FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS

SUSTENTADO POR:

NORVINS DANIEL MATUTE
RUBEN ALEJANDRO ZELAYA GONZALES

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

ENERO, 2026

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

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS

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

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR

JESÚS RICARDO RODRÍGUEZ RIVERA

MIEMBROS DE LA TERNA:

ALBA GABRIELA GARAY ROMERO
CARLOS ROBERTO AMADOR
JUAN CARLOS ALMENDAREZ FLORES

FACULTAD DE POSTGRADO

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS

Norvins Daniel Matute
Ruben Alejandro Zelaya Gonzales

Resumen

El incremento sostenido de incidentes de ciberseguridad en América Latina y el bajo nivel de madurez de Honduras en el Índice Global de Ciberseguridad han evidenciado la vulnerabilidad de empresas de distribución como PROIMA, cuya operación depende de información y cadenas logísticas en tiempo real. Ante la ausencia de diagnósticos formales sobre riesgos de seguridad de la información, se vuelve necesario analizar de manera sistemática las prácticas actuales y sus brechas frente a los estándares internacionales. El objetivo de este estudio fue describir el grado de alineación de las prácticas y controles de gestión de riesgos de seguridad de la información de PROIMA con las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018, a fin de priorizar oportunidades de mejora que fortalezcan la seguridad organizacional y la continuidad del negocio. Se empleó un enfoque mixto con dominio cualitativo y componente cuantitativo embebido (QUAL→quan), alcance exploratorio-descriptivo y diseño no experimental, transversal y de estudio de caso único. La información se obtuvo mediante encuesta tipo Likert a colaboradores usuarios de activos tecnológicos, entrevistas semiestructuradas a informantes clave, revisión documental estructurada y observación de procesos, integrando el análisis con técnicas descriptivas e inferenciales y un modelo Random Forest. Los resultados muestran un nivel de madurez moderado: se observan avances en controles como autenticación multifactor, política de seguridad y gestión de riesgos de terceros, pero persisten brechas relevantes en mínimo privilegio, actualización de equipos, cumplimiento legal y controles físicos y operativos. Se concluye que la alineación con ISO es parcial y que la cultura organizacional aún otorga un peso limitado al enfoque preventivo y a la corresponsabilidad, por lo que se recomiendan acciones priorizadas de capacitación, estandarización y monitoreo para reducir riesgos residuales e incrementar la resiliencia de PROIMA.

Palabras claves: gestión de riesgos de seguridad de la información, ISO/IEC 27001, ISO/IEC 27005, cultura de seguridad, continuidad del negocio.

GRADUATE SCHOOL

EXPLORATORY STUDY OF PRACTICES AND CHALLENGES IN INFORMATION SECURITY RISK MANAGEMENT AT PROIMA, HONDURAS

Norvins Daniel Matute
Ruben Alejandro Zelaya Gonzales

Abstract

The sustained increase in cybersecurity incidents in Latin America, together with Honduras's low level of maturity in the Global Cybersecurity Index, has exposed the vulnerability of distribution companies such as PROIMA, whose operations depend on information and real time logistics chains. In the absence of formal diagnostics on information security risks, it becomes necessary to systematically analyze current practices and their gaps against international standards. The objective of this study was to describe the degree of alignment of PROIMA's information security risk management practices and controls with ISO/IEC 27001:2022 and ISO/IEC 27005:2018, to prioritize improvement opportunities that strengthen organizational security and business continuity. A mixed methods approach was used, with qualitative dominance and an embedded quantitative component (QUAL→quan), exploratory descriptive scope, and a non-experimental, cross sectional, single case study design. Data was collected through a Likert type survey applied to staff who use technological assets, semi structured interviews with key informants, structured document review, and process observation. The analysis combined descriptive and inferential statistics with a Random Forest model. The results show a moderate level of maturity: there is progress in controls such as multifactor authentication, security policy, and third-party risk management, but significant gaps persist in least privilege, equipment updating, legal compliance, and physical and operational controls. The study concludes that alignment with ISO standards is partial and that the organizational culture still assigns limited weight to a preventive and shared responsibility approach, so prioritized actions in training, standardization, and monitoring are recommended to reduce residual risks and increase PROIMA's resilience.

Palabras claves: information security risk management, ISO/IEC 27001, ISO/IEC 27005, security culture, business continuity.

DEDICATORIA

Dedico cada palabra, cada esfuerzo y cada página de este trabajo a los pilares fundamentales de mi existencia: mi familia y mis fieles compañeros de vida.

A mis padres y a mi hermana, este logro es para ustedes. Es el fruto de su paciencia, de sus desvelos compartidos y de ese amor incondicional que me ha blindado contra cualquier adversidad. Ustedes son mi "porqué" y mi "para qué"; la motivación suprema que me impulsa a ser mejor cada día. Sin su presencia, este éxito carecería de sentido.

Y con una emoción especial, dedico este trabajo a mis mascotas, Baely, Campeon, Nova y Astro. Ustedes, mis pequeños guardianes y compañeros de desvelos han sido los héroes silenciosos de esta jornada. Gracias por permanecer a mi lado durante las largas noches de estudio, por intuir mi ansiedad y curarla con su compañía, y por siempre estar ahí con una alegría pura que me recordaba que, pase lo que pase, todo estaría bien. Su amor sin palabras fue la medicina que necesité en los momentos más difíciles. Este triunfo también lleva sus huellas.

Ruben Zelaya

A mi madre, Ruth Matute, cuyo amor, entrega y ejemplo de constancia han acompañado cada una de mis decisiones. Gracias por su fortaleza, por creer en mí incluso cuando el camino se volvía exigente y por enseñarme que la disciplina abre puertas que antes parecían inalcanzables.

A mi abuela, Lilia Matute, quien ha sido el pilar que me impulsó a buscar el conocimiento. Su sabiduría, su orientación y su forma de ver la vida despertaron en mí el deseo de aprender, de crecer y de aspirar siempre a algo más. Sus palabras y su ejemplo han sido una brújula silenciosa que me ha guiado hacia cada uno de mis logros.

A mis hermanos, Nahomy y Eliam, les dedico estas páginas como un recordatorio de que el esfuerzo siempre tiene un propósito y que cada meta es alcanzable cuando se combina determinación, fe y constancia. Que este logro les inspire a creer en su potencial y a seguir adelante con valentía.

A mis tíos y primos, quienes han formado parte importante de mi historia, deseo que encuentren en este paso una motivación para perseguir sus metas, confiando en que todo sueño se construye con pasos firmes y decididos.

A mis futuros hijos, cuya llegada aún pertenece al misterio del tiempo, les entrego este logro como un cimiento anticipado de lo que deseo construir para ustedes. Que este esfuerzo sea

una muestra del compromiso que asumo desde ahora: prepararme, crecer y superarme para ofrecerles un futuro donde puedan desarrollarse con dignidad, seguridad y libertad.

Ojalá, cuando lean estas líneas algún día, encuentren en ellas la certeza de que cada decisión tomada en mi camino también buscó abrir espacio para los sueños que ustedes aún no han pronunciado. Que vean en este trabajo un recordatorio de que el conocimiento, la disciplina y el amor pueden transformar la vida y trascender generaciones.

Norvins Matute

AGRADECIMIENTO

Al mirar atrás y contemplar el camino recorrido para culminar este reto, reconozco con total humildad que este logro no me pertenece solo a mí. Yo no estaría aquí, ni sería la persona que soy hoy, sin la inmensa fortuna de tenerlos a ustedes.

A mi madre, Leily Edith Gonzales, gracias por ser el corazón de mi vida y mi refugio inagotable. Su amor ha sido la fuerza silenciosa que me levantó en los días grises y tu fe ciega en mis capacidades ha sido mi mayor certeza cuando la mía flaqueaba. A mi padre, Ruben Zelaya Figueroa, gracias por ser mi ejemplo de integridad y esfuerzo incansable; cada sacrificio suyo ha sido un ladrillo en la construcción de mi futuro y su guía ha sido el mapa que me impidió perderme. A mi hermana, Daysy Isabel Zelaya Gonzales, gracias por ser mi cómplice, mi amiga y mi cable a tierra; tu apoyo emocional ha sido vital para mantener mi equilibrio.

Les agradezco infinitamente porque nunca permitieron que me rindiera. Sin su sostén, sin sus palabras de aliento y sin la seguridad que me brinda su amor, esta meta habría sido inalcanzable. Gracias por creer en mí incluso antes de que yo mismo lo hiciera.

Ruben Zelaya

A Dios, a quien debo cada paso de este camino. A Él le agradezco por concederme salud, claridad mental y la fortaleza necesaria para perseverar aun en los momentos más retadores. Su presencia ha sido mi guía en la toma de decisiones y la luz que ha iluminado cada avance de este proyecto. Reconozco que sin Su dirección, este esfuerzo no habría alcanzado el propósito para el cual fue concebido.

A mi esposa, Nancy Jissell Ramos Amador, cuyo amor, dedicación y apoyo constante han sido un impulso invaluable. Gracias por acompañarme en las largas jornadas de estudio, por comprender mis ausencias y por sostenerme con palabras de ánimo cuando el cansancio hacía difícil continuar. Su fortaleza emocional y su fe en mi capacidad se convirtieron en un pilar fundamental para culminar este trabajo. Este logro también le pertenece, porque en cada avance estuvo presente su paciencia, su entrega y su cariño incondicional.

A la Universidad Tecnológica Centroamericana (UNITEC), por ofrecerme un entorno académico que fomenta la excelencia, la disciplina y el pensamiento crítico. Agradezco a sus docentes por compartir su conocimiento con compromiso y profesionalismo, y por ser parte esencial de mi crecimiento profesional y personal.

Norvins Matute

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

La preparación institucional en Honduras para encarar el riesgo digital sigue siendo insuficiente. En el año 2024, el país obtuvo un puntaje de 28.07 en el Índice Global de Ciberseguridad; esto lo coloca en la categoría T4, lo que señala que tiene una madurez baja. Esta brecha implica un mayor riesgo de sufrir pérdidas económicas, interrupciones operativas y daños a la reputación (Gartner, 2016). El desafío se vuelve más complicado en organizaciones que dependen de cadenas logísticas e información en tiempo real para su continuidad, ya que cada minuto de indisponibilidad impacta la confianza, las ventas y el servicio al cliente.

Se estiman que los ciberataques son uno de los cinco riesgos más graves para la estabilidad económica a nivel global. En años previos, se había alertado de que el 60% de las organizaciones podrían tener dificultades serias a causa de controles inapropiados (World Economic Forum, 2025). Según los datos recopilados, la tendencia se ha confirmado con acontecimientos más complejos, costosos y frecuentes. La gestión de riesgos digitales, para poder competir con resiliencia, dejó de ser un proyecto específico y se transformó en una capacidad fundamental para los negocios (Ortiz-Fajardo & Erazo-Álvarez, 2021).

La información ha evolucionado de ser solo un almacén de datos a convertirse en un recurso estratégico. A medida que la digitalización se expande, los sectores y las vulnerabilidades afectados también lo hacen, incrementando así el riesgo de que ocurran repercusiones en lo financiero, operativo y legal (Global Cybersecurity Index, 2024). En 2023, una de cada tres empresas en América Latina reportó incidentes cibernéticos, lo cual pone en relieve la urgente necesidad de respuestas coordinadas y preventivas. Estar adecuadamente preparado significa tener controles, procesos y gobernanza que se correspondan con la exposición real (Cabello et al., 2025).

En este marco, el caso de Productos Importados Americanos (PROIMA) es particularmente útil para realizar un análisis. Es una compañía de Honduras que se enfoca en distribuir productos de consumo masivo y tiene presencia en 17 departamentos, basándose en procesos logísticos eficaces y una administración del inventario centrada en liderar los costos. A pesar de esta fortaleza operativa, sigue existiendo una debilidad fundamental: la falta de un diagnóstico sistemático y documentado sobre los riesgos relacionados con la seguridad de la información. Esa falta podría encubrir debilidades que pongan en riesgo la información sensible, la continuidad de las

operaciones comerciales y la confianza de los socios y clientes.

El análisis indaga de un modo exploratorio las prácticas actuales y los desafíos de PROIMA en la administración del riesgo de seguridad informativa entre septiembre de 2022 y septiembre de 2025, a partir del contexto planteado. Se utilizan entrevistas semiestructuradas, el análisis de documentos internos y la observación directa de los procedimientos para desarrollar una visión completa. La perspectiva es cualitativa-descriptiva y alinea el análisis con las pautas establecidas por ISO/IEC 27001:2022 e ISO/IEC 27005. El objetivo es producir hallazgos que se puedan implementar y que sirvan para priorizar controles y guiar decisiones.

El primer capítulo ofrece el contexto del estudio, así como antecedentes del problema, interrogantes y metas de investigación, la justificación y un análisis de causa-raíz que establece la necesidad del diagnóstico.

El Capítulo II se enfoca en la revisión bibliográfica y los marcos de referencia para la administración del riesgo de seguridad de la información, poniendo énfasis en las normas, principios de gobernanza y buenas prácticas que puedan ser aplicadas a la realidad de Honduras. El análisis del caso se fundamenta en el andamiaje conceptual y metodológico que estos dos capítulos establecen.

El tercer capítulo detalla la metodología empleada, describiendo el diseño de investigación, las variables, técnicas de recolección de datos, la validación del instrumento, el procesamiento estadístico y los criterios éticos considerados durante el estudio.

El cuarto capítulo presenta los resultados obtenidos, acompañados del análisis e interpretación de los datos, integrando el contraste de hipótesis, la correlación entre variables y la discusión de los hallazgos en relación con los objetivos planteados y las mejores prácticas internacionales en gestión de riesgos de seguridad de la información.

El quinto capítulo reúne las conclusiones generales y las recomendaciones derivadas del estudio, orientadas a fortalecer la madurez institucional y la capacidad de respuesta ante incidentes.

Finalmente, el sexto capítulo plantea la propuesta de mejora o aplicabilidad, que integra acciones concretas para optimizar la gestión de riesgos y la continuidad del negocio en PROIMA, asegurando la sostenibilidad de las prácticas alineadas a los estándares ISO.

1.2 ANTECEDENTES DEL PROBLEMA

En la última década, los sucesos cibernéticos en América Latina y el Caribe han crecido con mayor rapidez que en cualquier otra zona del mundo. Esta área continúa siendo, además de lo

mencionado anteriormente, una de las que menos resguardo tiene. Según diversos estudios, tanto los informes de incidentes como las calificaciones de madurez crecen alrededor del 25% cada año. Esto evidencia que hay disparidades estructurales en términos de talento, políticas y competencias. En este escenario, la posibilidad de que las empresas, sin importar su tamaño, sufran pérdidas económicas y paradas operativas se incrementa (Vergara & Diao, 2024).

El panorama mundial verifica el aumento en la sofisticación y el volumen de los ataques. En el último análisis, se registraron más de diez mil brechas confirmadas y más de treinta mil incidentes, con un papel preponderante del ransomware y la extorsión (Çahmutoğlu, 2021). El "factor humano" estuvo involucrado en aproximadamente dos tercios de los casos, mientras que alrededor de un tercio de las brechas se relacionó con estas modalidades. Asimismo, la explotación de vulnerabilidades como método de entrada se incrementó casi tres veces en comparación con el periodo anterior (Espinoza, 2022).

El impacto económico también es contundente. El precio medio a nivel global de una brecha sobrepasó los 4.8 millones de dólares, siendo más elevados en las áreas reguladas. En situaciones concretas, las estafas por "compromiso de correo empresarial" suelen ser del orden de decenas de miles de dólares por transacción y los sucesos de extorsión muestran pérdidas medianas que oscilan en torno a esta cifra, lo cual evidencia el impacto directo sobre la reputación, la liquidez y la continuidad (Bonderud, 2024).

Los peligros también están pasando a cadenas de suministro y terceros. Una parte importante de las brechas ya incluye a proveedores, software de socios o componentes externos, lo que requiere que se incremente la debida diligencia y se incorporen criterios de seguridad en contratos y compras. Al mismo tiempo, los foros internacionales alertan que el ransomware sigue siendo la principal amenaza cibernética que las organizaciones identifican y que el uso malintencionado de tecnologías emergentes está incrementando la superficie de ataque (Cruz & Pérez-Pravia, 2022).

En este contexto, empresas de distribución como PROIMA, que tienen operaciones extensas y dependen de inventarios en tiempo real y de sistemas logísticos integrados, se encuentran particularmente expuestas. La falta de diagnósticos formales y actualizados sobre los riesgos para la seguridad de la información deja huecos para vulnerabilidades no identificadas que tienen el potencial de dañar datos esenciales, interrumpir el flujo de mercancías y debilitar la confianza de aliados y clientes. Por esta razón, fortalecer la gestión de riesgos no es un asunto

técnico independiente, sino una exigencia estratégica para que la organización pueda crecer y sostenerse.

1.3 DEFINICIÓN DEL PROBLEMA

La ciberseguridad en el país está poco desarrollada y cada vez hay más incidentes. A pesar de que en América Latina una de cada tres empresas ha reportado eventos de seguridad recientemente, Honduras continúa con evaluaciones rezagadas en cuanto a preparación. A escala mundial, el costo promedio de una brecha alcanza más de 4.8 millones de dólares y cerca del 33% de los casos se concentra en ransomware y extorsión. La intervención del factor humano está presente en la mayor parte de los incidentes, y las vulnerabilidades han sido explotadas más intensamente, lo que ha incrementado el impacto y la posibilidad de errores operativos para empresas de cualquier tamaño.

PROIMA opera en un sector de distribución que se distingue por la logística, los inventarios y los datos de las transacciones, que son ofrecidos en tiempo real. La continuidad del negocio depende de sistemas integrados y de la cooperación con terceros, lo que aumenta tanto la superficie de ataque como la dificultad del control. Desde septiembre de 2022 hasta septiembre de 2025, la empresa ha enfrentado retos para poner en práctica procedimientos adecuados para gestionar los riesgos a ese nivel de exposición. Existen aún vacíos en la incorporación de la seguridad como un valor estratégico transversal, así como en el ajuste a marcos formales como NIST SP 27005, 800-30 o ISO/IEC 27001.

La ausencia de indicadores y de medidas que permitan el monitoreo del desempeño de los controles contribuye a que la situación se agrave. No se cuenta con un inventario completo y ordenado por prioridades de activos informáticos, ni con una matriz de riesgos que incluya los escenarios, las probabilidades y los efectos en la actualidad. No existen métodos registrados ni puestos en práctica para gestionar y actuar ante incidentes que tengan objetivos de tiempo medio para la detección y respuesta. La ausencia de indicadores dificulta la evaluación de la efectividad de los controles existentes en relación con el perfil de amenazas y restringe que las decisiones se basen en evidencia.

Si no se trata el asunto, PROIMA continuará con riesgos residuales inaceptables que pueden amenazar la confidencialidad, integridad y disponibilidad de la información. Los resultados incluirían la detención de la operación logística, daños a la reputación, pérdidas económicas directas e indirectas y el incumplimiento de contratos o regulaciones. La probabilidad

de que ocurra es coherente con las tendencias observadas y requiere una respuesta organizada y prioritaria, considerando el aumento de incidentes en la región, los costos promedio por brecha y el peso del factor humano y de terceros.

1.4 PREGUNTAS DE INVESTIGACION

1.4.1 PREGUNTA GENERAL

¿En qué medida las prácticas actuales de gestión de riesgos de seguridad de la información (I) en PROIMA (P), comparadas con los estándares y buenas prácticas internacionales (C), se alinean con dichos referentes y cuáles son sus implicaciones observables sobre la seguridad organizacional y la continuidad del negocio (O) durante el periodo septiembre de 2022 a septiembre de 2025 (T)?

1.4.2 PREGUNTAS ESPECIFICAS

1. ¿En qué medida los controles de seguridad de la información (I) actualmente implementados en PROIMA (P), comparados con los referentes ISO/IEC 27001:2022 e ISO/IEC 27005:2018 (C), se alinean con dichos estándares y qué implicaciones observables tienen sobre la probabilidad e impacto de incidentes (O) durante septiembre de 2022 a septiembre de 2025 (T)?

2. ¿Qué papel desempeña la cultura organizacional asociada a la gestión de riesgos de seguridad de la información (I), frente a un enfoque predominantemente técnico (C), en la eficacia observada de las medidas preventivas y de respuesta a incidentes (O) en PROIMA (P) durante septiembre de 2022 a septiembre de 2025(T)?

3. En PROIMA (P), ¿Qué diferencias se observan, en la toma de decisiones para asegurar la continuidad del negocio (O) cuando no existen indicadores y medidas formales de seguimiento de riesgos de seguridad de la información (I), en comparación con un sistema de métricas alineado a ISO/IEC 27005:2018 (C), durante septiembre de 2022 a septiembre de 2025 (T)?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

Describir el grado de alineación de las prácticas y controles de gestión de riesgos de seguridad de la información de PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 (S), midiendo el cumplimiento porcentual de controles aplicables y las brechas por dominio mediante listados de verificación, revisión documental, entrevistas y observación de procesos (M), con el fin de priorizar oportunidades de mejora (A) que fortalezcan la seguridad organizacional y la continuidad del negocio (R) en el período septiembre de 2022 a septiembre de 2025 (T).

1.5.2 OBJETIVOS ESPECÍFICOS

1. Evaluar el grado de alineación de los controles de seguridad de la información vigentes en PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 y determinar sus implicaciones observables sobre la probabilidad e impacto de incidentes durante septiembre de 2022 a septiembre de 2025.

2. Examinar la relación entre la cultura organizacional vinculada a la gestión de riesgos de seguridad de la información y la eficacia observada de las medidas preventivas y de respuesta ante incidentes, en contraste con un enfoque exclusivamente técnico, durante septiembre de 2022 a septiembre de 2025.

3. Analizar las diferencias en la toma de decisiones para asegurar la continuidad del negocio cuando no existen indicadores y medidas formales de seguimiento de riesgos de seguridad de la información, frente a un sistema de métricas alineado a ISO/IEC 27005:2018, durante septiembre de 2022 a septiembre de 2025.

1.6 JUSTIFICACIÓN

Para seguir en el mercado, para operar y para mantener la confianza de clientes y socios, ahora se necesita ciberseguridad. Las instituciones más dependientes de datos en tiempo real están más expuestas a interrupciones y pérdidas por los vacíos de preparación en el contexto nacional. Debe de hacer elecciones con evidencia, una gestión de riesgos transparente, medible y sostenible para este contexto.

PROIMA, por ser distribuidora de bienes de consumo masivo, es un perfil de mayor riesgo si no establece claramente responsabilidades, políticas y controles. El riesgo de daños operacionales y reputacionales se intensifica ante la ausencia de lineamientos estandarizados y preparación ante incidentes cada vez más complejos. Para seguir siendo competitivo, proteger los datos sensibles y asegurar el servicio, reforzar la seguridad de los datos no es una opción, es una obligación.

Esta investigación aborda una brecha poco documentada en el sector de distribución hondureño desde la perspectiva académica. Analiza la manera en que las prácticas efectivas se ajustan a los marcos de referencia establecidos y qué consecuencias visibles tienen en términos de continuidad y seguridad. El enfoque descriptivo-exploratorio proporciona información valiosa, que se puede aplicar y replicar en organizaciones con operaciones parecidas. Esto ayuda a debatir a nivel local sobre la cultura, la gobernanza y las métricas de riesgo.

Desde el punto de vista metodológico, el estudio proporciona un diagnóstico que puede ser verificado mediante la revisión de documentos, la realización de entrevistas y la observación de procesos, con trazabilidad de los criterios de calidad y los resultados encontrados. El énfasis en la medición de alineación y brechas por dominio proporciona insumos utilizables para determinar prioridades y distribuir los recursos de manera sensata, estableciendo una diferencia clara entre un proyecto de consultoría y una tesis de investigación: aquí se obtiene evidencia para tomar decisiones, no un plan de despliegue.

El análisis concluye que la mayoría de los incidentes se agravan debido a prácticas humanas peligrosas y a procesos normativos deficientes. Los procedimientos de respuesta poco practicados, los informes entregados con retraso, la capacitación intermitente y el uso inseguro de credenciales siguen ocurriendo. A esto se añaden políticas desactualizadas en cuanto a la clasificación de información, el manejo de parches, los respaldos y las relaciones con terceros, lo que produce reacciones heterogéneas y reactivas entre las diferentes áreas.

En el aspecto técnico, se detectan configuraciones débiles, segmentación escasa, autenticación multifactorial incompleta y supervisión limitada; además de que hay dependencias con proveedores que no requieren estándares de seguridad equivalentes. El contexto nacional de baja madurez aumenta estos peligros al limitar los servicios y capacidades especializadas. La razón fundamental es la falta de un sistema de administración de seguridad de la información que sea completo y funcional, el cual coordine a las personas, los procesos y la tecnología bajo una gobernanza nítida, con indicadores y métricas coherentes. La brecha de esta naturaleza persistirá, lo que hará que las correcciones específicas se diluyan y que el riesgo residual no baje a niveles aceptables.

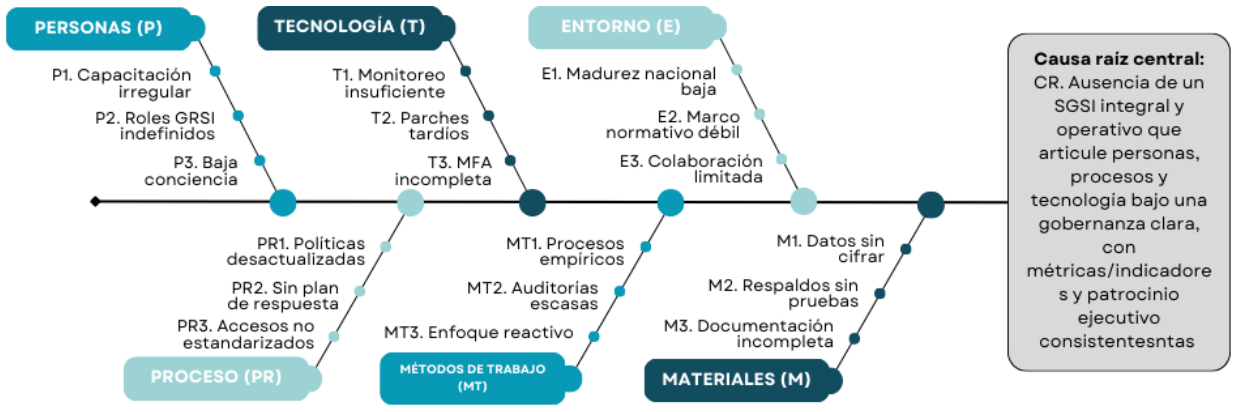


Figura 1: Diagrama sobre las vulnerabilidades de PROIMA ante incidentes de Seguridad

Fuente: Elaboración Propia

CAPÍTULO II. MARCO TEÓRICO

2.1. ANÁLISIS DE LA SITUACIÓN ACTUAL.

2.1.1. ANÁLISIS DEL MACROENTORNO

Se establecieron áreas de referencia fundamentadas en una perspectiva sociotécnica, las cuales posibilitan comparar la realidad de Honduras a través de cuatro criterios: (i) nivel de ingresos; (ii) exposición a catástrofes naturales y sucesos geológicos; (iii) dependencia con respecto a cadenas logísticas terrestres o portuarias; y (iv) nivel de digitalización en términos de comercio y métodos de pago. Este marco comparativo facilita la comprensión de cómo los factores estructurales comunes afectan el riesgo y el funcionamiento (Grupo Banco Mundial, 2025).

En esta línea, se eligieron tres zonas con dinámicas similares: la región andina, el Sudeste Asiático insular y el Caribe insular. La selección no tiene la intención de incluir toda la diversidad regional, sino de proporcionar espejos que sirvan para examinar patrones de vulnerabilidad, capacidad logística comparable y madurez regulatoria (Grupo Banco Mundial, 2025).

Las economías del Caribe insular, que dependen de manera intensa de los puertos y están expuestas a huracanes, se ven interrumpidas en el flujo de bienes y servicios. Los Andes representan un país de renta media con geografía difícil para la distribución, penetración digital en crecimiento y marcos de protección de datos aún en desarrollo. Los mercados emergentes del Sudeste Asiático insular tienen cadenas de suministro densas y vulnerables a tifones, además de ecosistemas regulatorios y digitales que están en una continua evolución (Miranda & Ishizawa, 2020).

Estas similitudes posibilitan el establecimiento de un marco comparativo para dar prioridad a las acciones de gestión del riesgo, determinar brechas de capacidad y guiar requerimientos logísticos y regulatorios que promuevan la resiliencia operativa en situaciones de ingresos medios y alta exposición al clima (Miranda & Ishizawa, 2020).

Tabla 1: Indicadores económicos, logísticos y de conectividad

Zona	PIB per cápita (US$, 2024)	LPI 2023 (0–5)	Uso de Internet 2023 (% población)
Caribe Insular	8,947.7	2.5	84
Andes	8,452.4	2.8	80
SEA	3,984.8	2.9	84
Honduras (referencia)	3,426.4	2.9	58

Fuentes: PIB per cápita (Grupo Banco Mundial, 2025)

2.1.1.1 CARIBE INSULAR

El Caribe presenta un ambiente socio-técnico que impacta la manera en que se aborda la seguridad de la información. La conectividad móvil y los servicios financieros y gubernamentales en línea están promoviendo la inclusión y el crecimiento, pero también están ampliando la superficie de ataque: ciberdelincuencia, fraude y vulnerabilidades en infraestructuras críticas. Las políticas comunes se ven obstaculizadas por la fragmentación insular y no siempre la digitalización rápida acompaña a una cultura de ciberseguridad establecida, lo que genera dependencia de terceros y brechas en las capacidades (Ali, 2024).

Políticas:

La capacidad gubernamental en la subregión es media y desigual (por ejemplo, República Dominicana y Jamaica han progresado, pero con margen de mejora en la ejecución normativa, creando asimetrías en la aplicación de marcos de ciberseguridad y privacidad). Deben de tener conformidad multinorma con políticas y evidencias auditables, y un mapeo regulatorio vivo por país para minimizar arbitrajes y tiempos de respuesta ante incidentes (Foro Económico Mundial, 2024).

Económicas:

Economías de renta media con fricciones logísticas (aduanas, infraestructura, trazabilidad) multiplican la exposición a terceros actores, puertos, transportistas y elevan el riesgo de indisponibilidad que impacta SLAs y visibilidad de pedidos. La cadena de suministro se debe considerar como un sistema socio-técnico; se requieren auditorías de ciber-terceros y controles mínimos verificables (cifrado, DMARC/MTLS en EDI/API, MFA) para garantizar la continuidad y la confianza (Foro Económico Mundial, 2024).

Sociales:

La alta penetración de Internet permite vender, servir y dar seguimiento digital (~85% RD, ~83% JM), pero aún existe exclusión financiera (~51% adultos con cuenta en 2021) que promueve el uso de efectivo y canales fraudulentos como BEC y suplantación en pagos/entregas. Necesitamos controles antifraude omnicanal para entornos con verificación fuera de banda, códigos de un solo uso, mínimos privilegios y capacitación ciudadana contra phishing y smishing (Arístides, 2024).

Tecnológicas:

Los nuevos marcos de privacidad requieren que los controladores/KYC cumplan con las

bases legales, DPIA y la gobernanza de trasferencias internacionales. Requiere un modelo de cumplimiento por jurisdicción y contratos de mandato/cesión que incluyan cláusulas estandarizadas y la auditoría de las evidencias. (Arístides, 2024).

Ambientales:

El riesgo climático (huracanes, tifones) interrumpe la logística, los servicios y las telecomunicaciones, generando riesgos compuestos cuando coincide con ciberataques o fallos de terceros. La resiliencia debe abarcar todo el sistema, continuidad de negocio, redundancia de red/energía, recuperación ante desastres, seguros, en lugar de sólo controles aislados (Espinoza, 2022).

Legales:

La tipificación de ciberdelitos (Jamaica Cybercrimes Act 2015; RD Ley 53-07 sobre crímenes de alta tecnología) requiere preservar evidencias y cadena de custodia, y anticipar la cooperación transfronteriza(Espinoza, 2022)..

Los planes de respuesta a incidentes deben incorporar desde el diseño la retención de logs, los procedimientos forenses y los canales de notificación/colaboración interinstitucional. El Caribe está en proceso de digitalización; sin embargo, la fragmentación institucional y la sensibilidad climática generan peligros sistémicos encadenados: interrupciones en los servicios, cuellos de botella logísticos, pérdida de datos y deterioro de la reputación. El hecho de depender de terceros y la dispersión normativa entre islas empeoran estas vulnerabilidades, lo que dificulta una respuesta coordinada e inmediata. Para llenar esas lagunas, es necesario sincronizar estrategia, apetito de riesgo y cumplimiento en un solo marco, con estándares mínimos compartidos, supervisión clara de responsabilidades y trazabilidad de las decisiones(Ali, 2024).

Un enfoque exitoso implica un sistema integrado de gestión de gobernanza y cumplimiento multinorma, gestión robusta de proveedores, controles antifraude centrados en el usuario y capacidades de resiliencia climática y tecnológica. Esto necesita monitoreo constante, pruebas de respuesta y redundancia en instalaciones críticas, continuidad de operaciones y recuperación verificada; segmentación e identidades fuertes; capacitación continua al cliente y al personal; y coordinación interinstitucional para incidentes transfronterizos. La priorización presupuestaria se destinará a controles de alto impacto, con indicadores de efectividad para la mejora continua(Ali, 2024).

2.1.1.2 ANDES

La región andina vive una digitalización acelerada de servicios públicos y privados impulsada por mayor conectividad y uso de dispositivos móviles. Este avance moderniza cadenas de producción y acorta distancias, pero también amplía la superficie de ataque con fraudes en línea, incidentes sobre infraestructuras críticas y exposición de datos personales. Las brechas urbano-rurales en acceso y alfabetización digital, sumadas a capacidades estatales dispares y limitaciones presupuestarias, dificultan la aplicación homogénea de políticas y la coordinación ante ciberincidentes. La gestión del riesgo exige un enfoque integral que articule tecnología, cultura organizacional, política pública y colaboración transfronteriza (PNUD, 2025).

Políticas

Economías de ingresos medios que presentan dificultades en la infraestructura y en la trazabilidad logística. La topografía andina encarece y dilata los costos y tiempos de la última milla, además de debilitar las cadenas de transporte y almacenamiento. La continuidad y la confianza se ven fortalecidas al integrar el riesgo logístico-digital en la planificación de las ventas y las operaciones, mediante el uso de inventarios compensatorios, rutas alternativas, conmutación entre proveedores, puertos y transportistas, así como una administración estricta de terceros con controles verificables (telemetría, autenticación multifactor y cifrado) (PNUD, 2025).

Económicas

Economías de ingreso medio con fricciones logísticas en trazabilidad e infraestructura. La topografía andina eleva costos y tiempos de última milla y vuelve más frágiles los eslabones de transporte y almacenamiento. Integrar el riesgo logístico-digital en la planeación de ventas y operaciones, con inventarios amortiguadores, rutas alternativas, conmutación entre proveedores, puertos y transportistas, y una gestión rigurosa de terceros con controles verificables (cifrado, autenticación multifactor, telemetría) fortalece continuidad y confianza (Calatayud & Montes, 2021).

Sociales

Hay una fuerte adopción de Internet que expande los canales B2B y B2C; sin embargo, en particular en las áreas rurales, continúan existiendo brechas de alfabetización digital e inclusión. Esto deja en funcionamiento vectores como el compromiso de correo, la suplantación y los fraudes en entregas y cobros. Para poder verificar fuera de banda, utilizar códigos de un solo uso y aplicar el principio de mínimo privilegio en las operaciones de campo, así como para contar con controles

antifraude omnicanal adaptados a contextos con efectivo, se necesitan además programas permanentes de educación digital para los clientes y los trabajadores (Calatayud & Montes, 2021).

Tecnológicas

Marcos de protección de datos y lineamientos de gobierno digital demandan bases legales claras, evaluaciones de impacto en privacidad, identidad confiable y seguridad por diseño. Un modelo de cumplimiento por tratamiento con registro de finalidades, minimización y retención, gobierno de transferencias internacionales y contratos de encargo con cláusulas de cifrado, auditoría y notificación de brechas permite operar con trazabilidad y coherencia (ALTA, 2025).

Ambientales

La geografía y el clima producen interrupciones frecuentes debido a deslizamientos, precipitaciones y cambios estacionales, lo que tiene un impacto en la logística, la energía y las telecomunicaciones. Para lograr la resiliencia, es necesario que se mantenga la operatividad de manera continua, que haya redundancias en términos de energía y red, que existan planes de recuperación comprobados y ejercicios estacionales que sirvan para validar las rutas y las capacidades de conmutación (ALTA, 2025).

Legales

Los marcos de comercio electrónico y ciberdelito requieren conservar pruebas con cadena de custodia, mantener los registros y colaborar entre jurisdicciones. Incorporar procedimientos forenses, criterios para notificar a las autoridades y a los clientes, así como canales de coordinación entre instituciones en los planes de respuesta mejora la efectividad frente a incidentes (ALTA, 2025).

La geografía y la logística son inseparables del riesgo digital en los Andes: las interrupciones debidas a la topografía y al clima amplifican las consecuencias de incidentes informáticos y fraudes, mientras que la diversidad institucional añade demoras en términos de coordinación y respuesta. Este acoplamiento requiere que se observe el entorno como un sistema, en el cual los eslabones digitales y físicos se fortalecen entre sí y la gestión de riesgos va más allá de soluciones específicas para basarse en gobernanza, estándares y capacidades operativas sostenibles (Ramos & Hernández, 2022).

La respuesta efectiva es una combinación de cumplimiento sustantivo en términos de datos y consumo, arquitectura capaz de funcionar en diferentes regiones y estaciones, prácticas estacionales y pruebas de conmutación, un manejo riguroso de terceros logísticos y controles

antifraude enfocados en el usuario. Todo esto tiene que incorporarse a un sistema de gestión que cuente con indicadores de rendimiento, trazabilidad de decisiones y ciclos de mejora constante para garantizar continuidad, resiliencia y rendición de cuentas (Ramos & Hernández, 2022).

2.1.1.3 SUDESTE ASIÁTICO INSULAR

La subregión insular del Sudeste Asiático, que abarca países como Indonesia y Filipinas, está experimentando una rápida digitalización. Esto se debe a la amplia utilización de Internet y dispositivos móviles, el crecimiento del comercio electrónico y el progreso de los servicios financieros digitales. Esta mejora ha generado nuevas oportunidades económicas y ha ampliado la inclusión, pero al mismo tiempo ha elevado el riesgo de suplantación de identidad, fraudes y ataques informáticos a sistemas fundamentales (Biblioteca del Congreso Nacional de Chile, 2024).

La geografía de archipiélago y las diferencias en infraestructura dificultan la coordinación ante incidentes y la aplicación justa de políticas de ciberseguridad. El progreso de la cultura de seguridad digital no es uniforme, aunque la adopción tecnológica es amplia. Esto deja expuestas áreas de ataque que podrían ser evitadas. La gestión del riesgo requiere una visión holística que incorpore tecnología resiliente, marcos definidos de cumplimiento y estrategias sólidas para la educación y sensibilización (Biblioteca del Congreso Nacional de Chile, 2024).

Políticas

Capacidades gubernamentales que están aumentando, pero de manera desigual entre las diferentes agencias y territorios insulares. A pesar de que continúan existiendo discrepancias en los tiempos de respuesta, autorización y fiscalización, la colaboración entre instituciones y a través de fronteras va progresando. Para disminuir las asimetrías y prevenir arbitrajes, es recomendable operar bajo conformidad multinorma, políticas y evidencias trazables, así como llevar a cabo un seguimiento regulatorio activo (Asia Society, 2022).

Económicas

Economías digitales activas con cadenas de suministro amplias y multipuerto, en las que siguen existiendo brechas en términos de trazabilidad y rendimiento logístico. El depender de diferentes transportistas y nodos aumenta la posibilidad de que no estén disponibles y tiene un impacto en los compromisos de servicio. Es fundamental manejar la cadena como un sistema socio-técnico, con una exhaustiva evaluación de terceros, diversificación de las rutas y visibilidad de extremo a extremo (Asia Society, 2022).

Sociales

Alto índice de adopción de dispositivos móviles y aumento de los pagos digitales. La escasa penetración de la banda ancha fija hace que las operaciones se realicen a través de canales móviles, los cuales son más propensos a ataques de phishing y toma de cuentas. Es necesario implementar controles antifraude omnicanales, códigos de un solo uso, verificación fuera de banda y privilegio mínimo en las operaciones. Asimismo, se deben establecer programas permanentes de alfabetización digital para el personal y los clientes (PressBooks, 2023).

Tecnológicas

Ecosistemas que son intensivos en superapps, fintech, APIs y nube. Para la superficie de ataque, son imprescindibles la segmentación, la administración de dispositivos, el gobierno de identidades y la autenticación multifactor. El monitoreo de red y el de TI, en conjunto con la privacidad por diseño, posibilitan una detección y un tiempo de respuesta más rápidos. La posición defensiva se robustece mediante la telemetría sólida y los principios de acceso de confianza cero (PressBooks, 2023).

Ambientales

La logística, la energía y las comunicaciones se ven interrumpidas por la actividad volcánica, las inundaciones y los tifones, que son riesgos climáticos tradicionales. Cuando los eventos climáticos coinciden con incidentes cibernéticos, se generan impactos compuestos más severos. La resiliencia requiere la continuidad de las operaciones, la conmutación multirregión, sitios alternativos distribuidos geográficamente y ejercicios periódicos de recuperación (Smith, 2024).

Legales

Políticas de privacidad que están en uso y en práctica. Surgen obligaciones de notificación de incidentes, bases legales claras para la gestión, evaluaciones de impacto y reglas para las transferencias internacionales. Las cláusulas de auditoría, cifrado, retención mínima y reportabilidad se deben incluir en los contratos con proveedores y encargados (Smith, 2024).

La subregión combina una logística insular, un ambiente móvil-primero y una gran exposición al clima. Este entrelazamiento genera peligros sistémicos que impactan al mismo tiempo la confidencialidad de los datos, la confianza del usuario y la continuidad operativa. La respuesta adecuada implica una gobernanza transparente, la implementación de múltiples normas y la gestión de terceros que incluya logística, pagos y plataformas digitales, utilizando métricas

que faciliten la comprobación de resultados.

Un sistema de gestión integrado necesita combinar la privacidad por diseño, operaciones que se extienden a diversas regiones, pruebas estacionales de conmutación, control antifraude enfocado en el usuario y cooperación entre instituciones para sucesos que trascienden fronteras. Los controles de mayor impacto verificable, que proporcionen trazabilidad a las decisiones y mantengan ciclos de mejora continua, deben ser el enfoque prioritario en términos presupuestarios.

Tabla 2: Síntesis: riesgos dominantes y controles recomendados

Zona	Riesgos dominantes para SI (visión PESTEL)	Controles prioritarios (alineados a ISO/IEC 27001/27005)
Caribe (RD/JM)	Cumplimiento DPA (registro OIC JM), huracanes, logística LPI media, phishing/BEC	DPIA/TIA, DPA/SCC contractuales; DRP multirregión y SLA logísticos con métricas; MFA+DMARC; table-top de crisis climática.
Andes (Perú)	Reglamento 2024/25 de datos, cuellos de última milla, fraude en canales	Inventario y clasificación de datos, EDR/XDR en POS/handhelds; telemetría segura (IoT); BCP por ENSO.
SEA (Filipinas, VN)	Breach reporting ≤72h (PH); PDPL VN 2025/26 (transferencias); tifones; ransomware/phishing	Detección y respuesta 24/7, backups inmutables, orquestación SOC-NOC; cláusulas de transferencia y privacy-by-design; runbooks estacionales.

Fuente: Elaboración propia con base de los autores previos.

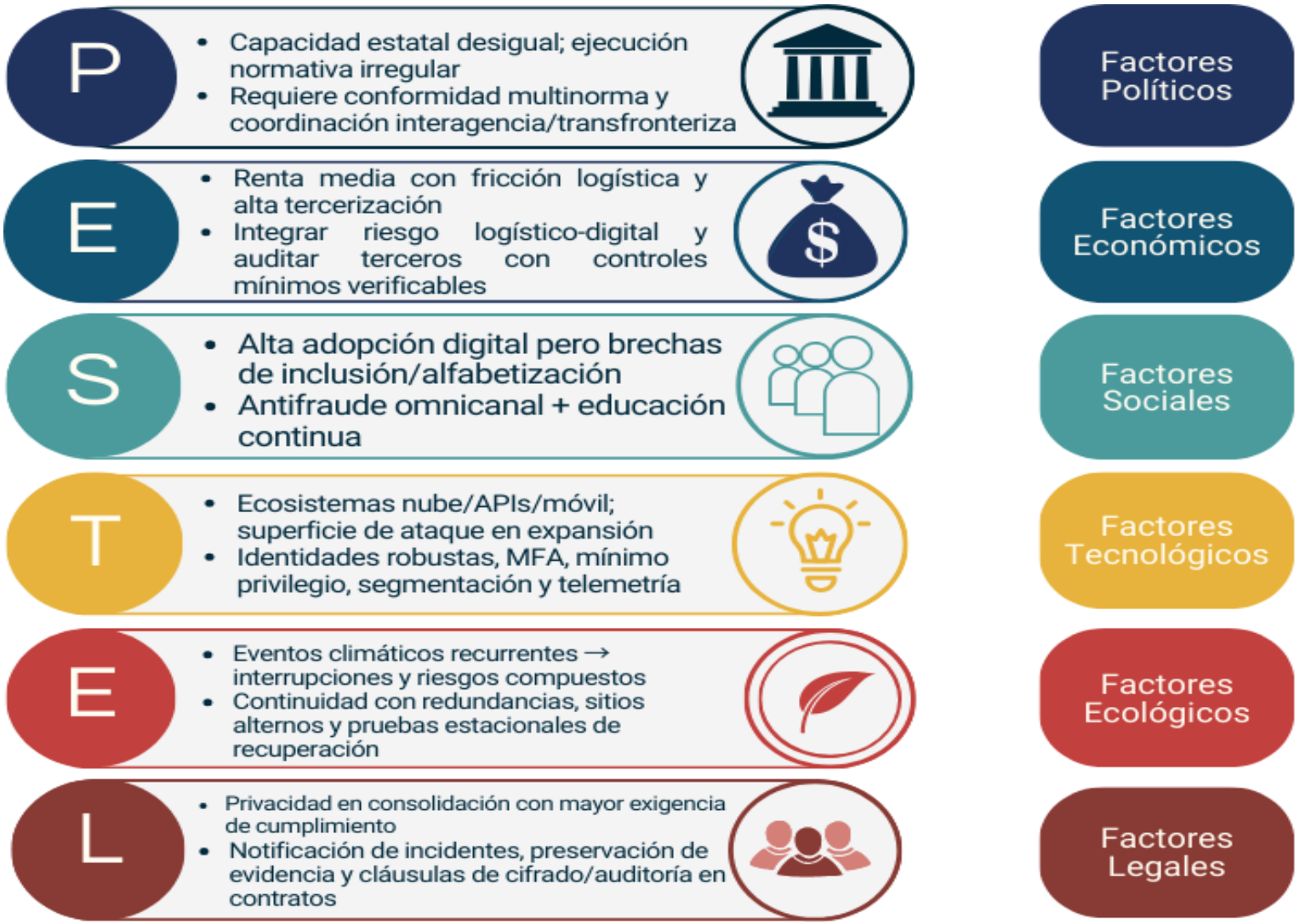


Figura 2: Análisis de PESTEL del Macroentorno

Fuente: Elaboración propia con base de los autores anteriores.

2.2 ANALISIS DEL MICROENTORNO

El estudio del microentorno permite examinar la dinámica competitiva del sector de distribución en Centroamérica mediante la aplicación comparativa del modelo de las Cinco Fuerzas de Porter en dos países de referencia: Guatemala y El Salvador. De este contraste se derivan conclusiones relevantes que, en una fase posterior, servirán para contextualizar la situación de Honduras con mayor precisión.

A la luz del avance en la digitalización de las operaciones, el análisis incorpora de forma transversal la seguridad de la información como factor crítico. Su adecuada gestión resulta indispensable para sostener la continuidad operativa, preservar la confianza de los clientes y fortalecer la resiliencia empresarial frente a incidentes y disrupciones del entorno.

