligentes en la política de seguridad.

1. Los edificios cumplen los requisitos de seguridad contra incendios (detectores de humo, sistema central de alarma contra incendios, extintores manuales) y se han implementado medidas antirrobo.

2. Si en el proceso de gestión técnica del edificio participa un socio externo (ej. el propietario del edificio de oficinas), todos los derechos, obligaciones, tareas y competencias del socio se fijan en el contrato de adquisición o arrendamiento.

3. Se ha establecido un procedimiento para admitir invitados al edificio y a las instalaciones

4. Se han establecido requisitos técnicos y organizacionales para el uso de la sala de servidores

5. El cableado ha sido marcado y documentado

6. Se han establecido procedimientos para el manejo y transporte de documentos y soporte de datos para el trabajo remoto.

7. La documentación actualizada de los edificios, la gestión de las instalaciones técnicas y los sistemas técnicos específicos (cableado, alcantarillado, sistema de calefacción, ventilación, alarma contra incendios, sistemas de acceso, sistemas de ascensores, CCTV, sistemas de control de automatización de edificios) están a disposición de las personas autorizadas, si es necesario.

8. Se han acordado y mapeado los componentes de TI del vehículo de la institución, qué datos (incluidos los datos personales) es permitida para sincronizarse con el sistema de información y entretenimiento del vehículo o ingresar manualmente y quién tiene acceso a estos datos.

9. Los cables no utilizados se retiran

10. Los planos de cableado y tuberías son válidos y revisado al menos una vez en los últimos 3 años.

11. Se monitorean los mensajes de fallas y otros mensajes de la automatización de la infraestructura (ej., sistemas de clima y UPS) y los mensajes se envían al actor del rol apropiado para la toma de medidas

12. Los sistemas de detección de peligros (intrusión, alarmas de incendio) también funcionan si se interrumpe la red de nivel superior (ej., la conexión a Internet)

13. La pantalla no está en el campo visual de personas ajenas; si es necesario, se utiliza un filtro de pantalla, la pantalla se bloquea cuando el empleado está ausente y los documentos se guardan lejos de la mesa.

14. Se realizan simulacros de alarma y seguridad contra incendios

15. Se documentan todos los sistemas técnicos integrados que interactúan con el sistema de automatización del edificio y las conexiones de comunicación necesarias para su interfaz

16. Para proteger la información que se muestra en la pantalla de un dispositivo informático utilizado en un lugar de trabajo móvil, los usuarios tienen a su disposición un filtro de pantalla para su uso (computadoras portátiles, teléfonos, dispositivos inteligentes).

17. La red de datos de los visitantes (ej. participantes de reuniones, clientes, etc.) se encuentra separado del LAN de la organización

18. Se ha elaborado y mantenido actualizado un inventario de los componentes informáticos integrados en los vehículos de la institución, incluidos los dispositivos inteligentes conectados vía Bluetooth (protocolo de inspección).

## ANEXO 4. Perfil Profesional: Gerente o Ejecutivo de Seguridad de la Información

| | |
|---|---|
| Nombre del puesto: | Gerente/Ejecutivo de Seguridad de la Información |
| Área: | Tecnología |
| Reporta a: | Gerencia de Tecnología |
| Ubicación: | Oficinas centrales de PRISMA |
| Tipo de puesto: | Tiempo completo |
| Salario aproximado: | L. 39,000 |
| Objetivo del puesto | |
| Planificar, implementar y supervisar las políticas, estrategias y controles de seguridad de la información en PRISMA, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, en cumplimiento con los marcos normativos ISO/IEC 27001, 27002 y las directrices institucionales. | |
| Funciones principales | |
| Diseñar e implementar el plan de seguridad de la información alineado a las necesidades y riesgos de PRISMA.<br>Gestionar evaluaciones de madurez (MASS) y diagnósticos con base en ISO/IEC 27001:2022.<br>Coordinar la definición e implementación de controles técnicos, administrativos y físicos.<br>Establecer planes de respuesta a incidentes, continuidad de negocio (BCP) y recuperación ante desastres (DRP).<br>Liderar simulacros de ciberseguridad, campañas de concienciación y capacitaciones.<br>Monitorear alertas, vulnerabilidades y eventos de seguridad en colaboración con el área de TI.<br>Participar activamente en el Comité de Seguridad de la Información.<br>Generar reportes ejecutivos de incidentes, riesgos y avances del plan de seguridad.<br>Coordinar auditorías internas o externas relacionadas con seguridad de la información. | |
| Requisitos académicos | |
| Ingeniería en Sistemas, Informática o carrera afín.<br>Deseable: estudios de posgrado o especialización en Ciberseguridad, Gestión de Riesgos o Tecnologías de Información. | |
| Experiencia requerida | |
| Mínimo 3 años en gestión de seguridad de la información o administración de sistemas seguros.<br>Experiencia práctica con normas ISO 27001/27002, gestión de incidentes, políticas y BCP.<br>Experiencia en empresas financieras o reguladas, deseable. | |
| Conocimientos técnicos | |
| Marco ISO/IEC 27001:2022 y 27002:2022.<br>Gestión de riesgos de TI.<br>Seguridad de redes y servidores.<br>Herramientas SIEM, antivirus corporativo, control de accesos.<br>Microsoft 365, Google Workspace, sistemas en la nube. | |
| Competencias | |
| Liderazgo y toma de decisiones.<br>Pensamiento analítico y enfoque a la mejora continua.<br>Comunicación efectiva y sensibilización de usuarios.<br>Trabajo en equipo con áreas TI, auditoría, cumplimiento y agencias. | |

**ANEXO 5. Fragmento de Cotizaciones.**

## 2. MONTO Y FORMAS DE PAGO POR LOS SERVICIOS PRESTADOS:

2.1. **EL CLIENTE** pagará el total del proyecto que asciende a L 172,712.85 (ISV incluido) el cual cubre lo siguiente:

| Descripción de los Servicios | Duración | Costo total |
|---|---|---|
| ✓ Tercerización Puesto de Seguridad de la Información contrato por un año. | 6 meses | L 153,522.60 |
| | **Subtotal** | **L 153,522.60** |
| | **12.50% ISV** | L **19,190.25** |
| | **Total** | **L 172,712.85** |

Nota: El trabajo se hará de manera remota, de requerir recurso en sitio se contemplará el pago de viáticos adicional al precio indicado en este contrato y el cual se hará de acuerdo con la tabla utilizada para este fin por parte de **EL PROVEEDOR**.

2.2. La forma de pago será de la siguiente forma:

| Descripción |
|---|
| 6 pagos mensuales por un valor total en cada pago de: L 28,785.47 incluye ISV. |