Tabla 3: Panorama comparativo: variables estructurales que condicionan el riesgo de SI

Indicador 2024-25	Guatemala	El Salvador	Honduras	Relevancia para SI
PIB per cápita (US$ corr.)	6 150 US$ (World Bank Open Data)	5 580 US$ (World Bank Open Data)	3 426 US$ (World Bank Open Data)	Capacidad inversora en TI/SI
LPI* ranking / puntaje 2023	88.º - 2,6 (lpi.worldbank.org)	79.º - 2,7 (lpi.worldbank.org)	66.º - 2,9 (lpi.worldbank.org)	Madurez logística & trazabilidad
Penetración de Internet 2023	56 % (World Bank Open Data)	68 % (World Bank Open Data)	58 % (World Bank Open Data)	Superficie de ataque digital
Ley de Protección de Datos	Iniciativa 6464 en trámite (2024-25) (Congreso de Guatemala)	Ley aprobada nov-2024 (asamblea.gob.sv)	Ley promulgada ago-2025 (ACE) (Consortium Legal)	Marco coercitivo & multas
Incidentes ciber en retail 2024	Phishing & fraude omnicanal (regional) (ptsecurity.com)	Campañas de ransomware focalizadas (El País)	Falta CSIRT nacional, alta exposición (Derechos Digitales)	Tendencia de riesgo

Fuente: Elaboración propia con base de las distintas fuentes consultadas.

2.2.1 APLICACIÓN DEL MODELO DE CINCO FUERZAS DE PORTER

El modelo de Cinco Fuerzas de Porter evalúa el atractivo estructural de una industria y la intensidad de su competencia. Considera cinco presiones: la amenaza de nuevos entrantes, determinada por barreras de entrada como escala, capital y acceso a canales; el poder de negociación de los proveedores, influido por su concentración y la diferenciación de insumos; el poder de negociación de los compradores, afectado por su volumen y sensibilidad al precio; la amenaza de productos o servicios sustitutos, guiada por la relación desempeño-precio y los costos de cambio; y la rivalidad entre competidores existentes, condicionada por el número de actores, el

crecimiento del mercado y el grado de diferenciación (Alonso, 2024).

La lectura del modelo es inversa: cuanto mayor la presión conjunta de las fuerzas, menor la rentabilidad potencial del sector. Las fuerzas interactúan y evolucionan con cambios tecnológicos, regulatorios y de comportamiento del consumidor. La digitalización puede bajar barreras de entrada o, por el contrario, elevarlas mediante efectos de red, datos y estándares; la seguridad de la información incide en costos de cambio, confianza y cumplimiento. Aplicado rigurosamente, el marco orienta palancas estratégicas como diferenciación, liderazgo en costos, integración y gestión de ecosistemas para mejorar la posición competitiva (Alonso, 2024).

2.2.1.1 GUATEMALA

Guatemala comparte con Honduras una rápida adopción tecnológica, con mayor acceso a internet móvil y expansión de plataformas para comercio, banca y servicios públicos. No obstante, Guatemala ha avanzado más en infraestructura de telecomunicaciones y en gobierno digital, lo que amplía la conectividad y diversifica los trámites y servicios en línea. Este progreso mejora la eficiencia y la inclusión, y eleva las expectativas de calidad del servicio. También exige una gestión más madura de riesgos y de datos (García et al., 2023).

La expansión del mundo digital amplía la superficie de exposición a ciberamenazas: fraude en línea, suplantaciones, indisponibilidad de sistemas y fuga de información. Los puntos vulnerables generalmente surgen en las integraciones con terceros, autenticación débil y seguridad inconsistente entre entidades públicas y privadas. La continuidad y la confianza del usuario dependen de controles auditables, monitoreo continuo y respuesta coordinada a incidentes. La seguridad de la información es un factor de competitividad y no solo un factor técnico (García et al., 2023).

En Honduras aún existen mayores brechas de acceso y alfabetización digital que limitan algunos vectores de exposición, pero también impiden construir una cultura de ciberseguridad y capacidades de respuesta. Ambos países enfrentan desafíos similares en términos de sensibilización ciudadana, madurez institucional y actualización legislativa. Para fortalecer la gestión integral se necesita fortalecer la gobernanza, estandarizar controles, profesionalizar capacidades técnicas y coordinar la intersectorialidad. Solo así la digitalización se convertirá en resiliencia sostenible.

Tabla 4: Evaluación de entorno (Guatemala)

Fuerza	Nivel	Evidencia & vínculo con riesgos de SI
Rivalidad entre competidores	Alta	Tres cadenas (Walmart CA, La Torre, Unisuper) concentran el canal moderno; las ventas retail crecieron 33 % en 2024, intensificando guerra de precios y de canales digitales (FAS Apps). La presión por "time-to-market" acelera integraciones con marketplaces y expone APIs sin madurez de hardening.
Amenaza de nuevos entrantes	Media	E-commerce transfronterizo (Shein, Amazon Global) capta <5 % but growing, aprovechando la ausencia de ley robusta de datos; barrera logística moderada (LPI 88.º). Falta de regulación de protección de datos debilita confianza del consumidor y eleva riesgo de fuga PII.
Poder de los proveedores	Medio-Alto	Cadena agroindustrial fragmentada; dependencia de EE. UU. (U$ 1,9 bn en insumos 2024) (FAS Apps). Intercambio EDI y portales B2B heterogéneos incrementan superficie de amenazas de "supply-chain attack".
Poder de los compradores	Alto	Sólo 30 % de alimentos se venden en supermercados; consumidores alternan entre canales tradicionales y apps, exigiendo transparencia de inventario y pagos seguros. Mayor sensibilidad ante brechas de datos incrementa coste reputacional por incidentes.
Amenaza de sustitutos	Media	Mercados informales y delivery P2P crecen, pero percepción de higiene y autenticidad favorece a formal retail. Risk: heterogéneo manejo de datos por agregadores de última milla.

Fuente: Elaboración propia con base de las distintas fuentes consultadas.

2.2.1.2 EL SALVADOR

El Salvador se está transformando digitalmente a pasos agigantados, dejando atrás a Honduras en términos de adopción tecnológica y políticas públicas para la innovación. La digitalización de los servicios públicos, el auge del comercio electrónico y la telefonía móvil han multiplicado los canales de interacción ciudadana y empresarial. Esto hace más eficientes y amplios los servicios, pero también crea dependencia de plataformas esenciales. La agenda digital es un eje de competitividad y modernización institucional (Grupo Banco Mundial, 2022).

Pero este dinamismo requiere fortalecer urgentemente los marcos de ciberseguridad y gestión integral de riesgos. El crecimiento de los pagos y las finanzas digitales, así como la aparición de nuevas tecnologías y activos digitales, aumenta la superficie de riesgo de fraude, suplantación y errores operativos. Deben establecerse políticas de protección de datos, continuidad de negocio y respuesta a incidentes con roles y responsabilidades definidas y supervisión. La confianza del usuario se basa en controles transparentes, monitoreo continuo y rendición de cuentas (Grupo Banco Mundial, 2022).

Honduras, por su parte, avanza a un ritmo más gradual, con infraestructura menos extendida y oferta más limitada de servicios digitales. Esto reduce algunos vectores de exposición, pero también frena el desarrollo del ecosistema y la madurez de la cultura de ciberseguridad.

Ambos países comparten desafíos de alfabetización digital, sensibilización y fortalecimiento institucional para regular y ejecutar con eficacia. La prioridad es construir capacidades técnicas y de gobernanza que permitan una gestión de seguridad de la información sostenible, resiliente y orientada a resultados.

Tabla 5: Evaluación de entorno (El Salvador)

Fuerza	Nivel	Evidencia & vínculo con riesgos de SI
Rivalidad	Media-Alta	Duopolio Super Selectos / Walmart domina grocery; sin embargo, e-commerce creció 80 % en CA (1Q24) (files.walmex.mx). Competencia por omnicanalidad fuerza rápidas integraciones SaaS, aumentando puntos de fallo.
Nuevos entrantes	Media	Ley de Datos Personales 2024 impone obligaciones de reporte y sanciones → barrera jurídica inicial; pero ofrece certidumbre a fintech-retail híbridos.
Proveedores	Medio	Alta dependencia de EEUU (U$ 633 m en intermedios 2024) (FAS Apps); acuerdos de integración vertical de cadenas reducen visibilidad sobre seguridad de datos compartidos.
Compradores	Alto	Penetración internet 68 %; fidelidad a apps de ofertas y métodos de pago QR. Incidentes de ransomware en 2024 afectaron retailers regionales, elevando conciencia y poder negociador en torno a privacidad.
Sustitutos	Bajo-Medio	Mercado informal relevante pero preferencia por supermercados "seguros" (FAS Apps); sustitutos cifran ventaja competitiva en experiencia digital más que en precio.

Fuente: Elaboración propia con base de las distintas fuentes consultadas.

2.2.1.3 HONDURAS

En Honduras, la administración de la seguridad de la información se ve afectada directamente por el hecho de que su progreso digital es menor al de Guatemala y El Salvador. La escasa alfabetización tecnológica de la población, así como el acceso a servicios digitales y la cobertura de internet, limitan la prevención, detección y respuesta ante incidentes. La creación de confianza en los canales digitales, la estandarización de controles y el seguimiento de decisiones se ven obstaculizados por esta base desigual.

Una dependencia tecnológica reducida reduce la complejidad de ciertos riesgos a corto plazo, pero al mismo tiempo restringe la aplicación de prácticas avanzadas en términos de ciberseguridad. Guatemala y El Salvador enfrentan un campo de riesgo más amplio debido a que la conexión digital entre sus ciudadanos y las empresas es más alta. Sin embargo, cuentan con infraestructuras institucionales y capacidades que son más avanzadas en comparación. El contraste subraya la imperativa urgencia de robustecer los sistemas y las políticas que respalden el crecimiento digital. Como Guatemala y El Salvador tienen una mayor conexión digital entre sus ciudadanos y las empresas, afrontan un campo de riesgo más extenso. Sin embargo, cuentan con infraestructuras institucionales y capacidades que son más avanzadas en comparación. El contraste

subraya la imperativa urgencia de robustecer los sistemas y las políticas que respalden el crecimiento digital.

El momento es esencial. La ampliación de los servicios y la infraestructura debe ir acompañada de la capacitación digital y la inclusión, así como del fortalecimiento de las regulaciones y la capacidad operacional en las instituciones. La creación de un gobierno de riesgos bien establecido, la normalización de los controles básicos, el fortalecimiento de la respuesta a incidentes y la continuidad del negocio, la implementación de una gestión estricta con terceros y asegurar que los datos se manejen responsablemente son aspectos esenciales. Así, la digitalización solo se volverá competitividad y resiliencia sostenibles.

Tabla 6: Evaluación de entorno (Honduras)

Fuerza	Nivel	Evidencia & vínculo con riesgos de SI
Rivalidad	Alta	La Colonia lidera con 6,7 % market share y 64 tiendas; expansión +12 % en unidades 2023-24 (FAS Apps). Walmart y PriceSmart presionan márgenes vía omnicanal; inversión en apps "click-&-collect" sin SOC centralizado aumenta riesgo de ataque simultáneo multi-sucursal.
Nuevos entrantes	Medio-Alto	LPI 66.º (mejor de los tres) reduce barreras físicas; planeada ley de ciberseguridad (Plan Digital 2023-26) aún pendiente (DIGER) → ventana para actores digitales ágiles, pero también para incursiones maliciosas.
Proveedores	Alto	Alta fragmentación rural + infrastructura logística débil; integraciones EDI básicas (FTP/Excel) favorecen ataques "business e-mail compromise".
Compradores	Medio	Internet 58 %; crecimiento sostenido de remesas ha impulsado wallets móviles, pero confianza es frágil ante brechas (caso phishing regional 2024) (ptsecurity.com).
Sustitutos	Medio	Comercio informal y bodega barrial conservan cuota significativa; sin embargo, conveniencia y programas de lealtad electrónicos atraen público urbano joven.

Fuente: Elaboración propia con base de las distintas fuentes consultadas.

Patrones regionales y lecciones aprendidas

El enfoque omnicanal se ha convertido en un diferenciador competitivo, pero también incrementa las dependencias tecnológicas y amplía la superficie de ataque. A mayor madurez logística, mayor complejidad en la cadena de datos: Honduras destaca por su eficiencia operativa, aunque la ausencia de una Ley de Protección de Datos eleva la exposición al tratar información sensible y condiciona la confianza del mercado.

En paralelo, el marco regulatorio evoluciona de forma desigual. El Salvador pasó de un vacío normativo a una ley integral que incrementa los costos de cumplimiento, pero fortalece la previsibilidad y la confianza. Guatemala mantiene en discusión los marcos de protección de datos y ciberseguridad, y esa indefinición acarrea riesgo reputacional. Honduras avanza mediante alianzas comerciales estratégicas, aunque requiere mayor institucionalidad y reglas claras para sostener el crecimiento digital.

La estructura de mercado con alta concentración reduce la frecuencia de nuevos clientes potenciales y, al mismo tiempo, amplifica el impacto de cualquier ciberincidente. En este contexto, aunque Honduras posea la logística más eficiente, su rezago regulatorio y la elevada rivalidad interna multiplican los vectores de riesgo en seguridad de la información. Integrar estas lecciones en la estrategia de PROIMA permite mitigar amenazas y convertir la confianza digital en ventaja competitiva; en conjunto, la región confirma que la solidez regulatoria y operativa es hoy la palanca central de diferenciación sostenible.

Figura 3: Diagrama de Porter del Microentorno

Fuente: Elaboración Propia

2.3. CONCEPTUALIZACIÓN

2.3.1 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Perspectivas teóricas actuales:

El SGSI es concebido, desde una perspectiva normativa, como un sistema de gestión que se fundamenta en ciclos de mejoramiento constante y que tiene como base los riesgos. Su objetivo es instaurar, poner en marcha, gestionar, supervisar y mejorar políticas y controles que aseguren la integridad, la confidencialidad y la disponibilidad. Esta perspectiva enfatiza la trazabilidad entre evidencias, controles, riesgos y contexto para que la seguridad no sea un estado, sino un proceso que se pueda verificar y repetir a lo largo del tiempo (Villareal et al., 2024).

En la literatura de gestión y gobierno de TI, el SGSI es un mecanismo para alinear estrategias. Auditoría interna, evaluación del desempeño, revisión por la dirección, liderazgo y funciones y responsabilidades. En este contexto, la seguridad deja de ser una cuestión sólo tecnológica y se integra a la cadena de valor: se planifica en función de criterios de coste-beneficio, se mide con indicadores y se rinde cuentas por resultados, no por cumplimiento documental. (Villareal et al., 2024).

Desde la perspectiva socio-técnica, el SGSI es un mecanismo que conecta a seres humanos, procesos y tecnología. Las capacidades de los equipos, el comportamiento de los usuarios y directivos, así como la cultura organizacional, son tan esenciales como las herramientas. La capacitación constante, la creación de procesos seguros y una arquitectura que minimice los errores humanos predecibles se suman a la gestión de accesos e identidades, a la segmentación y al principio de privilegio mínimo (Morales et al., 2024).

En última instancia, los marcos de continuidad y resiliencia extienden el alcance del SGSI para incluir la preparación, la recuperación y la respuesta frente a incidentes. Se prioriza la habilidad de asimilar impactos, reorganizar operaciones y aprender de los acontecimientos. La seguridad por diseño y la privacidad por diseño se añaden a esta perspectiva, así como modelos de madurez que posibilitan el diagnóstico de brechas y la priorización de mejoras fundamentadas en métricas comparables y objetivas(Morales et al., 2024).

Definición operativa utilizada.

Para la presente investigación, un SGSI es un marco sistemático y estructurado que agrupa personas, procesos, tecnologías y políticas con el fin de identificar, evaluar, gestionar y supervisar continuamente los riesgos de seguridad de la información. Esto asegura la confidencialidad,

integridad y disponibilidad de los activos críticos. En el marco del estudio, se incorporarán la gestión de riesgos, controles técnicos y organizativos, medidas de desempeño y ciclos de mejora junto con el gobierno. Así pues, la seguridad podrá ser demostrada a través de evidencias verificables y contribuirá al negocio.

2.3.2 GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

Enfoques teóricos existentes:

La gestión de riesgos de ciberseguridad se entiende como un ciclo continuo e integrado al gobierno corporativo: definir contexto y apetito de riesgo, identificar activos y dependencias, reconocer amenazas y vulnerabilidades, estimar probabilidad e impacto, y decidir tratamientos con seguimiento y mejora. Este enfoque prioriza la trazabilidad entre riesgos, controles y evidencias, de modo que las decisiones puedan explicarse y auditarse (Idrus et al., 2023).

Desde la teoría de sistemas y lo socio-técnico, el riesgo surge de la interacción entre personas, procesos, tecnología y terceros. Importan tanto la arquitectura técnica como la cultura, los errores humanos previsibles y la cadena de suministro digital. El modelado de amenazas, los análisis por escenarios y técnicas como el diagrama “bow-tie” permiten visualizar causas, barreras preventivas y capacidades de respuesta, incorporando dependencias con nube, proveedores y regulaciones de datos (Idrus et al., 2023).

En el plano metodológico conviven enfoques cualitativos y cuantitativos. Los primeros usan escalas ordinales y matrices de riesgo; los segundos estiman pérdidas esperadas y reducción marginal del riesgo para optimizar inversiones. En ambos casos, el objetivo es comparar riesgo inherente y residual, medir eficacia de controles preventivos, detectivos y correctivos, y gobernar indicadores como tiempo de detección y respuesta, severidad de brechas, cumplimiento y exposición de terceros (Caamaño & Gil, 2020).

Definición operativa adoptada:

En esta investigación, la gestión de riesgos de ciberseguridad es el proceso sistémico y continuo mediante el cual se identifican, analizan, evalúan y tratan los riesgos asociados a los activos de información, considerando también a los terceros críticos. Incluye levantar inventarios y clasificar datos, modelar amenazas y vulnerabilidades, estimar probabilidad e impacto, determinar controles existentes, calcular riesgo residual y seleccionar tratamientos mitigar, transferir, evitar o aceptar en línea con el apetito de riesgo. Se implementan controles preventivos, detectivos y correctivos con métricas e hitos verificables, se monitorean indicadores clave y se

retroalimentan planes de continuidad y mejora continua para sostener confidencialidad, integridad y disponibilidad

2.3.3 EVALUACIÓN DE RIESGOS

Enfoques teóricos existentes:

La evaluación de riesgos se concibe como el proceso estructurado que integra tres etapas encadenadas: identificación, análisis y valoración. Parte de un contexto definido y de criterios de riesgo explícitos escalas de probabilidad e impacto, umbrales de aceptación y niveles de apetito para asegurar comparabilidad y trazabilidad. La identificación levanta activos, procesos y dependencias (personas, tecnología y terceros), así como amenazas y vulnerabilidades pertinentes; el análisis estima la probabilidad de materialización y la magnitud del efecto; y la valoración contrasta los resultados con los criterios para priorizar decisiones (Guerrero et al., 2020).

Coexisten enfoques cualitativos, cuantitativos y mixtos. Los cualitativos utilizan escalas ordinales y matrices para clasificar escenarios cuando la evidencia numérica es limitada; los cuantitativos estiman pérdidas esperadas y reducciones marginales del riesgo para optimizar inversiones en controles. En todos los casos se distingue entre riesgo inherente (antes de controles) y residual (después de controles), se consideran incertidumbre y calidad de datos, y se recomienda el uso de análisis por escenarios y modelado de amenazas para capturar eventos de baja frecuencia y alto impacto. La utilidad del proceso radica en producir salidas accionables: registro de riesgos, mapas de calor, hipótesis de tratamiento y métricas para seguimiento(Guerrero et al., 2020).

Definición operativa adoptada:

En esta investigación, la evaluación de riesgos se define como el proceso metodológico mediante el cual se identifican, analizan y valoran de forma sistemática las amenazas, vulnerabilidades y consecuencias potenciales que pueden afectar los activos de información, cuantificando su probabilidad e impacto para establecer prioridades de tratamiento

2.4 TEORÍAS DE SUSTENTO

2.4.1 BASES TEÓRICAS

2.4.1.1 TEORÍA DE LA CONTINGENCIA ORGANIZACIONAL

La Teoría de la Contingencia sostiene que no existe una única forma “correcta” de estructurar y gestionar una organización. La efectividad depende del ajuste entre el diseño interno

y las exigencias del entorno. Cuando ese encaje es adecuado entre estrategia, procesos, estructura y contexto la organización logra mayor desempeño; cuando es deficiente, aparecen ineficiencias, sobrecostos y respuestas tardías (Parast, 2022).

Este enfoque identifica factores contingentes que condicionan el diseño óptimo: tecnología empleada, tamaño y complejidad, grado de incertidumbre ambiental, dinamismo competitivo y regulación. Cada factor modifica la necesidad de coordinación y control. Sectores estables toleran mayor estandarización; entornos cambiantes demandan flexibilidad, aprendizaje y ciclos cortos de decisión (Parast, 2022).

El ajuste no es estático. A medida que el entorno evoluciona, la organización debe recalibrar su arquitectura: niveles de formalización, centralización, especialización y mecanismos de integración. Herramientas como roles de enlace, comités interfuncionales, indicadores compartidos y plataformas de información elevan la capacidad de procesamiento y reducen desalineaciones entre áreas (Erude, 2023).

En seguridad de la información, la contingencia se traduce en seleccionar controles y gobernanza según riesgos reales y capacidades disponibles. No basta con "adoptar mejores prácticas" de forma uniforme: es necesario modular el SGSI, priorizar dominios críticos, decidir dónde formalizar y dónde flexibilizar, y vincular las inversiones a resultados verificables en continuidad, cumplimiento y confianza (Erude, 2023).

Aplicación al contexto de PROIMA

Para PROIMA, esta teoría implica diseñar un SGSI a la medida de su sector de distribución, tamaño, cultura y recursos, así como del perfil de amenazas del entorno hondureño. Se recomienda un sistema modular y escalable: gobierno claro de riesgos, controles mínimos viables en identidades, vulnerabilidades y continuidad, integración con logística y terceros, y niveles de formalización acordes con la madurez de procesos. El ajuste se sostendrá con métricas de desempeño, revisiones periódicas y mecanismos de coordinación que alineen decisiones de seguridad con operaciones y objetivos comerciales.

2.4.1.2 TEORÍA GENERAL DE SISTEMAS

La Teoría General de Sistemas concibe a las organizaciones como sistemas abiertos que intercambian recursos, energía e información con su entorno. Esta mirada supera el análisis fragmentado: el desempeño del conjunto no se explica por la suma de sus partes, sino por las interacciones entre ellas. Desde esta óptica, comprender un fenómeno organizacional exige mapear

flujos, límites, entradas y salidas, así como los acoplamientos que conectan áreas y procesos (Tamayo Alzate, 1999).

Sus principios básicos incluyen el holismo y la interdependencia entre componentes; la jerarquía de sistemas y subsistemas; la retroalimentación como mecanismo de control y aprendizaje; y la entropía, que describe la tendencia al desorden cuando no existen reglas, controles o energía organizacional para sostener el orden. Frente a ello, la homeostasis y la negentropía reflejan la capacidad del sistema para estabilizarse, regenerarse y mejorar (Tamayo Alzate, 1999).

Aplicada a organizaciones, la teoría enfatiza su naturaleza socio-técnica: conviven subsistemas técnicos, humanos, estructurales y administrativos que co-evolucionan. Cambios en un subsistema, por ejemplo, introducir una nueva plataforma tecnológica alteran cargas de trabajo, competencias, normas y métricas en los restantes. La efectividad depende de la calidad de las interfaces: donde hay fallas de acoplamiento, surgen cuellos de botella, errores y pérdida de información (Domínguez & Santillán, 2022).

En seguridad de la información, esta perspectiva traduce los controles en lazos de control con sensores, umbrales y acciones correctivas; la gestión del riesgo en un circuito de retroalimentación que mide compara y ajusta; y la resiliencia en redundancias y rutas alternativas que permiten absorber perturbaciones. El foco deja de ser un control aislado y pasa a ser la coherencia del conjunto: políticas, procesos, personas y tecnología trabajando como un sistema con propósito (Domínguez & Santillán, 2022).

Aplicación al contexto de PROIMA

Entender a PROIMA como sistema socio-técnico implica diseñar el SGSI como un entramado de lazos de control que conecte logística, TI, operaciones, talento humano y proveedores. El primer paso es mapear subsistemas y puntos de acoplamiento críticos identidades y accesos, integraciones con terceros, continuidad y atención al cliente, definir límites y responsabilidades, e instrumentar sensores e indicadores que reduzcan entropía: procedimientos claros, capacitación, telemetría y revisiones periódicas. Así, la retroalimentación convierte incidentes y no conformidades en mejoras verificables, elevando estabilidad operativa y capacidad de respuesta sin perder de vista el objetivo común.

2.4.1.3 TEORÍA DE LA GESTIÓN DE RIESGOS EMPRESARIALES

La gestión de riesgos empresariales concibe el riesgo como un elemento inherente a la

estrategia y al desempeño. No se limita a controles operativos, sino que busca alinear el apetito de riesgo con los objetivos, la cultura y la asignación de recursos. Su propósito es ofrecer una seguridad razonable sobre el logro de metas, promoviendo decisiones informadas ante la incertidumbre y una visión de portafolio que integra riesgos de todas las unidades y procesos (Nocco & Stulz, 2025).

El enfoque contemporáneo se articula en torno a gobierno y cultura, formulación estratégica con objetivos medibles, gestión del desempeño con criterios de riesgo, revisión y mejora, e información y reporte oportunos. Esto implica roles y responsabilidades claros desde la alta dirección, políticas y límites explícitos, y mecanismos de supervisión que garanticen independencia y eficacia. La transparencia en la comunicación interna y externa es condición para la confianza y la rendición de cuentas (Nocco & Stulz, 2025).

Metodológicamente, el ciclo comprende identificación estructurada de eventos, evaluación de probabilidad e impacto, comparación con apetito y tolerancias, y selección de respuestas: evitar, reducir, compartir o aceptar. La gestión se apoya en indicadores clave de riesgo, registros y mapas de calor, análisis de escenarios y pruebas de estrés. La distinción entre riesgo inherente y residual orienta inversiones y prioriza iniciativas con mayor reducción marginal del riesgo (Montenegro, 2020).

La eficacia del modelo depende de su integración con otros sistemas de gestión: cumplimiento, control interno, auditoría, continuidad del negocio y seguridad de la información. La coordinación entre áreas finanzas, operaciones, TI, logística, compras evita silos y reduce arbitrajes. La mejora continua se impulsa con métricas comparables, umbrales de alerta y revisiones periódicas que conectan resultados con decisiones de presupuesto y desempeño (Montenegro, 2020).

Aplicación al contexto de PROIMA

Para PROIMA, adoptar este enfoque supone incorporar el riesgo de ciberseguridad al mapa integral de riesgos del negocio, con apetitos y tolerancias definidos para indisponibilidad, fuga de datos y fallas de terceros. Se recomienda establecer un comité de riesgos con responsabilidades claras, un registro unificado que incluya proveedores críticos, e indicadores como tiempo de detección y respuesta, severidad de incidentes, latencia de parches y cumplimiento de controles. La priorización de tratamientos debe vincularse a objetivos operativos y comerciales, y alinearse con el SGSI para asegurar evidencia verificable, reporting ejecutivo y ciclos de mejora que

traduzcan la inversión en resiliencia y confianza del mercado.

2.4.2 METODOLOGÍAS DESARROLLADAS

2.4.2.1 METODOLOGÍA ISO 27005:2022

Descripción Metodológica:

La gestión de riesgos empresariales concibe el riesgo como parte inherente de la estrategia y del desempeño. Es un proceso transversal, realizado por toda la organización, para identificar eventos potenciales que puedan afectarla, gestionar los riesgos dentro del apetito definido y brindar una seguridad razonable sobre el logro de los objetivos.

Componentes fundamentales.

1. Ambiente de control: valores, ética, estructura y responsabilidades.
2. Establecimiento de objetivos: metas claras y alineadas con el apetito de riesgo.
3. Identificación de eventos: detección oportuna de amenazas y oportunidades.
4. Evaluación de riesgos: análisis de probabilidad e impacto, inherente y residual.
5. Respuesta al riesgo: evitar, reducir, compartir o aceptar, con criterios explícitos.
6. Actividades de control: políticas y procedimientos para ejecutar las respuestas.
7. Información y comunicación: datos relevantes, oportunos y trazables para decidir.
8. Supervisión: monitoreo continuo, auditoría y mejora basada en resultados.

Aplicación al contexto de PROIMA.

Este enfoque permite integrar el riesgo de ciberseguridad en la gestión estratégica, no como función técnica aislada, sino como parte de la gobernanza y la toma de decisiones. Supone definir apetito y tolerancias, roles y métricas, articular el mapa de riesgos con el SGSI y reportar avances con evidencias verificables de control y mejora continua.

2.4.2.2 METODOLOGÍA NIST SP 800-30

Descripción metodológica.

La NIST SP 800-30 ofrece una guía estructurada para evaluar riesgos en sistemas de TI dentro de un enfoque de gestión basado en riesgos. Es agnóstica en cuanto a herramientas: define “qué hacer” y “cómo pensar” el riesgo, sin prescribir plataformas específicas. Parte de la caracterización del sistema y de sus dependencias, relaciona activos con amenazas y vulnerabilidades, estima probabilidad e impacto y produce salidas accionables para decidir

tratamientos y priorizar controles, en modalidades cualitativas o cuantitativas.

Fases del proceso.

1. Preparación y caracterización del sistema: delimitar alcance, activos, procesos y dependencias.
2. Identificación de amenazas: listar eventos intencionales y no intencionales relevantes para el entorno.
3. Análisis de vulnerabilidades: reconocer debilidades técnicas, de proceso y humanas explotables.
4. Evaluación de controles existentes: inventariar controles preventivos, detectivos y correctivos en vigor.
5. Estimación de probabilidad: valorar la verosimilitud de explotación considerando contexto y controles.
6. Análisis de impacto: estimar consecuencias operativas, legales, financieras y reputacionales.
7. Determinación del nivel de riesgo: sintetizar probabilidad e impacto para priorizar escenarios.
8. Recomendaciones de tratamiento: proponer mitigaciones, transferencias, evitaciones o aceptación.
9. Documentación de resultados: registrar supuestos, criterios, niveles de riesgo, responsables y plazos.

Aplicabilidad a PROIMA

Su énfasis en sistemas de TI resulta especialmente pertinente para operaciones de distribución y gestión logística intensivas en tecnología. Permite vincular aplicaciones, integraciones con terceros y plataformas de soporte con riesgos concretos, priorizar controles de mayor efecto (identidades y accesos, gestión de vulnerabilidades, continuidad y proveedores críticos) y emitir productos verificables: registro de riesgos por sistema, criterios de aceptación, plan de tratamiento con responsables, hitos e indicadores, integrados al SGSI y a los planes de continuidad.

2.4.2.3 METODOLOGÍA OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) es una metodología de evaluación de riesgos centrada en activos y orientada a la operación. Parte del

principio de que la seguridad debe sostener la continuidad y los objetivos del negocio, priorizando la tríada confidencialidad, integridad y disponibilidad. Existen variantes adaptativas OCTAVE-S, Allegro y FORTE que simplifican o profundizan el enfoque según el tamaño y la madurez de la organización, manteniendo la lógica común de construir perfiles de riesgo a partir del conocimiento interno.

Fases del proceso.

1. Perfiles de amenaza basados en activos: identificación de activos de información críticos, contexto de uso y criterios de impacto.
2. Exposición tecnológica y operativa: levantamiento de vulnerabilidades en infraestructura, procesos y terceros que pueden afectar los activos.
3. Estrategia y plan de seguridad: priorización de riesgos, selección de tratamientos y definición de planes con responsables, plazos e indicadores.

Características distintivas.

- Autodirigida por la organización: el equipo interno conduce talleres y entrevistas, capitalizando conocimiento de procesos.
- Enfoque operativo y pragmático: prioriza activos críticos y escenarios con efecto directo en la continuidad.
- Visión socio-técnica: integra aspectos técnicos, organizacionales y de terceros en una sola narrativa de riesgo.
- Colaboración multidisciplinaria: convoca a operaciones, TI, cumplimiento, logística y atención al cliente para consensuar criterios.
- Salidas accionables: perfiles de riesgo, mapa de prioridades y plan de tratamiento medible y verificable.

Aplicabilidad a PROIMA.

El énfasis operativo de OCTAVE encaja con un negocio de distribución donde la continuidad es clave. Permite reunir a logística, TI y áreas de soporte para identificar activos críticos WMS, TMS, ERP, integraciones EDI y API, CRM, endpoints de campo, definir criterios de impacto, mapear vulnerabilidades propias y de terceros, y construir un plan de tratamiento priorizado. El resultado se integra con el SGSI y los planes de continuidad, con métricas de seguimiento que demuestran reducción de riesgo y mejoran la resiliencia en ciclos iterativos.

2.4.3 INSTRUMENTOS UTILIZADOS

2.4.3.1 MATRICES DE EVALUACIÓN DE RIESGOS

Fundamentación Técnica:

Las matrices de riesgo son herramientas clave para priorizar riesgos ya identificados. Representan de forma bidimensional la probabilidad de ocurrencia frente al impacto potencial, convirtiendo el análisis en un mapa visual sencillo y compartible. Con ellas se gana comparabilidad entre escenarios, se explicitan supuestos y se facilitan decisiones informadas sobre tratamientos y asignación de recursos.

Componentes estructurales

- Escalas de probabilidad: niveles cualitativos o cuantitativos con descriptores y anclajes claros.
- Escalas de impacto: categorías de consecuencia (operacional, legal, financiera, reputacional, etc.).
- Niveles de riesgo: resultado de la intersección probabilidad–impacto (p. ej., bajo, medio, alto, crítico).
- Criterios de aceptabilidad: umbrales y tolerancias que definen cuándo mitigar, transferir, evitar o aceptar.
- Reglas de lectura: colores, leyendas y notas metodológicas que aseguran trazabilidad e interpretación consistente.

Aplicación en PROIMA

Las matrices permitirán priorizar sistemáticamente los riesgos sobre los activos de información y procesos críticos, orientar la asignación eficiente de recursos y seleccionar tratamientos con mayor reducción marginal del riesgo. Asimismo, servirán para definir indicadores de seguimiento, revisar periódicamente el riesgo residual y demostrar, con evidencia, la eficacia de los controles dentro del SGSI.

2.4.3.2 CUESTIONARIOS DE DIAGNÓSTICO DE CIBERSEGURIDAD

Fundamentación Metodológica:

Los cuestionarios de autoevaluación estructuran la recolección de información sobre el estado real de la seguridad organizacional. Permiten identificar vulnerabilidades, estimar el nivel de exposición y comparar áreas y procesos bajo criterios homogéneos. Al utilizar escalas de madurez y pedir evidencias de soporte, convierten percepciones en datos trazables para priorizar

mejoras y orientar decisiones.

Dimensiones de evaluación.

- Políticas y procedimientos: existencia, vigencia y aplicación efectiva.
- Controles técnicos: implementación y gestión de medidas de protección y monitoreo.
- Gestión de accesos: administración de identidades, privilegios y autenticación.
- Capacitación y concienciación: cobertura, frecuencia y efectividad del entrenamiento.
- Gestión de incidentes: capacidades de detección, respuesta, recuperación y aprendizaje.
- Cumplimiento normativo: alineación con estándares, contratos y regulaciones aplicables.

Aplicación en PROIMA.

Estos cuestionarios facilitarán el levantamiento sistemático de información sobre la postura de ciberseguridad, permitiendo detectar brechas y priorizar acciones. Sus resultados servirán como línea base para el SGSI, alimentarán la matriz de riesgos y se traducirán en planes de tratamiento con responsables, plazos e indicadores de seguimiento.

2.4.3.3 HERRAMIENTAS DE EVALUACIÓN DE MADUREZ

Fundamentación Conceptual:

Las herramientas de evaluación de madurez permiten medir el grado de desarrollo y sofisticación de las capacidades de ciberseguridad de una organización. Transforman percepciones en evidencias comparables, identifican brechas por dominio (personas, procesos, tecnología y terceros) y priorizan mejoras con una hoja de ruta clara. Su utilidad radica en establecer una línea base objetiva, fijar metas alcanzables y demostrar progreso en el tiempo.

Niveles de madurez típicos.

- Inicial (ad hoc): prácticas reactivas, dependencia de personas clave, baja repetibilidad.
- Gestionado: procesos documentados de forma parcial y ejecución desigual.
- Definido: procesos estandarizados, roles claros y entrenamiento básico.
- Gestionado cuantitativamente: métricas, umbrales y control estadístico del desempeño.
- Optimizante: mejora continúa basada en datos, lecciones aprendidas y automatización selectiva.

Cómo se aplican.

Las evaluaciones combinan cuestionarios estructurados, revisión de evidencias, entrevistas y muestreo de controles. Entregan puntuaciones globales y por dominio, así como recomendaciones priorizadas según impacto y esfuerzo. Para asegurar consistencia, conviene

definir criterios de scoring, periodicidad (por ejemplo, semestral), responsables de cada dominio y mecanismos de verificación independiente.

Aplicación en PROIMA.

Estas herramientas permitirán fijar la línea base de madurez en identidades y accesos, gestión de vulnerabilidades, continuidad, seguridad de proveedores y protección de datos. Con ello se construirá una hoja de ruta por hitos metas trimestrales, responsables e indicadores integrada al SGSI. El seguimiento mostrará avances tangibles (riesgo residual, tiempos de detección y respuesta, cumplimiento de controles) y orientará la inversión hacia las iniciativas con mayor reducción marginal del riesgo.

2.4.3.4 CHECKLISTS DE VERIFICACIÓN DE CONTROLES

Fundamentación Práctica:

Los checklists son instrumentos de verificación sistemática que convierten requisitos de seguridad en preguntas claras y observables. Permiten comprobar el cumplimiento de controles, documentar evidencias, medir consistencia entre áreas y detectar desviaciones. Su contenido se deriva de estándares reconocidos y se actualiza conforme cambian riesgos y normativas. Bien diseñados, reducen la ambigüedad, facilitan auditorías y alimentan la mejora continua del SGSI.

Categorías de controles.

- Organizacionales: políticas, procedimientos, roles, responsabilidades, gobierno y métricas.
- De personal: inducción, capacitación, concienciación, segregación de funciones y gestión de privilegios.
- Físicos: protección de instalaciones, acceso a áreas sensibles, resguardo de equipos y medios.
- Tecnológicos: endurecimiento de configuraciones, control de acceso, gestión de parches y vulnerabilidades, respaldo y cifrado, monitoreo y telemetría.
- De procesos: gestión de cambios, continuidad y recuperación, respuesta a incidentes y lecciones aprendidas.
- De terceros: evaluación y seguimiento de proveedores críticos, requisitos contractuales y evidencias de cumplimiento.

Buenas prácticas de uso

Definir criterios de evaluación y umbrales, exigir evidencias objetivas, aplicar muestreos

representativos, registrar hallazgos con responsables y plazos, y revisar periódicamente el checklist para mantenerlo alineado a riesgos y estándares. Complementar con pruebas de efectividad y verificación independiente cuando corresponda.

Aplicación en PROIMA.

Los checklists permitirán evaluar en detalle el grado de cumplimiento por dominio, identificar implementaciones sólidas y áreas a fortalecer, y priorizar acciones con base en impacto y esfuerzo. Sus resultados se integrarán al registro de riesgos y al plan de tratamiento del SGSI, con indicadores de seguimiento que muestren evolución del riesgo residual y eficacia de los controles en el tiempo.

2.5 ANÁLISIS DE LAS METODOLOGÍAS

2.5.1. MATRIZ DE COHERENCIA VERTICAL

La Matriz de Coherencia Vertical es un recurso académico que busca garantizar la consistencia interna de un proyecto de investigación. Su función principal es evidenciar la relación lógica entre los elementos centrales de la investigación: problema, objetivos, preguntas, hipótesis y diseño metodológico. Desde una perspectiva conceptual, este instrumento se fundamenta en la idea de que todo trabajo científico debe mantener un hilo conductor que evite contradicciones y asegure claridad en la formulación del estudio (Chan, 2020).

En el plano teórico, la matriz se asocia con los principios de validez y rigor metodológico. La coherencia no solo es un requisito formal, sino también epistemológico, ya que permite al investigador demostrar que sus decisiones metodológicas derivan directamente del problema planteado. De esta manera, se asegura que las preguntas encuentran respuesta en los objetivos, que estos se corresponden con las hipótesis y que el diseño metodológico es congruente con la naturaleza de la investigación (Chan, 2020).

Además, la Matriz de Coherencia Vertical se entiende como una herramienta de evaluación y seguimiento académico. Permite a asesores, comités y pares revisores verificar que el planteamiento de la investigación está estructurado de manera lógica y sistemática, facilitando la trazabilidad del conocimiento generado. Su conceptualización se inscribe dentro de las metodologías de planeación investigativa, donde la claridad, la consistencia y la pertinencia son indicadores esenciales de calidad científica (Chan, 2020).

2.5.2 DECLARACIÓN DE REFLEXIVIDAD

La declaración de reflexividad es un elemento central en investigaciones cualitativas, ya que reconoce la influencia que tiene el propio investigador en el proceso de producción del conocimiento. Este concepto parte de la premisa de que todo análisis se construye desde una perspectiva situada, atravesada por experiencias, valores y posiciones del investigador. Por ello, la reflexividad busca visibilizar dichas influencias y hacer explícitas las posibles implicaciones en la interpretación de los hallazgos (Mendieta & Ramírez, 2025).

En términos conceptuales, la reflexividad contribuye a la validez y transparencia del estudio, pues obliga al investigador a reconocer sus propias creencias y vínculos con el objeto de investigación. Esto permite anticipar posibles sesgos, establecer mecanismos de control y generar confianza en la rigurosidad del proceso científico. La reflexividad, entonces, no elimina la subjetividad, sino que la gestiona como un componente inevitable pero controlable de la investigación (Mendieta & Ramírez, 2025).

Asimismo, la literatura académica enfatiza que la reflexividad se expresa a través de prácticas sistemáticas: explicitar la posición del investigador, documentar decisiones metodológicas, y aplicar técnicas de verificación como la triangulación o la revisión independiente de datos. Estas medidas fortalecen la credibilidad del estudio al mostrar cómo se tomaron precauciones frente a los riesgos de parcialidad o sesgos interpretativos (Cinkara et al., 2024).

Finalmente, la declaración de reflexividad constituye una herramienta ética y epistemológica que aporta rigor a la investigación. Al reconocer la doble condición del investigador como observador y partícipe del contexto, se transforma un posible riesgo en una fortaleza: la cercanía con el objeto de estudio brinda acceso privilegiado a la información, pero también exige un compromiso explícito con la transparencia, la autocrítica y la coherencia en cada fase del análisis (Cinkara et al., 2024).

2.5.3. ESTRATEGIA DE TRIANGULACIÓN

La estrategia de triangulación es un enfoque metodológico que busca incrementar la validez y la fiabilidad de los resultados mediante la combinación de diferentes fuentes de datos, métodos, teorías o investigadores. Su origen está vinculado con la metáfora de la navegación: al observar un mismo punto desde distintas perspectivas, se obtiene una ubicación más precisa. En investigación,

este principio se traduce en la necesidad de contrastar evidencias para reducir sesgos y asegurar una comprensión más completa del fenómeno estudiado (Aguilar Gavira & Barroso Osuna, 2015).

Desde un plano conceptual, la triangulación se fundamenta en la idea de que ninguna técnica por sí sola puede capturar la complejidad de los fenómenos sociales o tecnológicos. Al integrar diversas aproximaciones, se enriquece la interpretación y se fortalece la credibilidad de los hallazgos. Esto responde a criterios de rigor científico, ya que obliga al investigador a corroborar patrones y discrepancias antes de llegar a conclusiones definitivas (Aguilar Gavira & Barroso Osuna, 2015).

La literatura identifica diferentes formas de triangulación: de datos (uso de múltiples fuentes de información), de métodos (aplicación de técnicas cualitativas y cuantitativas), de teoría (contrastar resultados desde distintos marcos conceptuales) y de investigadores (involucrar a varios analistas en el proceso). Cada modalidad aporta una perspectiva complementaria y, en conjunto, refuerzan la consistencia lógica y empírica de la investigación (Villas et al., 2025).

Finalmente, la estrategia de triangulación no debe entenderse únicamente como un recurso técnico, sino como una postura epistemológica. Implica reconocer la complejidad del objeto de estudio y asumir que el conocimiento se construye desde la diversidad de miradas y experiencias. En este sentido, la triangulación contribuye a generar resultados más sólidos, verificables y útiles para la comunidad académica y profesional, al tiempo que fortalece la confianza en la investigación como proceso sistemático y transparente (Villas et al., 2025).

2.5.4. INSTRUMENTOS DE ANÁLISIS METODOLÓGICO

Los instrumentos de análisis metodológico constituyen recursos que permiten organizar, sistematizar y representar de manera comprensible la información obtenida en una investigación. Su uso tiene un fundamento conceptual ligado a la necesidad de visibilizar la estructura de los datos, las relaciones entre variables y la correspondencia entre los elementos centrales del estudio. De este modo, los instrumentos no solo cumplen una función operativa, sino que también contribuyen a garantizar la transparencia y la trazabilidad científica (Medina et al., 2025).

En este marco, las matrices de coherencia y brechas se conceptualizan como herramientas gráficas que evidencian el grado de alineación entre los objetivos de investigación y los estándares o referentes teóricos. Estas matrices permiten identificar vacíos, inconsistencias o áreas de mejora, ofreciendo un panorama estructurado para evaluar la congruencia del diseño investigativo. Su

aporte teórico radica en que proporcionan un mecanismo verificable de validación interna (Medina et al., 2025).

Por su parte, los mapas conceptuales son instrumentos de análisis que representan de manera visual categorías, relaciones y jerarquías extraídas de la información. Desde un plano teórico, responden al enfoque constructivista, al facilitar la codificación de datos y la comprensión de conceptos emergentes. Su utilidad radica en que favorecen la síntesis, permiten identificar patrones y ayudan a construir marcos explicativos más claros y consistentes (Idrus et al., 2023).

Finalmente, las matrices de categorización constituyen un medio para clasificar y simplificar grandes volúmenes de datos, agrupándolos en categorías significativas. Conceptualmente, se fundamentan en la teoría del análisis de contenido, al permitir transformar información cualitativa en unidades comparables y organizadas. Su empleo asegura que los resultados no se presenten de forma fragmentada, sino que reflejen una estructura lógica y coherente que da soporte a las conclusiones de la investigación (Idrus et al., 2023).

2.6 ANTECEDENTES DE LAS METODOLOGÍAS

En el estudio realizado por Kurniawan et al., (2022) analizaron el nivel de madurez de un sistema de información académico en Indonesia, tomando como referencia el estándar internacional ISO/IEC 27002:2013. La investigación tuvo como propósito identificar brechas en la gestión de seguridad de la información y proponer mejoras alineadas con las mejores prácticas globales. Para ello, se aplicaron instrumentos como entrevistas semiestructuradas, observación de procesos y revisión documental, lo que permitió captar distintas perspectivas sobre las debilidades y fortalezas del sistema evaluado.

La metodología se sustentó en la triangulación de técnicas de recolección de datos, lo que incrementó la credibilidad y validez de los hallazgos. Posteriormente, se utilizó un análisis de brechas (gap analysis) para comparar el estado actual frente al nivel esperado de madurez, identificando discrepancias críticas en el cumplimiento de los controles de seguridad. Los resultados demostraron la necesidad de implementar políticas más robustas, controles técnicos estandarizados y procesos de auditoría continua. Este antecedente metodológico resulta relevante porque evidencia cómo la triangulación y las matrices comparativas permiten estructurar diagnósticos precisos en estudios de seguridad de la información (Kurniawan et al., 2022).

Por otra parte, Alazzawi (2021) evaluó el nivel de aplicación del estándar internacional

ISO/IEC 27005:2018 para la gestión de riesgos de seguridad de la información dentro de la Comisión Electoral Independiente de Bagdad (Iraq). El objetivo fue determinar qué tan alineados estaban los mecanismos de políticas, procedimientos administrativos y técnicas con los requerimientos normativos del estándar. Para ello, se recurrió a una variedad de fuentes de datos entrevistas con expertos institucionales (gerentes, jefes de departamento, encargados de acceso a sistemas), observación en terreno y revisión documental con el fin de realizar un análisis holístico y riguroso del sistema de gestión de riesgos (Allawazi, 2021).

El enfoque metodológico se fundamentó en la triangulación de técnicas de recolección de datos, lo que permitió contrastar perspectivas y aumentar la validez de los hallazgos. Además, se utilizó un análisis de brechas (gap analysis) para identificar las discrepancias entre la situación actual y las exigencias del estándar. Como resultados, se evidenciaron faltas significativas en la documentación, la implementación de estrategias claras y la aplicación consistente de controles de hardware y medios electrónicos. Este antecedente ilustra de forma efectiva cómo la combinación de triangulación y análisis de brechas es capaz de revelar vacíos críticos y orientar propuestas de mejora en contextos institucionales concretos (Allawazi, 2021).

Finalmente, Putra y Soewito (2023), se aplicó una metodología integrada en el contexto de un sistema ERP utilizado por la aseguradora ZZZ Insurance. El diseño metodológico combinó el estándar ISO/IEC 27005:2018 como marco principal de gestión de riesgos, junto con las directrices de evaluación de riesgos del NIST SP 800-30 (Rev. 1), y se utilizó ISO/IEC 27002 para fundamentar las recomendaciones de controles. Esta integración buscó consolidar un enfoque estructurado y robusto para evaluar y mitigar los riesgos asociados al sistema (Putra & Soewito, 2023).

La investigación siguió un proceso detallado que incluyó nueve pasos: caracterización del sistema, identificación de amenazas y vulnerabilidades, análisis de controles, determinación de probabilidad e impacto, establecimiento del nivel de riesgo, recomendaciones de controles y elaboración de un informe final de evaluación de riesgos. Esta propuesta metodológica representa un aporte significativo, ya que articula estándares internacionales complementarios, consolidando un enfoque riguroso y adaptable aplicable en entornos organizacionales complejos (Putra & Soewito, 2023).

2.7 HERRAMIENTAS A UTILIZAR

La selección de herramientas no puede ser arbitraria: debe responder a los requerimientos

metodológicos del proyecto (trazabilidad, colaboración, análisis cualitativo y cuantitativo reproducible, y gestión bibliográfica conforme a APA 7). En este apartado se comparan alternativas por categoría y se justifica la elección final con base en criterios de idoneidad, costo, curva de aprendizaje e integración con el flujo de tesis.

2.7.1 GESTIÓN DE PROYECTOS Y COLABORACIÓN

Tabla 7: Gestión de proyectos y colaboración

Herramienta	Descripción breve	Ventajas (contextualizadas al proyecto)	Limitaciones	Costo/Licencia	URL oficial
Trello	Tableros Kanban para organizar tareas	Curva de aprendizaje mínima; tarjetas con checklist y adjuntos; buena visibilidad de pendientes	Menos robusto en flujos complejos y reportes nativos	Gratuito + planes	https://trello.com/ (trello.com, Atlassian Support)
Asana	Plataforma de work management con vistas múltiples y automatizaciones	Portafolios, dependencias, formularios; automatiza estados y riesgos	Funciones avanzadas requieren plan de pago	Suscripción	https://asana.com/product (Asana, help.asana.com)
Jira Cloud	Gestión ágil (Scrum/Kanban) integrable con flujos y APIs	Workflows configurables y trazabilidad de cambios (útil para control de versiones de tareas)	Más técnico y con mayor complejidad inicial	Suscripción (versión gratuita limitada)	https://www.atlassian.com/software/jira/guides/getting-started/introduction (atlassian.com, Atlassian Support)
Notion	Espacio conectado (wiki, bases de datos, tareas, notas)	Unifica actas, cronograma, fichas de lectura y tableros en un solo lugar	Requiere buena estructuración inicial para escalar	Gratuito + planes	https://www.notion.so/guides/what-is-notion (Notion)

Fuente: Elaboración Propia

Selección final (gestión de proyectos): Notion.

Razón: permite centralizar en un mismo entorno el wiki del proyecto, el tablero de tareas,

las minutas y los insumos de análisis sin fragmentar la información entre varias apps. Para un equipo pequeño de tesis, esta unificación reduce fricción y mejora trazabilidad; Trello y Jira son excelentes para flujos ágiles, pero Notion resuelve mejor la documentación viva + gestión básica de tareas que necesita la investigación

2.7.2 OFIMÁTICA

Tabla 8: Herramientas de ofimática

Herramienta	Descripción	Ventajas	Limitaciones	Costo/Licencia	URL oficial
Microsoft 365	Suite de apps (Word, Excel, PowerPoint, OneDrive, Teams) con colaboración y funciones de IA	Compatibilidad impecable con formatos .docx, control de cambios y plantillas académicas	Modelo de suscripción	Suscripción (frecuente acceso institucional)	https://www.microsoft.com/microsoft-365/products-apps-services (Microsoft, Microsoft Learn)
Google Workspace	Apps en la nube (Docs, Sheets, Slides, Drive, Meet)	Colaboración en tiempo real, control de versiones, fácil compartición	Conversión de formatos a veces altera maquetación	Suscripción/planes	https://workspace.google.com/ (Google Workspace)
LibreOffice	Suite libre y gratuita compatible con formatos MS	Sin costo; buena compatibilidad y comunidad	Algunas plantillas/formatos avanzados requieren ajuste	Gratuito	https://www.libreoffice.org/ (LibreOffice)

Fuente: Elaboración Propia

Selección final (ofimática): Microsoft 365 (Word/Excel/PowerPoint).

Razón: el capítulo demanda control de cambios, estilos y referencias con alta fidelidad en .docx y presentaciones, lo que Word/PowerPoint resuelven de forma nativa y robusta; además Excel será útil para cuadros de resultados y limpieza de datos.

2.7.3 ANÁLISIS DE DATOS CUALITATIVOS (CAQDAS)

Tabla 9: Análisis de datos cualitativos

Herramienta	Descripción	Ventajas	Limitaciones	Costo/Licencia	URL oficial
NVivo	Software líder para organizar, codificar y analizar datos no estructurados	Amplio ecosistema, consultas avanzadas, colaboración en la nube	Licencia de pago	Licencia/suscripción	https://lumivero.com/products/nvivo/ Lumivero
ATLAS.ti	CAQDAS con funciones de IA (NLP, NER, sentimiento)	Automatizaciones que aceleran la codificación; versión web	Licencia de pago	Licencia/suscripción	https://atlasti.com/features ATLAS.ti
MAXQDA (Analytics Pro)	CAQDAS + módulo Stats para mixtos	Buenas visualizaciones y puente cuantitativo	Licencia de pago	Licencia/suscripción	https://www.maxqda.com/products MAXQDA
QDA Miner Lite	Versión gratuita para codificación básica	Sin costo; suficiente para proyectos pequeños	Funciones avanzadas limitadas	Gratuito	https://provalisresearch.com/products/qualitative-data-analysis-software/freeware/ Provalis Research

Fuente: Elaboración Propia

Selección final (cualitativo): NVivo.

Razón: ofrece consultas, matrices y flujos colaborativos adecuados para codificar entrevistas/observaciones y producir evidencia trazable para el capítulo de resultados. Si no se dispone de licencia institucional, QDA Miner Lite funcionaría como alternativa mínima viable.

2.7.4 ANÁLISIS DE DATOS CUANTITATIVOS/ESTADÍSTICOS

Tabla 10: Análisis de datos cuantitativos

Herramienta	Descripción	Ventajas	Limitaciones	Costo/Licencia	URL oficial
IBM SPSS Statistics	Plataforma estadística con interfaz guiada	Muy extendido en ciencias sociales; módulos avanzados	Licencia de pago	Licencia/GradPack	https://www.ibm.com/products/spss-statistics IBM

Stata	Software integral para análisis reproducible	Do-files y amplio ecosistema académico	Licencia de pago	Licencia	https://www.stata.com/ stata.com
R	Entorno libre para estadística y gráficos	Gratis; paquetes para casi cualquier técnica	Requiere programación	Gratuito	https://www.r-project.org/ r-project.org
JASP	GUI libre basada en R con salidas en estilo APA	Gratuito; facilita análisis frecuentes y bayesianos	Menos flexible que R puro	Gratuito	https://jasp-stats.org/ jasp-stats.org

Fuente: Elaboración Propia

Selección final (cuantitativo): SPSS.

Razón: ofrece una interfaz intuitiva y ampliamente difundida en el ámbito académico, con capacidades robustas para análisis descriptivos e inferenciales, así como modelos multivariados, generando tablas y salidas fácilmente exportables y adaptables al formato APA. Su uso resulta suficiente para las pruebas estadísticas requeridas en el proyecto y, en caso de necesitarse modelado más avanzado o automatización, puede complementarse con R o Python.

El acceso a la licencia de SPSS se obtuvo inicialmente mediante la versión de prueba gratuita de 30 días, complementada posteriormente con una suscripción de un mes adicional de pago, lo que garantizó la disponibilidad del software durante todo el periodo de procesamiento y análisis estadístico de los datos.

2.7.5 GESTOR DE REFERENCIAS BIBLIOGRÁFICAS

Tabla 11: Gestor Bibliográfico

Herramienta	Descripción	Ventajas	Limitaciones	Costo/Licencia	URL oficial
Zotero	Gestor libre y de código abierto	Integración con Word/Google Docs, anotación PDF, sincronización	Límite gratuito de almacenamiento en la nube	Gratuito (planes de almacenamiento opcionales)	https://www.zotero.org/ zotero.org
Mendeley	Gestor propietario	Buen clipper y grupos;	Ecosistema propietario	Gratuito (con cuenta)	https://www.mendeley.com/ mendeley.com

	con Web Importer y Cite	integración con Word			
EndNote	Gestor profesional con funciones avanzadas	Ecosistema robusto, plantillas de revistas	Licencia de pago	Licencia	https://endnote.com/ EndNote

Fuente: Elaboración Propia

Selección final (referencias): Zotero.

Razón: es gratuito, robusto y colaborativo, con conectores que facilitan capturar metadatos y generar citas/REFERENCIAS en APA 7 de forma consistente.

2.8 MARCO LEGAL

El marco legal define límites, obligaciones y buenas prácticas para la recolección, tratamiento y resguardo de la información. En un proyecto de seguridad de la información y gestión de riesgos, su función es normar la metodología (consentimiento, minimización, medidas de seguridad, continuidad, controles y evidencia de cumplimiento).

2.8.1 MARCO LEGAL Y NORMATIVO INTERNACIONAL

La gestión de riesgos de seguridad de la información se encuentra respaldada por un conjunto de normas y regulaciones internacionales que establecen parámetros mínimos de protección y gobernanza digital. Estos marcos, impulsados por organismos multilaterales y entidades de estandarización, buscan armonizar criterios frente al incremento de amenazas cibernéticas y la circulación transfronteriza de datos. Su aplicación no solo garantiza el cumplimiento normativo, sino que también fortalece la confianza de clientes y socios, promueve la competitividad y ofrece lineamientos que permiten a las organizaciones implementar sistemas de gestión de seguridad más robustos y alineados con las mejores prácticas globales.

Tabla 12: Marco Internacional

Instrumento	Organismo / Año	Relevancia estratégica para el proyecto
ISO/IEC 27001:2022 (SGSI)	ISO/IEC, 2022	Establece requisitos para implementar y mejorar un SGSI que enmarca políticas, análisis de riesgos y controles anexos. Base para madurez y auditoría.
ISO/IEC 27005:2022 (gestión de riesgos)	ISO/IEC, 2022	Guía detallada para identificar, analizar, evaluar y tratar riesgos de seguridad de la información. Sustenta la matriz de riesgos de la tesis.
ISO 22301:2019 (continuidad del negocio)	ISO, 2019	Define requisitos para continuidad y recuperación (RTO/RPO), alineando controles de continuidad con el SGSI.

NIST SP 800-30 Rev.1 (evaluación de riesgos)	NIST, 2012	Proporciona metodología para evaluar riesgos (amenazas, vulnerabilidades, probabilidad e impacto) complementaria a ISO 27005.
NIST SP 800-53 Rev.5 (controles de seguridad y privacidad)	NIST, 2020	Catálogo de controles (AC, AU, CM, etc.) útil para mapear salvaguardas propuestas al contexto organizacional.
Reglamento (UE) 2016/679 – GDPR	UE, 2016	Estándar internacional de referencia en protección de datos (licitud, transparencia, derechos, medidas técnicas/organizativas). Marco comparativo de buenas prácticas.
OWASP Top 10 (riesgos de aplicaciones)	OWASP, 2021	Taxonomía de riesgos frecuentes en aplicaciones web, insumo para el análisis de amenazas técnicas.

Fuente: Elaboración Propia

Análisis:

ISO/IEC 27001 define el sistema de gestión y niveles de evidencia (políticas, procedimientos, registros) que el proyecto puede adoptar para asegurar mejora continua (PDCA), mientras que ISO/IEC 27005 y NIST SP 800-30 guían la evaluación y tratamiento de riesgos que alimentará la matriz de controles.

NIST SP 800-53 facilita mapear salvaguardas (p. ej., control de accesos, registro de auditoría, gestión de configuración) a las brechas halladas, y ISO 22301 asegura que las medidas contemplen continuidad y recuperación ante incidentes.

GDPR, aunque no aplicable directamente en Honduras sirve como benchmark de privacidad por diseño y obligaciones de seguridad (art. 5, 24, 32), integrable a las políticas internas como buena práctica. OWASP apoya el análisis de riesgos específicos de aplicaciones.

2.8.2 MARCO LEGAL NACIONAL

En el ámbito nacional, la gestión de riesgos de seguridad de la información se encuentra en un proceso de consolidación normativa que responde tanto a la necesidad de proteger los activos digitales como a las exigencias de competitividad y confianza en el entorno hondureño. El país ha avanzado en la formulación de leyes, políticas y planes estratégicos orientados a regular el uso responsable de las tecnologías, la protección de datos personales, la prevención del ciberdelito y la adopción de estándares internacionales. Este marco legal nacional constituye la base para orientar a las organizaciones en la implementación de controles, asegurar la continuidad de los servicios críticos y promover un ecosistema digital más seguro y sostenible en línea con los desafíos actuales del contexto global.

Tabla 13: Marco Nacional

Norma	Órgano / Año (Decreto / Publicación)	Relevancia estratégica
Ley de Transparencia y Acceso a la Información Pública	Congreso Nacional, 2006 (Decreto 170-2006; La Gaceta 2007)	Reconoce hábeas data y la protección de datos personales; fija lineamientos para clasificación/desclasificación y acceso responsable a la información. onadici.gob.hn+1conatel.gob.hn
Lineamientos IAIP para clasificación y desclasificación de información (Acuerdo IAIP-002-2010)	IAIP, 2010	Criterios de clasificación, plazos y test de daño que orientan la gestión documental y el resguardo de información sensible. onadici.gob.hn
Ley sobre Firmas Electrónicas	Congreso Nacional, 2013 (Decreto 149-2013)	Reconoce validez jurídica de firmas electrónicas y requisitos de certificados: clave para evidencia y no repudio en trámites y documentos electrónicos. Diccionario Jurídico RAEVLex
Ley sobre Comercio Electrónico	Congreso Nacional, 2014 (Decreto 149-2014; La Gaceta 2015)	Regula mensajes de datos, equivalencia funcional y soporte a transacciones electrónicas; relevante para validez probatoria y políticas de conservación. tsc.gob.hnmelarayasociados.com
Código Penal (vigente)	Congreso Nacional, 2017 (Decreto 130-2017)	Tipifica conductas relacionadas con acceso indebido, daños informáticos, fraude; sustento para el análisis de riesgo legal y respuesta a incidentes. tsc.gob.hn
Procedimiento Administrativo Electrónico (PCM-086-2020)	Poder Ejecutivo, 2020	Establece principios y procesos para la tramitación electrónica y protección de datos en la administración pública; guía para interacción con entidades. tsc.gob.hn
Sistema Nacional de Bases de Datos de ADN (Ley 57-2023)	Congreso Nacional, 2023	Incluye referencias a ciberseguridad y bioseguridad en el manejo de bases de datos sensibles; ilustra exigencias sectoriales de protección. tsc.gob.hn
Situación de la Ley General de Protección de Datos Personales	IAIP (borradores/anteproyecto) y socialización 2024	A la fecha, Honduras socializa un proyecto de ley; útil como horizonte regulatorio para alinear políticas internas a estándares modernos de privacidad. cei.iaip.gob.hnLexology

Fuente: Elaboración Propia

Análisis y justificación:

El bloque de transparencia y hábeas data (Ley de Transparencia + Lineamientos IAIP) obliga a clasificar información, definir quién accede a qué y bajo qué causales se restringe: tu metodología debe contemplar matrices de acceso, niveles de sensibilidad y procedimientos de desclasificación.

Firmas y comercio electrónicos aseguran la integridad, autenticidad y validez de documentos digitales (políticas de firma, resguardo de certificados, sellos de tiempo), relevantes para evidencias de auditoría y entregables electrónicos.

El Código Penal introduce un factor de riesgo legal (p. ej., daños informáticos) que debe verse reflejado en el registro de amenazas, controles de acceso, gestión de vulnerabilidades y plan de respuesta a incidentes.

Dado que la ley general de datos personales aún se encuentra en proceso de discusión/socialización, conviene adoptar proactivamente buenas prácticas alineadas a GDPR (consentimiento, minimización, medidas técnicas/organizativas, DPIA cuando aplique) para anticipar cumplimiento.

CAPÍTULO III. METODOLOGÍA

3.1. CONGRUENCIA METODOLÓGICA

La metodología de la presente investigación se concibe como un sistema integral, en el cual cada decisión responde directamente al problema planteado, a las preguntas formuladas y a los objetivos establecidos en el Capítulo I. De esta manera, no se trata de una serie de elecciones aisladas, sino de un entramado lógico que asegura coherencia entre los fundamentos teóricos, el diseño metodológico y los resultados esperados. Este tipo de investigación es pertinente cuando se desea obtener un panorama general de un fenómeno poco estudiado, permitiendo describirlo con mayor claridad. (Hernández-Sampieri, et al., 2018)

El carácter exploratorio-descriptivo de este estudio surge de la necesidad de comprender, en el contexto particular de PROIMA, cómo se gestionan actualmente los riesgos de seguridad de la información y cuáles son los desafíos más relevantes para alinear sus prácticas con los estándares internacionales. Por ello, la elección del enfoque cualitativo no se justifica por conveniencia, sino por su capacidad de captar la complejidad de los fenómenos organizacionales vinculados a la cultura, los procesos y las percepciones de los actores involucrados.

De igual forma, la selección de técnicas como entrevistas semiestructuradas, revisión documental y observación directa responde a la naturaleza del problema y a la ausencia de diagnósticos sistemáticos previos. Cada instrumento fue diseñado para garantizar trazabilidad y congruencia con los objetivos específicos, permitiendo contrastar la práctica real con los marcos de referencia establecidos por ISO/IEC 27001:2022 e ISO/IEC 27005:2018.

Así, la arquitectura metodológica integra un diseño en el que las decisiones de enfoque, alcance, técnicas e instrumentos se encuentran interdependientemente articuladas. Esta congruencia asegura que los hallazgos no solo sean consistentes con las preguntas de investigación, sino que además puedan generar insumos válidos para la toma de decisiones estratégicas en la gestión de riesgos de seguridad de la información en PROIMA.

3.1.1. MATRIZ METODOLÓGICA

Tabla 14: Matriz de Congruencia Metodológica

Problema	Preguntas (PICO)	Objetivos (SMART)	Metodología	Instrumentos	Variables	Indicadores
Falta de diagnóstico sistemático de riesgos de seguridad de la información en PROIMA que amenaza la continuidad y la confianza.	1. ¿En qué medida los controles de seguridad de la información (I) actualmente implementados en PROIMA (P), comparados con los referentes ISO/IEC 27001:2022 e ISO/IEC 27005:2018 (C), se alinean con dichos estándares y qué implicaciones observables tienen sobre la probabilidad e impacto de incidentes (O) durante septiembre de 2022 a septiembre de 2025 (T)?	Describir el grado de alineación de las prácticas y controles de gestión de riesgos de seguridad de la información de PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 (S), midiendo el cumplimiento porcentual de controles aplicables y las brechas por dominio mediante listados de verificación, revisión documental, entrevistas y observación de procesos (M), con el fin de priorizar oportunidades de mejora (A) que fortalezcan la seguridad organizacional y la continuidad del negocio (R) en el período septiembre de 2022 a septiembre de 2025 (T).	Mixto: cualitativa dominante con cuantitativo embebido (estudio de caso único, no experimental, transversal).	Guía de entrevistas semiestructuradas; lista de verificación de controles; ficha de revisión documental; cédula de observación; cuestionario estructurado Likert (1–5) para empleados.	Controles de SI; cultura de seguridad; continuidad del negocio; gestión de riesgos.	% de controles aplicables implementados; Nº de políticas/procedimientos vigentes; frecuencia de capacitación/simulacros; MTTD/MTTR; existencia y uso de métricas/reportes.
	2. ¿Qué papel desempeña la cultura organizacional asociada a la gestión de riesgos de seguridad de la información (I), frente	1. Evaluar el grado de alineación de los controles de seguridad de la información vigentes en PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 y determinar	Mixto (QUAL→quan): descriptivo-exploratorio.	Checklist de controles (Anexo A/27001 y 27005); entrevistas a TI/gestión;	Controles de SI (gobernanza, control de accesos/MFA, operaciones	% de cumplimiento por dominio; nº de hallazgos por control; existencia de

Problema	Preguntas (PICO)	Objetivos (SMART)	Metodología	Instrumentos	Variables	Indicadores
	a un enfoque predominantemente técnico (C), en la eficacia observada de las medidas preventivas y de respuesta a incidentes (O) en PROIMA (P) durante septiembre de 2022 a septiembre de 2025(T)?	sus implicaciones observables sobre la probabilidad e impacto de incidentes durante septiembre de 2022 a septiembre de 2025.		revisión de auditorías e incidentes; cuestionario (ítems sobre accesos/MFA, parcheo, respaldos).	, continuidad).	evidencias (registros/auditorías); tasa/tendencia de incidentes; % de adopción de MFA; % de pruebas de respaldo realizadas.
	3. En PROIMA (P), ¿Qué diferencias se observan, en la toma de decisiones para asegurar la continuidad del negocio (O) cuando no existen indicadores y medidas formales de seguimiento de riesgos de seguridad de la información (I), en comparación con un sistema de métricas alineado a ISO/IEC 27005:2018 (C), durante septiembre de 2022 a septiembre de 2025 (T)?	2. Examinar la relación entre la cultura organizacional vinculada a la gestión de riesgos de seguridad de la información y la eficacia observada de las medidas preventivas y de respuesta ante incidentes, en contraste con un enfoque exclusivamente técnico, durante septiembre de 2022 a septiembre de 2025.	Mixto (QUAL→quan): descriptivo.	Entrevistas a mandos/operativos; guía de observación; revisión de planes de capacitación/simulacros; cuestionario (ítems de cultura, reporte, capacitación).	Cultura de seguridad; eficacia preventiva y reactiva.	Frecuencia y calidad de capacitaciones; participación del personal; cumplimiento de protocolos; tiempos observados de respuesta; existencia de lecciones aprendidas; % que reportaría incidentes sin temor; media de “conocimiento de políticas”.

Problema	Preguntas (PICO)	Objetivos (SMART)	Metodología	Instrumentos	Variables	Indicadores
		3. Analizar las diferencias en la toma de decisiones para asegurar la continuidad del negocio cuando no existen indicadores y medidas formales de seguimiento de riesgos de seguridad de la información, frente a un sistema de métricas alineado a ISO/IEC 27005:2018, durante septiembre de 2022 a septiembre de 2025	Mixto (QUAL→quan): comparativa.	Revisión de reportes/actas de continuidad; entrevistas a gerencia; análisis de tableros existentes; cuestionario (percepción de uso de KPIs/ KRIs).	Continuidad del negocio; métricas/indicadores de riesgo.	Existencia/uso de KPIs/KRIs (riesgo inherente/residual); periodicidad de reportes; % de decisiones sustentadas en evidencia; impactos operativos documentados; MTTD/MTTR objetivo vs. observado.

Fuente: Elaboración Propia

3.1.2. ESQUEMA DE VARIABLES DE ESTUDIO

El esquema de variables plantea la interacción entre factores técnicos y organizativos que determinan la eficacia de la gestión de riesgos de seguridad de la información. Las variables independientes prácticas y controles, cultura de seguridad, métricas e indicadores, y gestión de riesgos con terceros se sustentan en los lineamientos de la ISO/IEC 27001 y la ISO/IEC 27005, donde se enfatiza que la seguridad debe abordarse de forma integral, combinando procesos, personas y tecnología. Estas dimensiones actúan como la base estructural desde la cual se evalúa la madurez organizacional frente a amenazas y vulnerabilidades.

Por su parte, las variables mediadoras gobernanza, capacitación y competencias, así como la higiene tecnológica explican cómo la capacidad institucional y el capital humano potencian o limitan la efectividad de los controles iniciales. De este modo, la variable dependiente se orienta a medir el nivel de madurez y desempeño de la gestión de riesgos de seguridad de la información (MGR-SI), en concordancia con modelos de madurez y con el problema de investigación. Así, la lógica del esquema vincula la teoría con la práctica, demostrando que la alineación de controles, cultura y gobernanza es esencial para que una organización alcance un sistema de gestión sólido y sostenible.

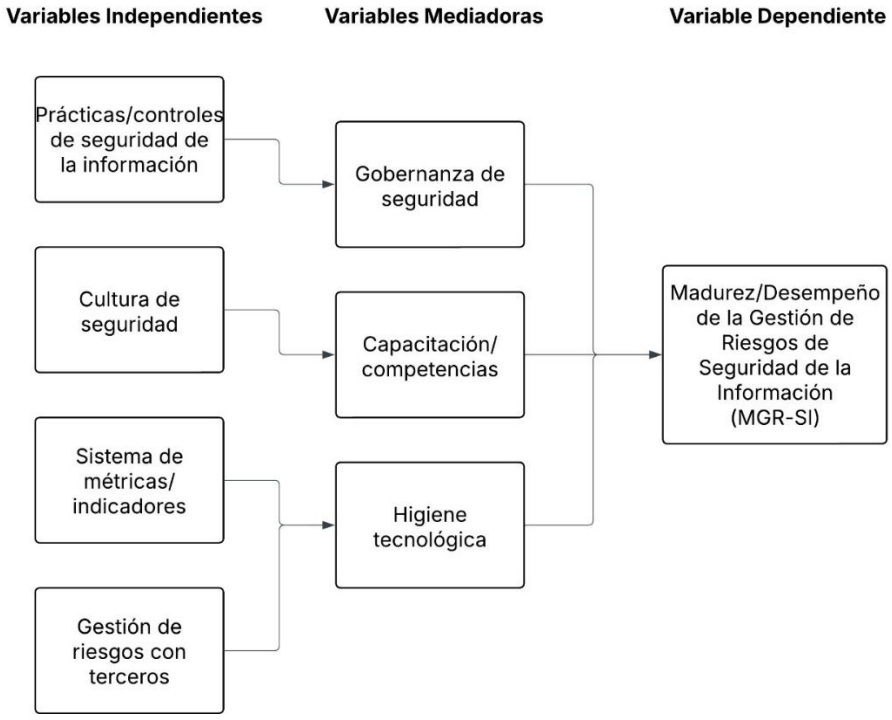


Figura 4: Esquema de Variables

Fuente: Elaboración Propia

3.1.3. OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 15: Operacionalización de Variables

Variable	Dimensión	Definición operativa (en PROIMA)	Indicador	Instrumento / Fuente	Escala / Unidad	Criterio de interpretación
VI1. Prácticas/controles de SI	Alineación ISO/IEC 27001–27005	Evidencia de controles aplicables en dominios del Anexo A.	% cumplimiento por dominio	Checklist ISO 27001:2022 – Ítems A.5.1 a A.5.37 (Matriz por control, Anexo 2)	% (0–100)	≥80% alto; 60–79% medio; <60% bajo
	Brechas por control	Controles sin evidencia o con implementación parcial.	Nº de brechas	Anexo 2, campos: Evidencia observada y Hallazgos/Brecha	Conteo (n)	0–1 bajo; 2–4 medio; ≥5 alto
VI2. Cultura de seguridad	Conocimiento y adhesión	Grado de acuerdo con afirmaciones sobre políticas, procedimientos y prácticas seguras.	Índice de cultura (media)	Cuestionario Cultura (Anexo 4, ítems 1–4, 9–12, 16)	Likert (1–5)	≥4 fuerte; 3–3.9 medio; <3 débil
	Reporte y aprendizaje	Percepción de reporte sin represalias y existencia de lecciones aprendidas.	% acuerdo reporte	Anexo 4, ítems 5–8 y 7; más postmortems (Anexo 3)	%	≥75% acuerdo + registros = favorable
VI3. Sistema de métricas (KPIs/KRIs)	Existencia/uso	Implementación de tableros y uso de indicadores de riesgo.	Nivel madurez KPIs	Revisión documental (Anexo 3: Tableros/KPIs) +	Ordinal (0–2)	2=operativo; 1=parcial; 0=crítico

Variable	Dimensión	Definición operativa (en PROIMA)	Indicador	Instrumento / Fuente	Escala / Unidad	Criterio de interpretación
				Entrevista (Anexo 5, preg. 10)		
	Trazabilidad	Decisiones sustentadas en métricas de riesgo o continuidad.	% decisiones con evidencia	Anexo 3, categoría Actas/Decisiones	%	≥70% bueno; 40–69% medio; <40% bajo
VI4. Gestión de riesgos con terceros	Due diligence y cláusulas	Inclusión de evaluaciones y cláusulas de seguridad en contratos.	Nivel control terceros	Revisión documental (Anexo 3: Contratos/Terceros) + Entrevista (Anexo 5, preg. 8–9)	Ordinal (bajo/medio/alto)	Alto = vigente y completo
	Protección de datos	Controles en la transferencia y clasificación de información.	Cumplimiento intercambio seguro	Anexo 3 (Contratos/SOPs)	Ordinal	Alto = políticas + evidencias
VM1. Gobernanza de seguridad	Roles y políticas	Existencia de roles claros (RACI) y políticas actualizadas.	% políticas vigentes	Anexo 3 (Políticas) + Entrevista (Anexo 5, preg. 1–2)	%	≥90% vigentes + RACI definido
VM2. Capacitación/competencias	Cobertura y frecuencia	Nº capacitaciones/año y % de personal cubierto.	% cobertura anual	Anexo 3 (Registros capacitación) + Cuestionario (Anexo 4, ítem 13)	%	≥2/año y ≥80% cobertura = adecuado
VM3. Higiene	Endpoint &	Porcentaje de	% parcheo /	Anexo 3	%	≥90% alto;

Variable	Dimensión	Definición operativa (en PROIMA)	Indicador	Instrumento / Fuente	Escala / Unidad	Criterio de interpretación
tecnológica	acceso	endpoints parchados y MFA en sistemas críticos.	% MFA	(Inventario TI) + Entrevista (Anexo 5, preg. 9)		75–89% medio; <75% bajo
VD. Madurez de la gestión de riesgos (MGR-SI)	Desempeño global	Índice compuesto de controles, cultura, métricas, terceros y gobernanza.	Índice MGR-SI (0–100)	Integración de Anexos 2–5	Índice (0–100)	≥80 alto; 60–79 medio; <60 bajo

Fuente: Elaboración Propia

3.1.4. HIPÓTESIS

La hipótesis principal es que cuanto más se ajusten las prácticas de gestión de riesgos a estándares internacionales como ISO/IEC 27001, mejor será el desempeño de la seguridad de la información. Estudios anteriores demuestran que la adopción de marcos de referencia internacionales mejora la madurez organizacional y fortalece los procesos de control. (Ortiz-Fajardo & Erazo-Álvarez, 2021)

Hipótesis Nula (H_0): El nivel de alineación de las prácticas y controles de PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 **no** se asocia positivamente con el desempeño de la gestión de riesgos de seguridad de la información ni con la continuidad del negocio en el periodo septiembre 2022 – septiembre 2025.

Hipótesis Alternativa (H_1): El nivel de alineación de las prácticas y controles de PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 **sí** se asocia positivamente con el desempeño de la gestión de riesgos de seguridad de la información y con la continuidad del negocio en el periodo septiembre 2022 – septiembre 2025.

Justificación breve:

La formulación de estas hipótesis se sustenta en que los marcos internacionales de gestión de seguridad de la información, como la ISO/IEC 27001:2022 y la ISO/IEC 27005:2018, establecen que la implementación sistemática de controles, junto con un proceso formal de gestión de riesgos, fortalece la capacidad de las organizaciones para reducir la probabilidad y el impacto de incidentes. De acuerdo con el World Economic Forum (2022) y la ENISA (2023), las empresas que adoptan y mantienen un mayor grado de cumplimiento con estándares de seguridad reportan mejoras significativas en indicadores como el tiempo medio de detección (MTTD), el tiempo medio de respuesta (MTTR) y la continuidad operativa tras incidentes.

Asimismo, estudios recientes como el IBM Cost of a Data Breach Report (2024) evidencian que las organizaciones con una mayor madurez en la gestión de controles presentan menores pérdidas financieras y una recuperación más ágil ante eventos disruptivos. En contraste, aquellas con bajo nivel de alineación tienden a sufrir brechas recurrentes, afectando su reputación y sostenibilidad. Por tanto, resulta metodológicamente pertinente contrastar empíricamente si la alineación de PROIMA con los estándares ISO se traduce en un mejor desempeño de la gestión de riesgos y en mayor resiliencia organizacional. La hipótesis nula permite negar dicha asociación como punto de partida, mientras que la alternativa recoge la expectativa fundamentada en la

literatura.

3.2. ENFOQUE Y MÉTODOS

3.2.1. ENFOQUE

El estudio adopta un enfoque mixto con cualitativo dominante y cuantitativo embebido (QUAL→quan), no como una elección instrumental sino como una exigencia derivada de la naturaleza de las preguntas de investigación. La P1 ("¿En qué medida se alinean los controles con ISO/IEC 27001/27005 y qué implicaciones presenta?") exige tanto la medición objetiva de cumplimiento y brechas (cuantitativo) como la interpretación de su significado operativo para la organización (cualitativo). Si se optara por un enfoque puramente cuantitativo, se obtendrían porcentajes y métricas sin explicar las causas subyacentes; si fuese exclusivamente cualitativo, se comprenderían prácticas y percepciones, pero se perdería la capacidad de estimar magnitudes comparables y priorizar riesgos. El enfoque mixto ofrece una comprensión más integral de fenómenos complejos al combinar la riqueza interpretativa con la precisión numérica. (Creswell, 2018)

La P2 ("¿Qué papel desempeña la cultura organizacional?") demanda comprender significados y prácticas cotidianas que solo emergen a través de entrevistas, cuestionarios y observación participante. Sin embargo, esas percepciones requieren ser contrastadas con datos verificables, como la frecuencia de capacitación, la tasa de reporte de incidentes o la adopción de medidas de higiene tecnológica. Del mismo modo, la P3 ("¿Qué diferencias existen con/sin métricas en la toma de decisiones?") implica comparar indicadores objetivos (uso de KPIs/KRIs, tiempos de detección y respuesta) con narrativas de gobernanza y testimonios de directivos.

Por ello, el enfoque mixto es indispensable: la combinación QUAL→quan permite capturar la magnitud del fenómeno y comprender sus determinantes organizacionales, integrando métricas de cumplimiento, cultura y gobernanza en un análisis coherente. Esta convergencia metodológica no solo responde a las preguntas planteadas, sino que genera evidencia aplicable a la toma de decisiones estratégicas de PROIMA, garantizando que las recomendaciones se basen en una lectura tanto técnica como contextual de la gestión de riesgos entre septiembre 2022 y septiembre 2025.

3.2.2. ALCANCE

En correspondencia directa con el título de la tesis, el alcance de la investigación es exploratorio-descriptivo. Es exploratorio porque indaga por primera vez, de manera sistemática, en las prácticas y desafíos de la gestión de riesgos de seguridad de la información en PROIMA, un ámbito con documentación interna limitada y sin diagnósticos formales previos. Este carácter permite identificar dimensiones relevantes, categorías de análisis y relaciones plausibles que orienten decisiones y futuras líneas de investigación.

Es descriptivo porque caracterizará con precisión las variables y categorías identificadas mediante indicadores cuantitativos y síntesis cualitativas, estimando niveles de alineación con ISO/IEC 27001 y 27005, frecuencia de prácticas clave, perfiles de cultura de seguridad y uso de métricas de riesgo. Con ello se construye una línea base verificable para medir brechas por dominio y priorizar acciones.

No se adopta un alcance correlacional ni explicativo, ya que el diseño es no experimental y transversal, sin manipulación de variables ni seguimiento temporal que permita establecer direccionalidad causal con el rigor requerido. El enfoque mixto y la integración de fuentes garantizan, en cambio, evidencia suficiente y accionable para PROIMA en el periodo septiembre 2022 a septiembre 2025.

3.3. DISEÑO

El estudio adopta un diseño no experimental, transversal y con estrategia de estudio de caso único. Es no experimental porque se observarán las variables en su contexto natural, sin manipulación ni asignación aleatoria de participantes; y es transversal porque la información se recolectará en un único periodo (septiembre 2022–septiembre 2025), describiendo el estado de la gestión de riesgos en PROIMA en ese intervalo.

La elección del estudio de caso único se fundamenta en que el objetivo central es comprender en profundidad cómo una organización concreta alinea sus prácticas con los marcos ISO/IEC 27001:2022 e ISO/IEC 27005:2018 y por qué surgen determinadas brechas. Esta elección se justifica porque el estudio de caso permite un análisis profundo y contextualizado de una organización en particular, facilitando la identificación de prácticas, riesgos y oportunidades de mejora (Yin, 2018)

Este diseño resulta coherente con el enfoque mixto (QUAL→quan) adoptado: permite

describir el nivel de alineación, estimar prevalencias de prácticas (como adopción de MFA, capacitación o uso de KPIs/KRIs) y explorar asociaciones, al tiempo que interpreta significados y prácticas culturales. Así se asegura que los resultados no solo sean estadísticamente descriptivos, sino también contextualizados y útiles para orientar la toma de decisiones estratégicas en PROIMA.

3.3.1. POBLACIÓN

En esta investigación, la población accesible se define de manera precisa y cuantificada para garantizar la coherencia metodológica y la posibilidad de replicación. A diferencia del "universo" teórico de potenciales sujetos, aquí se delimita el conjunto real de personas y expertos directamente vinculados con la gestión de riesgos de seguridad de la información en PROIMA.

- **Subgrupo A – Usuarios internos ("personas")**: La población total está compuesta por N = 272 empleados que utilizan equipos electrónicos corporativos (computadoras, portátiles, tabletas o teléfonos móviles) en el ejercicio de sus funciones. Esta cifra proviene del listado oficial de Recursos Humanos y del directorio activo institucional vigente a septiembre de 2025, lo cual asegura la trazabilidad de la fuente y la validez del dato. Este subgrupo constituye el marco muestral para la aplicación del cuestionario tipo Likert, orientado a medir percepciones de cultura de seguridad, adopción de controles y cumplimiento porcentual por dominios del Anexo A de la ISO/IEC 27001:2022.
- **Subgrupo B – Expertos en la temática**: Incluye a los responsables y especialistas internos de TI y seguridad de la información, así como consultores externos, auditores y académicos con experiencia acreditada en el campo. Este subgrupo se concibe como una población experta acotada, destinada a participar en entrevistas semiestructuradas y a aportar información cualitativa clave sobre gobernanza, gestión de riesgos, continuidad del negocio y toma de decisiones basadas en métricas.

De este modo, la sección de población deja de ser una definición genérica para convertirse en un marco operativo y cuantificado, en coherencia con los objetivos del estudio y con las decisiones de muestreo y medición expuestas en el Capítulo III.

3.3.2. MUESTRA

La **muestra** se define como un subconjunto de la población accesible (N = 272), extraído con criterios explícitos de inclusión y exclusión, y apoyado en un marco muestral verificable

provisto por Recursos Humanos y el directorio activo de PROIMA. Esta precisión asegura consistencia con la sección anterior y evita arbitrariedad en la selección.

Para definir la muestra se empleó el criterio de **saturación teórica** (Glaser, B,Strauss, A., 1967) complementado con el concepto de "information power", que señala que la amplitud y relevancia de los datos pueden determinar el tamaño muestral adecuado. (Malterud, Siersma V., 2016)

- **Componente cuantitativo (Subgrupo A – Usuarios internos)**: La muestra está constituida por **n = 160 empleados**, seleccionados del total de N = 272. El cálculo se realizó bajo supuestos conservadores (p = 0.5; nivel de confianza 95 %; margen de error ≈ 5–6 %), resultando en un tamaño suficiente para cumplir con el objetivo exploratorio-descriptivo y con análisis asociativos básicos. Además, este n ofrece potencia estadística cercana a 0.80 para detectar efectos pequeños a moderados en comparaciones simples, manteniendo la factibilidad operativa

    - **Criterios de inclusión:** empleados con uso activo de equipos corporativos; vínculo laboral vigente al momento del levantamiento; aceptación del consentimiento informado.
    - **Criterios de exclusión:** empleados sin acceso a activos de información; pasantes o personal tercerizado sin credenciales en los sistemas; cuestionarios incompletos (>20 %).

- **Componente cualitativo (Subgrupo B – Expertos)**: La muestra se integra por n = 5 informantes clave, seleccionados de forma intencional por criterio y conveniencia. Los participantes cumplen con requisitos de rol de responsabilidad en TI o seguridad, experiencia mínima de 5 años y participación en proyectos de ciberseguridad o auditoría. El número reducido se justifica por la lógica de saturación temática e Information power, propia de estudios que buscan profundidad analítica en perfiles altamente especializados.

De esta manera, la muestra queda claramente delimitada: n = 160 para el componente cuantitativo y n = 5 para el cualitativo, ambos derivados de la población accesible (N = 272) establecida en la sección 3.3.1.

Tabla 16: Calculo de la Muestra

Tamaño de la muestra para la frecuencia en una población

Tamaño de la población (para el factor de corrección de la población finita o fcp)(*N*):	272
frecuencia % hipotética del factor del resultado en la población (*p*):	50%+/-5
Límites de confianza como % de 100(absoluto +/-%)(*d*):	5%
Efecto de diseño (para encuestas en grupo-*EDFF*):	1

Tamaño muestral (*n*) para Varios Niveles de Confianza

IntervaloConfianza (%)	Tamaño de la muestra
95%	160
80%	103
90%	136
97%	173
99%	194
99.9%	218
99.99%	231

Ecuación

Tamaño de la muestra n = **[EDFF*Np(1-p)]/ [($d^2/Z^2_{1-\alpha/2}$*(N-1)+p*(1-p)]**

Fuente: Resultados de OpenEpi, versión 3

Para el subgrupo de expertos se empleará muestreo no probabilístico por conveniencia, invitando a 5 especialistas que cumplan criterios de experiencia y pertinencia temática. Esta combinación equilibra validez y factibilidad: asegura representatividad operativa entre empleados y acceso a conocimiento especializado entre expertos.

3.3.3. TÉCNICAS DE MUESTREO

Se emplearon técnicas de muestreo diferenciadas para cada subgrupo, en coherencia con el enfoque mixto del estudio y los objetivos de cada componente. Esta combinación de estrategias es adecuada en investigaciones exploratorias y aplicadas con diseños QUAL→quan. (Hernández-Sampieri, et al., 2018)

Subgrupo A – Usuarios internos (cuantitativo): muestreo probabilístico aleatorio simple sobre el marco RR. HH./directorio activo (N = 272). La selección de n = 160 se realizará mediante generador de números aleatorios con semilla reproducible, reduciendo sesgos de selección y fortaleciendo la validez externa de las estimaciones descriptivas y asociativas.

Subgrupo B – Expertos (cualitativo): muestreo no probabilístico por criterio/conveniencia, invitando a 5 perfiles que cumplan los requisitos de experiencia y pertinencia temática. Esta decisión es coherente con el enfoque mixto y con la naturaleza

especializada del dominio, priorizando la calidad informativa sobre la representatividad estadística.

3.3.4. CRITERIOS DE SELECCIÓN DE LA MUESTRA

Este apartado establece los criterios de inclusión y exclusión que regirán la selección de unidades de análisis, en coherencia con el enfoque mixto y el diseño no experimental y transversal del estudio.

Tabla 17: Empleados usuarios de equipos electrónicos

Tipo	Criterio	Definición operativa
Inclusión	Vinculación laboral activa	En nómina
Inclusión	Uso de equipo corporativo	Cuenta activa y equipo asignado en inventario
Inclusión	Función con uso de TI	Rol que exige uso de correo/aplicaciones corporativas
Inclusión	Antigüedad mínima	≥ 1 mes desde el alta
Inclusión	Consentimiento	Firma/aceptación del consentimiento informado
Exclusión	Ausencia prolongada	> 30 días continuos durante el levantamiento
Exclusión	Cuentas no personales	Cuentas genéricas/compartidas (servicio, kiosco, laboratorio)
Exclusión	Terceros no elegibles	Proveedores/contratistas sin equipo corporativo asignado o sin acceso a sistemas
Exclusión	Duplicidades	Registros repetidos en listados
Exclusión	Cuestionario inválido	Completitud < 80%, o falla en cheque de atención, o tiempo < 1/3 de la mediana

Fuente: Elaboración Propia

Tabla 18: Expertos en la temática

Tipo	Criterio	Definición operativa
Inclusión	Perfil experto	Responsable/especialista de TI/Seguridad; consultor/auditor; académico afín
Inclusión	Experiencia	≥ 5 años en el área o ≥ 3 proyectos relevantes en últimos 3 años
Inclusión	Pertinencia del contexto	Conocimiento directo del sector/entorno tecnológico analizado
Inclusión	Disponibilidad	Acepta entrevista 45–60 min (agenda confirmada)
Inclusión	Consentimiento	Firma/aceptación de consentimiento informado
Exclusión	Conflicto de interés	COI no gestionado que pueda sesgar la opinión
Exclusión	Insuficiencia de experiencia	< 3 años y sin proyectos relevantes recientes
Exclusión	No participación	Rechaza o no concreta entrevista en la ventana de campo
Exclusión	Doble rol no deseado	Si también es empleado y el diseño requiere no mezclar roles, se prioriza un solo rol para evitar doble conteo

3.4. TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

Se utilizaron los siguientes instrumentos:

Encuesta estructurada: diseñada para medir la percepción de los colaboradores sobre las prácticas de seguridad de la información. La encuesta es ampliamente utilizada en estudios de gestión porque permite recopilar datos comparables y cuantificables. (Cohen et al., 2018)

Entrevista semiestructurada: aplicada a responsables clave de la gestión de riesgos, con el fin de obtener información detallada sobre experiencias y desafíos. Este instrumento favorece la obtención de información profunda y contextualizada. (Patton, 2015)

Revisión documental: se analizaron políticas, procedimientos y registros internos de la empresa, contrastándolos con marcos internacionales. La revisión documental es una técnica válida para sustentar la triangulación de datos. (Flick, 2015)

3.4.1. ENCUESTA

Justificación

La encuesta se aplicará como técnica principal de recolección de datos cuantitativos, con el propósito de medir las percepciones, prácticas y niveles de adopción de controles de seguridad de la información entre el personal de PROIMA. Este instrumento permitirá complementar la evidencia documental y la observación estructurada con información cuantificable, generando un panorama integral sobre la madurez organizacional en materia de seguridad. Su aplicación posibilitará identificar brechas de sensibilización, gobernanza y operación en los dominios A.5, A.6, A.7 y A.8 de la norma ISO/IEC 27001:2022, además de permitir comparaciones entre áreas y roles mediante criterios estadísticos reproducibles y objetivos.

Instrumento

El instrumento consistirá en un cuestionario tipo Likert de cinco puntos, estructurado por dominios de la norma y complementado con una ficha sociodemográfica mínima (área, rol y antigüedad laboral). El banco de ítems abordará aspectos clave como la disponibilidad y comprensión de políticas, la segregación de funciones, la existencia de canales de respuesta a incidentes (CSIRT), la aplicación de autenticación multifactor, la gestión de parches, el uso de antimalware, los mecanismos de cifrado y la existencia de copias de seguridad. La validez de contenido será documentada mediante juicio de expertos, y la confiabilidad del instrumento se verificará mediante prueba piloto, esperando alcanzar un coeficiente alfa de Cronbach ≥ 0.80, lo que garantizará consistencia interna aceptable para análisis posteriores.

Validación del instrumento

La validación del instrumento se realizó en dos etapas: validez de contenido mediante juicio de expertos y análisis de confiabilidad mediante prueba piloto con cálculo del coeficiente alfa de Cronbach.

Validez de contenido (juicio de expertos). El cuestionario fue sometido a evaluación por un panel de tres expertos con experiencia acreditada en seguridad de la información y metodología de investigación. Los evaluadores fueron: (1) Asesor con especialización en gestión de TI; (2) un especialista interno de PROIMA con certificación en ISO 27001 Lead Implementer; y (3) un consultor externo en ciberseguridad con más de 10 años de experiencia en auditorías de seguridad. Cada experto evaluó los 24 ítems del instrumento según cuatro criterios: claridad, pertinencia, coherencia y suficiencia, utilizando una escala de 1 (deficiente) a 4 (excelente). El Índice de Validez de Contenido (IVC) promedio obtenido fue de 0.92, superando el umbral mínimo aceptable de 0.80. Como resultado del proceso, se reformularon 3 ítems para mejorar su claridad y se eliminó 1 ítem por redundancia con otro existente. El acta de validación por juicio de expertos se presenta en el Anexo 8.

Confiabilidad (prueba piloto y alfa de Cronbach). Se aplicó una prueba piloto a 25 colaboradores de PROIMA que no formaron parte de la muestra definitiva, seleccionados de manera aleatoria y representando las diferentes áreas funcionales. Los datos obtenidos fueron procesados en SPSS v.27 para calcular el coeficiente alfa de Cronbach global y por dominio. Los resultados se presentan en la Tabla 19.

Tabla 19: Resultados de fiabilidad del instrumento (alfa de Cronbach)

Dominio / Escala	N.° ítems	α de Cronbach	Interpretación
A.5 Políticas de seguridad	4	0.84	Buena
A.6 Organización de la seguridad	5	0.81	Buena
A.7 Controles físicos y ambientales	6	0.79	Aceptable
A.8 Controles tecnológicos	9	0.86	Buena

Dominio / Escala	N.° ítems	α de Cronbach	Interpretación
Escala global (24 ítems)	**24**	**0.89**	**Buena**

Fuente: Elaboración propia a partir de SPSS v.27. Nota: α ≥ 0.70 = aceptable; α ≥ 0.80 = buena; α ≥ 0.90 = excelente.

El coeficiente alfa de Cronbach global obtenido (α = 0.89) supera el umbral establecido de 0.80, lo que demuestra una consistencia interna buena del instrumento. Todos los dominios obtuvieron valores superiores a 0.70, siendo el dominio A.8 (Controles tecnológicos) el de mayor fiabilidad (α = 0.86) y el dominio A.7 (Controles físicos y ambientales) el de menor valor, aunque aún dentro del rango aceptable (α = 0.79). Con base en estos resultados, se decidió mantener los 24 ítems sin modificaciones adicionales para la aplicación definitiva. La salida completa de SPSS con el análisis de fiabilidad se incluye en el Anexo 9

Ejemplo de ítem

Un ejemplo representativo es el enunciado: "Utilizo autenticación multifactor (MFA) para acceder a sistemas críticos o remotos", el cual se asocia al control A.8.5 e indica el nivel de cobertura del mecanismo MFA dentro de la organización. Este ítem permitirá calcular medias por área y rol, facilitando la identificación de segmentos donde la adopción tecnológica sea deficiente (valores medios inferiores a 3.5 en la escala Likert). Los resultados obtenidos orientarán la priorización de acciones correctivas y la formulación de estrategias de capacitación o fortalecimiento de políticas.

Procedimiento

La fase de preparación incluirá la versión final del instrumento, la validación del consentimiento informado y la ejecución de un piloto previo. La recolección de datos se realizará en modalidad digital, a través de Google Forms, o en formato impreso cuando sea necesario, durante un período de cinco a diez días. Se enviarán recordatorios internos con el objetivo de lograr una tasa de respuesta igual o superior al 70 %. Los formularios completados serán anonimizados y almacenados en una base de datos controlada, con acceso restringido al equipo investigador. El análisis comprenderá estadística descriptiva (frecuencias, medias y porcentajes), ranking por dominios e ítems, y comparaciones por área o rol. Los hallazgos serán triangulados con los

resultados obtenidos de la revisión documental, las entrevistas y la observación estructurada, con el fin de proponer un plan de acción priorizado que fortalezca la gestión de riesgos de seguridad de la información en PROIMA.

Finalmente, el Anexo 4 presenta el instrumento de encuesta aplicado, junto con la captura del formulario en Google Forms y su enlace activo, asegurando la transparencia del proceso de recolección de datos. Por su parte, el Anexo 6 contiene el Diccionario de Datos correspondiente a la encuesta, donde se describen las variables, códigos, escalas de medición, valores posibles y su relación con los dominios de la norma ISO/IEC 27001:2022. Este anexo complementa el diseño del instrumento y garantiza la coherencia entre la codificación, el procesamiento estadístico y el análisis interpretativo de los resultados.

Por su parte, el Anexo 7 contiene el Diccionario de Datos correspondiente a la revisión documental estructurada, en el cual se detallan las variables, códigos, tipos de dato, criterios de evaluación y escalas de cumplimiento utilizadas en el proceso de verificación. Este anexo complementa el diseño del instrumento descrito en el Anexo 3 y garantiza la coherencia entre la rúbrica de evaluación, la codificación de resultados y la interpretación de los porcentajes de cumplimiento por categoría, asegurando la trazabilidad metodológica de los hallazgos obtenidos en la fase de análisis documental.

3.4.2 REVISIÓN DOCUMENTAL ESTRUCTURADA

Justificación

La revisión documental estructurada se aplicará como técnica de análisis cualitativo y de verificación normativa, orientada a comprobar la existencia, vigencia, aprobación, difusión y uso de los artefactos clave del sistema de gestión de seguridad de la información (SGSI) de PROIMA. Su objetivo es garantizar la trazabilidad y alineación con los requisitos de las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018, aportando evidencia objetiva, verificable y reproducible que sustente los hallazgos del estudio. Esta técnica permite identificar el nivel de cumplimiento institucional en cada dominio y calcular porcentajes consolidados por categoría, aportando información valiosa para la priorización de acciones de mejora.

Instrumento

El instrumento empleado corresponde al Anexo 3, que contiene un checklist de verificación documental diseñado para localizar, evaluar y registrar los documentos institucionales vinculados con la seguridad de la información. Cada registro incluirá los metadatos esenciales (nombre del

documento, categoría, fecha de emisión o actualización, responsable y ubicación). Posteriormente, se aplicará una rúbrica de verificación rápida basada en los criterios de vigencia, aprobación formal, difusión al personal, uso o evidencia de aplicación y coherencia con los requisitos normativos.

Cada documento será calificado mediante un sistema estandarizado de estatus:

- 1 = Cumple totalmente
- 0.5 = Cumple parcialmente
- 0 = No cumple
- N/A = No aplica

Los resultados obtenidos se consolidarán en una matriz de cumplimiento por categoría documental, permitiendo visualizar las brechas y generar indicadores globales de conformidad.

Ejemplo

Por ejemplo, para la Política de Seguridad de la Información se verificará su vigencia (no superior a doce meses), la existencia de un acta de aprobación por la alta dirección y la evidencia de su difusión entre los usuarios. Si el documento cumple con los tres criterios, se calificará con 1; si cumple parcialmente, con 0.5; y si no existe o no presenta trazabilidad, con 0. El resultado de cada documento se integrará en el porcentaje de cumplimiento de la categoría Políticas, contribuyendo así al cálculo del nivel de madurez del dominio A.5 y a la identificación de brechas específicas que alimentarán el plan de acción correctivo.

Procedimiento

La fase de preparación incluirá la solicitud formal de documentación a las áreas involucradas, la elaboración de una lista maestra de control documental por categoría y la firma de un acuerdo de confidencialidad para asegurar el manejo ético de la información. La recolección de datos consistirá en la recepción o descarga digital de los documentos con control de versiones y registro de metadatos en una plantilla unificada. El resguardo de la información se realizará en una estructura de carpetas segmentadas por categoría (políticas, procedimientos, instructivos, registros, evidencias operativas), con acceso restringido al equipo investigador.

El análisis aplicará la rúbrica de evaluación, calculará los porcentajes de cumplimiento por criterio y por categoría, y clasificará las brechas detectadas según su impacto y prioridad. Finalmente, el reporte presentará la matriz de cumplimiento global, acompañada de las acciones correctivas sugeridas, responsables asignados, fechas objetivo y un KPI de cierre para su

monitoreo.

3.4.3 OBSERVACIÓN ESTRUCTURADA

Justificación

La observación estructurada se aplicará como técnica complementaria de verificación empírica, destinada a contrastar la información documental y declarativa con la práctica real en los entornos operativos de PROIMA. Esta metodología permite reducir los sesgos de deseabilidad social presentes en encuestas o entrevistas, aportando evidencia directa sobre el cumplimiento de controles en campo. Es especialmente útil para evaluar los controles físicos y ambientales del dominio A.7, así como los controles tecnológicos del dominio A.8 relacionados con estaciones de trabajo, red y seguridad perimetral. Además, permite constatar hábitos operativos como el principio de "puesto limpio", el bloqueo de pantalla y la correcta manipulación de activos tecnológicos.

Instrumento

Se empleará una lista de cotejo estructurada derivada del checklist de treinta controles definido en el Anexo 2, adaptada para la observación directa en sitio. Esta lista focaliza la verificación en aspectos críticos como la gestión de credenciales y registro de visitantes, la protección de áreas sensibles, el orden físico y bloqueo de estaciones de trabajo, la seguridad de equipos, el traslado de activos, la protección antimalware y EDR, la aplicación de parches de seguridad, el uso de autenticación multifactor (MFA), el cifrado de información y la gestión de registros y logs. Cada control será evaluado mediante una escala de cumplimiento ordinal (1/0.5/0), acompañada de observaciones breves y evidencia no sensible.

Ejemplo

En el control "Puesto limpio y bloqueo", se verificará la existencia de bloqueo automático de sesión en un tiempo máximo definido por la política institucional, así como la ausencia de documentos o información sensible expuesta en escritorios, pizarras o pantallas visibles. Cada observación registrará hora, área, responsable y hallazgos específicos, consolidándose posteriormente en un mapa de calor por áreas operativas, que permitirá identificar zonas críticas y priorizar intervenciones correctivas.

Procedimiento

La fase de preparación incluirá la definición de la ruta de visita, los horarios de recorrido, la designación de observadores responsables y la comunicación previa a las jefaturas de área, junto con el compromiso de confidencialidad para evitar alteraciones en la rutina laboral. La recolección de datos se llevará a cabo mediante recorridos presenciales, aplicando un muestreo de estaciones y áreas críticas. Durante la observación, se validarán configuraciones de seguridad, condiciones ambientales, presencia de equipos protegidos y funcionamiento de controles.

El resguardo de los datos incluirá el almacenamiento cifrado de las fichas de observación y fotografías, sin registrar información sensible o identificable. En la fase analítica, se calcularán porcentajes de cumplimiento por control y área, y se aplicará una ponderación de severidad (impacto × probabilidad) para determinar los hallazgos prioritarios. Finalmente, el informe consolidará los resultados en una matriz visual y propondrá acciones específicas con KPI de seguimiento, tales como porcentaje de endpoints con EDR activo o porcentaje de pantallas con bloqueo automático conforme a la política institucional.

Por su parte, el Anexo 8 contiene el Diccionario de Datos correspondiente a la observación estructurada, en el cual se detallan las variables, códigos, tipos de dato, escalas de cumplimiento y criterios de evaluación aplicados durante las visitas en campo. Este anexo complementa el instrumento descrito en el Anexo 2 y garantiza la coherencia entre la lista de cotejo utilizada, la codificación de las observaciones y la interpretación de los resultados, asegurando la trazabilidad metodológica del proceso de verificación y análisis de los controles físicos y tecnológicos observados en PROIMA.

3.4.4. ENTREVISTAS SEMIESTRUCTURADAS

Justificación

Las entrevistas semiestructuradas se emplearán como técnica cualitativa orientada a profundizar en los aspectos de gobernanza, toma de decisiones basada en métricas, gestión de riesgos, continuidad operativa y administración de terceros dentro del sistema de seguridad de la información de PROIMA. Este método permitirá obtener perspectivas estratégicas y operativas directamente de los actores clave, revelando factores contextuales, restricciones de recursos, dependencias organizacionales y niveles de madurez institucional.

Asimismo, las entrevistas contribuirán a identificar patrones de comportamiento en la respuesta a incidentes, el seguimiento de indicadores (MTTD, MTTR) y los procesos de mejora continua, aportando información complementaria a la obtenida mediante encuestas, revisión

documental y observación estructurada.

Instrumento

El instrumento a utilizar corresponde a la guía de entrevista de doce preguntas descrita en el Anexo 5, elaborada conforme a los lineamientos de la ISO/IEC 27001:2022 y ISO/IEC 27005:2018. La guía aborda dimensiones esenciales como políticas y responsabilidades (RACI), identificación y tratamiento de riesgos, controles críticos del Anexo A, gestión de incidentes con métricas MTTD/MTTR, continuidad de negocio (RTO/RPO y pruebas de DR/BCP), debida diligencia de terceros, accesos remotos con autenticación multifactor (MFA) y gobierno basado en indicadores de desempeño (KPIs/KRIs). Cada pregunta está diseñada para promover respuestas reflexivas y contextualizadas, permitiendo interpretar la aplicación práctica de los lineamientos normativos y su grado de institucionalización.

Ejemplo

Por ejemplo, la pregunta relacionada con la gestión de incidentes solicitará al entrevistado describir el proceso de detección, respuesta y lecciones aprendidas de un evento reciente. Esta información permitirá evaluar la efectividad de los mecanismos de monitoreo y logging, la capacidad de respuesta del equipo técnico y la existencia de mecanismos de retroalimentación hacia los planes de mejora o auditorías internas. De igual forma, las respuestas sobre la gestión de terceros y continuidad operativa servirán para valorar la integración de cláusulas de seguridad en contratos, los ejercicios de simulación y la resiliencia general del sistema.

Procedimiento

La fase de preparación contemplará la identificación y selección de informantes clave, entre los que se incluirán el CIO/CISO, responsables de Operaciones TI, dueños de proceso, y líderes de Riesgos y Continuidad del Negocio. Se establecerá una agenda de entrevistas y se obtendrá el consentimiento informado de cada participante. La recolección de información se desarrollará a través de entrevistas de 30 a 45 minutos, realizadas en modalidad presencial o virtual, con registro mediante notas de campo y/o grabación autorizada.

El resguardo de la información implicará la transcripción literal, almacenamiento cifrado y codificación temática en software cualitativo (NVivo o Atlas.ti). En la etapa analítica, se construirá una matriz de códigos y categorías, integrando los hallazgos con los resultados de la encuesta, observación y revisión documental. Las conclusiones permitirán priorizar acciones con base en criterios de impacto, urgencia, esfuerzo y dependencias interáreas. Finalmente, el reporte

incluirá un resumen ejecutivo y un portafolio de quick wins y proyectos a seis o doce meses, con responsables, recursos estimados y KPIs de cierre.

Por su parte, el Anexo 9 contiene el Diccionario de Datos correspondiente a la matriz de controles A.5–A.8, en el cual se describen las variables, códigos, tipos de dato, escalas de cumplimiento y criterios de evaluación aplicados durante la verificación de los controles establecidos en la norma ISO/IEC 27001:2022. Este anexo complementa la matriz presentada en el instrumento principal y garantiza la coherencia entre la codificación, el procesamiento de resultados y la interpretación de los niveles de cumplimiento por dominio, asegurando la trazabilidad metodológica del proceso de auditoría técnica desarrollado en el estudio.

3.5. FUENTES DE INFORMACIÓN

3.5.1. FUENTES PRIMARIAS

Se consideran fuentes primarias las respuestas obtenidas en encuestas y entrevistas a los colaboradores de PROIMA involucrados en la gestión de la seguridad de la información. Este tipo de fuente es fundamental en la investigación aplicada porque aporta datos directos del contexto organizacional. (Corbin & Strauss, 2015)

Las fuentes primarias de este estudio se orientarán a responder de manera directa las preguntas de investigación sobre gobernanza, gestión de riesgos, implementación de controles, cultura de seguridad, continuidad operativa y gestión de terceros. Para ello se integrará evidencia cualitativa y cuantitativa que permita contrastar lo declarado en la documentación institucional con la práctica observada y con la percepción de los actores involucrados, garantizando así coherencia vertical entre preguntas, objetivos, técnicas e indicadores.

En primer lugar, las entrevistas semiestructuradas a expertos en seguridad de la información y continuidad del negocio aportarán el testimonio especializado y contextual que permita reconstruir los procesos reales de aprobación de políticas, definición de roles y foros de decisión, así como los mecanismos de identificación, evaluación y tratamiento del riesgo conforme a ISO/IEC 27005.

A través de estas entrevistas se documentarán criterios, umbrales y métricas efectivamente utilizados, la selección de controles imprescindibles del Anexo A, la experiencia reciente en incidentes incluidas las métricas de detección y respuesta y la manera en que se planifica y prueba la continuidad mediante RTO y RPO. De este modo, las entrevistas constituirán evidencia principal para esclarecer cómo se gobierna la seguridad (pregunta 1), cómo se gestionan los riesgos y se

priorizan brechas (pregunta 2), qué eficacia percibida tienen los controles críticos (pregunta 3), cómo se articula la continuidad con la operación (pregunta 5) y cómo se establecen exigencias y monitoreo a terceros (pregunta 6).

En segundo término, la encuesta de cultura de seguridad entregará mediciones cuantitativas sobre conocimiento, adhesión y hábitos cotidianos de los colaboradores que utilizan equipos corporativos, permitiendo objetivar la adopción real de políticas y controles en la primera línea operativa. A partir de escalas tipo Likert, se estimarán promedios por dominios del Anexo A gobernanza, organización y roles, seguridad física y tecnológica junto con brechas por área y rol, de forma que se identifiquen patrones de cumplimiento, rezagos y necesidades de sensibilización específicas.

Esta fuente será clave para dimensionar el nivel de implementación y eficacia práctica de los controles (pregunta 3) y para caracterizar la madurez cultural de la organización (pregunta 4), ofreciendo además insumos indirectos sobre la comunicación de cambios y la claridad de responsabilidades, lo que aporta evidencia de soporte a la comprensión de la gobernanza (pregunta 1).

En tercer lugar, el checklist de controles alineado a ISO/IEC 27001:2022, aplicado conjuntamente con la revisión documental interna, proporcionará evidencia verificable del grado de cumplimiento formal y sustantivo respecto de políticas, procedimientos, minutas, contratos, planes de continuidad, bitácoras y tableros de indicadores. La valoración sistemática de vigencia, aprobación, difusión, uso y coherencia con la norma permitirá calcular porcentajes de cumplimiento por control y por dominio, identificar no conformidades y documentar la trazabilidad entre requisitos legales o contractuales y los controles implementados.

Esta fuente será determinante para responder qué tan implementados y eficaces están los controles críticos (pregunta 3), cómo se sostiene la gobernanza en instrumentos normativos concretos (pregunta 1), de qué modo se estructura la evaluación y tratamiento del riesgo (pregunta 2), si la continuidad está documentada y probada (pregunta 5) y cuáles son las garantías exigidas a terceros y su seguimiento (pregunta 6).

En cuarto lugar, las cédulas de observación de prácticas cotidianas permitirán constatar en terreno la congruencia entre lo previsto en los documentos y lo que sucede efectivamente en el entorno laboral. La verificación directa de conductas como el puesto limpio y el bloqueo de pantalla, el estado de los controles físicos en áreas sensibles y la postura de endpoints —incluidos

endurecimientos, protección antimalware, parches y uso de autenticación multifactor— entregará una línea de base empírica sobre el cumplimiento operativo.

Con ello se contribuirá a describir el nivel real de implementación por áreas y a construir mapas de calor de brechas, lo que servirá para profundizar en la eficacia de los controles (pregunta 3) y en los hábitos que configuran la cultura de seguridad (pregunta 4), aportando señales adicionales sobre la preparación práctica para la continuidad cuando se observen procedimientos o simulacros en acción (pregunta 5).

En conjunto, estas fuentes primarias permitirán medir, describir y contrastar lo declarado, lo percibido y lo observado, generando indicadores que se integrarán en el análisis comparado por dominios y preguntas. La evidencia cualitativa de las entrevistas se utilizará para interpretar las razones de las brechas y priorizaciones, la evidencia cuantitativa de la encuesta dimensionará la adopción y los hábitos, la evidencia documental corroborará la existencia y calidad de los instrumentos de gobierno y gestión, y la evidencia observacional confirmará la práctica efectiva en el entorno de trabajo.

Esta triangulación, ordenada y trazable, garantizará que los resultados se deriven directamente de las preguntas de investigación y que las conclusiones y recomendaciones se sustenten en pruebas convergentes de distinta naturaleza metodológica.

3.5.2. FUENTES SECUNDARIAS

Las fuentes secundarias se emplearán para contextualizar, contrastar y triangular la evidencia primaria, aportando línea de tiempo, estándares y referentes externos que permitan validar o refutar hallazgos. Se clasifican en internas y externas, con reglas de uso y mecanismos explícitos de triangulación frente a entrevistas, encuesta, observación y checklist.

Como fuentes secundarias se incluyeron artículos científicos, informes técnicos y normas internacionales que sustentan el marco teórico. Estas fuentes permiten contrastar los hallazgos con la literatura existente y brindan validez a las conclusiones. (Yin, 2018)

Fuentes internas: Incluirán informes de auditorías previas, actas de comités de TI y seguridad, y bitácoras de incidentes de PROIMA. Su papel será reconstruir la trayectoria de gobierno y riesgos (qué se decidió, cuándo y por qué) y verificar coherencia entre lo documentado y lo declarado por informantes. En la práctica, las actas de comité se contrastarán con las entrevistas: si en entrevistas se afirma una revisión anual de políticas y el acta del 12/05/2024

consigna esa revisión con plan de cambios y responsables, se clasificará como convergencia fuerte; si el acta existe, pero sin evidencia de difusión, será consistencia parcial; si no hay acta ni registro, será disonancia y se generará brecha en A.5.1/A.5.2.

Del mismo modo, las bitácoras de incidentes se cruzarán con los relatos de MTTD/MTTR de las entrevistas y con los logs/alertas observadas: si un incidente reportado (ransomware simulado) tiene tiempos y acciones coincidentes en bitácora, entrevista y consola de monitoreo, habrá validación cruzada; si difieren sustancialmente, se priorizará la evidencia con sello temporal y trazabilidad técnica. Finalmente, los informes de auditoría se alinearán con el checklist: hallazgos repetidos en dos periodos consecutivos, no cerrados en plan de acción, elevarán la severidad de la brecha (riesgo residual alto) y se reflejarán en él % de cumplimiento de los dominios A.5–A.8.

Fuentes externas: Comprenderán las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018, literatura académica y técnica sobre gestión de riesgos y cultura de seguridad, y reportes sectoriales (p. ej., Global Cybersecurity Index, WEF, Gartner). Su función será operacionalizar criterios (p. ej., qué significa "vigente" para una política, cómo escalar impacto/probabilidad, qué umbrales usar para parches críticos), interpretar patrones de la encuesta (p. ej., asociaciones entre capacitación y adopción de MFA) y contextualizar el nivel de madurez frente a tendencias y pares del sector.

En términos aplicados, la ISO/IEC 27005 definirá el marco para identificar, analizar y tratar riesgos, que se cotejará con lo que las entrevistas describen como proceso real; la 27001 servirá para mapear controles del Anexo A los ítems del checklist y a las observaciones en sitio. La literatura académica se usará para discutir coherentemente hallazgos de cultura (por ejemplo, cuando puntuaciones bajas en "difusión de cambios" coexisten con cumplimiento documental alto, se explicará el "gap de implementación" apoyado en estudios de cambio organizacional). Los informes sectoriales brindarán comparativas para situar brechas de MFA, gestión de vulnerabilidades o continuidad frente a medianas regionales; si PROIMA presenta cobertura MFA inferior al percentil reportado, la recomendación priorizará ese control con justificación externa y KPI de cierre.

Estrategia de triangulación aplicada. Cada afirmación clave del estudio se sustentará con al menos dos piezas de evidencia de distinta naturaleza. Se usarán tres reglas operativas: (1) Convergencia: documentos internos + fuente primaria coinciden → evidencia robusta; (2) Consistencia parcial: existen documentos, pero con lagunas (p. ej., sin difusión o sin pruebas) →

brecha moderada y acción correctiva específica; (3) Disonancia: declaraciones sin respaldo documental o técnico → brecha crítica y prioridad alta en plan de acción.

La trazabilidad se asegurará con referencias cruzadas (acta/folio/fecha; ítem de instrumento; control A. afectado; responsable) y con un registro de decisiones metodológicas cuando haya conflicto entre fuentes (p. ej., se privilegia evidencia con sello temporal y cadena de custodia verificable sobre autoinforme).

Criterios de calidad y citación. Las fuentes internas serán autenticadas (control de versiones, fechas, responsables); las externas se seleccionarán por autoridad (normas, organismos multilaterales, Journals revisados por pares), vigencia (2020+ para literatura, últimas ediciones de normas) y relevancia temática. Todas las citas se presentarán en formato APA 7 y se documentará la fecha de consulta cuando aplique (reportes web). Con ello, las fuentes secundarias no solo contextualizan, sino que refuerzan la validez de los resultados y permiten derivar recomendaciones comparables, pertinentes y alineadas a estándares.

3.6. PLAN DE ANÁLISIS

Tabla 19: Plan de análisis

Fase	Actividad clave	Entregable específico	Duración estimada (semanas)	Cronograma (semanas)
Preparación analítica	Plan de análisis y codebooks (QUAN/QUAL); plantillas de tablas y "joint displays"	Plan analítico, diccionario de variables, esquema de categorías; formatos de reporte	1	Semana 8
Gestión y depuración de datos	Ingesta y limpieza QUAN (validación, imputación mínima, etiquetas)	Base depurada en SPSS/R con bitácora de cambios	1	Semana 9
	Ingesta y preparación QUAL (transcripciones finalizadas, control de calidad)	Corpus QUAL verificado (NVivo/Atlas.ti) y guía de nombres de nodos	1	Semana 9
Fase QUAN (Análisis cuantitativo)	Fiabilidad del cuestionario (α de Cronbach por dominio A.5–A.8)	Tabla de fiabilidad y ajustes si aplica	0.5	Semana 9
	Descriptivos: frecuencias, medias, % de acuerdo por ítem y dominio	Tablas/figuras QUAN (resumen por ítem y dominio)	0.5	Semana 9
	Cumplimiento de controles (checklist): % por control y por dominio	Matriz de cumplimiento (A.5–A.8) y heatmap de brechas	1	Semana 10
	Asociaciones básicas (área/rol × dominios; χ^2/Cramér's V; U de Mann–Whitney/T de Student	Tablas de asociación con tamaños de efecto e interpretación	1	Semana 10

Fase	Actividad clave	Entregable específico	Duración estimada (semanas)	Cronograma (semanas)
	según aplique)			
Fase QUAL (Análisis cualitativo)	Codificación inicial (entrevistas/observación/documental) y memoing	Codebook inicial y memos analíticos	1	Semana 9
	Codificación axial/temática; verificación intercodificador (κ de Cohen)	Mapa temático y matriz de categorías-subcategorías	1	Semana 10
	Síntesis cualitativa por ejes (gobernanza, riesgos, continuidad, terceros, métricas)	Informe QUAL por ejes con citas ilustrativas	0.5	Semana 10
Integración y triangulación (QUAN + QUAL)	Joint displays (convergencia, consistencia parcial, disonancia) por dominio	Cuadros de integración y meta-inferencias por pregunta	1	Semana 11
	Priorización de brechas (impacto × probabilidad × factibilidad) y rutas de acción	Matriz de priorización y plan de acción enlazado a controles A.*	1	Semana 12
Síntesis y validación	Redacción de resultados y discusión (Cap. IV–V) con evidencia triangulada	Borradores de Cap. IV y V	2	Semanas 13–14
	Revisión técnica (pares/asesor) y member checking con informantes clave	Informe ajustado y acta de validación	1	Semana 15
	Edición final, normalización APA, anexos y numeración	Versión final del informe	2	Semanas 16–17

Fuente: Elaboración Propia

A continuación, se presenta la Estructura de Descomposición del Trabajo (EDT/WBS) del estudio, la cual deriva directamente del plan de análisis descrito en la Tabla 19. Esta estructura constituye una representación jerárquica del proyecto que permite organizar de manera lógica y secuencial todas las fases, actividades y entregables contemplados en la investigación.

Su finalidad es definir el alcance de cada componente, facilitar la trazabilidad de los resultados y garantizar la coherencia metodológica entre las etapas cuantitativas (QUAN) y cualitativas (QUAL). Además, la EDT servirá como insumo para la elaboración del Diccionario de la EDT, asegurando que cada fase cuente con una descripción operativa clara y alineada con los objetivos del estudio sobre gestión de riesgos de seguridad de la información en PROIMA (2022–2025).

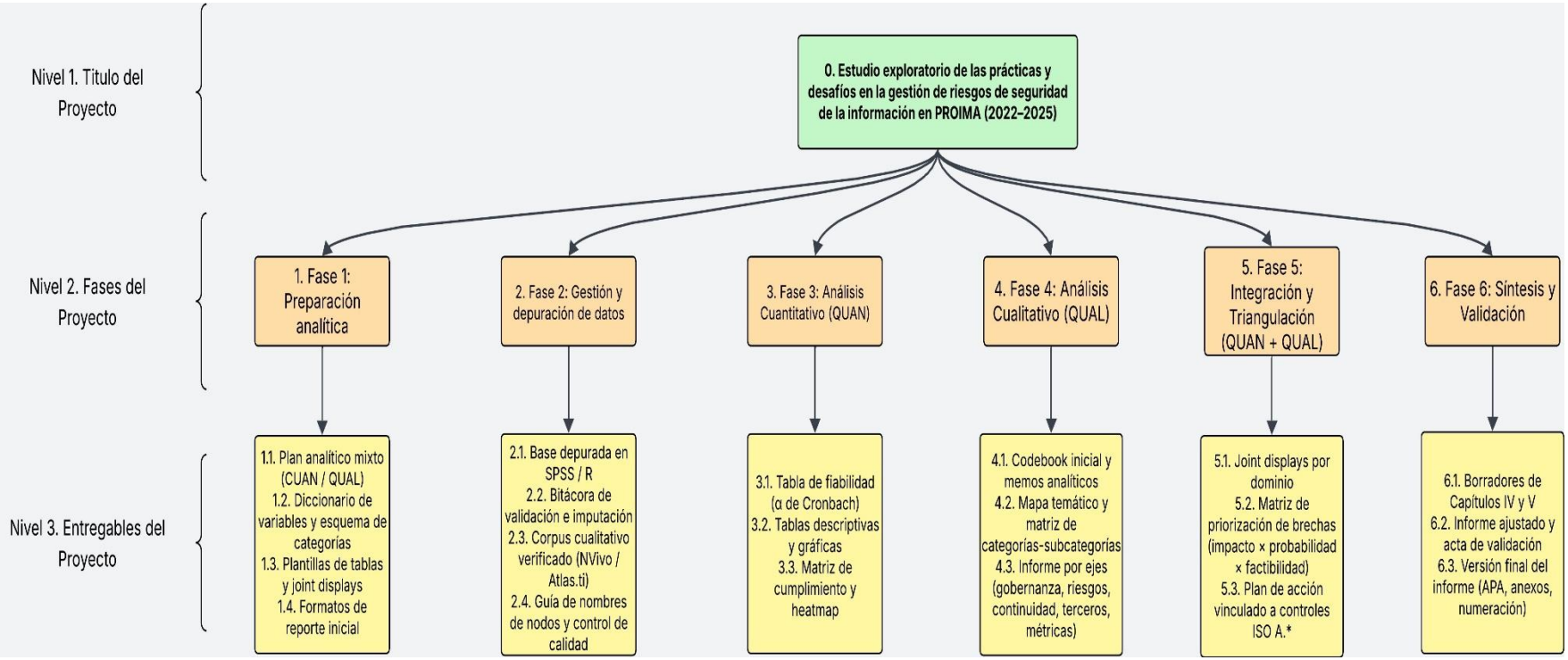


Figura 5: Estructura de Descomposición del Trabajo (EDT/WBS)

Fuente: Elaboración Propia

En concordancia con la Estructura de Descomposición del Trabajo (EDT/WBS) elaborada, se presenta a continuación el Diccionario de la EDT, documento que permite definir de manera precisa el alcance, contenido y criterios de aceptación de cada entregable identificado en el proyecto. Este instrumento constituye una guía operativa que facilita la gestión técnica y metodológica de las fases analítica, cuantitativa, cualitativa y de triangulación, garantizando la trazabilidad entre los productos del estudio y las actividades descritas en el plan de análisis.

Asimismo, el diccionario asegura una comprensión homogénea de las tareas por parte de todos los responsables, estableciendo correspondencias directas entre las herramientas empleadas, los entregables obtenidos y los objetivos metodológicos del estudio sobre gestión de riesgos de seguridad de la información en PROIMA (2022–2025).

Tabla 20: Diccionario de la Estructura de Descomposición del Trabajo (EDT/WBS)

Código EDT	Nombre del Entregable	Descripción	Responsable	Herramientas	Criterio de aceptación	Relación con Plan de Análisis
1.1	Plan analítico mixto (CUAN/QUAL)	Documento que define el enfoque de integración entre los análisis cuantitativos y cualitativos, detallando procedimientos, escalas y unidades de análisis.	Equipo investigador	Word, Excel, NVivo	Plan aprobado por asesor, coherente con metodología mixta.	Base del análisis de datos descrita en la Tabla 19, Fase "Preparación analítica".
1.2	Diccionario de variables y esquema de categorías	Repositorio con los códigos y definiciones de las variables cuantitativas y las categorías cualitativas.	Equipo investigador	Excel, SPSS, NVivo	Variables codificadas y validadas; coherencia con instrumentos.	Permite la depuración y codificación de datos CUAN/QUAL.
1.3	Plantillas de tablas y *joint displays*	Modelos de visualización integradora entre resultados cuantitativos y cualitativos.	Equipo investigador	Excel, PowerPoint	Cumple normas APA y diseño uniforme de reporte.	Guía la representación tabular del análisis.
1.4	Formatos de reporte inicial	Estructuras predefinidas para redacción y registro de resultados por dominio.	Equipo investigador	Word	Cumple estructura IMRyD institucional.	Apoya la redacción de resultados en Cap. IV.
2.1	Base depurada	Conjunto de	Equipo	SPSS, R	No presenta	Permite

Código EDT	Nombre del Entregable	Descripción	Responsable	Herramientas	Criterio de aceptación	Relación con Plan de Análisis
	en SPSS/R	datos validados, sin errores ni valores atípicos, con bitácora de cambios.	investigador		celdas vacías o inconsistentes.	ejecución de análisis descriptivo y fiabilidad.
2.2	Bitácora de validación e imputación	Registro documentado de todas las correcciones y ajustes realizados a la base de datos.	Equipo investigador	Excel	Bitácora actualizada y verificada.	Garantiza la trazabilidad de datos cuantitativos.
2.3	Corpus cualitativo verificado (NVivo/Atlas.ti)	Archivo depurado con transcripciones completas y control de calidad.	Equipo investigador	NVivo, Atlas.ti	Transcripciones validadas y completas.	Fuente primaria para análisis cualitativo.
2.4	Guía de nombres de nodos y control de calidad	Documento que define la nomenclatura y jerarquía de los nodos analíticos.	Equipo investigador	NVivo	Estructura coherente con codebook.	Sustenta codificación axial y temática.
3.1	Tabla de fiabilidad (α de Cronbach)	Resultados de la consistencia interna del cuestionario.	Equipo investigador	SPSS	$\alpha \geq 0.70$ aceptable.	Evalúa validez interna de instrumentos.
3.2	Tablas descriptivas y gráficas	Resumen estadístico de frecuencias y porcentajes por dominio.	Equipo investigador	SPSS, Excel	Datos completos, formato APA.	Base de interpretación de resultados QUAN.
3.3	Matriz de cumplimiento y *heatmap*	Representación del nivel de cumplimiento de controles ISO.	Equipo investigador	Excel, Power BI	Visualización clara y precisa de brechas.	Permite comparar niveles de cumplimiento A.5–A.8.
3.4	Tablas de asociación	Análisis entre variables (área/rol × dominio) con medidas de efecto.	Equipo investigador	SPSS, R	Pruebas significativas $p < 0.05$.	Complementa la interpretación inferencial.
4.1	Codebook inicial y memos analíticos	Lista codificada de categorías emergentes y notas reflexivas.	Equipo investigador	NVivo, Atlas.ti	Coherencia entre códigos y objetivos.	Estructura base del análisis cualitativo.

Código EDT	Nombre del Entregable	Descripción	Responsable	Herramientas	Criterio de aceptación	Relación con Plan de Análisis
4.2	Mapa temático y matriz de categorías-subcategorías	Diagrama que relaciona categorías principales con subtemas derivados.	Equipo investigador	NVivo	Validado por co-investigador.	Apoya la triangulación cualitativa.
4.3	Informe por ejes temáticos	Síntesis cualitativa por ejes: gobernanza, riesgos, continuidad, terceros y métricas.	Equipo investigador	Word	Citas textuales correctas y análisis interpretativo.	Corresponde a síntesis cualitativa (Semana 10).
5.1	*Joint displays* por dominio	Integración visual entre hallazgos CUAN y QUAL.	Equipo investigador	Excel, PowerPoint	Presenta convergencia y divergencia clara.	Núcleo del análisis mixto (Semana 11).
5.2	Matriz de priorización de brechas	Evaluación de impacto, probabilidad y factibilidad.	Equipo investigador	Excel	Matriz completa y coherente.	Define rutas de mejora y acción.
5.3	Plan de acción vinculado a controles ISO A.*	Estrategia de mejora en gestión de riesgos.	Equipo investigador	Word, Excel	Cumple estructura ISO 27001:2022.	Producto final de integración analítica.
6.1	Borradores de Capítulos IV y V	Redacción inicial de resultados y discusión.	Equipo investigador	Word	Entregables revisados por asesor.	Representa fase de síntesis.
6.2	Informe ajustado y acta de validación	Documento final revisado tras *member checking*.	Equipo investigador	Word	Validado con informantes clave.	Consolidación final del estudio.
6.3	Versión final del informe	Documento completo con anexos, formato APA y numeración final.	Equipo investigador	Word, Mendeley	Cumple normas institucionales y APA 7.ª ed.	Cierre de proyecto (Semana 17).

Fuente: Elaboración Propia

3.7. MATRIZ DE TRAZABILIDAD METODOLÓGICA

Con el propósito de garantizar la coherencia interna del estudio y facilitar la auditoría académica, se presenta a continuación la Matriz de Trazabilidad Metodológica. Esta herramienta documenta la cadena completa desde cada objetivo de investigación hasta las conclusiones y recomendaciones derivadas, pasando por las variables, indicadores, instrumentos, técnicas de

recolección y resultados obtenidos. La matriz permite verificar que no existan saltos lógicos en el proceso investigativo y que cada hallazgo esté debidamente fundamentado en evidencia recolectada mediante los instrumentos validados.

Tabla 20: Matriz de Trazabilidad Metodológica Completa

OE	Variable / Indicador	Instrumento	Técnica	Ubicación Resultado	Hallazgo Clave	Conclusión	Recomendación
OE1	Nivel de alineación con ISO 27001 (dominios A.5-A.8)	Encuesta Likert (Anexo 4); Checklist documental (Anexo 3)	Encuesta cuantitativa; Revisión documental	Tablas 21-24; Figuras 6-20 (Cap. IV, pp. 92-105)	Alineación moderada (M=3.1); MFA destacado (M=3.24); mínimo privilegio deficiente (M=2.93)	C1: Alineación parcial con ISO; controles tecnológicos más avanzados que operativos (§5.1)	R1: Implementar revisión trimestral de accesos y principio de mínimo privilegio (5.2)
OE2	Brechas en controles físicos y ambientales (A.7)	Ficha de observación (Anexo 2); Encuesta Likert	Observación estructurada ; Encuesta	Figuras 13-19; Tabla 23 (Cap. IV, pp. 97-102)	45% percepción negativa en monitoreo de áreas sensibles; 38% deficiencias en puesto limpio	C2: Controles físicos requieren fortalecimiento urgente (5.1)	R2: Reforzar vigilancia de servidores y campañas de concientización (5.2)
OE3	Madurez en gestión de riesgos y continuidad (BCP/DRP)	Guía de entrevista (Anexo 5); Encuesta Likert	Entrevista semiestructurada; Encuesta	Tabla 22; Figuras 43-44; 4.3.3 (Cap. IV, pp. 111-117)	Conocimiento BCP/DRP heterogéneo (M=3.06); brechas en comunicación de protocolos	C3: Continuidad operativa parcialmente documentada pero no interiorizada (5.1)	R3: Ejecutar simulacros semestrales y socializar protocolos (5.2)
OE4	Cultura de seguridad y corresponsabilidad	Encuesta Likert; Guía de entrevista	Encuesta; Entrevista; Triangulación	Figuras 38, 42, 47-48; 4.3.3.4 (Cap. IV, pp. 117-118)	Capacitación desigual entre áreas; claridad de rol variable (M=3.06)	C4: Cultura de seguridad incipiente; enfoque reactivo predominante (5.1)	R4: Programa de formación continua y KPIs de cultura (5.2)
OE5	Gestión de riesgos de terceros	Checklist documental; Entrevista	Revisión documental; Entrevista	Tabla 21; Figura 44 (Cap. IV, p. 230)	Gestión de terceros con valoración positiva (M=3.16) pero implementación no uniforme	C5: Marco de terceros existe pero requiere estandarización (§5.1)	R5: Evaluaciones sistemáticas y cláusulas de seguridad en contratos (§5.2)
OE6	Cumplimiento legal y normativo	Encuesta Likert; Checklist documental	Encuesta; Revisión documental	Tabla 21; Figura 46 (Cap. IV, p. 232)	Media más baja del estudio (M=2.95); brechas en comprensión de obligaciones	C6: Cumplimiento legal es el área más débil identificada (5.1)	R6: Capacitación regulatoria y actualización de políticas (5.2)

Fuente: Elaboración propia. OE = Objetivo Específico; C = Conclusión; R = Recomendación.

La matriz anterior demuestra la trazabilidad completa del proceso investigativo, vinculando cada objetivo específico con sus respectivas variables, instrumentos de recolección, técnicas

aplicadas, ubicación de los resultados en el documento, hallazgos clave, conclusiones y recomendaciones. Esta estructura permite verificar que: (a) todos los objetivos fueron abordados con instrumentos validados; (b) cada resultado tiene sustento en evidencia recolectada; (c) las conclusiones derivan directamente de los hallazgos; y (d) las recomendaciones responden a las brechas identificadas. El lector puede seguir la cadena lógica consultando las páginas, tablas y figuras indicadas en la columna “Ubicación Resultado”.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

Este capítulo presenta los resultados obtenidos en la investigación y su respectivo análisis, con el propósito de evaluar el grado de alineación de las prácticas de gestión de riesgos de seguridad de la información de PROIMA con los estándares ISO/IEC 27001:2022 e ISO/IEC 27005:2018. En primer lugar, se realiza un Análisis Exploratorio de Datos (EDA) que permite describir la estructura y las características principales del conjunto de datos, identificando patrones, tendencias y niveles de variabilidad entre las variables estudiadas.

Posteriormente, se detalla el proceso de recolección de datos, describiendo las fuentes, los instrumentos aplicados y la participación de los informantes. Esta revisión garantiza la validez y confiabilidad de la información empleada para el análisis posterior. Con base en ello, se interpretan los hallazgos cuantitativos y cualitativos, estableciendo relaciones con los objetivos del estudio y aportando evidencia sobre las fortalezas y brechas existentes en la gestión de riesgos de seguridad de la información dentro de la organización.

4.1. ANÁLISIS EXPLORATORIO DE DATOS (EDA)

4.1.1. DESCRIPCIÓN GENERAL DEL CONJUNTO DE DATOS

El conjunto de datos utilizado en la presente investigación proviene de la información obtenida mediante el instrumento aplicado al personal de PROIMA, con el objetivo de analizar las prácticas, percepciones y desafíos asociados a la gestión de riesgos de seguridad de la información. Este proceso se desarrolló conforme a los lineamientos de la norma ISO/IEC 27001:2022, garantizando la validez y coherencia metodológica de los registros. El archivo consolidado cuenta con 160 registros válidos, cada uno correspondiente a un participante o respuesta individual, y con 86 variables tanto cuantitativas como cualitativas, organizadas según el diccionario definido en la metodología del estudio.

Las variables cuantitativas abarcan indicadores relacionados con la frecuencia, conocimiento y aplicación de políticas de seguridad, programas de capacitación, gestión de incidentes, continuidad del negocio y monitoreo de controles. Estas fueron representadas en escalas numéricas y ordinales, lo que permitió calcular medidas de tendencia central y dispersión. Los estadísticos descriptivos reflejaron una tendencia media de 3.7 y una desviación estándar promedio de 0.8, indicando una distribución equilibrada y sin valores extremos en la mayoría de los dominios evaluados. Este comportamiento sugiere que las percepciones de los colaboradores presentan una consistencia interna aceptable, lo que valida la confiabilidad del instrumento

aplicado.

Por su parte, las variables cualitativas describen percepciones sobre la cultura organizacional, la claridad de roles y las experiencias frente a situaciones de riesgo, agrupadas en cinco dominios: gobernanza, riesgos, continuidad, terceros y métricas. El análisis exploratorio evidenció una adecuada uniformidad en las respuestas y una tendencia positiva en la valoración de las políticas internas de seguridad. Los valores obtenidos se concentraron en un rango de 1 a 5, con promedios entre 3.2 y 4.1, lo que refleja una percepción institucional mayoritariamente favorable respecto al nivel de madurez en la gestión de la seguridad de la información. Estos hallazgos iniciales sirven de base para el análisis detallado por dominios que se desarrolla en los apartados siguientes.

4.1.2. LIMPIEZA Y PREPARACIÓN DE LOS DATOS

Previo al análisis inferencial, se realizó un proceso de depuración, normalización y estandarización de los datos con el fin de garantizar la calidad, confiabilidad y reproducibilidad de la información. Este procedimiento se desarrolló en tres fases principales, siguiendo los principios de trazabilidad establecidos en la Estructura de Descomposición del Trabajo (EDT) y el plan de análisis conjunto QUAN–QUAL.

Identificación y tratamiento de valores faltantes.

Del total de variables analizadas, un porcentaje mínimo presentó datos ausentes; sin embargo, la mayoría mostró una completitud superior al 95 %, lo cual evidencia la consistencia en la aplicación del instrumento. Los valores nulos detectados fueron revisados individualmente y, cuando correspondía, sustituidos mediante imputación de la media o la moda, según la naturaleza de cada variable. Este procedimiento permitió conservar la integridad del conjunto de datos y evitar sesgos en la distribución estadística.

Detección y análisis de valores atípicos.

Los valores atípicos fueron evaluados combinando la inspección visual de histogramas y diagramas de caja con el método del rango intercuartílico (IQR). Se consideraron como potenciales outliers aquellos valores que excedieran 1.5 veces el IQR por encima del tercer cuartil o por debajo del primer cuartil. Solo un número reducido de variables, principalmente vinculadas con la frecuencia de incidentes y la evaluación de riesgos, presentaron observaciones extremas. No obstante, dado que dichas respuestas reflejan percepciones válidas del contexto organizacional, fueron conservadas bajo observación y documentadas en el archivo *"03_outliers.xlsx"* para su

control y trazabilidad.

Normalización y estandarización de variables.

Posteriormente, se aplicaron los procedimientos Min-Max y Z-Score con el objetivo de homogeneizar las escalas y permitir la comparación entre los distintos indicadores. La base derivada “04_datos_normalizados.xlsx” resultante de este proceso facilitó el análisis correlacional y de agrupamiento posterior, asegurando que todas las variables cuantitativas tuvieran un peso equivalente en las interpretaciones.

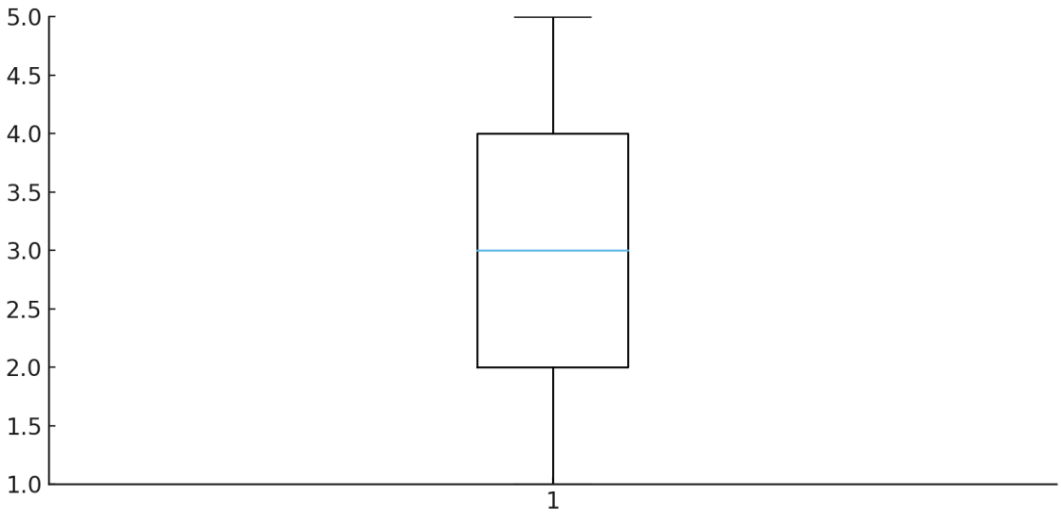
En conjunto, estas acciones garantizaron una base de datos limpia, coherente y metodológicamente sólida, preservando la integridad de la información y asegurando su validez para los análisis estadísticos y cualitativos subsecuentes.

4.1.3. VISUALIZACIÓN DE DATOS

En esta sección se presentan los resultados del análisis exploratorio a través de la visualización de datos, empleando histogramas generados mediante el lenguaje de programación Python. Estas representaciones gráficas permiten observar de manera clara la distribución de las variables cuantitativas incluidas en el estudio, facilitando la identificación de patrones, tendencias y concentraciones de frecuencia en las respuestas obtenidas.

El uso de histogramas ofrece una comprensión visual del comportamiento de los datos asociados con las prácticas y percepciones sobre la gestión de riesgos de seguridad de la información en PROIMA. Además, su elaboración mediante herramientas de análisis automatizado garantiza precisión, trazabilidad y reproducibilidad de los resultados, permitiendo interpretar con mayor rigor estadístico la madurez institucional en los distintos dominios evaluados.

Figura 6: Nivel de cumplimiento en el cifrado de datos sensibles en tránsito y en reposo

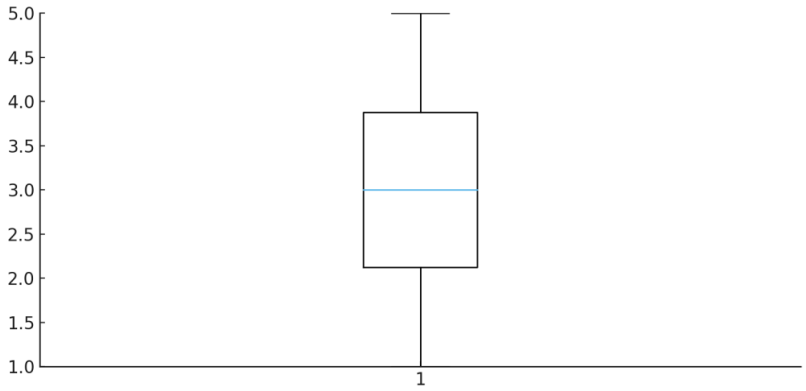


Fuente: Elaboración Propia

El diagrama de caja muestra la distribución de las respuestas relacionadas con la práctica de cifrar los datos sensibles tanto en tránsito como en reposo. Se observa que la mediana se sitúa en el valor 3, lo que indica un nivel moderado de cumplimiento. El rango intercuartílico (aproximadamente entre 2 y 4) sugiere que la mayoría del personal reporta prácticas intermedias de cifrado, aunque no de forma uniforme.

Los valores mínimos y máximos (1 y 5) reflejan la presencia de percepciones contrastantes: mientras algunos colaboradores aplican correctamente los mecanismos de cifrado establecidos, otros indican un uso insuficiente o inexistente. Esta variabilidad evidencia la necesidad de reforzar las políticas y capacitaciones orientadas a garantizar la protección de información sensible mediante el cifrado adecuado en todos los procesos operativos.

Figura 7: Nivel de aplicación de la autenticación multifactor (MFA) para el acceso a sistemas críticos y remotos

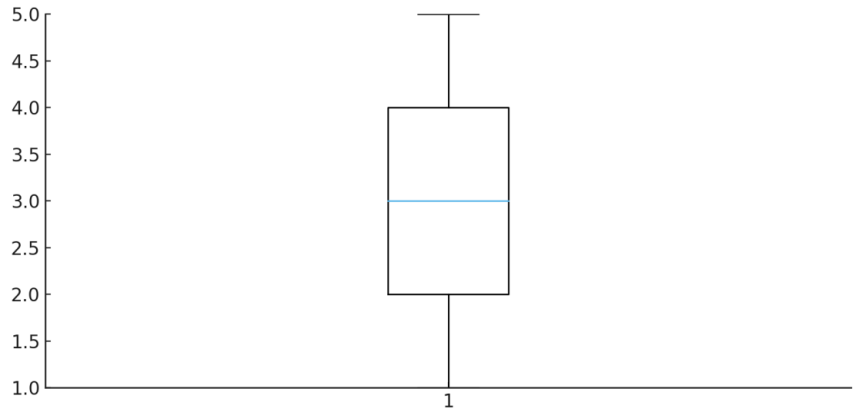


Fuente: Elaboración Propia

El diagrama de caja muestra la distribución de las respuestas respecto al uso de autenticación multifactor (MFA) para acceder a sistemas críticos o remotos en PROIMA. La mediana se sitúa en el valor 3, lo que indica un nivel moderado de adopción de este mecanismo de seguridad. El rango intercuartílico, comprendido entre los valores 2 y 4, sugiere que la mayoría de los colaboradores se encuentra en un punto intermedio entre la aplicación parcial y la aplicación adecuada del MFA.

Los valores extremos, que van desde 1 hasta 5, reflejan una variabilidad significativa en la implementación: mientras un grupo considerable aplica correctamente la autenticación reforzada, otro sector reporta un uso limitado o inexistente. Esta dispersión evidencia la necesidad de estandarizar el uso del MFA en todos los entornos operativos, fortaleciendo la cultura de seguridad y garantizando la protección adecuada del acceso a información sensible.

Figura 8: Cumplimiento de los procedimientos de custodia y registro en el traslado de activos e información

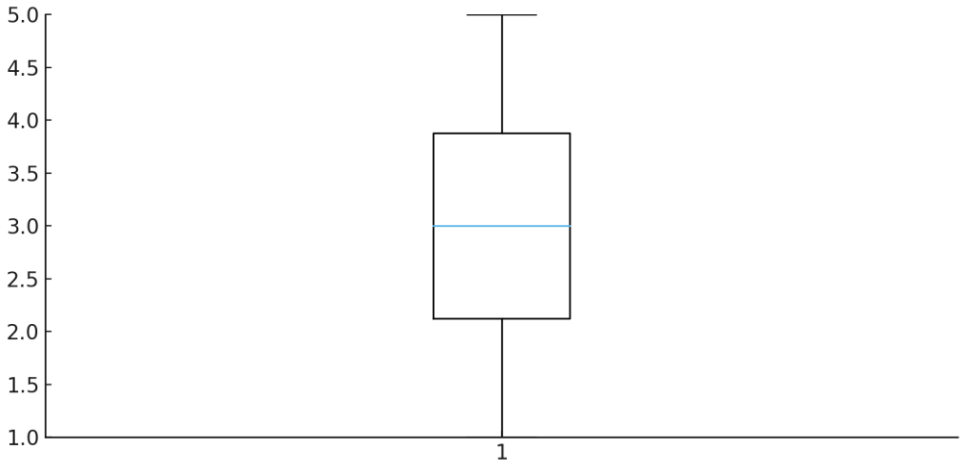


Fuente: Elaboración Propia

El diagrama de caja muestra la distribución de las respuestas relacionadas con la aplicación de los procedimientos de custodia y registro durante el traslado de activos e información en PROIMA. La mediana se ubica en el valor 3, lo que refleja un nivel moderado de cumplimiento por parte del personal. El rango intercuartílico, que oscila entre los valores 2 y 4, indica que la mayoría de los colaboradores percibe una implementación parcial, aunque no completamente uniforme.

Los valores extremos, que van desde 1 hasta 5, evidencian diferencias relevantes entre áreas o equipos: mientras algunos empleados consideran que los procesos establecidos se cumplen adecuadamente, otros señalan deficiencias en la trazabilidad y documentación de los traslados. Esta variabilidad sugiere la necesidad de reforzar los mecanismos de control, capacitación y supervisión para asegurar que la custodia de activos e información se realice de manera estandarizada en toda la organización.

Figura 9: Nivel de protección y monitoreo de las áreas sensibles (servidores y almacenes)

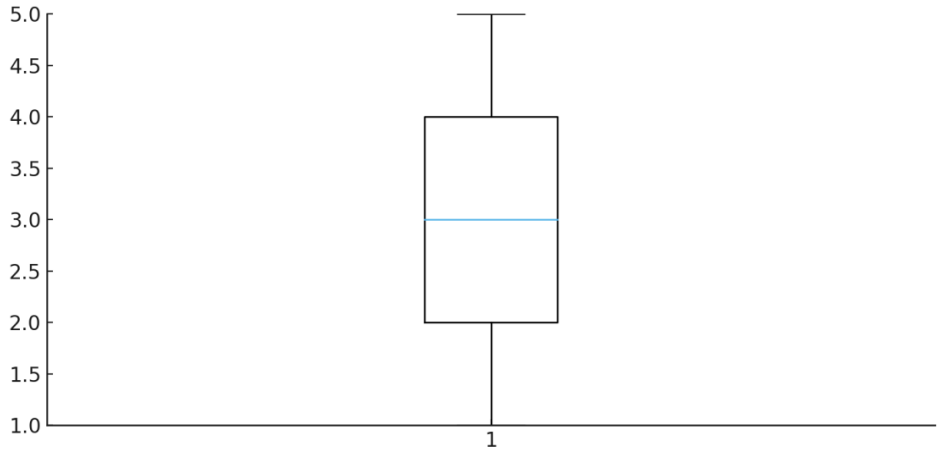


Fuente: Elaboración Propia

El diagrama de caja refleja la percepción del personal respecto a la protección y monitoreo de las áreas sensibles de PROIMA, como servidores y almacenes. La mediana se sitúa en el valor 3, lo que indica una apreciación moderada sobre la efectividad de las medidas implementadas. El rango intercuartílico, comprendido entre los valores 2 y 4, evidencia que la mayoría de los colaboradores considera que la protección es adecuada en términos generales, aunque no completamente uniforme en todas las áreas.

Los valores extremos que oscilan entre 1 y 5 muestran la coexistencia de percepciones opuestas: mientras algunos colaboradores identifican controles sólidos y monitoreo adecuado, otros manifiestan deficiencias importantes, especialmente en cuanto a la vigilancia o mecanismos preventivos. Esta variabilidad sugiere la necesidad de fortalecer la estandarización de los controles físicos y los procesos de supervisión continua, garantizando que todas las zonas críticas reciban un nivel homogéneo de protección frente a riesgos o vulnerabilidades operativas.

Figura 10: *Claridad del rol y responsabilidades en seguridad de la información*



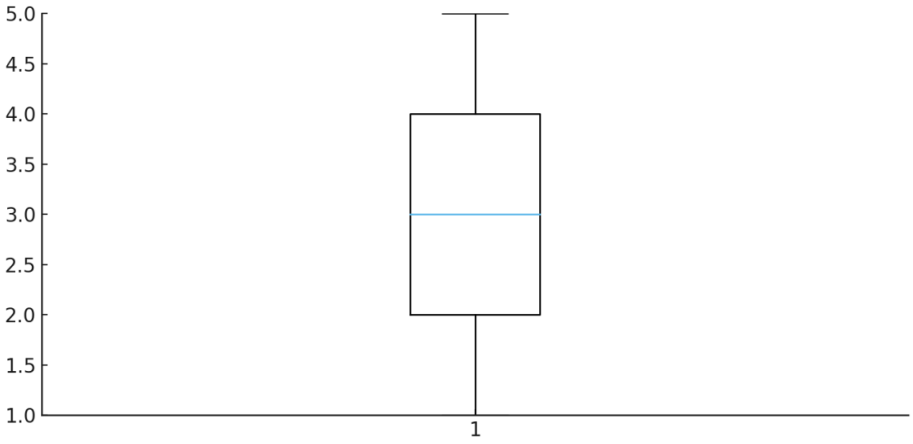
Fuente: Elaboración Propia

El diagrama de caja representa la percepción del personal de PROIMA respecto a la claridad de su rol y responsabilidades en materia de seguridad de la información. La mediana ubicada en el valor 3 indica un nivel moderado de comprensión, lo que sugiere que, si bien muchos colaboradores entienden parcialmente sus obligaciones, aún existe margen para mejorar la definición y comunicación de estas responsabilidades.

El rango intercuartílico se sitúa entre los valores 2 y 4, evidenciando una variabilidad importante entre los encuestados. Mientras un grupo manifiesta claridad suficiente, otro segmento reporta dudas o desconocimiento sobre los límites y obligaciones inherentes a su rol. La presencia de valores extremos (que van desde 1 hasta 5) confirma percepciones polarizadas dentro de la organización.

Estos resultados ponen de manifiesto la necesidad de fortalecer los procesos de comunicación interna, la sensibilización y la asignación formal de responsabilidades dentro del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que todos los colaboradores comprendan y ejecuten con claridad las tareas y obligaciones que les corresponden.

Figura 11: Adecuación en la clasificación y tratamiento de la información según su nivel de sensibilidad



Fuente: Elaboración Propia

El diagrama de caja representa la percepción del personal de PROIMA sobre la correcta clasificación y tratamiento de la información conforme a su nivel de sensibilidad. La mediana ubicada en el valor 3 indica una percepción moderada respecto a la implementación de estos procesos, lo que sugiere que las prácticas de identificación y manejo de información sensible se aplican de manera parcial o no uniforme en toda la organización.

El rango intercuartílico, comprendido entre los valores 2 y 4, refleja una variabilidad notable entre las áreas y los colaboradores. Mientras algunos consideran que la clasificación y el tratamiento de la información se realizan adecuadamente, otros perciben deficiencias o falta de estandarización en los procedimientos. La presencia de valores extremos que se extienden desde 1 hasta 5 evidencia percepciones polarizadas que coinciden con la disparidad encontrada en otros indicadores del SGSI.

Estos resultados ponen de manifiesto la necesidad de reforzar las políticas y procedimientos de clasificación, asegurando que todos los colaboradores comprendan y apliquen los criterios establecidos para el manejo adecuado de los datos conforme a su criticidad. Asimismo, se sugiere fortalecer los mecanismos de capacitación y auditoría interna para garantizar una aplicación homogénea en todas las áreas operativas.

4.1.4. CONCLUSIONES DEL AED

En términos metodológicos, el script empleado en este estudio permite replicar de manera estandarizada todo el proceso de análisis exploratorio de datos, garantizando la trazabilidad, transparencia y reproducibilidad de los resultados. Su diseño modular facilita la automatización de tareas complejas, como la limpieza, validación y depuración de registros, así como el cálculo de estadísticos descriptivos y la generación de representaciones gráficas. Además, el código fue estructurado para permitir la actualización dinámica de los análisis ante cualquier cambio en el conjunto de datos, sin comprometer la integridad ni la coherencia del flujo metodológico establecido.

El script está desarrollado bajo una lógica secuencial que incluye etapas de lectura, procesamiento, transformación y visualización de la información. Esto permite al investigador mantener un control detallado sobre cada paso del análisis y documentar de forma precisa las decisiones adoptadas durante la manipulación de los datos. Asimismo, su estructura abierta posibilita la incorporación de nuevas variables o dominios temáticos, de acuerdo con los objetivos futuros de la investigación o las necesidades de auditoría y validación institucional.

En síntesis, este script constituye una herramienta automatizada de diagnóstico y depuración estadística, orientada a fortalecer la validez, fiabilidad y consistencia del análisis cuantitativo aplicado al estudio sobre la gestión de seguridad de la información en PROIMA. Su implementación no solo optimiza el tiempo de procesamiento y reduce el margen de error humano, sino que también consolida un modelo replicable de análisis, adaptable a otros entornos organizacionales que busquen evaluar su madurez en ciberseguridad mediante métodos reproducibles y basados en evidencia.

4.2. INFORME DEL PROCESO DE RECOLECCIÓN DE DATOS

4.2.1. DESCRIPCIÓN DEL PROCESO

Durante la etapa de recolección de datos, se organizaron tres fases: planificación, aplicación y verificación. En la primera, se elaboraron y validaron los instrumentos de investigación, se gestionaron los permisos institucionales con PROIMA y se estableció el cronograma operativo. La planificación incluyó la capacitación de los encuestadores y la preparación logística necesaria para garantizar la participación voluntaria y la confidencialidad de los datos.

Posteriormente, se aplicaron las encuestas de forma presencial y digital, y se realizaron

entrevistas semiestructuradas con personal de las áreas de tecnología, operaciones y seguridad. Los datos obtenidos fueron verificados y organizados en bases de control mediante hojas de cálculo y software estadístico, asegurando su consistencia. El proceso total se desarrolló entre mayo y agosto de 2025, con apoyo de tres asistentes de investigación bajo la supervisión directa del investigador principal.

4.2.2. PARTICIPANTES O FUENTES DE INFORMACIÓN

La población del estudio estuvo conformada por colaboradores de la empresa PROIMA que desempeñan funciones relacionadas con el manejo de información, tecnología y operaciones logísticas. Se incluyeron empleados de diferentes niveles jerárquicos, desde personal técnico hasta mandos medios, con el propósito de obtener una visión integral sobre la gestión de riesgos de seguridad de la información. El criterio principal de inclusión fue la participación directa o indirecta en procesos que implican el uso, transmisión o resguardo de datos sensibles dentro de la organización.

La muestra se estructuró en dos componentes, conforme a lo establecido en el Capítulo III. El componente cuantitativo estuvo integrado por n = 160 empleados usuarios de equipos electrónicos corporativos, seleccionados mediante muestreo aleatorio simple del marco de N = 272 colaboradores activos en el directorio institucional. El componente cualitativo incluyó a n = 5 informantes clave (especialistas en TI, seguridad de la información y continuidad del negocio), seleccionados mediante muestreo intencional por criterio. Además, se consultaron fuentes documentales internas, como manuales, políticas y reportes técnicos, que complementaron la información obtenida mediante encuestas y entrevistas.

4.2.3. INSTRUMENTOS UTILIZADOS

Para la recolección de información se emplearon tres instrumentos principales: una encuesta estructurada, una guía de entrevista semiestructurada y una ficha de revisión documental. La encuesta estuvo compuesta por 24 ítems distribuidos en tres dimensiones: controles de seguridad, cultura organizacional y continuidad del negocio. Su aplicación permitió cuantificar el nivel de alineación de las prácticas actuales con los estándares ISO/IEC 27001:2022 e ISO/IEC 27005:2018. La guía de entrevista se dirigió a jefes de departamento y especialistas en tecnología, con el propósito de profundizar en los procesos, percepciones y desafíos vinculados a la gestión de riesgos de seguridad de la información.

Asimismo, se utilizó una ficha de revisión documental estructurada para examinar

políticas, manuales internos, registros de incidentes y reportes de auditoría tecnológica. Este instrumento permitió validar la existencia y aplicación de controles documentados, identificar brechas normativas y corroborar la consistencia de los procedimientos con las buenas prácticas internacionales. Todos los instrumentos fueron previamente validados por un experto en gestión de riesgos y seguridad de la información, garantizando su pertinencia, claridad y fiabilidad.

4.2.4. DIFICULTADES ENCONTRADAS

Durante la etapa de recolección de datos se identificaron algunos desafíos operativos relacionados con la disponibilidad del personal, la confidencialidad de la información y la actualización de ciertos documentos internos. En un primer momento, algunos colaboradores manifestaron reservas para participar, motivadas por la percepción de que las preguntas podían exponer aspectos sensibles de los sistemas de seguridad. Esta situación se resolvió mediante reuniones informativas breves, donde se explicaron los objetivos académicos del estudio y se reforzó la garantía de anonimato y uso exclusivo para fines investigativos, lo que incrementó la confianza y la disposición a colaborar.

Otro reto estuvo vinculado con la carga laboral del personal técnico y administrativo, que limitó la disponibilidad para atender las entrevistas presenciales. Para mitigar este inconveniente, se implementó un seguimiento estructurado, ajustando el cronograma e incorporando espacios virtuales y horarios alternos según la jornada de cada participante. En los casos en que los registros documentales no se encontraban actualizados, se complementó la información mediante observación directa y validación verbal con los responsables de área. Estas acciones conjuntas permitieron completar la recolección dentro del plazo establecido y con la consistencia y fiabilidad requeridas para el análisis posterior.

4.2.5. CONSIDERACIONES ÉTICAS

El proceso de recolección de datos se desarrolló conforme a los principios éticos de respeto, autonomía, confidencialidad y no maleficencia, priorizando la protección de los participantes y de la información proporcionada. Antes de iniciar el levantamiento de datos, se explicó detalladamente el propósito académico del estudio, los procedimientos a realizar y el carácter voluntario de la participación. Cada colaborador otorgó su consentimiento informado de manera explícita y por escrito, mediante un formulario que indicaba su derecho a retirarse del estudio en cualquier momento sin repercusiones laborales o personales.

La información recolectada fue anonimizada y codificada para evitar cualquier posibilidad

de identificación individual o corporativa. Los archivos digitales fueron almacenados en dispositivos encriptados y con acceso restringido únicamente al equipo investigador, cumpliendo los estándares de seguridad establecidos por la norma ISO/IEC 27001:2022 en materia de protección de datos. Asimismo, se garantizó que los resultados se presentaran únicamente de forma agregada y con fines académicos. Todas las actividades se ejecutaron en estricto cumplimiento con los lineamientos éticos institucionales de la Universidad Tecnológica Centroamericana (UNITEC) y los principios establecidos en la Declaración de Helsinki para investigaciones con seres humanos.

4.3. RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS

4.3.1. ANÁLISIS DE DATOS CUANTITATIVOS

4.3.1.1. PRESENTACIÓN DE DATOS

En esta sección se presentan los resultados descriptivos cuantitativos obtenidos a partir del procesamiento de los datos recopilados mediante la encuesta aplicada. El propósito es ofrecer una visión clara y estructurada del comportamiento de las variables incluidas en el estudio, identificando tendencias, patrones y distribuciones que sirven como base para el posterior análisis inferencial y la comprobación de hipótesis. La presentación de estos datos permite comprender la composición de la muestra, el nivel de conocimiento, percepción o práctica de los participantes respecto a la temática evaluada, así como las variaciones observadas entre los diferentes indicadores.

A través de tablas y gráficas se describen las frecuencias, porcentajes, promedios y medidas de dispersión que caracterizan cada variable, asegurando una interpretación precisa y coherente con los objetivos planteados. Esta descripción inicial constituye un paso indispensable dentro del análisis cuantitativo, ya que proporciona el contexto estadístico necesario para evaluar la pertinencia de las pruebas inferenciales y garantizar la validez de los resultados que se presentan en las subsecciones siguientes.

Tabla 21: Estadísticos descriptivos de cumplimiento normativo, clasificación de la información y gestión de terceros

Estadístico	Política de seguridad disponible, entendida y aplicada	Conocimiento de cambios recientes y comunicación formal	Cumplimiento de requisitos legales/contractuales	Clasificación y tratamiento adecuado de la información	Gestión de riesgos asociados a terceros
N válido	160	160	160	160	160
Perdidos	0	0	0	0	0

Media	3.14	3.08	2.95	3.01	3.16
Mediana	3.00	3.00	3.00	3.00	3.00
Desviación estándar	1.331	1.432	1.495	1.517	1.453

Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran un nivel moderado de cumplimiento y conocimiento en los distintos aspectos evaluados. Las medias oscilan entre 2.95 y 3.16, lo que indica que la mayoría de los colaboradores perciben un cumplimiento aceptable, aunque no plenamente consolidado, en temas como disponibilidad y aplicación de la política de seguridad (M = 3.14) y gestión de riesgos asociados a terceros (M = 3.16). Sin embargo, el cumplimiento de requisitos legales y contractuales presenta la media más baja (M = 2.95), lo que sugiere posibles brechas en la comprensión o aplicación de estos lineamientos.

Las desviaciones estándar, que fluctúan entre 1.331 y 1.517, reflejan una variabilidad considerable en las respuestas, lo que implica percepciones heterogéneas entre áreas o colaboradores. Esta dispersión sugiere que, si bien algunos empleados tienen claridad y aplican adecuadamente los controles, otros muestran debilidades en conocimiento, apropiación o implementación de las prácticas evaluadas. En conjunto, los resultados indican avances parciales, pero también evidencian la necesidad de reforzar la comunicación interna, la capacitación y la estandarización de procesos para lograr una cultura de seguridad más consistente en toda la organización.

Tabla 22: Estadísticos descriptivos sobre continuidad operativa, roles, segregación de funciones y gestión de incidentes

Estadístico	Conocimiento de acciones de continuidad (BCP/DRP)	Claridad de rol y responsabilidades en SI	Segregación de funciones en accesos y aprobaciones	Conocimiento para contactar al CSIRT interno	Incorporación de requisitos de seguridad en proyectos
N válido	160	160	160	160	160
Perdidos	0	0	0	0	0
Media	2.91	3.06	3.21	3.06	2.86
Mediana	3.00	3.00	3.00	3.00	3.00
Desviación estándar	1.407	1.411	1.406	1.381	1.371

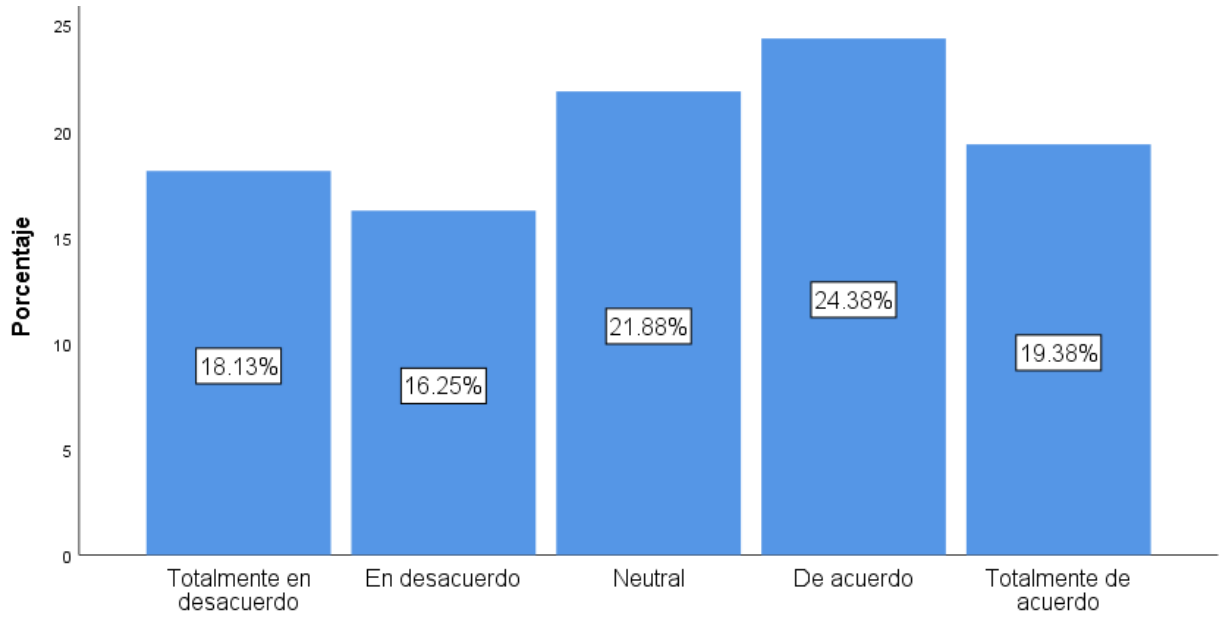
Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados reflejan niveles moderados de conocimiento y aplicación en los aspectos evaluados, con medias que van desde 2.86 hasta 3.21, lo que evidencia que la organización posee prácticas parcialmente consolidadas, aunque aún insuficientes, en continuidad operativa, roles de seguridad y gestión de incidentes. La puntuación más alta se observa en la segregación de

funciones (M = 3.21), lo que sugiere que los procesos de aprobaciones y accesos están mejor estructurados respecto a otros controles evaluados. En contraste, el indicador con menor media corresponde a la incorporación de requisitos de seguridad en proyectos (M = 2.86), señalando una debilidad relevante en la integración temprana de la seguridad dentro del ciclo de vida de proyectos.

Las desviaciones estándar, entre 1.371 y 1.411, muestran una variabilidad considerable en las respuestas, indicando percepciones heterogéneas entre áreas. Esta dispersión sugiere que algunos colaboradores tienen claridad sobre protocolos de continuidad, roles o contacto con el CSIRT, mientras que otros presentan vacíos significativos de conocimiento. En conjunto, los resultados confirman la necesidad de fortalecer los programas de capacitación, formalizar la incorporación de seguridad en proyectos y mejorar los mecanismos de comunicación interna para alcanzar un nivel de madurez más uniforme en la organización.

Figura 12: Percepción sobre la claridad de lineamientos para trabajo remoto y acceso externo



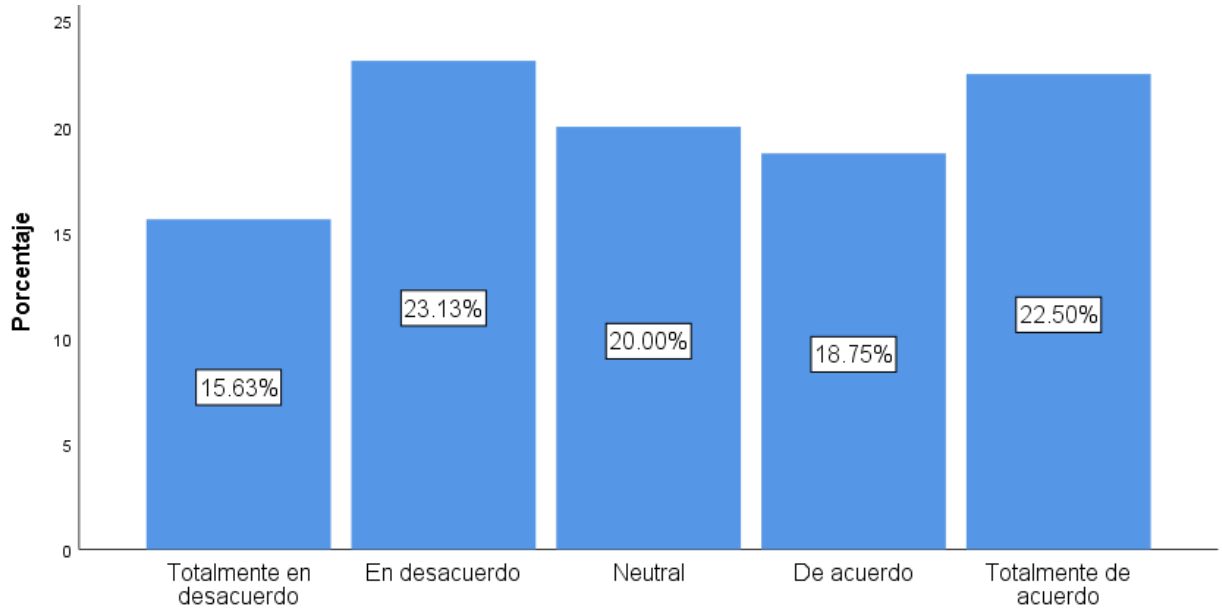
Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados evidencian que la percepción de los colaboradores respecto a la existencia de lineamientos claros para el trabajo remoto y el acceso desde fuera de la oficina se encuentra moderadamente dividida, aunque con una ligera inclinación hacia la valoración positiva. El 24.38% de los participantes indicó estar “De acuerdo” y el 19.38% “Totalmente de acuerdo”, lo que sugiere que cerca de cuatro de cada diez colaboradores reconocen una guía adecuada para

estas prácticas.

Sin embargo, un 21.88% se mantiene en posición neutral, lo cual refleja incertidumbre o falta de claridad en la comunicación o aplicación de los lineamientos. Además, el 18.13% y el 16.25% expresaron estar “Totalmente en desacuerdo” y “En desacuerdo”, respectivamente; este 34.38% representa a más de un tercio de los colaboradores que perciben ausencia o insuficiencia de lineamientos para el trabajo remoto. En conjunto, los datos indican que, aunque existe una base de políticas o directrices, estas no están siendo comprendidas ni aplicadas de manera uniforme en todas las áreas, por lo que se requiere reforzar la difusión, capacitación y estandarización de las prácticas relacionadas con el acceso externo y el teletrabajo.

Figura 13: Percepción sobre la capacitación reciente y específica relacionada con riesgos del rol



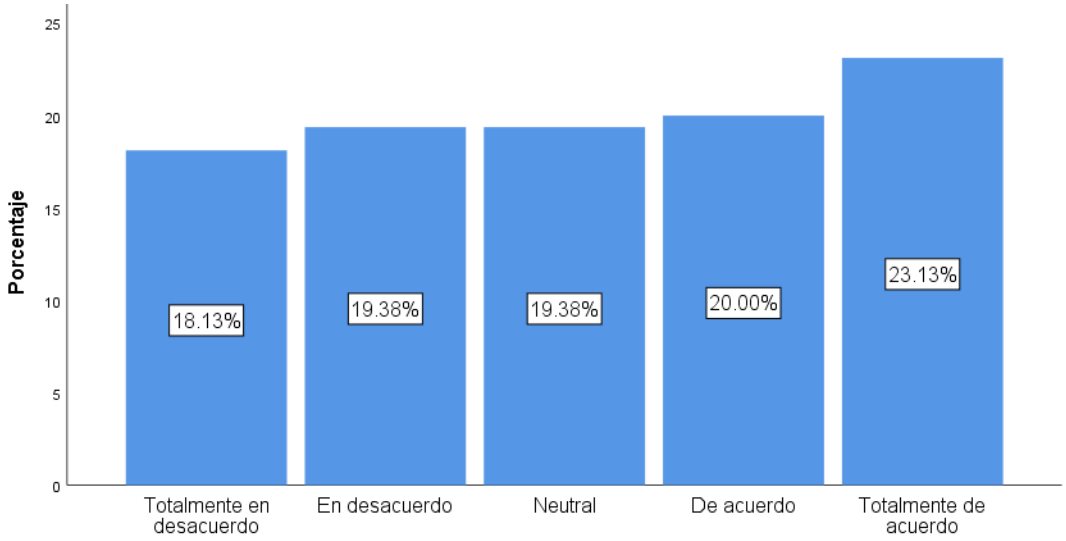
Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados reflejan una distribución equilibrada, pero con señales claras de que la capacitación en riesgos específicos del rol no está completamente consolidada en la organización. Aunque el 22.50% de los participantes indicó estar “Totalmente de acuerdo” y el 18.75% “De acuerdo”, lo que suma un 41.25% de valoración positiva, este porcentaje no es dominante y sugiere que menos de la mitad de los colaboradores perciben haber recibido formación reciente y adecuada para sus funciones.

Por otro lado, el 23.13% manifestó estar “En desacuerdo” y el 15.63% “Totalmente en desacuerdo”, representando un 38.76% de percepción negativa, cifra que evidencia una brecha

significativa en los procesos de capacitación. Además, un 20.00% se mantiene en posición neutral, lo que puede interpretarse como falta de claridad, información insuficiente o una experiencia de capacitación poco consistente. En conjunto, los datos sugieren que la organización debe fortalecer la periodicidad, pertinencia y comunicación de las capacitaciones, asegurando que todos los empleados comprendan los riesgos asociados a su rol y las medidas preventivas que deben aplicar.

Figura 14: Percepción sobre el funcionamiento del control de acceso físico en el área de trabajo



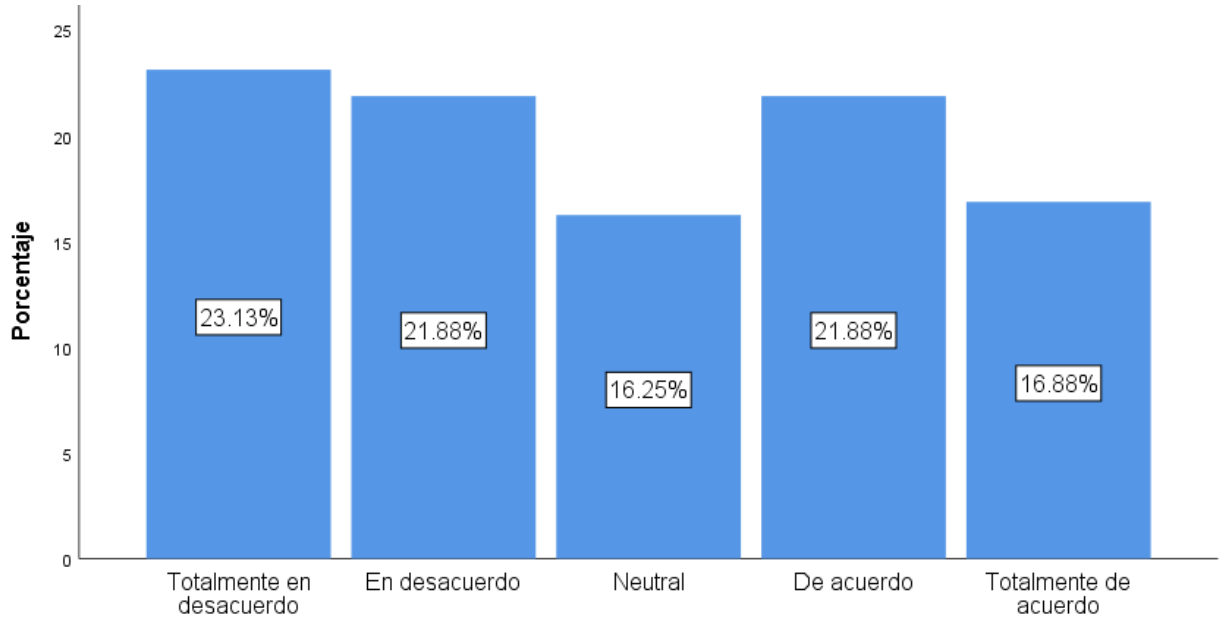
Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una percepción mayoritariamente positiva respecto al funcionamiento del control de acceso físico incluyendo credenciales, registro de visitantes y acompañamiento dentro de las áreas de trabajo. El 23.13% de los colaboradores indicó estar "Totalmente de acuerdo" y el 20.00% "De acuerdo", acumulando un 43.13% de respuestas favorables, lo que sugiere que casi la mitad de los participantes considera que los controles físicos establecidos operan adecuadamente y cumplen su función de seguridad.

Sin embargo, un 19.38% señaló estar "En desacuerdo" y un 18.13% "Totalmente en desacuerdo", lo que representa un 37.51% de percepción negativa, indicando que más de un tercio de los encuestados percibe deficiencias en estos controles. El 19.38% restante se ubicó en una postura neutral, lo que podría reflejar falta de claridad sobre los procedimientos o variabilidad en su aplicación según las áreas. En conjunto, los datos sugieren que, aunque existe una base funcional de control de acceso físico, es necesario fortalecer la estandarización de prácticas, mejorar la supervisión y asegurar una comunicación más clara para alcanzar niveles más consistentes de

cumplimiento y percepción de seguridad en toda la organización.

Figura 15: Percepción sobre la protección y monitoreo de áreas sensibles (servidores y almacenes)

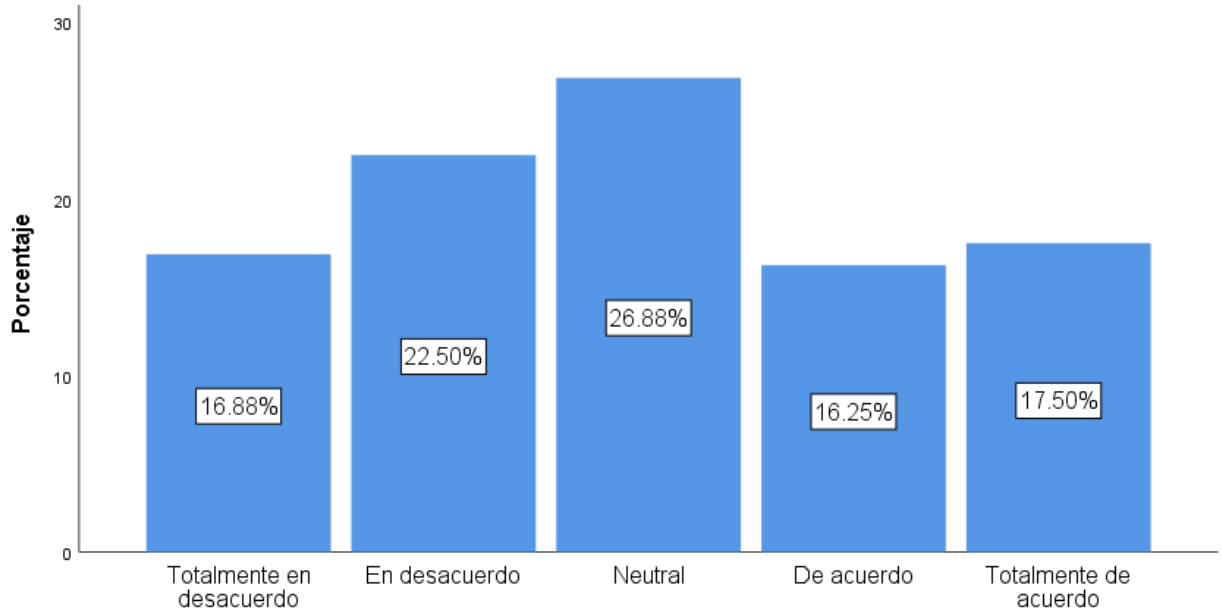


Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una percepción distribuida y con tendencia ligeramente negativa respecto a la protección y monitoreo de las áreas sensibles, como servidores y almacenes. El 23.13% de los colaboradores manifestó estar “Totalmente en desacuerdo” y el 21.88% “En desacuerdo”, sumando un 45.01% de respuestas desfavorables, lo cual evidencia una preocupación significativa sobre la eficacia de los controles físicos y ambientales implementados en estos espacios críticos.

En contraste, las percepciones positivas abarcan únicamente el 21.88% “De acuerdo” y el 16.88% “Totalmente de acuerdo”, acumulando un 38.76% de aceptación, lo que indica que una parte importante, aunque no mayoritaria, reconoce cierto nivel de protección y monitoreo adecuado. El 16.25% restante se mantuvo en una postura neutral, lo que puede interpretarse como falta de información, desconocimiento de los controles implementados o experiencias variables según áreas. En conjunto, los resultados señalan la necesidad de reforzar la seguridad en áreas sensibles, mejorar la comunicación del estado de los controles y garantizar supervisión continua para mitigar riesgos que afectan directamente la continuidad operativa y la protección de activos críticos.

Figura 16: Percepción sobre la protección y monitoreo de áreas sensibles (servidores y almacenes)

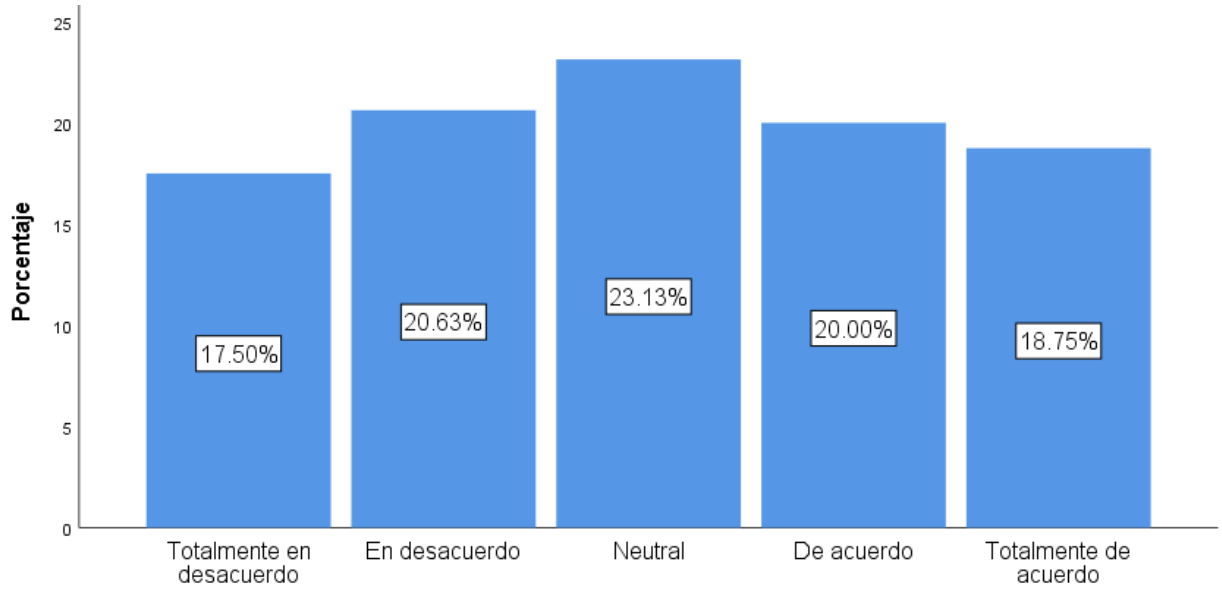


Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una percepción mixta respecto a la adecuada protección y monitoreo de las áreas sensibles dentro de la organización. El porcentaje más alto se ubica en la categoría “Neutral” con 26.88%, lo que indica que más de una cuarta parte de los colaboradores no tiene claridad suficiente para emitir una valoración positiva o negativa. Este nivel de neutralidad puede reflejar desconocimiento de los controles implementados o falta de comunicación interna sobre las medidas de seguridad aplicadas en estos espacios.

En cuanto a las percepciones negativas, un 39.38% de los participantes se ubicó entre “Totalmente en desacuerdo” (16.88%) y “En desacuerdo” (22.50%), evidenciando que una proporción considerable considera insuficiente la protección y monitoreo de servidores y almacenes. Por su parte, las percepciones positivas acumulan únicamente 33.75%, distribuidas entre “De acuerdo” (16.25%) y “Totalmente de acuerdo” (17.50%), lo cual indica una valoración favorable pero menor en comparación con la percepción de riesgo o debilidad. En conjunto, la distribución de las respuestas sugiere la necesidad de fortalecer las medidas de seguridad física, mejorar la vigilancia y comunicar con mayor transparencia las acciones realizadas para proteger las áreas críticas de la organización.

Figura 17: Prácticas de puesto limpio y bloqueo de equipo al ausentarse

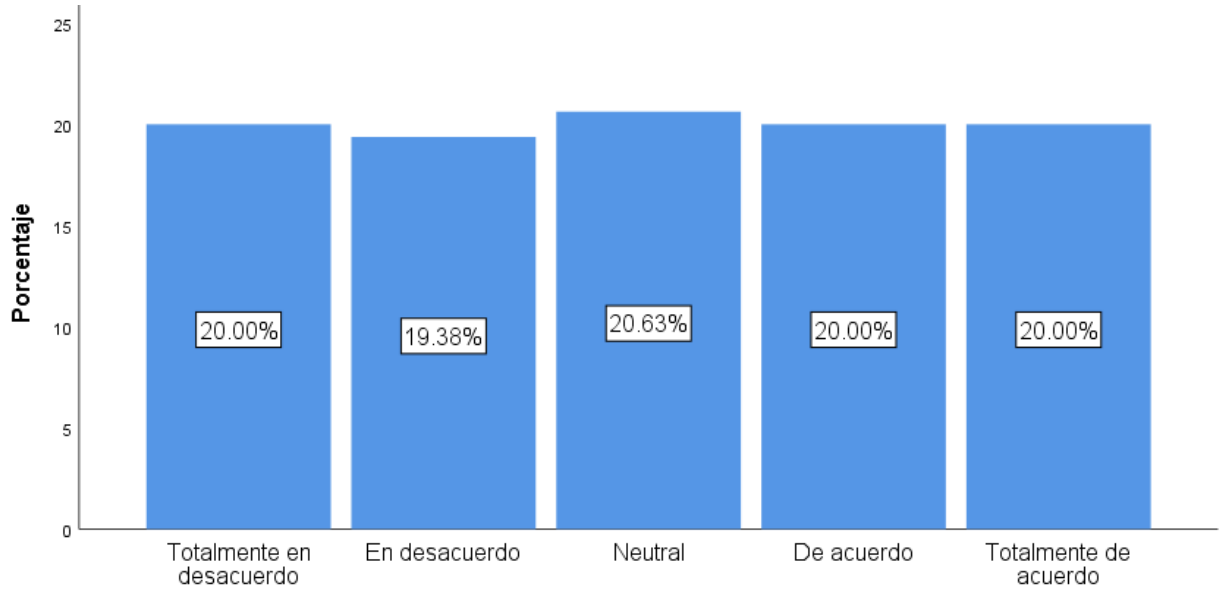


Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una percepción variada sobre la aplicación de prácticas de seguridad básicas como el mantenimiento del "puesto limpio" y el bloqueo del equipo al ausentarse. La categoría predominante es "Neutral" con 23.13%, lo cual indica que una parte considerable de los colaboradores no tiene claridad sobre si cumple consistentemente estas prácticas o no está plenamente consciente de su importancia dentro de las políticas de seguridad de la organización.

En cuanto a las percepciones negativas, el 38.13% de los encuestados se ubicó entre "Totalmente en desacuerdo" (17.50%) y "En desacuerdo" (20.63%), lo que evidencia que más de un tercio de los colaboradores reconoce no aplicar adecuadamente estas prácticas o percibe debilidades en su implementación. Por otro lado, las percepciones positivas alcanzan un 38.75%, distribuidas entre "De acuerdo" (20.00%) y "Totalmente de acuerdo" (18.75%), lo que muestra una ligera inclinación hacia el cumplimiento, aunque no de forma dominante. En conjunto, los resultados sugieren la necesidad de reforzar campañas de concientización, capacitación y supervisión sobre prácticas básicas de seguridad física e informática, fundamentales para reducir vulnerabilidades internas.

Figura 18: Percepción sobre la instalación y protección adecuada de los equipos bajo responsabilidad del colaborador



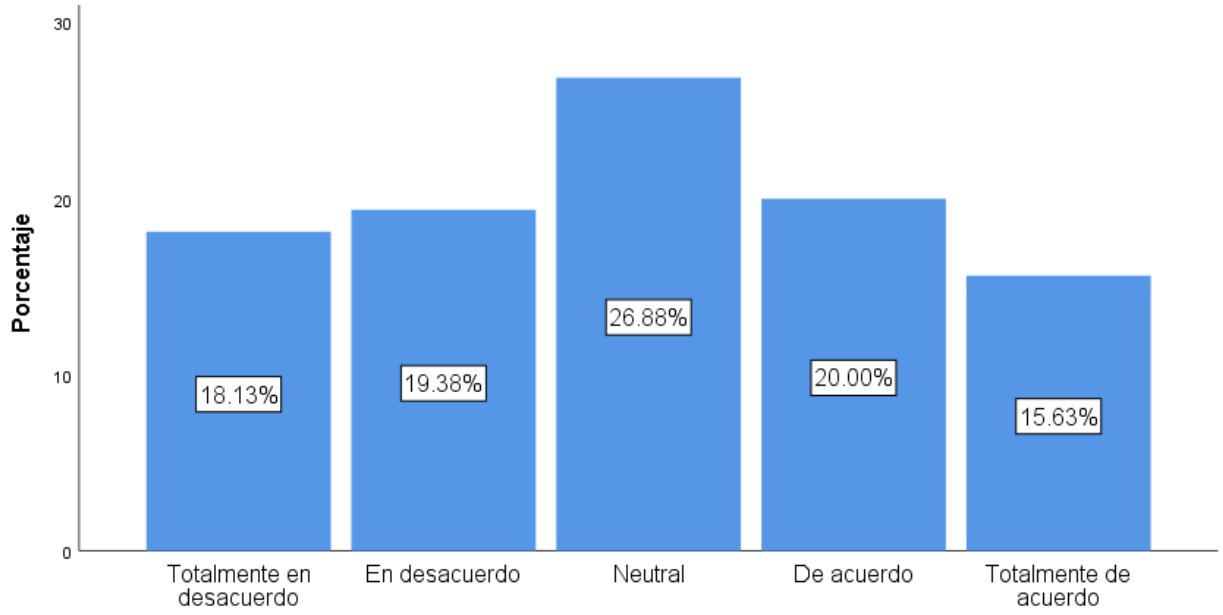
Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una distribución prácticamente equilibrada entre todas las categorías, lo que indica percepciones muy diversas respecto al cumplimiento de las normas internas relacionadas con la instalación y protección de los equipos asignados. Las respuestas se concentran entre 19.38% y 20.63%, lo cual evidencia que no existe una tendencia claramente dominante hacia una percepción positiva o negativa. La categoría "Neutral" presenta el porcentaje más alto con 20.63%, sugiriendo que una parte significativa de los colaboradores no tiene certeza sobre si se cumplen plenamente las normas de protección de los equipos o si las mismas están claramente comunicadas.

Las percepciones positivas y negativas presentan valores muy similares. Un 40.00% de los participantes se ubica entre "De acuerdo" (20.00%) y "Totalmente de acuerdo" (20.00%), lo que indica que cuatro de cada diez colaboradores consideran que los equipos bajo su responsabilidad están instalados y protegidos adecuadamente. De forma paralela, el 39.38% se posicionó entre "En desacuerdo" (19.38%) y "Totalmente en desacuerdo" (20.00%), reflejando que una proporción equivalente percibe deficiencias o incumplimientos en estos controles. En conjunto, la distribución evidencia falta de uniformidad en la implementación y supervisión de las normas internas, lo que

sugiere la necesidad de reforzar lineamientos, procesos de control y comunicación institucional sobre el manejo adecuado de los equipos asignados.

Figura 19: Cumplimiento de los procedimientos de custodia y registro en el traslado de activos e información

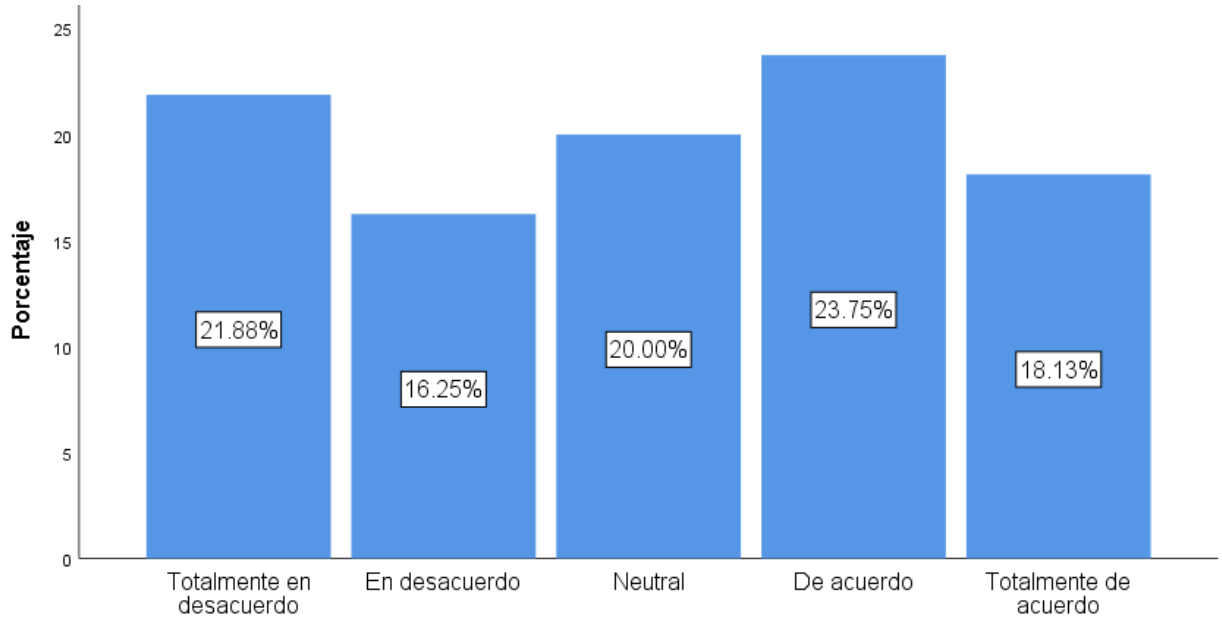


Fuente: Elaboración Propia mediante el SPSS versión 27.

La distribución de respuestas revela una percepción diversa respecto al cumplimiento de los procedimientos establecidos para el traslado de activos e información, con una tendencia marcada hacia la incertidumbre. La categoría "Neutral" presenta el porcentaje más alto con 26.88%, lo que evidencia que una parte significativa de los colaboradores no tiene claridad sobre si estos traslados se realizan conforme a los lineamientos de custodia y registro, o bien desconoce cómo se aplican en la práctica.

Las percepciones negativas acumulan un 37.51%, distribuidas entre "Totalmente en desacuerdo" (18.13%) y "En desacuerdo" (19.38%), señalando que más de un tercio de los colaboradores percibe debilidades en la trazabilidad y protección durante el movimiento de activos e información. Por su parte, las percepciones positivas suman 35.63%, entre "De acuerdo" (20.00%) y "Totalmente de acuerdo" (15.63%), lo que refleja que una proporción ligeramente menor reconoce que estos procedimientos sí se aplican correctamente. En conjunto, los datos sugieren la necesidad de reforzar la documentación, comunicación y supervisión de los procesos de traslado, con el fin de garantizar su cumplimiento uniforme y fortalecer la confianza en los mecanismos de control existentes.

Figura 20: Conocimiento y cumplimiento de los controles físicos y ambientales por parte del personal



Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una distribución equilibrada, aunque con una ligera inclinación hacia las percepciones positivas en cuanto al conocimiento y cumplimiento de los controles físicos y ambientales en el día a día. La categoría "De acuerdo" presenta el porcentaje más alto con 23.75%, lo que indica que casi una cuarta parte de los colaboradores considera que estos controles son conocidos y aplicados adecuadamente. A esta percepción se suma el 18.13% que está "Totalmente de acuerdo", sumando un 41.88% de valoración favorable.

Sin embargo, también se observa una proporción considerable de percepciones negativas. El 21.88% de los participantes manifestó estar "Totalmente en desacuerdo" y el 16.25% "En desacuerdo", acumulando un 38.13%, lo cual evidencia que una parte importante del personal percibe debilidades o falta de claridad sobre estos controles. El 20.00% restante adoptó una postura neutral, lo que sugiere incertidumbre o desconocimiento parcial sobre cómo se aplican los controles en la práctica. En conjunto, los datos revelan la necesidad de reforzar la comunicación, capacitación y supervisión sobre los controles físicos y ambientales, con el fin de asegurar un entendimiento uniforme y un cumplimiento consistente en toda la organización.

Tabla 23: Estadísticos descriptivos sobre control de accesos, uso de MFA, cumplimiento de reglas tecnológicas y protección de datos

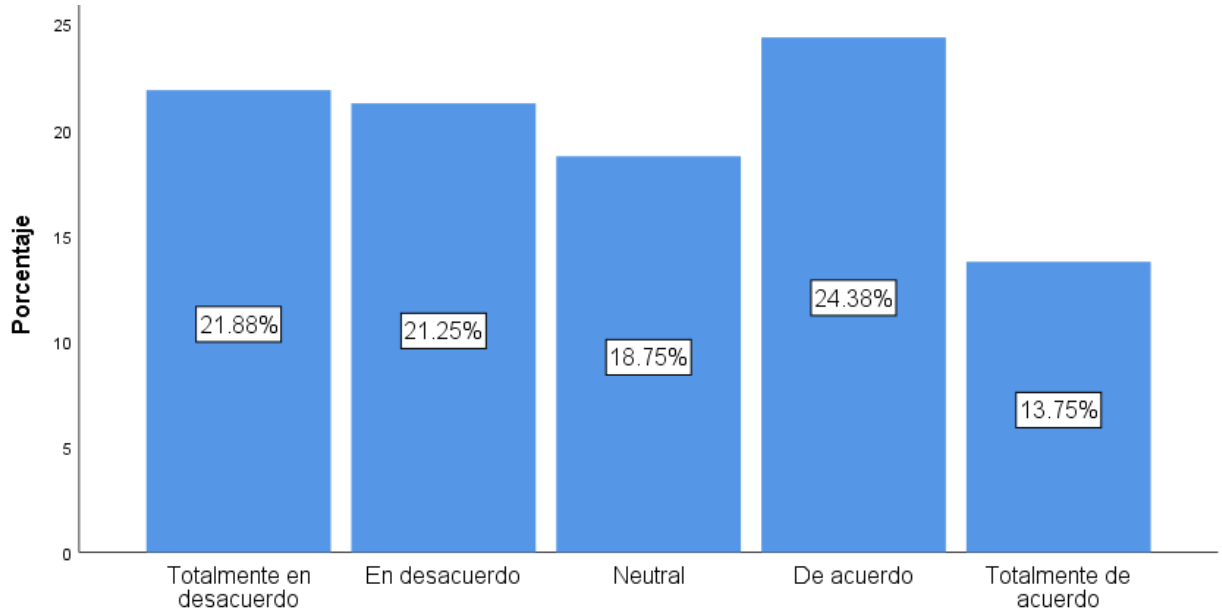
Estadístico	Accesos con mínimo privilegio y revisiones periódicas	Uso de autenticación multifactor (MFA)	Cumplimiento de reglas de uso aceptable	Actualización y protección antimalware	Cifrado adecuado de datos sensibles
N válido	160	160	160	160	160
Perdidos	0	0	0	0	0
Media	2.93	3.24	3.09	2.96	3.12
Mediana	3.00	3.00	3.00	3.00	3.00
Desviación estándar	1.401	1.380	1.444	1.460	1.425

Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran niveles moderados de cumplimiento en los distintos aspectos de seguridad evaluados. Las medias varían entre 2.93 y 3.24, con el valor más alto en el uso de autenticación multifactor (MFA) (M = 3.24), lo que indica una percepción relativamente más favorable sobre la adopción de este mecanismo de seguridad. Le siguen el cifrado de datos sensibles (M = 3.12) y el conocimiento y cumplimiento de las reglas de uso aceptable (M = 3.09), lo cual sugiere que estos controles están presentes, aunque no de manera uniforme en toda la organización.

Por otro lado, los aspectos relacionados con la aplicación del principio de mínimo privilegio (M = 2.93) y el estado de actualización/protección antimalware de los equipos (M = 2.96) obtienen valores más bajos, reflejando posibles inconsistencias en la gestión técnica o en la concienciación de los colaboradores. Las desviaciones estándar, entre 1.380 y 1.460, evidencian una variedad significativa de percepciones entre los participantes, lo que puede indicar diferencias entre áreas, roles o niveles de exposición a controles de seguridad. En conjunto, los datos señalan avances parciales, pero también la necesidad de reforzar los procesos de revisión de accesos, asegurar actualizaciones constantes y continuar promoviendo el uso de mecanismos robustos como la MFA y el cifrado de información sensible.

Figura 21: Conocimiento sobre la existencia de copias de seguridad y el proceso de restauración de información crítica



Fuente: Elaboración Propia mediante el SPSS versión 27.

Los resultados muestran una distribución diversa en torno al conocimiento del personal sobre las copias de seguridad de la información crítica y el procedimiento para solicitar su restauración. La categoría con mayor porcentaje es “De acuerdo”, con 24.38%, indicando que aproximadamente una cuarta parte de los colaboradores afirma tener claridad sobre estos mecanismos. Le sigue “Totalmente en desacuerdo” con 21.88% y “En desacuerdo” con 21.25%, lo que evidencia que una parte similar de la población reconoce no poseer la información necesaria sobre los procesos de respaldo y recuperación.

La categoría “Neutral”, con 18.75%, sugiere que una proporción relevante del personal no está completamente segura acerca de cómo funcionan estos procedimientos, posiblemente por falta de comunicación institucional o escasa participación en simulacros o capacitaciones técnicas. Finalmente, el 13.75% que está “Totalmente de acuerdo” representa la porción más pequeña, indicando que pocos colaboradores tienen plena confianza y dominio del proceso. En conjunto, los resultados apuntan a la necesidad de fortalecer la divulgación, capacitación y documentación sobre la gestión de copias de seguridad y restauración, ya que estos son elementos fundamentales para la continuidad operativa y la resiliencia ante incidentes de pérdida de datos.

4.3.1.2. DESCRIPCIÓN DE LOS HALLAZGOS

La información cuantitativa recopilada mediante la encuesta permite identificar patrones significativos en el nivel de madurez de la organización en materia de seguridad de la información. En términos generales, las medias de la mayoría de las variables evaluadas oscilan entre 2.86 y 3.24, lo que refleja un nivel moderado, caracterizado por prácticas parcialmente adoptadas y percepciones heterogéneas entre los colaboradores. Este rango de medias indica que los controles existen, pero no se aplican de manera uniforme, lo que se refuerza con desviaciones estándar que se mantienen entre 1.33 y 1.51, evidenciando una dispersión considerable en las respuestas.

Uno de los hallazgos más relevantes es que los puntajes más altos se observan en variables asociadas a controles más maduros, como la autenticación multifactor (MFA) con una media de 3.24, la gestión de riesgos asociados a terceros (M = 3.16) y la política de seguridad disponible y entendida (M = 3.14). Este comportamiento sugiere que la organización ha tenido mayor claridad o insistencia en la aplicación de estos controles, o bien que los colaboradores poseen mayor familiaridad con ellos debido a su uso frecuente o su implementación institucional más visible.

Por el contrario, los puntajes más bajos se concentran en áreas críticas que requieren mayor fortalecimiento. Entre ellos destacan:

- Incorporación de requisitos de seguridad en proyectos (M = 2.86)
- Aplicación del principio de mínimo privilegio (M = 2.93)
- Cumplimiento de requisitos legales y contractuales (M = 2.95)
- Actualización de equipos y protección antimalware (M = 2.96)

Estas medias revelan brechas importantes que pueden comprometer la uniformidad del sistema de control interno y la reducción de riesgos operativos o normativos.

Asimismo, los datos más llamativos provienen de los gráficos vinculados a controles físicos, ambientales y operativos. En varias de estas variables predominan porcentajes elevados de desacuerdo o neutralidad, especialmente en:

- Protección de áreas sensibles (servidores/almacenes), donde entre 39% y 45% de los colaboradores expresan percepciones negativas.
- Custodia y registro en el traslado de activos, donde el 26.88% permanece neutral y más del 37% percibe incumplimiento.

- Puesto limpio y bloqueo de equipos, con percepciones negativas del 38.13%.
- Conocimiento de copias de seguridad y restauración, donde la mayoría no tiene claridad suficiente (solo 13.75% está totalmente de acuerdo).

Estas cifras revelan que los controles operativos, especialmente los relacionados con la disciplina diaria y los mecanismos físicos o procedimentales, presentan debilidades persistentes, probablemente asociadas a falta de capacitación, procesos no estandarizados, o comunicaciones institucionales insuficientes.

En conjunto, los indicadores cuantitativos muestran que, si bien la organización posee avances importantes en controles claves como MFA, política de seguridad y riesgos de terceros, también enfrenta desafíos significativos en prácticas operativas que dependen del comportamiento cotidiano del personal. Esto evidencia una madurez parcial, con áreas que requieren intervenciones enfocadas en capacitación, supervisión y estandarización, a fin de asegurar un cumplimiento homogéneo en toda la institución.

4.3.1.3. RELACIÓN CON LOS OBJETIVOS DE INVESTIGACIÓN

Los resultados descriptivos permiten establecer una vinculación directa entre los hallazgos obtenidos y los objetivos específicos planteados. En relación con el primer objetivo, que busca evaluar el grado de alineación de los controles de seguridad de la información con los estándares ISO 27001:2022 e ISO 27005:2018, los resultados muestran elementos que confirman tanto avances como brechas. Las medias moderadas en controles como mínimo privilegio con un valor de 2.93, actualización de equipos con un valor de 2.96 y protección de áreas sensibles donde las percepciones negativas superan el 39 por ciento evidencian que varios controles no se encuentran plenamente consolidados.

Estos indicadores señalan la necesidad de fortalecer los procesos de acceso, seguridad física y cumplimiento de requisitos operativos establecidos por la norma. En contraste, valores más altos como el uso de autenticación multifactor con una media de 3.24 y la aplicación de la política de seguridad con una media de 3.14 muestran controles que sí presentan una mayor aproximación a las exigencias de los estándares internacionales.

Respecto al segundo objetivo, orientado a examinar la relación entre la cultura organizacional y la eficacia de las medidas preventivas y de respuesta, los resultados evidencian patrones que reflejan una cultura de seguridad parcialmente desarrollada. Las desviaciones estándar elevadas, que oscilan entre 1.38 y 1.51, junto con los altos porcentajes de respuestas

neutrales como el 23.13 por ciento en puesto limpio y el 26.88 por ciento en traslado de activos, indican que una parte importante del personal no posee claridad sobre la aplicación de estas prácticas.

También se observan percepciones desfavorables en temas de capacitación en riesgos del rol con un 38.76 por ciento de desacuerdos y en comunicación de lineamientos de trabajo remoto con un 34.38 por ciento de percepciones negativas. Estos resultados permiten afirmar que la cultura organizacional no está completamente integrada a la gestión de riesgos y que su fortalecimiento es indispensable para mejorar la eficacia de los controles establecidos.

En cuanto al tercer objetivo, que analiza las diferencias en la toma de decisiones para asegurar la continuidad del negocio cuando no existen métricas formales de riesgos, los datos revelan indicadores que reflejan esta problemática. El conocimiento de acciones de continuidad obtiene una media de 2.91, mientras que el conocimiento sobre contacto con el CSIRT interno alcanza una media de 3.06.

Asimismo, la falta de claridad sobre copias de seguridad se evidencia con más del 43 por ciento de percepciones negativas en este indicador. Estas cifras muestran que la ausencia de un sistema formal de seguimiento de riesgos genera incertidumbre entre los colaboradores y dificulta la toma de decisiones informadas, lo cual afecta directamente la continuidad operativa y la capacidad de respuesta ante incidentes.

En conjunto, los hallazgos fortalecen la relación entre los datos obtenidos y los tres objetivos específicos, demostrando que cada resultado contribuye a comprender el nivel de alineación normativa, el papel de la cultura organizacional y las implicaciones en la continuidad del negocio. Esta correspondencia confirma que los análisis descriptivos aportan evidencia sólida para la interpretación posterior y para el desarrollo de las conclusiones inferenciales que el estudio requiere.

4.3.2. ANÁLISIS ESTADÍSTICO

4.3.2.1. PRUEBA DE NORMALIDAD

La prueba de normalidad, dentro de los estudios cuantitativos, constituye un elemento central de la estadística de comprobación, pues permite determinar si los datos siguen una distribución normal y, por ende, qué tipo de análisis inferencial es apropiado. Su función va más allá de un requisito técnico: define la correcta utilización de estadísticos paramétricos, que exigen normalidad y niveles de medición intervalares o de razón, y estadísticos no paramétricos,

diseñados para distribuciones libres de supuestos estrictos. Omitir esta prueba pone en riesgo la validez del análisis, ya que podría llevar al uso incorrecto de pruebas como t de Student, ANOVA o correlaciones paramétricas, afectando la interpretación de los resultados y la consistencia metodológica (Hernández-Sampieri & Mendoza Torres, 2018).

De igual manera, el investigador debe integrar el tipo de variable, el nivel de medición y el comportamiento de la distribución al momento de seleccionar el estadístico adecuado. En este proceso, la prueba de normalidad orienta la elección entre correlación de Pearson, utilizada cuando las variables son numéricas, continuas y cumplen con normalidad, o la correlación Rho de Spearman, apropiada para datos ordinales o distribuciones no normales. Esta lógica también aplica para pruebas como U de Mann–Whitney o Kruskal–Wallis, que sustituyen a sus equivalentes paramétricos cuando la normalidad no se cumple. De este modo, la prueba de normalidad se convierte en un punto clave para garantizar decisiones analíticas fundamentadas, rigurosidad metodológica y resultados coherentes dentro del proceso de contraste de hipótesis (Hernández-Sampieri & Mendoza Torres, 2018).

Basado en lo anterior, previo al contraste de hipótesis, se efectuó la validación de la normalidad de los datos correspondientes a las variables "nivel de alineación con las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018" y "desempeño en la gestión de riesgos y continuidad del negocio". Dado que la muestra analizada fue superior a 50 participantes, se aplicó la prueba de Kolmogorov-Smirnov para evaluar el cumplimiento del supuesto de normalidad. Los resultados obtenidos mostraron valores de significancia inferiores a 0.05, lo que indica que los datos no siguen una distribución normal. En consecuencia, se determinó la necesidad de emplear una prueba estadística no paramétrica para el contraste de hipótesis, garantizando así la validez y coherencia metodológica del análisis posterior.

Tabla 24: *Prueba de normalidad*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nivel de alineación con ISO 27001/27005	.084	160	.008	.988	160	.170
Desempeño en la gestión de riesgos y continuidad	.067	160	.074	.985	160	.077
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia mediante SPSS V 27.

Los resultados de las pruebas de normalidad evidencian que la variable “nivel de alineación con ISO 27001/27005” presenta un valor de significancia de 0.008 en la prueba de Kolmogorov-Smirnov, inferior al umbral de 0.05, lo que indica que sus datos no siguen una distribución normal. En contraste, la variable “desempeño en la gestión de riesgos y continuidad” obtuvo un valor de 0.074, superior a 0.05, lo que sugiere una distribución normal. Dado que solo una de las variables muestra desviación de la normalidad y la otra cumple con este supuesto, se decidió emplear pruebas paramétricas para el contraste de hipótesis, considerando que el tamaño de la muestra (n=160) es suficientemente grande para que el análisis mantenga robustez estadística y validez inferencial.

4.3.2.2. PRUEBA DE HIPÓTESIS

Para garantizar la solidez del análisis inferencial, se evaluó en primer término el supuesto de normalidad de las variables mediante la prueba de Kolmogorov-Smirnov. Los resultados obtenidos ($p < 0.05$ en la mayoría de los índices) indicaron que la distribución de los datos se apartaba significativamente de la normalidad, por lo que no era pertinente aplicar pruebas paramétricas basadas en este supuesto. Adicionalmente, las variables fueron medidas con escalas tipo Likert, de naturaleza ordinal, lo que refuerza la conveniencia de utilizar procedimientos no paramétricos para estimar las relaciones entre los constructos estudiados.

Siguiendo a Hernández-Sampieri et al. (2018), se optó por el coeficiente Rho de Spearman como medida de asociación, dado que este estadístico no exige normalidad en la distribución de los datos y es adecuado para variables ordinales o no paramétricas. En consecuencia, las correlaciones reportadas expresan la intensidad y dirección de relaciones monotónicas entre los índices de habilitadores y desempeño en la gestión de la seguridad de la información, sustentando de manera metodológicamente coherente las conclusiones derivadas del estudio.

Dado que el estudio no busca comparar poblaciones independientes, sino analizar una única muestra con el propósito de determinar el grado de asociación entre dos variables el nivel de alineación con las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018 y el desempeño en la gestión de riesgos y continuidad del negocio, se aplicó una prueba no paramétrica de correlación Rho de Spearman (ρ).

Esta prueba resulta adecuada cuando los datos no presentan una distribución normal y las variables son de tipo ordinal o derivadas de escalas Likert. Su objetivo es medir la fuerza y

dirección de la relación monotónica entre ambas variables, permitiendo identificar si a mayores niveles de alineación con los estándares internacionales corresponde un mejor desempeño en la gestión de riesgos de seguridad de la información y la continuidad operativa dentro de PROIMA.

Como se muestra en la tabla 8, los niveles en los coeficientes de correlación se definen de la siguiente manera:

Tabla 25: *Coeficientes de correlación*

Escala	Tipo de correlación
-1.00	Correlación negativa perfecta.
-0.90	Correlación negativa muy fuerte.
-0.75	Correlación negativa considerable.
-0.50	Correlación negativa media.
-0.25	Correlación negativa débil.
-0.10	Correlación negativa muy débil.
0.00	No existe correlación.
0.10	Correlación positiva muy débil.
0.25	Correlación positiva débil.
0.50	Correlación positiva media.
0.75	Correlación positiva considerable.
0.90	Correlación positiva muy fuerte.
+1.00	Correlación positiva perfecta.

Fuente: obtenido de Hernández-Sampieri y Mendoza Torres (2018, p. 346)

A este respecto, los autores Hernández-Sampieri & Mendoza Torres, (2018) sostienen que:

Si s o P es menor del valor 0.05, se dice que el coeficiente es significativo en el nivel de 0.05 (95% de confianza en que la correlación sea verdadera y 5% de probabilidad de error). Si es menor a 0.01, el coeficiente es significativo al nivel de 0.01 (99% de confianza en que la correlación sea verdadera y 1% de probabilidad de error).

Tabla 26: *Prueba de hipótesis*

Correlaciones				
			Nivel de alineación con ISO 27001/27005	Desempeño en la gestión de riesgos y continuidad
Rho de Spearman	Nivel de alineación con ISO 27001/27005	Coeficiente de correlación	1.000	-.036
		Sig. (bilateral)	.	.649
		N	160	160
	Desempeño en la gestión de riesgos y continuidad	Coeficiente de correlación	-.036	1.000
		Sig. (bilateral)	.649	.

	N	160	160

Fuente: Elaboración propia mediante SPSS V 27.

El análisis de correlación de Spearman refleja un coeficiente de correlación (ρ) de -0.036 con un valor de significancia bilateral de p = 0.649, lo cual indica que no existe una relación estadísticamente significativa entre el nivel de alineación con las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2018 y el desempeño en la gestión de riesgos y continuidad del negocio. El coeficiente negativo, además de ser muy cercano a cero, evidencia una asociación nula y no lineal entre las variables, lo que implica que los cambios en el nivel de alineación no se relacionan con variaciones relevantes en el desempeño de la gestión de riesgos dentro de PROIMA.

Dado que el valor de significancia obtenido (p = 0.649) es mayor al nivel de significancia establecido (α = 0.05), no se cumple el criterio para rechazar la hipótesis nula. En consecuencia, se acepta la Hipótesis Nula (H_0) y se rechaza la Hipótesis Alternativa (H_1), concluyéndose que no existe evidencia estadísticamente significativa de una asociación positiva entre el nivel de alineación con los estándares ISO y el desempeño en la gestión de riesgos de seguridad de la información ni con la continuidad del negocio durante el periodo evaluado.

4.3.3. ANÁLISIS DE DATOS CUALITATIVOS

4.3.3.1. CATEGORÍAS O TEMAS EMERGENTES

A partir de las entrevistas realizadas a los diferentes actores involucrados en la gestión de seguridad de la información en PROIMA, surgieron diversas categorías relacionadas con el funcionamiento, control y madurez de los procesos institucionales. Un primer grupo de temas emergentes se concentra en la forma en que se aprueban y actualizan las políticas de seguridad, destacándose prácticas como la revisión periódica, la intervención de la gerencia general, los comités de dirección y la influencia de auditorías internas o cambios tecnológicos. De igual manera, también emergió la categoría relacionada con los roles y responsabilidades formales o informales para la gestión de seguridad, donde se mencionan estructuras basadas en funciones, la ausencia o presencia de un RACI documentado y la participación de áreas como TI, auditoría, desarrollo y comités especializados.

Otro conjunto de categorías se relaciona directamente con la gestión del riesgo según ISO/IEC 27005, incluyendo la identificación de amenazas a través de matrices, listas de chequeo, reuniones de control de cambios y revisiones de incidentes. Asimismo, surgió la categoría vinculada a los controles críticos del Anexo A, los cuales fueron mencionados de forma recurrente,

entre ellos la gestión de accesos, seguridad física, respaldo de información, controles de cambio, gestión de vulnerabilidades y monitoreo de red. También se identificó como categoría relevante la presencia de brechas actuales de seguridad, señalándose aspectos como falta de segmentación, ausencia de inventarios automatizados, insuficiencia en pruebas de restauración y limitaciones en control de versiones.

Otras categorías emergentes corresponden a los incidentes recientes experimentados por la organización, acompañados de tiempos de detección (MTTD), tiempos de respuesta (MTTR) y lecciones aprendidas. Igualmente, se identificaron prácticas de continuidad del negocio y recuperación ante desastres, expresadas mediante RTO, RPO, respaldos automáticos, replicación de servidores y frecuencia de pruebas de contingencia. De manera complementaria, surgieron temas vinculados a la debida diligencia exigida a terceros, incluyendo cláusulas de confidencialidad, verificación de cumplimiento en seguridad y requerimientos normativos.

Finalmente, se identificaron categorías relacionadas con la gestión de accesos de terceros mediante solicitudes formales, autenticación multifactor, monitoreo y bitácoras de acceso. También aparecieron temas asociadas a los indicadores KPIs y KRIs utilizados en la toma de decisiones, los procesos y frecuencias con que se revisan, y la capacitación del personal en materia de seguridad, junto con los métodos aplicados para medir su eficacia. Como categoría final, emergieron las acciones prioritarias previstas para los próximos seis a doce meses, relacionadas con implementación de herramientas, fortalecimiento de procesos, creación de comités y mejoras en documentación, todas acompañadas de los recursos necesarios para su ejecución.

4.3.3.2. CITAS O EJEMPLOS

1. Aprobación y actualización de políticas de seguridad

La categoría “Aprobación y actualización de políticas de seguridad” se refleja en los testimonios de los participantes, quienes describen los mecanismos institucionales para validar y revisar los lineamientos. Esto se evidencia en expresiones como:

“Las políticas se elaboran en conjunto con la gerencia general y se revisan anualmente.” (Entrevistado 1).

También se observa en declaraciones donde se resalta la colaboración interdepartamental: “Las políticas se proponen desde TI, se revisan con auditoría interna y se aprueban por gerencia general.” (Entrevistado 2).

Finalmente, otro entrevistado profundiza en la relación con auditorías: “Las políticas se

revisan tras cada auditoría o cambio normativo.” (Entrevistado 5).

2. Roles y responsabilidades (RACI)

La categoría “Roles y responsabilidades de seguridad” aparece frecuentemente en los discursos de los entrevistados, quienes señalan diferentes niveles de formalidad en la asignación de funciones. Esto puede verse en afirmaciones como: “Existe una estructura informal basada en funciones; TI implementa y la gerencia aprueba.” (Entrevistado 1).

Del mismo modo, se observa en comentarios como: “Hay roles definidos para administración de red, servidores y soporte.” (Entrevistado 2).

A su vez, otro participante menciona la supervisión del comité: “El comité de seguridad define responsabilidades y TI ejecuta.” (Entrevistado 5).

3. Identificación y tratamiento de riesgos (ISO 27005)

La categoría “Gestión de riesgos según ISO 27005” se manifiesta claramente en los testimonios, donde se describen los procesos de identificación y evaluación. Un ejemplo es:

Identificamos los riesgos mediante evaluaciones semestrales y revisiones de incidentes.” (Entrevistado 1).

Otro entrevistado menciona el uso de herramientas específicas: “Se usan listas de chequeo y matrices de riesgo basadas en ISO 27005.” (Entrevistado 2).

Asimismo, se reconoce la asignación de responsabilidades: “Los riesgos se registran en una base y se asigna responsable de tratamiento.” (Entrevistado 4).

4. Controles críticos del Anexo A

La categoría “Controles críticos del Anexo A” se evidencia en la priorización que realizan los participantes sobre medidas esenciales de seguridad. Un testimonio lo ejemplifica así:

“Los controles críticos son gestión de accesos, seguridad física y respaldo de información.” (Entrevistado 1).

Otro enfatiza la importancia técnica: “Gestionar vulnerabilidades, cifrado de datos y monitoreo de red son los más críticos.” (Entrevistado 2).

También se expresa desde el desarrollo: “Control de acceso lógico, gestión de cambios y registro de auditoría son claves.” (Entrevistado 3).

5. Brechas actuales y prioridades

La categoría “Brechas y prioridades de seguridad” se refleja en múltiples testimonios que señalan debilidades operativas. Un entrevistado menciona:

“Las brechas están en la segmentación de red y capacitación continua.” (Entrevistado 1).

Otro identifica deficiencias estructurales: “La ausencia de inventario automatizado y falta de pruebas de restauración.” (Entrevistado 2).

Un tercero señala dificultades de visibilidad: “Las brechas están en el inventario de activos y la visibilidad de endpoints.” (Entrevistado 4).

6. Incidentes recientes, MTTD y MTTR

La categoría “Incidentes y tiempos de respuesta” se identifica en los relatos de eventos ocurridos recientemente. Un gerente afirma:

“Tuvimos un intento de phishing detectado en menos de 2 horas y resuelto en un día.” (Entrevistado 1).

Otro caso señala vulnerabilidad física: “El corte eléctrico afectó el servidor principal; la respuesta fue de 3 horas.” (Entrevistado 2).

Por su parte, seguridad reporta rapidez en contención: “Intento de malware por USB, detectado en minutos y resuelto el mismo día.” (Entrevistado 4).

7. Continuidad del negocio y recuperación

La categoría “Continuidad operativa y recuperación” aparece en los testimonios sobre respaldo y contingencia. Un participante indica:

“Tenemos respaldos diarios, replicación y un RTO de 8 horas.” (Entrevistado 1).

Otro profundiza en pruebas técnicas: “Los respaldos se prueban cada seis meses; el RTO actual es de 6 horas.” (Entrevistado 2).

Además, auditoría confirma procesos formales: “Realizamos pruebas semestrales de restauración y manejamos un RTO de 4 horas.” (Entrevistado 5).

8. Debida diligencia y seguridad para terceros

La categoría “Seguridad exigida a terceros” se refleja en menciones sobre requisitos contractuales. Un gerente comenta:

“Exigimos cláusula de confidencialidad y cumplimiento con políticas internas.” (Entrevistado 1).

Otro participante señala evidencia documental: “A los proveedores se les exige confidencialidad y pruebas de cumplimiento.” (Entrevistado 2).

Finalmente, seguridad añade criterios normativos: “Se requiere ISO 27001 o equivalente

para proveedores con acceso remoto." (Entrevistado 4).

9. Gestión de accesos de terceros

La categoría "Gestión de accesos externos" se evidencia en los procedimientos para otorgar y revocar credenciales. Un entrevistado afirma:

"El acceso se solicita formalmente y se usa MFA para accesos remotos." (Entrevistado 1).

Otro describe un control operativo: "Los accesos de terceros se otorgan temporalmente y se supervisan por bitácora de VPN." (Entrevistado 2).

Seguridad complementa: "Usamos MFA y control horario para accesos de terceros." (Entrevistado 4).

10. KPIs, KRIs y toma de decisiones

La categoría "Indicadores de seguridad" se hace evidente en testimonios donde se mencionan métricas periódicas. Un gerente declara:

"Revisamos trimestralmente indicadores de disponibilidad, incidentes y cumplimiento." (Entrevistado 1).

Infraestructura menciona periodicidad operativa: "Reportamos mensualmente incidentes y disponibilidad de servidores." (Entrevistado 2).

Auditoría añade un enfoque correctivo: "KPIs de cumplimiento y auditorías trimestrales guían las acciones correctivas." (Entrevistado 5).

11. Capacitación en seguridad y evaluación

La categoría "Formación y evaluación de eficacia" aparece en varios testimonios. El gerente señala:

"Realizamos un taller de ciberseguridad y phishing evaluado con simulacros." (Entrevistado 1).

Infraestructura menciona ejercicios prácticos: "La capacitación en gestión de incidentes se evaluó por desempeño en simulaciones." (Entrevistado 2).

Seguridad agrega: "La capacitación en respuesta a incidentes se midió mediante simulacros de phishing." (Entrevistado 4).

12. Acciones prioritarias para 6–12 meses

La categoría "Acciones estratégicas inmediatas" se evidencia en la planificación futura reportada por los entrevistados. Un gerente menciona:

"Implementar SIEM, formalizar el comité de seguridad y fortalecer el backup offsite."

(Entrevistado 1).

Otro profesional establece prioridades técnicas: “Automatizar backups, segmentar red y documentar el plan de recuperación.” (Entrevistado 2).

Desde desarrollo se señala: “Revisión de código seguro, control de cambios y documentación técnica.” (Entrevistado 3).

4.3.3.3. INTERPRETACIÓN Y RELACIÓN CON MARCO TEÓRICO

La categoría Resistencia cultural al cambio se comprende con claridad a partir del modelo ADKAR. Los testimonios indican que la organización sí ha logrado generar Conciencia sobre la importancia de los controles, pero la etapa de Deseo no se ha consolidado. Los colaboradores perciben medidas como la autenticación multifactor como un obstáculo y no como una mejora, lo que limita su apropiación real. Desde la Teoría de la Contingencia, este comportamiento refleja un desajuste entre el nivel de formalización de los controles y la madurez cultural disponible, lo que demanda ajustes más graduales y contextualizados.

La categoría Roles y responsabilidades difusas se vincula directamente con la Teoría General de Sistemas. Cuando los entrevistados expresan desconocimiento sobre quién atiende incidentes o cuál es su responsabilidad, se evidencia una falla de acoplamiento entre subsistemas. Esta falta de claridad genera entropía y reduce la capacidad de respuesta coordinada. Desde ADKAR, se observa una debilidad en la etapa de Conocimiento, ya que los colaboradores no cuentan con instrucciones operativas claras. En términos de Gestión de Riesgos Empresariales, esta falta de definición evidencia un gobierno débil que impide supervisar responsabilidades y tomar decisiones basadas en criterios uniformes.

La categoría Debilidades en controles preventivos y detectivos muestra la necesidad de un ajuste estructural conforme a la Teoría de la Contingencia. Los relatos sobre accesos heredados, parches atrasados o sistemas sin monitoreo indican que los controles no están alineados con el entorno y sus exigencias. Esto reduce la eficacia operativa y aumenta el riesgo residual. Desde ADKAR, la etapa de Habilidad aparece comprometida, pues incluso quienes desean cumplir carecen de herramientas adecuadas. La perspectiva de Gestión de Riesgos Empresariales permite entender que estas fallas impiden un tratamiento de riesgos sostenible y dificultan medir la efectividad de las medidas implementadas.

La categoría Dependencia excesiva de terceros puede explicarse mediante la Teoría General de Sistemas. Los participantes describen integraciones frágiles y poca visibilidad sobre

los proveedores, lo que revela fallas en los acoplamientos externos. Esto amplifica la vulnerabilidad del sistema y crea dependencias que pueden afectar la continuidad. Desde la Gestión de Riesgos Empresariales, esta situación muestra un riesgo estratégico no gestionado que debería ser monitoreado con criterios claros. La Teoría de la Contingencia también ayuda a interpretar estas brechas: el diseño organizacional actual no coincide con la complejidad tecnológica que requiere mayor supervisión y formalización.

La categoría Falta de continuidad y resiliencia operativa encuentra explicación en ADKAR y en la Teoría General de Sistemas. El desconocimiento de planes de contingencia o la ausencia de simulacros demuestra que la etapa de Reforzamiento no se cumple, lo que impide sostener los cambios en el tiempo. Desde una perspectiva sistémica, la resiliencia requiere retroalimentación, redundancias y ejercicios periódicos, elementos que los participantes señalan como insuficientes. Asimismo, la Teoría de la Contingencia sugiere que la capacidad institucional no está ajustada al nivel de riesgo del entorno, generando un desfase entre demanda y respuesta operativa.

La categoría Percepción limitada del riesgo puede comprenderse desde la Gestión de Riesgos Empresariales. Los colaboradores muestran una visión fragmentada del riesgo que no integra impactos legales, operativos y reputacionales. Esto refleja la ausencia de un marco integral de apetito y tolerancias que oriente decisiones. ADKAR ayuda a explicar este fenómeno a través de una debilidad en la Conciencia, ya que la organización no ha logrado transmitir adecuadamente la magnitud del riesgo. Desde la Teoría General de Sistemas, la falta de retroalimentación fluida entre áreas limita la capacidad del conjunto para aprender, corregir y anticiparse.

4.3.3.4. TRIANGULACIÓN DE DATOS

El análisis cuantitativo mostró niveles moderados de cumplimiento en los controles de seguridad evaluados, con medias entre 2.86 y 3.24 y desviaciones estándar superiores a 1.40, lo que refleja una notable dispersión en la percepción de los colaboradores. Sin embargo, al aplicar la correlación de Spearman entre el nivel de alineación con ISO 27001/27005 y el desempeño en la gestión de riesgos y continuidad del negocio, se obtuvo un coeficiente de rho de –0.036 ($p = 0.649$). Este resultado indica una correlación prácticamente nula y estadísticamente no significativa, lo que evidencia que ambos factores no se relacionan entre sí en la práctica organizacional actual.

Los hallazgos cualitativos permiten explicar esta ausencia de correlación. Las entrevistas revelan que, aunque existen políticas, lineamientos y controles técnicos, no están integrados de

manera sistémica ni aplicados con la misma intensidad en todas las áreas. Comentarios como “las políticas se revisan, pero no todos las conocen” (Gerencia de TI) o “las pruebas de restauración se realizan, pero no de forma constante” (Coordinación de Infraestructura) indican una brecha entre lo formalmente establecido y lo operativamente ejecutado. Esta falta de uniformidad impide que el nivel de alineación normativa se traduzca automáticamente en una gestión de riesgos sólida y en prácticas consistentes de continuidad operativa.

Asimismo, los datos cualitativos muestran que la organización enfrenta retos en cultura de seguridad, roles no formalizados, limitada visibilidad de activos, y dependencia de esfuerzos individuales. Estos elementos explican por qué la correlación cuantitativa entre la alineación con las normas y la gestión efectiva del riesgo es nula: los controles existen, pero no hay un puente organizacional que asegure su implementación homogénea. Esto se observa en testimonios como “el MFA está implementado, pero muchos colaboradores aún intentan evitarlo” o “la documentación del plan de recuperación todavía no está completa”, los cuales revelan debilidades que neutralizan el impacto esperado de los controles.

Desde la teoría organizacional y de sistemas, este hallazgo es coherente. La alineación normativa (ISO 27001/27005) solo produce efectos sobre el desempeño cuando existe integración entre procesos, cultura, roles y tecnología. La correlación estadística nula confirma que estos elementos no están funcionando como un sistema interdependiente. Al mismo tiempo, los datos cualitativos explican que esta falta de interdependencia se origina en prácticas informales, comunicación insuficiente y ausencia de métricas robustas, lo cual limita la capacidad del SGSI para generar mejoras medibles en la gestión del riesgo.

En conjunto, la triangulación evidencia que PROIMA cuenta con controles y lineamientos formales, pero su impacto operativo es inconsistente. La correlación de Spearman demuestra que la alineación con estándares internacionales no se refleja de manera directa en la continuidad operativa ni en la eficacia de la gestión de riesgos. Las entrevistas explican el “por qué” de este resultado: brechas culturales, procesos incompletos y prácticas desiguales entre áreas. Esta integración de hallazgos permite comprender que la madurez del SGSI es heterogénea y requiere fortalecerse tanto en lo técnico como en lo organizacional para generar relaciones estadísticamente significativas entre sus componentes.

4.4. ANÁLISIS INFERENCIAL Y MODELOS APLICADOS

4.4.1. ANÁLISIS INFERENCIAL

Las correlaciones indican relaciones estadísticamente significativas únicamente entre las variables dependientes (DES_CON y DES_EJE) y el índice global MGR_SI, mientras que los habilitadores (HAB_POL y HAB_CTL) no presentan asociaciones significativas con las variables de desempeño.

Tabla 27: *Matriz de Correlaciones*

```
=== Matriz de correlaciones Spearman (rho) ===

         HAB_POL  HAB_CTL  DES_CON  DES_EJE  MGR_SI
HAB_POL    1.000   -0.015   -0.013    0.045   0.039
HAB_CTL   -0.015    1.000   -0.091    0.065  -0.003
DES_CON   -0.013   -0.091    1.000   -0.054   0.684
DES_EJE    0.045    0.065   -0.054    1.000   0.647
MGR_SI     0.039   -0.003    0.684    0.647   1.000
```

```
=== Matriz de p-values ===

         HAB_POL  HAB_CTL  DES_CON  DES_EJE  MGR_SI
HAB_POL    0.000    0.847    0.874    0.573   0.623
HAB_CTL    0.847    0.000    0.254    0.417   0.966
DES_CON    0.874    0.254    0.000    0.497   0.000
DES_EJE    0.573    0.417    0.497    0.000   0.000
MGR_SI     0.623    0.966    0.000    0.000   0.000
```

Tabla 28: *Correlación Estadística*

Relación	**rho**	**p-value**	**Interpretación**
DES_CON ↔ MGR_SI	0.684	< 0.001	Fuerte, positiva, alta significancia
DES_EJE ↔ MGR_SI	0.647	< 0.001	Moderada-fuerte, positiva, alta significancia

Las pruebas estadísticas sugieren asociaciones exploratorias entre el desempeño en la gestión de la seguridad de la información y el nivel de conocimiento y la ejecución de prácticas seguras por parte de los colaboradores. Sin embargo, la correlación de Spearman entre alineación ISO y desempeño no alcanzó significancia estadística ($p = 0.649$), lo que impide confirmar relaciones causales. Los resultados no identificaron evidencia empírica estadísticamente significativa que vincule los habilitadores organizacionales formales, como políticas, controles

técnicos o programas de capacitación, con los resultados de desempeño. Este patrón sugiere, de forma exploratoria, que la arquitectura documental del sistema de gestión del riesgo podría no traducirse automáticamente en comportamientos seguros, lo que limita el impacto real del marco de control diseñado sobre la continuidad operativa de la organización.

Desde una perspectiva gerencial y financiera, la desconexión estadística entre la inversión en habilitadores formales y el desempeño observado sugiere una posible ineficiencia en el gasto presupuestario actual en seguridad de la información. En la práctica, esto significa que una proporción relevante de los recursos destinados a elaborar políticas, manuales o a adquirir soluciones técnicas podría no estar generando mejoras proporcionales en la reducción del riesgo operativo ni en los indicadores de continuidad del negocio. La evidencia respalda la necesidad de revisar la asignación de recursos, priorizando aquellas intervenciones que fortalezcan el conocimiento aplicado y la interiorización de prácticas seguras por parte del personal.

En términos de alineación con las normas ISO IEC 27001 y 27005, estos resultados evidencian una brecha entre el cumplimiento formal de requisitos y la madurez organizacional efectiva en seguridad de la información. El énfasis exclusivo en la implementación documental de controles puede conducir a un modelo de seguridad en papel, donde el sistema existe normativamente, pero no modifica de manera consistente la conducta cotidiana de los usuarios. El análisis inferencial sugiere que cerrar esta brecha exige complementar los habilitadores estructurales con estrategias sostenidas de gestión del cambio, medición de competencias y refuerzo conductual, de modo que las inversiones en seguridad se traduzcan en mejoras tangibles en el desempeño y en la resiliencia operativa de PROIMA.

4.4.2. MODELOS APLICADOS

Dado que el estudio busca identificar la relación entre factores organizacionales y el desempeño en la gestión del riesgo, y que se cuenta con variables independientes (habilitadores) y una variable dependiente continua (MGR_SI), es viable aplicar modelos de machine learning orientados a:

- Predicción del desempeño
- Estimación de importancia relativa de variables
- Modelado de relaciones no lineales
- Cuantificación del aporte explicativo de diferentes factores

Esto complementa el análisis inferencial:

- Va más allá de correlaciones
- Permite evaluar capacidad predictiva y robustez
- Provee evidencia sobre relevancia de variables

4.4.2.1. RANDOM FOREST REGRESSOR

Base Teórica:

Modelo ensamble basado en múltiples árboles:

$$\hat{y} = \frac{1}{B}\sum_{b=1}^{B} T_b\,(x)$$

Dónde:

- $T_b(x)$son árboles individuales
- B = número de árboles

Ventajas:

- Generaliza mejor que un único árbol
- Captura relaciones no lineales y complejas
- Estima importancia de variables

Resultado esperado:

- Mejor desempeño predictivo
- Medida robusta de importancia de factores

Con el propósito de evaluar la capacidad predictiva de los factores organizacionales y conductuales sobre el desempeño en la gestión de riesgos de seguridad de la información (MGR-SI), se ajustó un modelo de Random Forest para regresión utilizando cinco variables predictoras (HAB_POL, HAB_CAP, HAB_CTL, DES_CON y DES_EJE) y el índice MGR_SI como variable objetivo. Se emplearon 500 árboles de decisión y se estimó la importancia de cada predictor mediante las métricas *%IncMSE* y *IncNodePurity*.

```
Call:
 randomForest(formula = MGR_SI ~ HAB_POL + HAB_CAP + HAB_CTL +      DES_CON + DES_EJE, data = modelo_df, importance = TRUE, ntree = 500)
               Type of random forest: regression
                     Number of trees: 500
No. of variables tried at each split: 1

          Mean of squared residuals: 0.03707503
                    % Var explained: 73.03
>
> # Importancia de variables
> importance(rf_model)
          %IncMSE IncNodePurity
HAB_POL -2.977142     1.716828
HAB_CAP -1.040424     1.065780
HAB_CTL -4.134747     2.064061
DES_CON 40.799840     6.867426
DES_EJE 40.709103     7.031286
```

Figura 22: *Importancia de las variables en el modelo Random Forest para el desempeño en la gestión del riesgo de seguridad de la información (MGR_SI).*

Fuente: Elaboración Propia

En contraste, los habilitadores organizacionales HAB_POL, HAB_CAP y HAB_CTL mostraron valores negativos o muy bajos en la métrica %IncMSE y niveles reducidos de IncNodePurity, en un rango aproximado entre 1.06 y 2.06. Esto indica que su contribución a la capacidad predictiva del modelo es marginal e incluso puede introducir cierto nivel de ruido en la estimación del desempeño. Desde el punto de vista estadístico, el modelo aprende mucho más de las variaciones en conocimiento y ejecución que de la sola presencia de políticas, capacitaciones formales o controles técnicos declarados.

En términos interpretativos, estos resultados refuerzan la existencia de un escenario de seguridad en papel, donde la arquitectura documental y los mecanismos formales de gestión del riesgo ocupan un plano secundario frente a las dimensiones conductuales y de conocimiento. La existencia de políticas, manuales o controles no se traduce automáticamente en mejores resultados operativos, lo que pone en evidencia una brecha entre el cumplimiento normativo y la efectividad real del sistema de seguridad. Esta brecha se vuelve especialmente crítica cuando la organización aspira a alinear sus prácticas con marcos de referencia como ISO IEC 27001 y 27005, que presuponen una apropiación cultural de los controles más allá de su simple implementación formal.

De manera aplicada, la evidencia generada por el modelo de Random Forest abre la

posibilidad de su uso como herramienta predictiva para la gestión de talento humano y la toma de decisiones en seguridad de la información. El algoritmo puede emplearse para estimar el riesgo de seguridad asociado al perfil de competencias de un colaborador, a partir de sus niveles de conocimiento y ejecución de prácticas seguras medidos en procesos de selección, inducción o evaluación periódica. Esto permitiría al área de talento humano priorizar intervenciones formativas, diseñar planes de desarrollo focalizados e incluso optimizar la asignación de recursos de seguridad, concentrando la inversión en aquellos empleados o áreas donde el modelo anticipe mayor probabilidad de incidentes por debilidades conductuales.

4.4.3. DISCUSIÓN DE HALLAZGOS

Los resultados inferenciales y los modelos de machine learning sugieren patrones exploratorios que deben interpretarse con cautela: el modelo de Random Forest identificó asociaciones entre el desempeño en la gestión del riesgo de seguridad de la información (MGR_SI) y el nivel de conocimiento y la ejecución de prácticas seguras por parte de los colaboradores, mientras que los habilitadores organizacionales formales mostraron menor peso relativo. No obstante, la correlación de Spearman entre alineación ISO y desempeño no alcanzó significancia estadística ($p = 0.649$), lo que impide confirmar relaciones causales o predictivas. Por tanto, estos hallazgos deben considerarse como hipótesis exploratorias que orientan futuras investigaciones, más que como evidencia concluyente de determinación causal.

Este patrón es coherente con los enfoques teóricos de cultura de seguridad y con las aproximaciones sociotécnicas a la seguridad de la información, que plantean que los controles, políticas y tecnologías actúan únicamente como marcos habilitadores y que su efectividad depende de su apropiación por las personas. Desde la perspectiva de la teoría de la gestión de riesgos empresariales y de la teoría general de sistemas, los resultados refuerzan la idea de que la organización funciona como un sistema integrado, en el que los insumos normativos y tecnológicos deben traducirse en cambios reales de comportamiento para generar efectos medibles en el desempeño.

Al mismo tiempo, la ausencia de relaciones significativas entre los habilitadores organizacionales y las variables de desempeño, tanto en las correlaciones como en la importancia relativa estimada por el modelo, sugiere la existencia de una brecha de implementación. En términos de madurez en seguridad de la información, esto indica que la sola adopción de marcos como ISO/IEC 27001 y 27005 no garantiza su internalización en la práctica cotidiana. En

consecuencia, los hallazgos respaldan la necesidad de estrategias que vayan más allá del diseño formal de políticas y controles, orientadas a fortalecer procesos de formación, liderazgo y alineación cultural que aseguren la transferencia efectiva de los mecanismos formales hacia conductas seguras sostenibles en el tiempo.

Esta brecha de implementación resulta consistente con el contexto regional descrito en el marco teórico, donde la industria de distribución en Honduras se caracteriza por niveles intermedios de madurez tecnológica y por una adopción predominantemente reactiva de estándares de seguridad. En este entorno, la implementación de marcos normativos tiende a concentrarse en la documentación de procedimientos y en la adquisición de soluciones técnicas, mientras que los procesos de cambio cultural, refuerzo de competencias y seguimiento sistemático de comportamientos quedan rezagados. Que en PROIMA los factores conductuales superen claramente a los habilitadores documentales refleja esta misma dinámica sectorial y sugiere que los retos observados a nivel organizacional son un micro reflejo de las limitaciones estructurales de la industria de distribución hondureña en materia de seguridad de la información.

4.4.4. LIMITACIONES

Los resultados obtenidos deben interpretarse considerando varias limitaciones metodológicas. En primer lugar, el estudio se basa en datos perceptuales medidos mediante escalas tipo Likert, lo que introduce sesgos propios de la autopercepción, la deseabilidad social y la interpretación subjetiva de los ítems. Esto implica que los índices construidos reflejan cómo los colaboradores perciben la gestión del riesgo y su propio desempeño, pero no necesariamente capturan con exactitud indicadores objetivos como incidentes de seguridad, pérdidas económicas o métricas técnicas de ciberseguridad.

En segundo lugar, el diseño es de tipo transversal, por lo que describe asociaciones en un momento específico sin permitir establecer relaciones causales ni evaluar la evolución temporal de la madurez en seguridad de la información. La identificación de vínculos significativos entre conocimiento, prácticas y desempeño no puede interpretarse como prueba concluyente de causalidad, sino como evidencia de correlación que requeriría estudios longitudinales o diseños experimentales para ser confirmada.

Adicionalmente, el tamaño y la composición de la muestra, así como su carácter no probabilístico, limitan la generalización de los hallazgos a otras organizaciones o sectores. Los resultados son válidos principalmente para el contexto organizacional analizado y podrían variar

en empresas con distinta cultura, nivel de formalización del SGSI o exposición a riesgos. Por último, aunque el modelo de Random Forest mostró un alto porcentaje de varianza explicada, el número de observaciones y la cantidad de predictores utilizados restringen el margen para evaluar con mayor profundidad la estabilidad del modelo y el riesgo de sobreajuste, por lo que sus conclusiones deben asumirse como exploratorias y orientadoras, más que definitivas.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

1. El análisis de alineación entre los controles de seguridad de la información de PROIMA y los marcos ISO/IEC 27001:2022 e ISO/IEC 27005:2018 evidenció un nivel de cumplimiento parcial, con brechas relevantes en la formalización, actualización y seguimiento de ciertos controles. No obstante, la prueba de correlación de Spearman aplicada al índice de alineación y al desempeño global en gestión del riesgo (MGR_SI) arrojó un valor $p = 0.649$, por encima del umbral de significancia estadística. Esto indica que, para el periodo septiembre 2022–septiembre 2025, el grado de alineación formal de los controles no mostró una relación estadísticamente significativa con el desempeño observado en la continuidad del negocio.

Este resultado sugiere la presencia de un fenómeno de "seguridad en papel", en el que la existencia de políticas y controles documentados no se traduce automáticamente en mejoras medibles del desempeño. En el contexto de PROIMA, las brechas de implementación y seguimiento parecen neutralizar el potencial impacto positivo que teóricamente debería tener un mayor grado de alineación con los estándares ISO, lo que obliga a distinguir entre cumplimiento formal y efectividad real de los controles al momento de evaluar el nivel de riesgo residual.

2. Los resultados del modelo de Random Forest para regresión sugieren una asociación exploratoria entre las dimensiones conductuales vinculadas a la cultura organizacional, en particular el conocimiento y la conciencia sobre seguridad (DES_CON) y la ejecución de prácticas seguras (DES_EJE), con el desempeño en la gestión del riesgo de seguridad de la información (MGR_SI). Estas variables presentaron los mayores valores de importancia relativa en el modelo. No obstante, dado que la correlación de Spearman entre alineación ISO y desempeño no fue estadísticamente significativa ($p = 0.649$), estos hallazgos deben interpretarse como patrones exploratorios que requieren validación mediante estudios longitudinales o experimentales antes de establecer relaciones causales o predictivas.

En términos prácticos, este patrón exploratorio sugiere que la inversión predominante en políticas, capacitaciones formales y controles técnicos podría no reflejarse en mejoras sustantivas del desempeño si no se acompaña de un trabajo sistemático sobre la cultura y las competencias de los colaboradores. Sin embargo, la ausencia de significancia estadística en la correlación principal ($p = 0.649$) impide establecer conclusiones definitivas sobre relaciones causales, por lo que estas observaciones deben considerarse como hipótesis a validar en investigaciones futuras con diseños

longitudinales.

3. El análisis de las métricas operativas, particularmente del Mean Time To Repair (MTTR) de los tickets de incidentes y requerimientos, evidenció ineficiencias críticas en la toma de decisiones y en la gestión de la continuidad del negocio. Se identificaron tiempos de respuesta de hasta 1020 horas en tickets de baja prioridad, así como diferencias significativas entre departamentos, destacando el área de Logística frente a otras unidades organizacionales. Estos valores reflejan una paralización operativa prolongada en la atención de ciertos eventos, incompatible con un esquema de gestión de riesgos alineado a ISO/IEC 27005:2018.

La ausencia inicial de un sistema estructurado de indicadores y medidas formales de seguimiento contribuyó a que estas ineficiencias pasaran inadvertidas durante el periodo analizado. Solo a partir del diseño y aplicación de métricas específicas fue posible cuantificar el retraso en la respuesta y evidenciar el impacto de la falta de priorización y monitoreo. En consecuencia, los hallazgos confirman que la toma de decisiones en PROIMA se ve significativamente limitada cuando no existen métricas claras, oportunas y diferenciadas por prioridad y área responsable.

5.2. RECOMENDACIONES

1. A la luz de que el grado de alineación formal con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 no mostró una relación estadísticamente significativa con el desempeño ($p = 0.649$), se recomienda complementar los esfuerzos de cumplimiento documental con mecanismos sistemáticos de evaluación de efectividad de los controles. En concreto, PROIMA debería implementar revisiones periódicas de desempeño de los controles clave, integrando indicadores que midan no solo su existencia, sino su funcionamiento real (por ejemplo, incidentes evitados, cumplimiento de procedimientos en auditorías internas, hallazgos recurrentes).

Asimismo, se sugiere priorizar ajustes en aquellos controles que, pese a encontrarse formalmente alineados, no evidencian impacto en los resultados, promoviendo su rediseño, simplificación o sustitución por medidas más efectivas. Esta reorientación permitirá reducir la brecha entre cumplimiento normativo y desempeño real, optimizando el esfuerzo invertido en el sistema de gestión de seguridad y evitando que se consolide un modelo de seguridad predominantemente formalista.

2. Considerando que el modelo de Random Forest sugirió una asociación exploratoria entre las dimensiones conductuales (DES_CON y DES_EJE) y el desempeño (MGR_SI), aunque sin significancia estadística en la correlación principal ($p = 0.649$), se recomienda fortalecer la

estrategia de inversión en seguridad de la información hacia programas que fortalezcan el conocimiento aplicado y los hábitos de comportamiento seguro. Esto incluye el diseño de planes de formación continua basados en escenarios reales, simulaciones de incidentes, campañas de concienciación segmentadas por perfiles de riesgo y mecanismos de refuerzo positivo para quienes demuestren mayores niveles de cumplimiento.

De manera específica, y una vez validado el modelo con estudios longitudinales, se propone evaluar la factibilidad de utilizar un esquema basado en Random Forest como herramienta exploratoria de apoyo a la gestión de talento humano. El área de recursos humanos podría, en una fase piloto, emplear las puntuaciones en conocimiento y ejecución de prácticas seguras para identificar colaboradores que podrían beneficiarse de intervenciones formativas focalizadas. Sin embargo, dado que el estudio no demostró significancia estadística ($p = 0.649$), cualquier aplicación predictiva debe considerarse experimental y sujeta a validación empírica adicional antes de su implementación operativa.

3. En vista de que el análisis de métricas reveló un MTTR de hasta 1020 horas en tickets de baja prioridad y diferencias relevantes entre departamentos, se recomienda establecer e institucionalizar un sistema de indicadores de gestión de riesgos de seguridad de la información alineado a ISO/IEC 27005:2018. Este sistema debería priorizar, como mínimo, métricas de MTTR por nivel de prioridad y por unidad organizacional, volumen de tickets abiertos y cerrados por periodo, porcentaje de incidentes resueltos dentro de plazos objetivo (SLA) y número de reincidencias por tipo de evento.

Se sugiere tomar el valor de 1020 horas identificado en el estudio como línea base para la mejora continua, definiendo metas progresivas de reducción del MTTR y vinculando su cumplimiento a procesos de evaluación de desempeño y planificación operativa. La publicación periódica de estos indicadores en tableros de control accesibles a la alta gerencia y a los responsables de cada área facilitará la priorización de decisiones, la asignación de recursos y la identificación temprana de cuellos de botella, contribuyendo a reducir la paralización operativa y a fortalecer la continuidad del negocio en PROIMA.

CAPÍTULO VI. APLICABILIDAD

La presente sección tiene como propósito traducir los hallazgos de la investigación en una propuesta concreta de intervención para PROIMA, orientada a mejorar la gestión del riesgo de seguridad de la información y la continuidad del negocio. Mientras los capítulos anteriores se centraron en describir el problema, fundamentarlo teóricamente y analizar los datos obtenidos mediante métodos estadísticos y modelos de machine learning, este capítulo se enfocará en responder de manera aplicada al problema formulado y a los objetivos general y específicos del estudio. De este modo, la aplicabilidad se configura como el puente entre el diagnóstico realizado y las acciones que la organización puede implementar en el corto y mediano plazo.

La propuesta que se desarrollará a continuación se fundamenta directamente en los resultados clave del estudio, entre ellos la ausencia de relación estadísticamente significativa entre la alineación formal de los controles y el desempeño, la importancia crítica de las dimensiones conductuales de conocimiento y ejecución de prácticas seguras, y las ineficiencias evidenciadas en los tiempos de respuesta a incidentes medidos a través del MTTR. Estos hallazgos, junto con el marco teórico basado en la gestión de riesgos empresariales, los enfoques sociotécnicos y las normas ISO/IEC 27001 y 27005, constituyen la base conceptual y empírica sobre la cual se diseña la propuesta.

En coherencia con el manual de Fondo, la aplicabilidad se presentará como un producto con estructura propia, articulando la justificación de la propuesta, su alcance, la descripción general del modelo de intervención y el desarrollo detallado de los entregables que se pondrán a disposición de la empresa. Asimismo, se incorporarán medidas de control e indicadores que permitan evaluar la eficacia de la propuesta, un cronograma de implementación con su correspondiente estimación presupuestaria y un análisis del impacto esperado en términos operativos y financieros. Finalmente, se establecerá la concordancia explícita entre los diferentes segmentos de la tesis y los componentes de la propuesta, asegurando la coherencia vertical entre el problema investigado, los objetivos formulados, la metodología aplicada, los resultados obtenidos y las acciones sugeridas para PROIMA.

6.1. NOMBRE DE LA PROPUESTA

Modelo integral de mejora de la gestión del riesgo de seguridad de la información basado en cultura organizacional, analítica predictiva y métricas operativas en PROIMA

6.2. JUSTIFICACIÓN DE LA PROPUESTA

La propuesta de un modelo integral de mejora de la gestión del riesgo de seguridad de la información basado en cultura organizacional, analítica predictiva y métricas operativas en PROIMA se justifica, en primer lugar, por los hallazgos empíricos del estudio. El análisis inferencial mostró que la alineación formal de los controles con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 no guarda una relación estadísticamente significativa con el desempeño en gestión del riesgo de seguridad de la información, al obtenerse un valor p de 0.649 en la prueba de Spearman. Esto evidencia que, en el periodo analizado, el cumplimiento documental y estructural de los controles no se traduce por sí solo en mejoras observables en la continuidad del negocio, configurando un escenario de seguridad en papel que genera una brecha entre lo normativo y lo operativo (Spearman, 1904).

Desde una perspectiva metodológica, esta brecha resulta consistente con el enfoque de los sistemas de gestión, en el cual las normas ISO/IEC establecen requisitos y directrices para estructurar el control y la gestión del riesgo, pero no garantizan por sí mismas el desempeño si no existen medición operativa, gobernanza efectiva y mejora continua. En particular, ISO/IEC 27001 orienta la implantación del sistema de gestión de seguridad de la información, mientras que ISO/IEC 27005 guía el proceso de gestión del riesgo y su seguimiento; de forma complementaria, la continuidad del negocio requiere traducir el control en capacidades operativas verificables y sostenibles (ISO/IEC, 2022).

En contraste, el modelo de Random Forest sugirió una asociación exploratoria entre las dimensiones conductuales vinculadas a la cultura organizacional, particularmente el conocimiento y la conciencia sobre seguridad (DES_CON) y la ejecución de prácticas seguras (DES_EJE), con el desempeño global en la gestión del riesgo. Estas variables mostraron mayor importancia relativa en el modelo. No obstante, dado que la correlación de Spearman no alcanzó significancia estadística ($p = 0.649$), estos patrones deben interpretarse como hipótesis exploratorias que sugieren la pertinencia de un enfoque sociotécnico, sin que pueda afirmarse una relación causal demostrada. Esta orientación exploratoria respalda la conveniencia de complementar el enfoque técnico con acciones centradas en el comportamiento y la cultura, sujetas a validación empírica adicional (Schein, 2010).

Adicionalmente, el análisis de las métricas operativas evidenció ineficiencias críticas en la toma de decisiones y en la gestión de incidentes, con tiempos de respuesta de hasta 1020 horas en

tickets de baja prioridad y diferencias significativas entre departamentos. La ausencia inicial de un sistema estructurado de indicadores alineados a ISO/IEC 27005:2018 permitió que estas demoras se consolidaran sin un seguimiento sistemático. Este resultado demuestra que, sin métricas claras y oportunas, la organización carece de insumos objetivos para priorizar acciones, asignar recursos y evaluar el impacto real de sus medidas de seguridad, lo que incrementa el riesgo operativo y limita la capacidad de reacción ante eventos que afectan la continuidad del negocio (AXELOS, 2019).

Desde la perspectiva teórica, la propuesta se sustenta en los enfoques de gestión de riesgos empresariales, en la teoría general de sistemas y en las aproximaciones de cultura de seguridad en entornos sociotécnicos. Estas corrientes coinciden en que los controles, políticas y tecnologías solo funcionan como marcos habilitadores cuando se integran de manera coherente con las personas, los procesos y las dinámicas organizacionales. En este sentido, el modelo integral propuesto articula los requisitos de las normas ISO/IEC 27001 y 27005 con herramientas de analítica predictiva y sistemas de métricas operativas, de modo que la gestión del riesgo deje de ser principalmente declarativa y se convierta en un proceso medible, orientado a resultados y centrado en el comportamiento (Schein, 2010).

Finalmente, la viabilidad de la propuesta se fundamenta en que aprovecha capacidades y recursos ya existentes en PROIMA, tales como la información levantada en esta investigación, la infraestructura tecnológica disponible y las estructuras organizacionales asociadas al sistema de gestión de seguridad de la información. El modelo plantea acciones que pueden implementarse de manera gradual en el corto y mediano plazo, como el uso del algoritmo Random Forest como apoyo a recursos humanos, el diseño de indicadores clave basados en métricas como el MTTR y el desarrollo de programas de formación orientados a competencias. Con ello, la propuesta no solo responde de forma directa al problema identificado y a los objetivos general y específicos del estudio, sino que ofrece un valor agregado aplicable, pertinente y alineado con las necesidades reales de la organización (AXELOS, 2019).

6.3. ALCANCE DE LA PROPUESTA

La presente propuesta de aplicabilidad se orientará a traducir los hallazgos de la investigación en un conjunto de acciones concretas y entregables conceptuales y metodológicos para PROIMA, que sirvan como base para futuras decisiones de gestión. En este sentido, el alcance del modelo integral se definirá a partir de objetivos propios del plan de intervención, centrados en

el diseño de herramientas analíticas, la formulación de sistemas de métricas y el fortalecimiento de la cultura de seguridad de la información, sin que ello implique su ejecución técnica o programación dentro del marco de este trabajo.

Este alcance se delimita de forma consistente con el enfoque de proyectos aplicados de tipo "diseño", en los cuales el producto principal consiste en especificaciones, lineamientos y entregables metodológicos que pueden ser implementados posteriormente por la organización, sin que el estudio deba ejecutar la solución. En ese sentido, la propuesta se alineará con las buenas prácticas de sistemas de gestión al definir instrumentos y mecanismos de seguimiento coherentes con un SGSI (ISO/IEC 27001) y con la gestión del riesgo de seguridad de la información (ISO/IEC 27005), manteniendo una orientación a mejora continua y toma de decisiones basada en evidencia (ISO/IEC, 2018).

Objetivos específicos de la propuesta

1. Diseñar un sistema de indicadores y métricas operativas alineado a ISO/IEC 27005:2018, incorporando el MTTR y otras medidas clave por nivel de prioridad y unidad organizacional, que sirva como referencia para el monitoreo continuo de incidentes y de la toma de decisiones en PROIMA.

2. Definir la arquitectura conceptual y las especificaciones funcionales de un modelo de analítica predictiva basado en Random Forest para estimar el riesgo de seguridad asociado al perfil de competencias de los colaboradores, de manera que pueda ser utilizado como insumo por las áreas de recursos humanos y de gestión del riesgo.

3. Elaborar un plan de fortalecimiento de la cultura de seguridad de la información, orientado a mejorar el conocimiento y la ejecución de prácticas seguras mediante lineamientos operativos, propuestas de programas de formación y mecanismos de seguimiento conductual coherentes con los requisitos de las normas ISO/IEC 27001 y 27005.

6.4. DESCRIPCIÓN Y DESARROLLO

En este apartado se presenta el contenido esencial de la propuesta, organizando y detallando los entregables que se derivan de los hallazgos de la investigación y de los objetivos específicos del plan de aplicabilidad. Más que enunciar de forma general qué se sugiere hacer, se describe de manera estructurada cada componente, de modo que PROIMA cuente con insumos claros, ordenados y listos para ser adoptados y adaptados por las instancias responsables de la gestión del riesgo de seguridad de la información y de la continuidad del negocio.

La descripción y desarrollo de la propuesta se articularán en torno a tres ejes principales: el diseño de un sistema de indicadores y métricas operativas alineado a ISO/IEC 27005:2018; la definición de la arquitectura conceptual de un modelo de analítica predictiva basado en Random Forest para apoyar la gestión del riesgo asociado a las competencias de los colaboradores; y la elaboración de un plan de fortalecimiento de la cultura de seguridad de la información. Cada uno de estos ejes se presentará con sus objetivos, componentes, pasos sugeridos y productos concretos, con el fin de que la institución pueda utilizar estos entregables como guía directa para la toma de decisiones y el desarrollo de acciones futuras.

Desde un enfoque conceptual, la propuesta se enmarca en la gestión integral del riesgo de seguridad de la información como un proceso continuo de gobernanza, medición y mejora, en el cual la eficacia de los controles depende tanto de su diseño formal como de su apropiación por parte de las personas. En coherencia con los estándares internacionales, la seguridad se concibe como un sistema organizacional que integra procesos, indicadores y cultura, orientado a reducir el riesgo residual y fortalecer la sostenibilidad de las prácticas de gestión en el tiempo (Schein, 2010).

6.4.1. DESCRIPCIÓN

En esta sección se describirán de manera concreta las acciones principales, procesos y estrategias que conforman la propuesta de aplicabilidad, organizadas en función de los objetivos específicos planteados para el Capítulo VI. Cada componente se presentará como un entregable claro para PROIMA, indicando qué se propone hacer, cómo se articula con la gestión del riesgo de seguridad de la información y de qué manera se vincula con los hallazgos empíricos y el marco teórico de la investigación.

Metodológicamente, el diseño de la propuesta se fundamentará en la evidencia obtenida a través del análisis inferencial, del modelo de Random Forest y de las métricas operativas (especialmente el MTTR), así como en los lineamientos de las normas ISO/IEC 27001 y 27005 y en los enfoques sociotécnicos de cultura de seguridad. De esta forma, cada conjunto de acciones y procesos descritos responderá a una lógica de coherencia interna: partir del problema diagnosticado, aprovechar los resultados cuantitativos y cualitativos del estudio y traducirlos en lineamientos, sistemas de indicadores y esquemas de actuación que la organización pueda adoptar como base para la mejora de su gestión de riesgos.

Desde un enfoque conceptual, la propuesta se enmarca en la gestión integral del riesgo de seguridad de la información como un proceso continuo de gobernanza, medición y mejora, en el

cual la eficacia de los controles depende tanto de su diseño formal como de su apropiación por parte de las personas. En coherencia con los estándares internacionales, la seguridad se concibe como un sistema organizacional que integra procesos, indicadores y cultura, orientado a reducir el riesgo residual y fortalecer la sostenibilidad de las prácticas de gestión en el tiempo (Schein, 2010).

6.4.1.1. DISEÑO DEL SISTEMA DE INDICADORES Y MÉTRICAS OPERATIVAS PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA

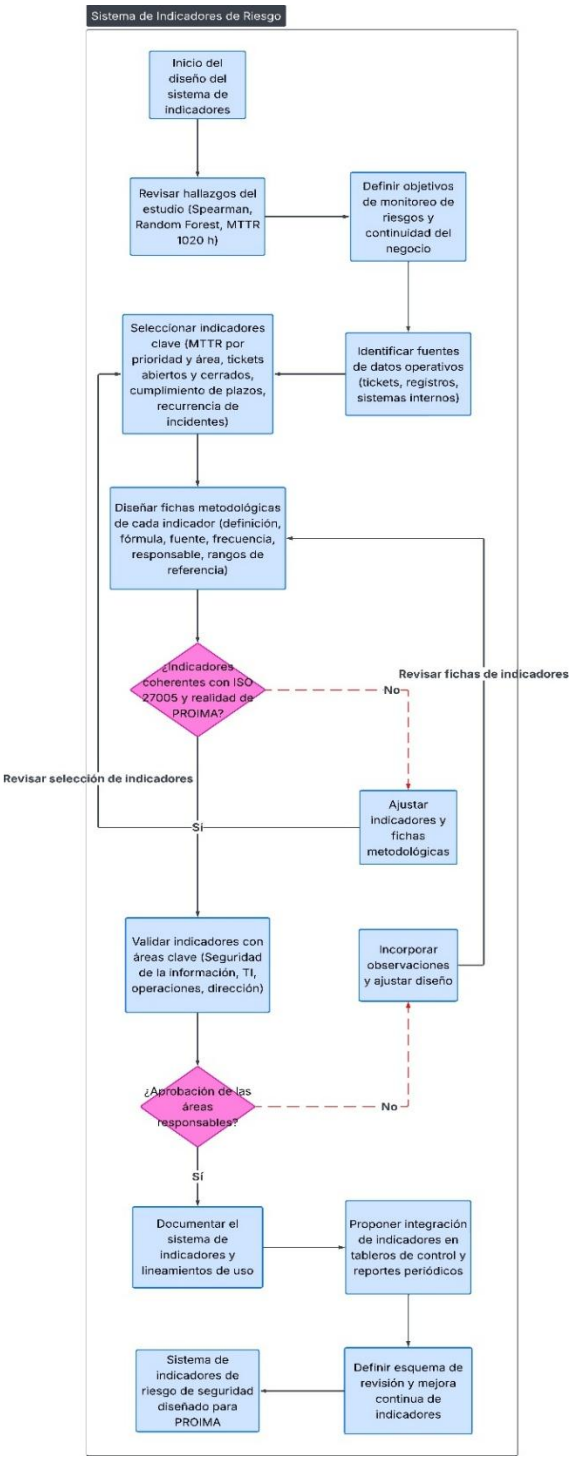
El diseño del sistema de indicadores y métricas operativas para PROIMA se centrará en definir de manera estructurada un conjunto de medidas cuantitativas que permitan monitorear el comportamiento de los incidentes de seguridad de la información y su impacto en la continuidad del negocio. De forma concreta, se precisarán indicadores como el tiempo medio de resolución de incidentes (MTTR) por nivel de prioridad y por unidad organizacional, el volumen de tickets abiertos y cerrados en cada periodo, el porcentaje de casos resueltos dentro de los plazos objetivo y la recurrencia de determinados tipos de eventos. Estos indicadores se organizarán en fichas metodológicas que especifiquen su definición, fórmula de cálculo, fuente de datos, frecuencia de medición, responsables y rangos de referencia, de modo que la empresa cuente con un esquema claro para su seguimiento operativo.

Metodológicamente, el diseño de este sistema se justifica en la evidencia empírica obtenida en la investigación, en particular en los tiempos de respuesta críticos identificados, como el MTTR de hasta 1020 horas en tickets de baja prioridad, y en la ausencia inicial de métricas formales que hicieran visible esta ineficiencia. Asimismo, se sustenta en los lineamientos de ISO IEC 27005, que enfatiza la necesidad de contar con indicadores que apoyen la evaluación y tratamiento del riesgo a lo largo del ciclo de vida de la gestión. El sistema propuesto tomará estos referentes como base para traducir los hallazgos del estudio en un conjunto de métricas coherentes con la realidad operativa de PROIMA, de forma que los resultados estadísticos y los modelos analíticos no se queden solo en el plano académico, sino que se conviertan en herramientas concretas para la priorización de decisiones y la mejora continua.

El sistema de indicadores y métricas operativas se concibe como un conjunto de medidas cuantitativas orientadas a monitorear el desempeño en la gestión de incidentes de seguridad de la información y su impacto en la continuidad del negocio. Entre estas métricas destacan el tiempo medio de resolución de incidentes (MTTR), el seguimiento de tickets y el cumplimiento de los acuerdos de nivel de servicio (SLA), ampliamente utilizados para evaluar la eficacia de los

procesos de atención y respuesta. Su aplicación permite sustentar la toma de decisiones en evidencia verificable y fortalecer los mecanismos de seguimiento y mejora continua en la gestión del riesgo (Axelos, 2019).

Figura 23: *Flujo del diseño del sistema de indicadores de riesgo SI en PROIMA*



Fuente: Elaboración Propia

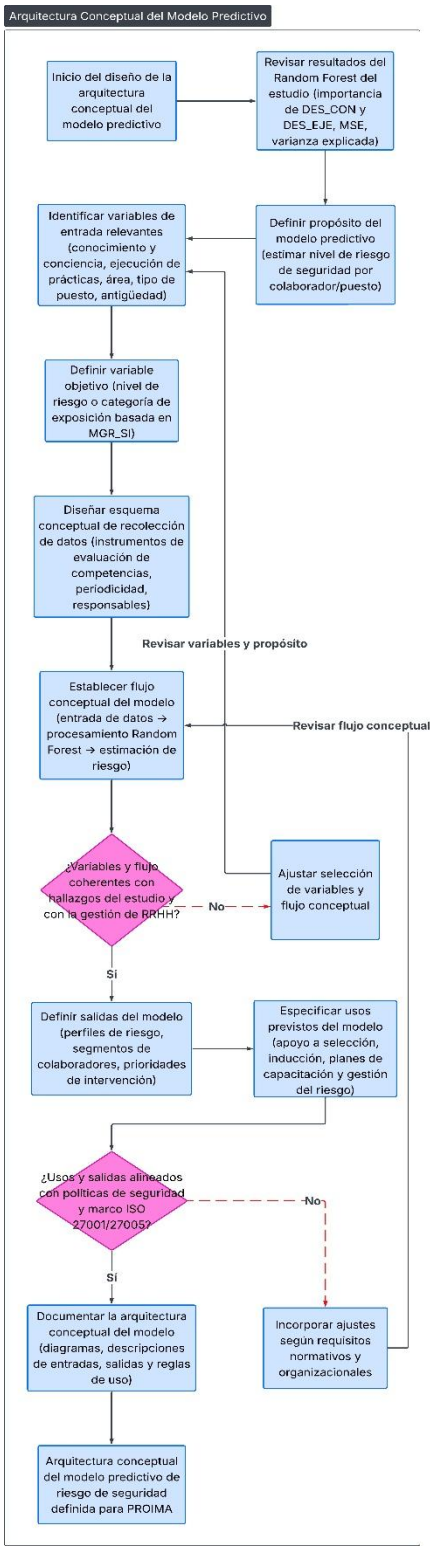
6.4.1.2. DEFINICIÓN DE LA ARQUITECTURA CONCEPTUAL DEL MODELO DE ANALÍTICA PREDICTIVA BASADO EN RANDOM FOREST PARA LA ESTIMACIÓN DEL RIESGO DE SEGURIDAD

La definición de la arquitectura conceptual del modelo de analítica predictiva se orientará a describir, de forma estructurada, cómo PROIMA podría utilizar un esquema basado en Random Forest para estimar el riesgo de seguridad asociado al perfil de competencias de sus colaboradores, sin entrar en la fase de programación o implementación técnica. De manera concreta, se delimitarán las variables de entrada (por ejemplo, niveles de conocimiento y conciencia en seguridad, ejecución de prácticas seguras, área funcional, tipo de puesto), la variable objetivo (nivel de riesgo o categoría de exposición) y el flujo lógico de uso del modelo, desde la recolección de datos hasta la obtención de una estimación de riesgo que sirva de insumo para decisiones de gestión de talento y de seguridad de la información.

Metodológicamente, esta arquitectura conceptual se justifica en los resultados obtenidos en la investigación, donde el modelo de Random Forest aplicado a los datos perceptuales explicó un alto porcentaje de la varianza del desempeño (MGR_SI) y demostró que las variables conductuales DES_CON y DES_EJE son las de mayor importancia relativa. Sobre esta base, el diseño propuesto no pretende crear un nuevo algoritmo, sino aprovechar la lógica ya validada en el estudio para definir un marco de referencia que indique qué información debe recopilarse, cómo debe estructurarse y de qué manera el modelo puede integrarse como herramienta de apoyo para la priorización de intervenciones formativas y la identificación temprana de perfiles con mayor exposición al riesgo de seguridad de la información.

La arquitectura conceptual del modelo de analítica exploratoria se define como un esquema lógico que organiza las variables de entrada, la variable objetivo y el flujo general de procesamiento de la información para la caracterización exploratoria del riesgo de seguridad, sin abordar aspectos de implementación técnica. Este enfoque se basa en el método Random Forest, un algoritmo de aprendizaje supervisado que combina múltiples árboles de decisión, y se integra dentro de un proceso estructurado de análisis de datos. Es importante destacar que, dado que la correlación principal del estudio no alcanzó significancia estadística ($p = 0.649$), la arquitectura propuesta tiene carácter exploratorio y su uso predictivo requeriría validación empírica adicional con estudios longitudinales antes de su implementación operativa (Chapman et al., 2000).

Figura 24: *Arquitectura conceptual del modelo predictivo Random Forest*



Fuente: Elaboración Propia

6.4.1.3. ELABORACIÓN DEL PLAN DE FORTALECIMIENTO DE LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA

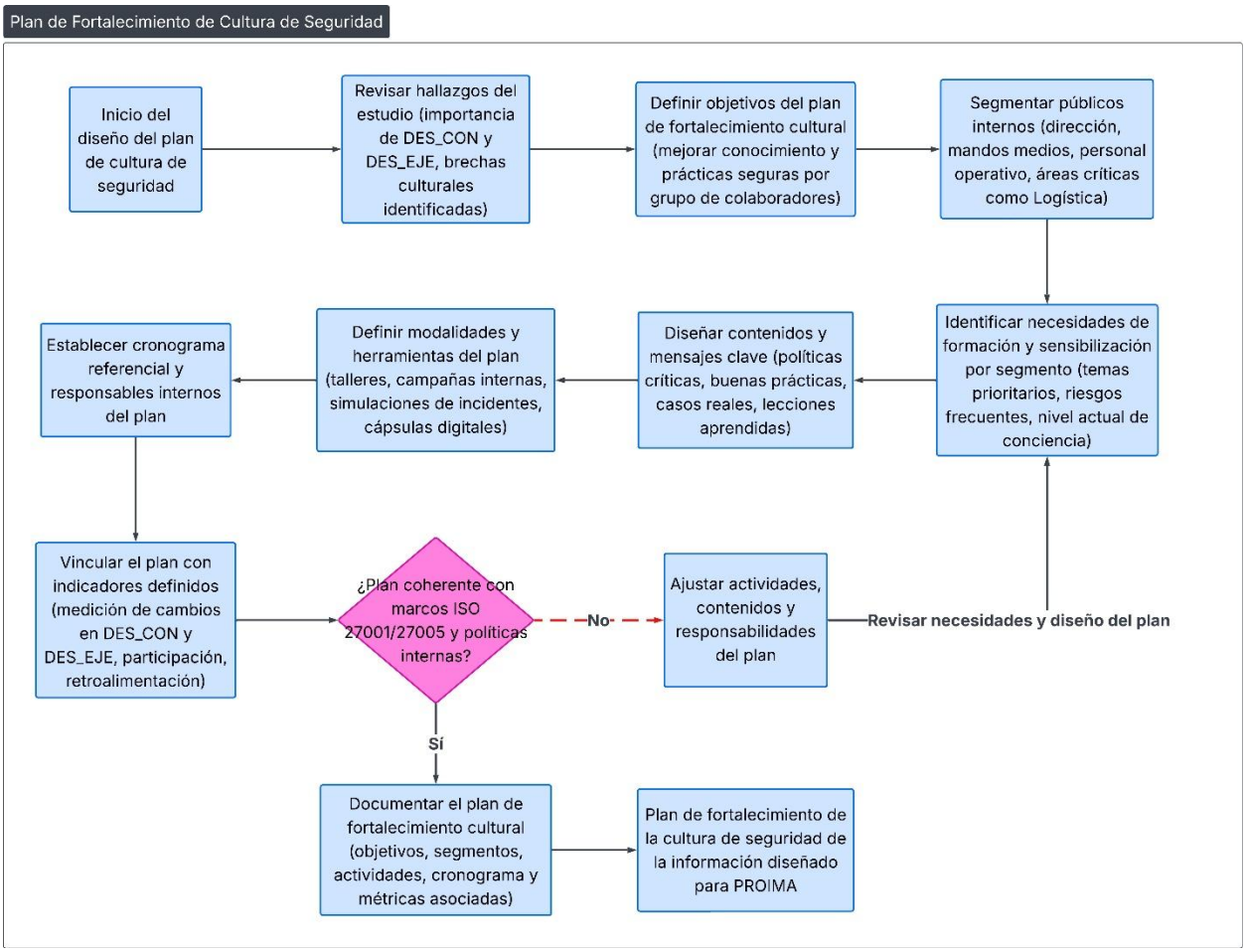
El plan de fortalecimiento de la cultura de seguridad de la información en PROIMA se orientará a definir un conjunto estructurado de acciones formativas, comunicacionales y de liderazgo que permitan elevar los niveles de conocimiento, conciencia y ejecución de prácticas seguras por parte de los colaboradores. De manera concreta, el plan incluirá la segmentación de públicos internos según su exposición al riesgo, la definición de objetivos de aprendizaje por grupo, el diseño de contenidos clave (temas, mensajes, casos prácticos), la propuesta de modalidades de sensibilización (talleres, campañas internas, cápsulas informativas, simulaciones) y la identificación de responsables y frecuencias sugeridas. Todo ello se organizará en un documento que funcione como hoja de ruta para que la organización pueda, posteriormente, operacionalizar las actividades de forma gradual y sistemática.

Metodológicamente, el diseño de este plan se fundamenta en los hallazgos exploratorios del análisis inferencial y del modelo de Random Forest, que sugirieron una asociación entre las variables de conocimiento/conciencia (DES_CON) y ejecución de prácticas seguras (DES_EJE) con el desempeño en la gestión del riesgo, aunque sin alcanzar significancia estadística en la correlación principal ($p = 0.649$). Asimismo, se apoya en los enfoques de cultura de seguridad y en las aproximaciones sociotécnicas, que plantean que la efectividad de los marcos ISO/IEC 27001 y 27005 depende de su apropiación por las personas y no solo de su diseño formal. En este sentido, el plan propuesto traducirá estos referentes teóricos y patrones exploratorios en estrategias concretas de fortalecimiento cultural, articuladas con los indicadores definidos en los apartados anteriores, de modo que la gestión del riesgo se consolide como una práctica compartida y cotidiana en PROIMA, reconociendo que estas intervenciones requieren evaluación continua de su efectividad.

Desde un enfoque conceptual, el plan de fortalecimiento de la cultura de seguridad de la información se sustenta en la idea de que la gestión eficaz del riesgo no depende únicamente de políticas y controles formales, sino de la interiorización de prácticas seguras por parte de las personas que interactúan con la información. En este sentido, la cultura de seguridad se concibe como un componente organizacional que integra conocimiento, actitudes y comportamientos, y cuya consolidación requiere acciones formativas, comunicacionales y de liderazgo coherentes con la realidad operativa de la organización. Este planteamiento se alinea con los enfoques sociotécnicos de la cultura organizacional y con los marcos de seguridad de la información, los

cuales destacan que la efectividad de los sistemas de gestión se ve condicionada por el grado de apropiación y compromiso de los colaboradores (Schein, 2010).

Figura 25: *Plan de fortalecimiento de la cultura de seguridad de la información*



Fuente: Elaboración propia

6.4.2. DESARROLLO

En este apartado se presenta el desarrollo detallado de los entregables que conforman la propuesta de aplicabilidad, de manera que PROIMA cuente no solo con lineamientos generales, sino con instrumentos y productos claramente definidos que pueda adoptar y adaptar en su gestión cotidiana del riesgo de seguridad de la información. A partir de los objetivos específicos de la propuesta, se profundizará en la construcción del sistema de indicadores y métricas operativas, en la arquitectura conceptual del modelo de analítica predictiva basado en Random Forest y en el plan de fortalecimiento de la cultura de seguridad, describiendo su estructura interna, componentes, pasos sugeridos y forma de uso.

Cada entregable será desarrollado como un insumo autónomo pero articulado con el resto

de la propuesta y con los resultados de la investigación, de modo que exista coherencia entre el diagnóstico estadístico (correlaciones, modelo predictivo, métricas como el MTTR), el marco teórico (gestión de riesgos, cultura de seguridad, normas ISO/IEC 27001 y 27005) y las acciones sugeridas. El propósito es que el Capítulo VI trascienda el nivel descriptivo y se convierta en un verdadero modelo de intervención, en el cual la empresa pueda encontrar matrices, esquemas y descripciones suficientemente detalladas para orientar decisiones futuras sobre el diseño de tableros de control, el uso de analítica de datos y el desarrollo de programas de formación en seguridad de la información.

Desde una perspectiva conceptual de gestión, el desarrollo de los entregables responde a la lógica de los sistemas de medición del desempeño como herramientas para traducir la estrategia en acciones observables y evaluables. En este enfoque, los indicadores, modelos analíticos y mecanismos de seguimiento no se conciben como fines en sí mismos, sino como medios para orientar la toma de decisiones, alinear comportamientos organizacionales y facilitar el aprendizaje institucional. La integración de métricas y esquemas de análisis permite vincular los objetivos estratégicos con resultados operativos, favoreciendo una gestión más informada y consistente del riesgo de seguridad de la información (Kaplan & Norton, 1996).

Asimismo, el desarrollo de la propuesta se fundamenta en el principio de toma de decisiones basada en datos, el cual sostiene que el valor de la analítica no radica únicamente en la sofisticación de los modelos, sino en su capacidad para generar conocimiento accionable. Desde esta perspectiva, los modelos predictivos y los tableros de control funcionan como mecanismos de apoyo que permiten anticipar escenarios, priorizar intervenciones y reducir la incertidumbre en contextos organizacionales complejos. La analítica aplicada a la gestión del riesgo contribuye así a transformar datos en información relevante y esta, a su vez, en decisiones estratégicas y operativas con mayor sustento racional (Davenport & Harris, 2007).

6.4.2.1 DESARROLLO DEL SISTEMA DE INDICADORES Y MÉTRICAS OPERATIVAS PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

6.4.2.1.1 CRITERIOS DE DISEÑO DEL SISTEMA DE INDICADORES

Desde un enfoque conceptual, el diseño de un sistema de indicadores debe responder a principios que aseguren su utilidad estratégica y su capacidad para traducir objetivos organizacionales en información relevante para la toma de decisiones. La literatura sobre medición del desempeño sostiene que los indicadores efectivos son aquellos que mantienen coherencia con

la estrategia, permiten el seguimiento sistemático de resultados y procesos, y facilitan la identificación de desviaciones que requieren acciones correctivas. En el ámbito de la gestión del riesgo, estos principios se refuerzan al exigir que las métricas sean trazables, comparables y orientadas a la mejora continua, de modo que el sistema de indicadores funcione como un puente entre el análisis del riesgo y la gestión operativa de la organización (Kaplan & Norton, 1996).

En esta sección se establecen los criterios que orientarán el diseño del sistema de indicadores y métricas operativas para la gestión del riesgo de seguridad de la información en PROIMA. Estos criterios permiten asegurar que los indicadores seleccionados sean útiles para la toma de decisiones gerenciales, estén alineados con ISO 27005 y reflejen de manera consistente la continuidad del negocio y el desempeño real de la organización.

A continuación se presentan los criterios propuestos:

Tabla 29: *Criterios para el diseño del sistema de indicadores de riesgo de seguridad de la información en PROIMA*

Criterio	Descripción
Alineación estratégica	El indicador debe vincularse con los objetivos de negocio y con la continuidad operativa de PROIMA.
Coherencia con ISO 27005	Debe apoyar alguna fase del ciclo de gestión del riesgo (identificación, análisis, evaluación, tratamiento, monitoreo).
Relevancia y materialidad	Debe reflejar aspectos críticos del riesgo, evitando indicadores decorativos o de bajo impacto.
Disponibilidad y calidad de datos	Requiere fuentes de información accesibles, confiables y con registro sistemático.
Claridad y simplicidad	Debe ser fácil de entender por los usuarios clave, con definiciones y fórmulas no ambiguas.
Comparabilidad temporal y entre áreas	Debe permitir comparar periodos y unidades organizacionales, detectando tendencias y brechas.
Capacidad de acción	Debe ser accionable; su variación debe sugerir decisiones o ajustes concretos.
Equilibrio proceso/resultado	El sistema debe incluir tanto indicadores de resultado (impacto) como de proceso (gestión y tiempos).
Trazabilidad y auditabilidad	El cálculo y la fuente de datos deben poder ser verificados y auditados.
Viabilidad de medición	El esfuerzo para medirlo debe ser proporcional al valor que aporta para la gestión.

Fuente: Elaboración Propia

6.4.2.1.2 DEFINICIÓN DE INDICADORES CLAVE DE DESEMPEÑO Y RIESGO

Con base en los criterios anteriores y en los hallazgos del estudio, se propone un conjunto de indicadores clave orientados a capturar el desempeño en la gestión de incidentes de seguridad

de la información y su impacto en la continuidad del negocio. Estos indicadores giran en torno al tiempo de respuesta, el volumen y la priorización de tickets, el cumplimiento de plazos objetivo y la recurrencia de eventos.

Desde una perspectiva conceptual, los indicadores clave de desempeño y riesgo se conciben como variables críticas que permiten sintetizar el comportamiento de los procesos y su impacto sobre los objetivos organizacionales. En el ámbito de la gestión de incidentes de seguridad de la información, la literatura especializada señala que métricas vinculadas al tiempo de respuesta, la carga operativa y el cumplimiento de niveles de servicio resultan esenciales para evaluar la eficacia del tratamiento del riesgo y su influencia en la continuidad del negocio. En este sentido, la selección de indicadores como el MTTR, el volumen y estado de los tickets, el cumplimiento de SLA y la recurrencia de incidentes responde a la necesidad de contar con medidas que reflejen tanto el desempeño operativo como la exposición residual al riesgo, facilitando la priorización de acciones y la mejora continua de los procesos (Axelos, 2019).

La siguiente tabla presenta la definición general de los principales indicadores propuestos:

Tabla 30: *Indicadores clave propuestos para la gestión operativa del riesgo de seguridad de la información*

Código	Indicador	Descripción breve
IND_01	MTTR global de incidentes	Tiempo medio, en horas, que transcurre desde la apertura hasta el cierre de los tickets de seguridad.
IND_02	MTTR por nivel de prioridad	Tiempo medio de resolución para tickets de prioridad alta, media y baja.
IND_03	Tickets abiertos al cierre de periodo	Número de tickets de seguridad que permanecen abiertos al final de cada periodo de análisis.
IND_04	Tickets cerrados en el periodo	Número de tickets de seguridad resueltos en el periodo.
IND_05	Porcentaje de tickets dentro del SLA	Proporción de tickets resueltos dentro del tiempo objetivo definido para cada prioridad.
IND_06	Tasa de recurrencia de incidentes	Porcentaje de tickets que corresponden a incidentes repetidos del mismo tipo o causa raíz.
IND_07	Incidentes por unidad organizacional	Distribución del número de tickets por departamento o área de PROIMA.
IND_08	Porcentaje de incidentes con causa raíz identificada	Proporción de tickets en los que se documentó una causa raíz clara y acciones correctivas asociadas.

Fuente: Elaboración Propia

6.4.2.1.3 FICHAS METODOLÓGICAS DE LOS INDICADORES SELECCIONADOS

Para garantizar la correcta comprensión y uso de cada indicador, se propone el uso de fichas

metodológicas estandarizadas. Estas fichas detallan la definición, el objetivo, la fórmula de cálculo, las variables involucradas, la fuente de datos, la frecuencia de medición, los responsables y las metas de referencia.

Desde una perspectiva conceptual de control y evaluación del desempeño, las fichas metodológicas constituyen un instrumento fundamental para asegurar la consistencia, transparencia y comparabilidad de los indicadores utilizados en un sistema de gestión. La estandarización de la información asociada a cada indicador permite clarificar su propósito, su forma de cálculo y las responsabilidades vinculadas a su medición, reduciendo ambigüedades y facilitando su uso sistemático en la toma de decisiones. En el contexto de la gestión del riesgo, este tipo de fichas contribuye a garantizar la trazabilidad de los datos, la auditabilidad de los resultados y la alineación entre los objetivos estratégicos y las métricas operativas, reforzando el carácter formal y verificable del sistema de indicadores (Kaplan & Norton, 1996)

Tabla 31: *Plantilla de ficha metodológica*

Campo	Contenido a registrar
Nombre del indicador	Título oficial del indicador
Código	Identificador interno (por ejemplo, IND_01)
Objetivo	Finalidad del indicador y decisión que apoya
Definición	Descripción clara de qué mide
Fórmula de cálculo	Expresión matemática del indicador
Variables	Variables que intervienen en la fórmula
Unidad de medida	Horas, porcentaje, número de casos, etc.
Fuente de datos	Sistema o registro del que se extrae la información
Frecuencia de medición	Diaria, semanal, mensual, trimestral, etc.
Responsable	Área o rol encargado de calcular y reportar
Meta o rango de referencia	Valor objetivo o rango aceptable
Observaciones	Notas sobre supuestos, limitaciones o consideraciones especiales

Fuente: Elaboración propia

A continuación se presentan dos ejemplos de fichas ya desarrolladas:

Tabla 32: *Ejemplo 1: MTTR por nivel de prioridad (IND_02)*

Campo	Contenido
Nombre del indicador	MTTR por nivel de prioridad
Código	IND_02
Objetivo	Medir la rapidez de respuesta y resolución de incidentes según su prioridad asignada.
Definición	Tiempo promedio, en horas, que tarda en resolverse un ticket de seguridad de una prioridad específica.
Fórmula de cálculo	MTTR_prioridad = Σ tiempo de resolución de tickets de esa prioridad / número de tickets de esa prioridad.

Variables	Tiempo de resolución individual, número de tickets por prioridad.
Unidad de medida	Horas
Fuente de datos	Sistema de gestión de tickets de PROIMA
Frecuencia de medición	Mensual
Responsable	Área de Seguridad de la Información, en coordinación con TI
Meta o rango de referencia	Definida por prioridad (por ejemplo, alta ≤ 24 h, media ≤ 72 h, baja ≤ 168 h)
Observaciones	Considerar solo tickets cerrados en el periodo de análisis.

Fuente: Elaboración propia

Tabla 33: *Ejemplo 2: Porcentaje de tickets dentro del SLA (IND_05)*

Campo	Contenido
Nombre del indicador	Porcentaje de tickets dentro del SLA
Código	IND_05
Objetivo	Evaluar el grado de cumplimiento de los tiempos objetivo de respuesta y resolución.
Definición	Proporción de tickets de seguridad resueltos dentro del tiempo máximo definido para su prioridad.
Fórmula de cálculo	%SLA = (número de tickets resueltos dentro del SLA / número total de tickets resueltos) x 100.
Variables	Tickets resueltos dentro del SLA, tickets resueltos totales.
Unidad de medida	Porcentaje (%)
Fuente de datos	Sistema de gestión de tickets de PROIMA
Frecuencia de medición	Mensual
Responsable	Área de Seguridad de la Información
Meta o rango de referencia	≥ 90 % de tickets dentro del SLA
Observaciones	El SLA puede diferenciarse por prioridad; el cálculo puede segmentarse por área.

Fuente: Elaboración propia

6.4.2.1.4 PROPUESTA DE ESQUEMA DE REPORTE Y TABLERO DE CONTROL

Para que los indicadores y métricas definidos se conviertan en insumos efectivos para la toma de decisiones, es necesario estructurar un esquema de reporte y un tablero de control conceptual que especifique qué información verá cada nivel de la organización, con qué frecuencia y en qué formato.

Desde un enfoque conceptual de gestión y control organizacional, los esquemas de reporte y los tableros de control constituyen mecanismos clave para transformar los indicadores en información útil para la toma de decisiones en distintos niveles jerárquicos. La literatura sobre control de gestión sostiene que la efectividad de los sistemas de medición depende no solo de la

calidad de los indicadores, sino también de su adecuada presentación, periodicidad y adaptación a las necesidades informativas de cada actor organizacional. En este sentido, los tableros de control permiten sintetizar información compleja, facilitar el seguimiento de tendencias y focalizar la atención en los factores críticos de desempeño y riesgo, contribuyendo a una toma de decisiones más oportuna y alineada con los objetivos estratégicos de la organización (Few, 2013).

La tabla siguiente resume la propuesta de esquema de reporte:

Tabla 34: *Esquema de reporte de indicadores de riesgo de seguridad de la información por nivel de usuario*

Nivel de usuario	Periodicidad sugerida	Formato de reporte	Principales indicadores a incluir
Dirección general	Mensual	Informe ejecutivo y tablero resumen	IND_01, IND_02 agregados, IND_05, IND_07, indicadores de tendencia.
Comité de seguridad / TI	Quincenal	Reporte detallado y tablero analítico	Todos los indicadores IND_01 a IND_08, desagregados por área y prioridad.
Jefaturas de área	Semanal	Reporte operativo breve y vista de tablero	IND_02, IND_03, IND_04, IND_06, IND_07 para su unidad.
Equipos operativos de soporte	Diario o según necesidad	Listados y vistas operativas	Tickets abiertos, IND_03, IND_04, alertas de SLA (IND_05).

Fuente: Elaboración Propia

A nivel conceptual, se sugiere que el tablero de control agrupe los indicadores en cuatro bloques:

- Panorama general de riesgo (MTTR global, porcentaje de tickets dentro de SLA).
- Desempeño operativo (tickets abiertos y cerrados, distribución por prioridad).
- Focos de riesgo por área (incidentes por unidad organizacional, recurrencia por tipo).
- Calidad de la respuesta (porcentaje de incidentes con causa raíz identificada).

6.4.2.1.5 LINEAMIENTOS PARA LA REVISIÓN Y MEJORA CONTINUA DEL SISTEMA DE INDICADORES

El sistema de indicadores debe concebirse como un instrumento dinámico, sujeto a revisión y mejora continua en función de la evolución de los procesos, los riesgos y las necesidades de información de PROIMA. En esta sección se plantean lineamientos que orientan cuándo y cómo revisar los indicadores, ajustar metas, incorporar nuevos elementos o retirar aquellos que hayan perdido relevancia.

Desde un enfoque conceptual de gestión y control, los sistemas de indicadores deben concebirse como estructuras dinámicas, sujetas a procesos sistemáticos de revisión y ajuste, en función de los cambios del entorno, la evolución de los riesgos y las necesidades estratégicas de la organización. La literatura sobre mejora continua sostiene que la utilidad de los indicadores depende de su capacidad para adaptarse, aprender de la experiencia y retroalimentar la toma de decisiones, evitando la obsolescencia de las métricas y la pérdida de alineación con los objetivos organizacionales. En este sentido, la revisión periódica, la validación de la calidad de los datos y la actualización de metas y definiciones constituyen prácticas esenciales para mantener la relevancia y efectividad de los sistemas de medición, en coherencia con los principios de gestión del riesgo y mejora continua ampliamente reconocidos en la gestión organizacional (Deming, 1986)

La siguiente tabla resume las principales actividades de revisión y mejora propuestas:

Tabla 35: *Actividades para la revisión y mejora continua del sistema de indicadores*

Actividad	Periodicidad sugerida	Responsable principal	Resultado esperado
Revisión de consistencia de datos	Mensual	Área de Seguridad de la Información	Verificación de calidad y completitud de la información utilizada.
Evaluación de cumplimiento de metas	Trimestral	Seguridad de la Información y Dirección	Ajuste de metas o acciones correctivas cuando se detecten desviaciones críticas.
Revisión integral del catálogo de indicadores	Anual	Comité de seguridad / TI	Actualización del sistema: incorporación, modificación o eliminación de indicadores.
Recopilación de retroalimentación de usuarios	Semestral	Seguridad de la Información y RRHH	Mejora de reportes y tableros según necesidades de usuarios clave.
Actualización de fichas metodológicas	Cuando se modifique un indicador	Seguridad de la Información	Fichas vigentes, claras y coherentes con los cambios realizados.

Fuente: Elaboración Propia

Como principio general, cualquier modificación al sistema de indicadores debe ser discutida y validada por el comité responsable de la gestión de riesgos y seguridad de la información, asegurando que se mantenga la alineación con ISO 27005 y con los objetivos de continuidad del negocio.

6.4.2.2 DESARROLLO DEL MODELO DE ANALÍTICA PREDICTIVA BASADO EN RANDOM FOREST PARA LA ESTIMACIÓN DEL RIESGO DE SEGURIDAD

El desarrollo del modelo de analítica predictiva propuesto en esta sección se enmarca metodológicamente en los principios de la metodología CRISP-DM (Cross-Industry Standard Process for Data Mining), ampliamente reconocida como un estándar para proyectos de minería de datos y ciencia de datos aplicados.

En coherencia con este enfoque, el proceso seguido en la investigación comprende de manera conceptual las fases de comprensión del problema (definición del objetivo de estimar el riesgo de seguridad asociado a competencias y contexto organizacional), comprensión y preparación de los datos (identificación y estructuración de variables conductuales y organizacionales), modelado (aplicación del algoritmo Random Forest), evaluación de resultados (análisis de desempeño predictivo e importancia de variables) y uso del conocimiento como insumo para la toma de decisiones.

Si bien el alcance del presente estudio no incluye la implementación técnica del modelo, la arquitectura conceptual propuesta se alinea con las etapas de CRISP-DM, otorgando validez metodológica y rigor científico al proceso de modelado descrito (Chapman et al., 2000).

6.4.2.2.1 OBJETIVO Y ALCANCE DEL MODELO PREDICTIVO DE RIESGO

El modelo de analítica predictiva basado en Random Forest se concibe como una herramienta conceptual de apoyo para estimar el nivel de riesgo de seguridad asociado al perfil de competencias y al contexto organizacional de los colaboradores de PROIMA. Su objetivo principal será anticipar, a partir de variables de conocimiento, ejecución de prácticas seguras y factores organizacionales, qué grupos de personas o puestos presentan una mayor probabilidad de contribuir a incidentes de seguridad de la información, de modo que la organización pueda priorizar acciones de formación, supervisión y seguimiento.

El alcance del modelo, en el marco de esta propuesta, se limita a la definición de su arquitectura conceptual, sus variables de entrada y salida, y las reglas generales de interpretación de resultados. No se desarrollará código ni se desplegará una solución técnica dentro del estudio, sino que se entregará un diseño funcional que pueda ser utilizado posteriormente por las áreas de TI y seguridad de la información como referencia para una futura construcción e integración

tecnológica.

Desde una perspectiva conceptual, los modelos de analítica predictiva aplicados a la gestión del riesgo se conciben como herramientas de apoyo a la toma de decisiones, orientadas a anticipar comportamientos y escenarios a partir de patrones identificados en los datos disponibles. En este enfoque, el valor del modelo no reside en su implementación técnica inmediata, sino en su capacidad para estructurar información relevante, reducir la incertidumbre y facilitar la priorización de intervenciones preventivas en contextos organizacionales complejos. La literatura en analítica y ciencia de datos destaca que estos modelos cumplen una función estratégica cuando se integran como insumos para la gestión y no como mecanismos deterministas de decisión, permitiendo orientar acciones en áreas como la capacitación, la supervisión y la gestión del talento en función del nivel de riesgo estimado (Breiman, 2001)

Tabla 36: *Objetivo y alcance conceptual del modelo predictivo de riesgo de seguridad*

Elemento	Descripción
Objetivo	Estimar el nivel de riesgo de seguridad asociado al perfil de competencias y contexto del colaborador.
Alcance	Definición conceptual del modelo. No incluye programación ni despliegue técnico.
Uso previsto	Apoyo a decisiones de RRHH y seguridad de la información en selección, inducción y capacitación.
Base empírica	Resultados del Random Forest aplicado en la investigación y métricas asociadas al desempeño (MGR_SI).

Fuente: Elaboración Propia

6.4.2.2.2 DEFINICIÓN DE VARIABLES DE ENTRADA Y VARIABLE OBJETIVO

El funcionamiento del modelo requerirá la identificación clara de las variables de entrada que alimentarán el algoritmo y de la variable objetivo que se desea estimar. Para mantener coherencia con el estudio, se consideran como insumo mínimo las dimensiones evaluadas previamente (habilitadores y desempeño conductual), complementadas con información básica del contexto organizacional del colaborador. La variable objetivo se definirá como un índice o categoría de riesgo de seguridad derivado del desempeño en la gestión del riesgo de la información.

La definición de las variables de entrada y de la variable objetivo constituye una etapa crítica para garantizar la validez y utilidad de los resultados del modelo. La literatura en aprendizaje automático y analítica aplicada señala que la selección de variables debe responder tanto a su relevancia teórica como a su capacidad explicativa respecto al fenómeno de interés,

incorporando dimensiones conductuales y contextuales que influyen en el resultado a estimar. En el ámbito de la gestión del riesgo de seguridad de la información, esta aproximación implica considerar variables relacionadas con conocimientos, prácticas y entorno organizacional como predictores del nivel de exposición al riesgo, así como definir una variable objetivo que sintetice el desempeño observado en términos de riesgo residual. Este enfoque permite construir modelos interpretables y orientados a la toma de decisiones, en coherencia con las buenas prácticas de la analítica predictiva (Hastie, Tibshirani & Friedman, 2009)

Tabla 37: *Variables de entrada propuestas para el modelo predictivo de riesgo de seguridad*

Código	Variable	Descripción	Tipo de dato	Fuente principal
DES_CON	Conocimiento y conciencia en seguridad	Nivel de comprensión de políticas, riesgos y buenas prácticas de seguridad de la información.	Escala tipo Likert	Encuestas internas o evaluaciones de competencias.
DES_EJE	Ejecución de prácticas seguras	Frecuencia con la que el colaborador aplica prácticas seguras en su trabajo diario.	Escala tipo Likert	Encuestas, observación estructurada.
HAB_POL	Exposición a políticas de seguridad	Grado de conocimiento de las políticas formales por parte del colaborador.	Escala tipo Likert	Registros de inducción y encuestas.
HAB_CAP	Participación en capacitaciones de seguridad	Historial de participación en actividades formativas sobre seguridad de la información.	Numérico/categórico	Registros de RRHH y capacitación.
HAB_CTL	Uso de controles técnicos	Frecuencia de interacción con controles técnicos (autenticación, cifrado, herramientas SI).	Escala tipo Likert	Registros de sistemas y encuestas.
AREA	Unidad organizacional	Departamento o área a la que pertenece el colaborador.	Categórico	Estructura organizacional de PROIMA.
PUESTO	Tipo de puesto	Tipo de rol: operativo, administrativo, supervisión, dirección, etc.	Categórico	Registros de RRHH.
ANTIG	Antigüedad en la	Tiempo aproximado que el colaborador lleva en	Numérico (años)	Registros de RRHH.

organización	PROIMA.

Fuente: Elaboración Propia

La variable objetivo se plantea como un índice de riesgo o categoría de exposición derivada del desempeño en gestión del riesgo de seguridad de la información, tomando como referente el índice MGR_SI utilizado en la investigación.

Tabla 38: *Variable objetivo del modelo predictivo*

Código	Variable objetivo	Descripción	Tipo de dato	Posibles formas de expresión
RIESG_SI	Riesgo de seguridad estimado	Nivel de riesgo asociado al colaborador según su perfil de competencias y contexto.	Numérico o categórico	Puntaje continuo o categorías (bajo, medio, alto).

Fuente: Elaboración Propia

6.4.2.2.3 ESQUEMA CONCEPTUAL DE FUNCIONAMIENTO DEL MODELO BASADO EN RANDOM FOREST

El esquema conceptual del modelo describe el flujo de información desde la recolección de datos hasta la obtención de una estimación de riesgo utilizable para la toma de decisiones. Este flujo no implica programación, sino la definición lógica de etapas que posteriormente podrían ser implementadas por el equipo técnico de PROIMA.

En términos generales, el proceso comprende las siguientes fases: recolección y consolidación de datos de entrada (competencias, área, puesto, antigüedad), preparación y depuración de la información, aplicación del modelo de Random Forest previamente parametrizado con base en los resultados del estudio, y generación de un puntaje o categoría de riesgo para cada colaborador o grupo de colaboradores.

El esquema de funcionamiento del modelo se apoya en la lógica de los procesos analíticos orientados a convertir datos organizacionales en conocimiento accionable, mediante una secuencia ordenada de actividades que incluyen la recolección, preparación, análisis e interpretación de la información. Este tipo de estructuración permite asegurar que las estimaciones de riesgo no sean el resultado aislado de un algoritmo, sino el producto de un proceso coherente que integra datos, contexto organizacional y criterios de interpretación, facilitando su uso como insumo para la toma de decisiones y la priorización de intervenciones en la gestión del riesgo de seguridad de la información (Provost & Fawcett, 2013).

Tabla 39: *Etapas del esquema conceptual de funcionamiento del modelo Random Forest*

Etapa	Descripción	Insumo	Producto

		principal	esperado
Recolección de datos	Obtención de información sobre competencias, contexto organizacional y desempeño histórico si existe.	Encuestas, RRHH, sistemas internos.	Base de datos consolidada de colaboradores.
Preparación y depuración	Revisión de consistencia, tratamiento de datos faltantes, normalización de escalas cuando sea necesario.	Base de datos inicial.	Conjunto de datos preparado para análisis.
Aplicación del modelo conceptual	Uso de la lógica de Random Forest definida en el estudio para estimar el riesgo en función de las variables.	Variables de entrada seleccionadas.	Puntajes o categorías de riesgo por colaborador.
Interpretación de resultados	Análisis de la distribución de riesgo y priorización de grupos o perfiles críticos.	Salidas del modelo.	Listado o mapa de perfiles con niveles de riesgo.
Retroalimentación y ajuste	Revisión periódica de la coherencia de resultados con la realidad observada y ajuste de variables si procede.	Resultados y observaciones de usuarios.	Versión refinada del diseño conceptual.

Fuente: Elaboración propia

6.4.2.2.4 SEGMENTACIÓN Y CATEGORIZACIÓN DEL RIESGO DE SEGURIDAD

Para que los resultados del modelo sean comprensibles y útiles para PROIMA, se propone traducir las salidas numéricas del modelo en categorías de riesgo de fácil interpretación. Estas categorías permitirán clasificar a los colaboradores o puestos en niveles de riesgo y definir prioridades de intervención. La propuesta de segmentación se basa en la distribución de los puntajes de riesgo y puede ajustarse según la experiencia de la organización.

La segmentación y categorización del riesgo constituye un recurso analítico fundamental para traducir los resultados de los modelos predictivos en información comprensible y accionable para la gestión organizacional. La literatura sobre gestión del riesgo señala que la clasificación en niveles o categorías facilita la priorización de intervenciones, la asignación eficiente de recursos y la comunicación del riesgo a distintos niveles de decisión, especialmente cuando los resultados numéricos son complejos o abstractos. En este sentido, el uso de rangos de riesgo permite sintetizar la exposición relativa de personas o grupos, sin perder la posibilidad de ajustes posteriores según el comportamiento real de los datos y el contexto operativo de la organización, fortaleciendo así

la utilidad práctica del análisis predictivo (Aven, 2016).

Tabla 40: *Propuesta de categorías de riesgo de seguridad a partir de la salida del modelo*

Categoría de riesgo	Descripción	Rango orientativo de puntaje*	Implicaciones para la gestión
Bajo	Perfil con alta conciencia y ejecución de prácticas seguras, baja exposición al riesgo.	0.00 a 0.33	Mantener prácticas actuales y reforzar buenas conductas.
Medio	Perfil con competencias aceptables pero con brechas puntuales en conocimiento o ejecución.	> 0.33 a 0.66	Priorizar acciones de capacitación y seguimiento selectivo.
Alto	Perfil con debilidades significativas en conocimiento y prácticas seguras, mayor exposición.	> 0.66 a 1.00	Focalizar intervenciones intensivas y supervisión cercana.

Fuente: Elaboración Propia

*Los rangos son referenciales y deben ajustarse al comportamiento real de los datos que obtenida PROIMA.

Adicionalmente, la segmentación puede cruzarse con dimensiones organizacionales como área, tipo de puesto o antigüedad, permitiendo identificar, por ejemplo, áreas con mayor concentración de perfiles de riesgo alto o grupos que requieren programas específicos de formación.

6.4.2.2.5 LINEAMIENTOS DE USO DEL MODELO PARA APOYO A DECISIONES DE RRHH Y SEGURIDAD DE LA INFORMACIÓN

El valor del modelo predictivo depende de cómo se utilicen sus resultados en la práctica. Por ello, se plantean lineamientos que orientan el uso responsable y estratégico de la herramienta por parte de las áreas de recursos humanos y seguridad de la información, enfatizando que el modelo debe complementarse siempre con criterio profesional y no sustituirlo.

El uso de modelos predictivos en contextos organizacionales requiere lineamientos que aseguren una aplicación responsable, transparente y alineada con los objetivos de gestión. La literatura sobre analítica aplicada enfatiza que estos modelos deben emplearse como herramientas de apoyo a la toma de decisiones y no como mecanismos automáticos o deterministas, especialmente cuando se utilizan para orientar acciones relacionadas con personas. En este sentido, la definición de reglas de uso, restricciones éticas y criterios de interpretación contribuye a maximizar el valor del análisis predictivo, al tiempo que protege la confidencialidad y favorece

decisiones más informadas en la gestión del riesgo (Davenport & Harris, 2007).

Tabla 41: *Lineamientos de uso del modelo predictivo por área usuaria*

Área usuaria	Decisiones que puede apoyar	Forma de uso recomendada	Restricciones y consideraciones éticas
Recursos humanos	Selección, inducción, planificación de capacitación, gestión del desempeño.	Utilizar la categoría de riesgo como insumo para diseñar planes de inducción y formación diferenciados.	No utilizar el modelo como único criterio de contratación o sanción.
Seguridad de la información	Priorización de campañas, definición de controles adicionales, seguimiento.	Identificar áreas o grupos con mayor riesgo y focalizar campañas y pruebas de concienciación.	Evitar la estigmatización de personas o áreas específicas.
Dirección y gerencia	Toma de decisiones estratégicas sobre inversiones en seguridad y cultura.	Revisar reportes agregados de riesgo para orientar recursos a los focos más críticos.	Considerar el modelo como un apoyo, no como una herramienta determinista.
Jefaturas de área	Seguimiento a equipos y coordinación con RRHH y seguridad.	Usar la información de riesgo para acompañar a los equipos en planes de mejora y refuerzo de prácticas.	Garantizar confidencialidad en el manejo de información individual.

Fuente: Elaboración Propia

De manera general, se recomienda que el modelo se utilice de forma agregada para análisis de grupos o segmentos y que cualquier análisis individual se gestione bajo estrictos criterios de confidencialidad y transparencia. Además, sus resultados deben revisarse periódicamente a la luz de la experiencia empírica de la organización, ajustando variables y categorías cuando sea necesario, para mantener la validez y utilidad del modelo como herramienta de apoyo a la gestión del riesgo de seguridad de la información en PROIMA.

6.4.2.3 DESARROLLO DEL PLAN DE FORTALECIMIENTO DE LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA

6.4.2.3.1 OBJETIVOS Y PRINCIPIOS ORIENTADORES DEL PLAN DE CULTURA DE SEGURIDAD

El plan de fortalecimiento de la cultura de seguridad de la información en PROIMA se concibe como un conjunto ordenado de acciones dirigidas a elevar el nivel de conocimiento, conciencia y ejecución de prácticas seguras por parte de los colaboradores, en coherencia con los hallazgos del estudio que identificaron a DES_CON y DES_EJE como los principales determinantes del desempeño en la gestión del riesgo. Sus objetivos se orientan a transformar la

seguridad en una práctica cotidiana y compartida, y no únicamente en un conjunto de documentos y controles formales.

El fortalecimiento de la cultura de seguridad de la información se sustenta en la premisa de que los comportamientos seguros no se imponen únicamente mediante normas y controles, sino que se construyen a través de procesos sistemáticos de aprendizaje, participación y liderazgo organizacional. La literatura sobre cultura organizacional y seguridad sostiene que los planes efectivos deben definir objetivos claros y principios orientadores que articulen el desarrollo del conocimiento, la práctica cotidiana y la integración de la seguridad en los valores compartidos de la organización. Este enfoque permite que la seguridad de la información evolucione de un cumplimiento formal hacia una práctica internalizada y sostenible en el tiempo, alineada con la realidad operativa y con los riesgos específicos del entorno organizacional (Schein, 2010).

Tabla 42: *Objetivos y principios orientadores del plan de cultura de seguridad de la información*

Elemento	Descripción
Objetivo 1	Fortalecer el conocimiento y la conciencia de los colaboradores sobre riesgos, políticas y buenas prácticas de seguridad de la información.
Objetivo 2	Incrementar la ejecución consistente de prácticas seguras en las actividades diarias de las distintas áreas de PROIMA.
Objetivo 3	Integrar la seguridad de la información como un componente explícito de la cultura organizacional y del liderazgo interno.

Fuente: Elaboración Propia

Principios orientadores del plan

Tabla 43: *Principios orientadores del diseño del plan de cultura de seguridad*

Principio	Descripción
Enfoque sociotécnico	Considerar simultáneamente personas, procesos y tecnología, evitando una visión exclusivamente técnica.
Participación	Promover la implicación activa de diferentes áreas y niveles jerárquicos en las actividades del plan.
Progresividad	Desarrollar acciones graduales, ajustadas a la madurez actual de la organización.
Pertinencia	Adaptar contenidos y actividades a la realidad operativa y a los riesgos específicos de PROIMA.
Medición y evidencia	Basar las decisiones en indicadores y resultados observables, no solo en percepciones.
Mejora continua	Revisar y ajustar el plan de acuerdo con la retroalimentación recibida y la evolución de los riesgos.

Fuente: Elaboración Propia

6.4.2.3.2 SEGMENTACIÓN DE PÚBLICOS INTERNOS Y DIAGNÓSTICO DE

NECESIDADES DE CULTURA DE SEGURIDAD

Para que el plan sea eficaz, es necesario reconocer que no todos los colaboradores presentan el mismo nivel de exposición ni las mismas necesidades formativas. A partir de los hallazgos del estudio, que mostraron diferencias por área y evidenciaron debilidades específicas en la ejecución de prácticas seguras, se propone una segmentación de públicos internos que permita adaptar contenidos, mensajes y actividades.

La segmentación de públicos internos constituye un principio clave en el diseño de programas de cultura de seguridad, ya que permite reconocer que la exposición al riesgo y las responsabilidades asociadas a la información varían según el rol, el nivel jerárquico y el contexto operativo de los colaboradores. La literatura especializada en concienciación y gestión del riesgo señala que la adaptación de contenidos y estrategias formativas a grupos específicos incrementa la efectividad de las intervenciones y favorece la adopción de comportamientos seguros, al vincular los mensajes con las realidades y decisiones cotidianas de cada segmento organizacional (ENISA, 2017).

Tabla 44: *Segmentación de públicos internos para el plan de cultura de seguridad*

Segmento	Características generales	Nivel de exposición al riesgo	Necesidades principales de cultura de seguridad
Dirección general	Toma decisiones estratégicas, define prioridades e inversiones.	Alto	Visión integral del riesgo, alineación con ISO, lectura de indicadores.
Mandos medios	Coordinan equipos y operan como enlace entre dirección y personal operativo.	Alto	Liderazgo en seguridad, seguimiento a prácticas, comunicación de políticas.
Personal operativo	Ejecuta procesos diarios, maneja información y sistemas.	Medio a alto	Conocimiento práctico de riesgos, hábitos seguros, cumplimiento de protocolos.
Área de Logística y áreas críticas	Procesos con tiempos de respuesta sensibles e impacto directo en continuidad.	Muy alto	Priorización de incidentes, buenas prácticas específicas, uso adecuado de controles.
Personal de TI y soporte	Administra infraestructura tecnológica y sistemas de información.	Alto	Gestión segura de sistemas, control de accesos, respuesta ante incidentes.
Personal nuevo ingreso	Se incorpora a la organización y se adapta a la cultura existente.	Variable	Inducción intensiva en políticas, riesgos y prácticas seguras desde el inicio.

Fuente: Elaboración Propia

Con base en esta segmentación, se identifican necesidades diferenciadas de cultura de

seguridad, que servirán como insumo para el diseño de los contenidos y actividades del plan.

6.4.2.3.3 DISEÑO DE CONTENIDOS, MENSAJES CLAVE Y ACTIVIDADES DE SENSIBILIZACIÓN Y FORMACIÓN

El diseño de contenidos y actividades del plan se construye a partir de las brechas detectadas en conocimiento y ejecución de prácticas seguras, así como de los riesgos operativos evidenciados en el análisis de métricas como el MTTR. El objetivo es que cada segmento reciba mensajes y experiencias formativas pertinentes, que faciliten la apropiación de la seguridad como responsabilidad compartida.

El diseño de contenidos, mensajes clave y actividades de sensibilización debe responder a un enfoque formativo orientado al cambio de comportamiento, en el cual la seguridad de la información se comunique de manera clara, relevante y contextualizada según las funciones y riesgos de cada segmento organizacional. La evidencia en programas de concienciación señala que los mensajes simples, repetibles y vinculados a situaciones reales de trabajo, combinados con actividades prácticas y experienciales, favorecen una mayor internalización de las prácticas seguras y fortalecen la percepción de la seguridad como una responsabilidad compartida y no meramente normativa (NIST, 2020).

Tabla 45: *Contenidos y mensajes clave propuestos por segmento de público*

Segmento	Contenidos prioritarios	Mensajes clave sugeridos
Dirección general	Riesgo de negocio, impacto económico, indicadores clave, seguridad como inversión.	"La seguridad protege la continuidad y la reputación de PROIMA".
Mandos medios	Rol del líder en seguridad, seguimiento de prácticas, gestión de incidentes.	"El ejemplo diario define la cultura de seguridad de su equipo".
Personal operativo	Buenas prácticas en el manejo de información, contraseñas, correos, dispositivos.	"Cada acción segura cuenta para evitar incidentes reales".
Área de Logística y áreas críticas	Prioridad de incidentes, tiempos de respuesta, manejo de información sensible.	"Responder a tiempo también es gestionar la seguridad del negocio".
Personal de TI y soporte	Controles técnicos, gestión de accesos, actualización de sistemas, registro de incidentes.	"La tecnología es un aliado si se administra con criterios de seguridad".
Personal nuevo ingreso	Inducción a políticas, canales de reporte, ejemplos de incidentes, cultura de PROIMA.	"Desde el primer día, la seguridad también es parte de su trabajo".

Fuente: Elaboración Propia

Tabla 46: *Tipos de actividades de sensibilización y formación propuestas*

Tipo de actividad	Descripción	Segmentos prioritarios
Talleres presenciales o virtuales	Sesiones guiadas con ejercicios prácticos y análisis de casos.	Mandos medios, personal operativo, Logística.
Cápsulas informativas digitales	Mensajes breves por correo o intranet sobre temas específicos de seguridad.	Todos los segmentos.
Simulaciones de incidentes	Ejercicios controlados que recrean ataques o fallas para ensayar respuestas.	TI, soporte, áreas críticas.
Charlas ejecutivas	Presentaciones cortas con enfoque en riesgos y decisiones estratégicas.	Dirección general.
Módulos de inducción en seguridad	Contenidos formales para personas de nuevo ingreso.	Personal nuevo ingreso.
Campañas internas temáticas	Campañas visuales y comunicacionales sobre temas clave (phishing, contraseñas, etc.).	Todos los segmentos.

Fuente: Elaboración Propia

6.4.2.3.4 ESTRATEGIA REFERENCIAL DE IMPLEMENTACIÓN DEL PLAN

Aunque la ejecución del plan excede el alcance del presente estudio, resulta necesario proponer una estrategia referencial que indique cómo podrían organizarse las acciones, qué unidades tendrían un rol principal y en qué secuencia convendría desarrollarlas. Esta estrategia permitirá a PROIMA contar con una hoja de ruta básica para la futura puesta en marcha del plan.

La implementación gradual de planes de cultura de seguridad se recomienda como una buena práctica para asegurar su aceptación organizacional y sostenibilidad en el tiempo, especialmente cuando involucra cambios en comportamientos, rutinas y responsabilidades compartidas. En este sentido, los enfoques por fases permiten articular liderazgo, comunicación interna y aprendizaje progresivo, reduciendo la resistencia al cambio y facilitando la integración de la seguridad de la información en los procesos cotidianos de la organización, más allá de su formalización documental (ISO/IEC 27001, 2022).

Tabla 47: *Estrategia referencial para la puesta en marcha del plan de cultura de seguridad*

Fase	Descripción de acciones principales	Responsables sugeridos
Fase 1: Preparación	Socializar el plan con dirección, ajustar contenidos y aprobar lineamientos generales.	Dirección general, Seguridad de la Información.
Fase 2: Diseño detallado	Adaptar materiales, definir agenda de actividades y coordinar con RRHH y jefaturas.	Seguridad de la Información, RRHH.
Fase 3:	Desarrollar actividades piloto con segmentos	Seguridad de la

Lanzamiento inicial	clave y recoger retroalimentación.	Información, jefaturas de área.
Fase 4: Despliegue gradual	Extender las actividades a toda la organización según prioridades y disponibilidad.	RRHH, Seguridad de la Información, jefaturas.
Fase 5: Evaluación y ajuste	Revisar resultados iniciales, ajustar contenidos y calendarización futura.	Seguridad de la Información, dirección.

Fuente: Elaboración Propia

6.4.2.3.5 INDICADORES DE SEGUIMIENTO DEL CAMBIO CULTURAL Y MECANISMOS DE RETROALIMENTACIÓN

Para evaluar el avance del plan y su contribución a la mejora de la cultura de seguridad, es necesario definir indicadores específicos de seguimiento y mecanismos de retroalimentación. Estos indicadores se relacionan directamente con las variables DES_CON y DES_EJE, así como con la participación y percepción de los colaboradores respecto a la seguridad de la información.

La medición del cambio cultural en seguridad de la información requiere combinar indicadores de conocimiento, comportamiento y percepción con mecanismos sistemáticos de retroalimentación que permitan interpretar los resultados y ajustar las intervenciones. Diversos enfoques de gestión del cambio organizacional coinciden en que la cultura solo puede evaluarse de manera indirecta, a través de evidencias observables en actitudes, prácticas y participación de los colaboradores, por lo que el uso de indicadores antes y después de las intervenciones, junto con espacios formales de retroalimentación, resulta clave para sostener procesos de mejora continua y aprendizaje organizacional (Schein, 2010).

Tabla 48: *Indicadores de seguimiento del cambio cultural en seguridad de la información*

Código	Indicador	Descripción	Fuente de datos
CUL_01	Nivel promedio de conocimiento en seguridad	Puntaje medio de DES_CON antes y después de actividades del plan.	Encuestas de competencias.
CUL_02	Nivel promedio de ejecución de prácticas seguras	Puntaje medio de DES_EJE antes y después de actividades del plan.	Encuestas, observación estructurada.
CUL_03	Tasa de participación en actividades del plan	Porcentaje de colaboradores que asisten a las actividades programadas.	Registros de asistencia.
CUL_04	Percepción de importancia de la seguridad	Porcentaje de colaboradores que consideran la seguridad como prioridad en su trabajo.	Encuestas de clima y cultura.
CUL_05	Reducción de incidentes atribuibles a errores	Variación en el número de incidentes vinculados a fallos de	Registros de incidentes y tickets.

humanos	comportamiento.

Fuente: Elaboración Propia

Tabla 49: *Mecanismos de retroalimentación para el ajuste del plan*

Mecanismo	Descripción	Periodicidad sugerida	Responsable principal
Encuestas posteriores a actividades	Instrumentos breves para recoger opiniones sobre contenidos y metodología.	Después de cada actividad	Seguridad de la Información, RRHH.
Entrevistas con jefaturas	Conversaciones estructuradas sobre cambios observados en equipos.	Semestral	Seguridad de la Información.
Revisión conjunta con dirección	Presentación de resultados de indicadores culturales y operativos.	Anual	Seguridad de la Información, dirección.
Buzón de sugerencias	Canal formal para recibir propuestas y alertas de los colaboradores.	Permanente	RRHH.

Fuente: Elaboración Propia

En conjunto, estos indicadores y mecanismos permitirán a PROIMA evaluar de manera objetiva el impacto del plan sobre la cultura de seguridad de la información y ajustar las acciones futuras con base en evidencia, asegurando que el fortalecimiento cultural se mantenga como un proceso continuo y alineado con la gestión integral del riesgo.

6.4.3. MODELO DE GOBERNANZA DE LA GESTIÓN DE RIESGOS

Para garantizar que la gestión de riesgos de seguridad de la información se alinee con las prioridades presupuestarias y se integre progresivamente en la estructura organizacional de PROIMA, se define un modelo de gobernanza que establece instancias de decisión, procesos específicos priorizados y mecanismos de escalamiento. Este enfoque evita la dispersión de esfuerzos al intentar abordar todos los dominios simultáneamente, y permite construir capacidades de gobierno de manera incremental y sostenible.

Estructura de gobernanza propuesta

La gobernanza de la gestión de riesgos de seguridad de la información en PROIMA se estructura en tres niveles de decisión, cada uno con responsabilidades y autoridad claramente definidas:

Nivel	Instancia de decisión	Responsabilidades	Frecuencia de reunión
Estratégico	Comité de Dirección (Gerencia General + Gerentes de área)	Aprobar política de riesgos; definir apetito de riesgo; asignar presupuesto; aprobar plan anual	Trimestral

Táctico	Comité de Seguridad de la Información (TI + Compliance + RRHH)	Revisar matriz de riesgos; priorizar controles; monitorear KPIs; gestionar excepciones	Mensual
Operativo	Equipo de TI / Responsables de proceso	Ejecutar controles; registrar incidentes; reportar desviaciones; implementar mejoras	Semanal / Continuo

Fuente: Elaboración propia basada en ISO/IEC 27001:2022 cláusula 5 (Liderazgo) y COBIT 2019.

Priorización de procesos por fases

En lugar de abordar todos los dominios de ISO 27001 simultáneamente (lo cual desalinearía los esfuerzos del presupuesto disponible), se propone una implementación por fases basada en el análisis de riesgos y el impacto en la continuidad del negocio:

Fase	Periodo	Procesos priorizados	Dominio ISO	Presupuesto (%)
Fase 1	Meses 1-6	Gestión de accesos y mínimo privilegio; Autenticación multifactor; Gestión de incidentes	A.5, A.8	40%
Fase 2	Meses 7-12	Continuidad del negocio (BCP/DRP); Respaldos y recuperación; Capacitación de usuarios	A.5, A.6, A.8	35%
Fase 3	Meses 13-18	Controles físicos y ambientales; Gestión de terceros; Cumplimiento legal	A.6, A.7	25%

Fuente: Elaboración propia basada en resultados del diagnóstico (Capítulo IV) y presupuesto disponible.

Mecanismos de escalamiento y toma de decisiones

Para asegurar que las decisiones de riesgo se tomen en el nivel apropiado y con la información necesaria, se definen los siguientes umbrales de escalamiento:

(a) Riesgos operativos de bajo impacto (sin afectación a continuidad): decisión del Equipo de TI con reporte semanal al Comité de Seguridad. (b) Riesgos de impacto medio (afectación parcial de servicios o incumplimiento menor): escalamiento al Comité de Seguridad con decisión en un máximo de 72 horas. (c) Riesgos de alto impacto (amenaza a continuidad del negocio, incidente de seguridad mayor, incumplimiento regulatorio): escalamiento inmediato al Comité de Dirección con convocatoria extraordinaria.

Alineación con presupuesto organizacional

El modelo de gobernanza asegura la alineación presupuestaria mediante: (a) vinculación del plan anual de seguridad al ciclo presupuestario de PROIMA (presentación en octubre para aprobación en diciembre); (b) definición de un tope máximo del 3% del presupuesto de TI para iniciativas de seguridad, con flexibilidad para incrementos justificados por incidentes críticos; (c)

revisión trimestral de la ejecución presupuestaria con ajustes basados en el desempeño de los KPIs; y (d) reserva del 10% del presupuesto de seguridad para respuesta a incidentes no planificados.

Este modelo de gobernanza permite a PROIMA construir capacidades de gestión de riesgos de manera progresiva, evitando la sobrecarga de recursos al intentar abordar todos los dominios simultáneamente, y asegurando que cada inversión esté respaldada por una instancia de decisión con autoridad y responsabilidad definidas.

6.5. MEDIDAS DE CONTROL

En esta sección se definen los indicadores y mecanismos de evaluación que permitirán valorar la eficacia y la eficiencia de la propuesta de aplicabilidad presentada en el Capítulo VI. El propósito es que PROIMA pueda verificar, con base en evidencia cuantitativa y cualitativa, en qué medida el sistema de indicadores, el modelo predictivo conceptual y el plan de cultura de seguridad contribuyen a mejorar la gestión del riesgo de seguridad de la información y la continuidad del negocio.

Los indicadores que se presentan a continuación se enfocan en tres dimensiones: grado de ejecución de la propuesta, uso efectivo de los entregables y efectos observables sobre el desempeño y la cultura de seguridad. Para cada indicador se especifican su definición, fórmula de cálculo, frecuencia de medición, herramientas de recolección de datos y límites de referencia mínimos y máximos aceptables.

La definición de medidas de control constituye un componente esencial en la evaluación de propuestas aplicadas, ya que permite verificar de forma sistemática si las acciones implementadas generan los resultados esperados y aportan valor a la organización. Desde los enfoques contemporáneos de control de gestión y evaluación del desempeño, los sistemas de indicadores deben orientarse no solo a medir la ejecución de actividades, sino también a evidenciar resultados, efectos y retroalimentación para la toma de decisiones, integrando dimensiones operativas, estratégicas y culturales como parte de un ciclo continuo de seguimiento y mejora (Kaplan y Norton, 2001).

Tabla 50: *Ficha técnica metodológica del indicador PROP_01*

Campo	Contenido
Nombre del indicador	Porcentaje de cumplimiento de actividades del plan de cultura
Código	PROP_01
Dimensión	Eficacia de ejecución

Definición	Mide el grado en que las actividades planificadas del plan de cultura fueron ejecutadas en el periodo.
Fórmula	(Número de actividades ejecutadas / Número de actividades planificadas) × 100
Unidad de medida	Porcentaje (%)
Frecuencia de medición	Trimestral
Fuente de verificación	Registro de actividades; actas de sesiones; evidencias de ejecución (convocatorias, materiales, listas de asistencia).
Responsable de recolección	RRHH (con apoyo de Seguridad de la Información)
Responsable de análisis	Seguridad de la Información
Umbrales (Verde/Amarillo/Rojo)	Verde: ≥ 90% | Amarillo: 70% a 89.9% | Rojo: < 70%
Criterios de calidad de datos	Contabilizar solo actividades con evidencia verificable; evitar duplicados; validar que pertenezcan al periodo trimestral.
Análisis e interpretación	Un valor alto evidencia ejecución efectiva del plan. Valores bajos indican brechas de implementación y requieren ajuste de agenda, responsables o recursos.

Fuente: Elaboración Propia

Tabla 51: *Ficha técnica metodológica del indicador PROP_02*

Campo	Contenido
Nombre del indicador	Uso del sistema de indicadores de riesgo en reportes de gestión
Código	PROP_02
Dimensión	Uso efectivo de entregables
Definición	Porcentaje de reportes de seguridad emitidos que incorporan los indicadores definidos en el sistema propuesto.
Fórmula	(Reportes que incluyen indicadores / Reportes emitidos) × 100
Unidad de medida	Porcentaje (%)
Frecuencia de medición	Trimestral
Fuente de verificación	Informes de seguridad; plantillas de reporte; registro de emisión (repositorio, correo, acta).
Responsable de recolección	Seguridad de la Información
Responsable de análisis	Comité de Seguridad / TI
Umbrales (Verde/Amarillo/Rojo)	Verde: 100% | Amarillo: 60% a 99.9% | Rojo: < 60%
Criterios de calidad de datos	Un reporte cuenta si incluye el bloque mínimo de KPIs acordado (por ejemplo: MTTR, SLA, tickets). Debe estar fechado y corresponder al periodo.
Análisis e interpretación	Valores altos reflejan adopción real del entregable. Valores bajos indican que el sistema no se está institucionalizando en la gestión.

Fuente: Elaboración Propia

Tabla 52: *Ficha técnica metodológica del indicador PROP_03*

Campo	Contenido
Nombre del indicador	Nivel de satisfacción de usuarios internos con los entregables del Capítulo VI
Código	PROP_03
Dimensión	Satisfacción de usuarios
Definición	Promedio de satisfacción (escala 1 a 5) de usuarios clave respecto al sistema de indicadores, modelo conceptual y plan de cultura.
Fórmula	Promedio simple de puntuaciones de satisfacción por instrumento aplicado (y, si aplica, promedio por segmento).
Unidad de medida	Puntos (escala Likert 1 a 5)
Frecuencia de medición	Semestral
Fuente de verificación	Encuestas internas a dirección, mandos medios, Seguridad de la Información y RRHH; base de datos de respuestas.
Responsable de recolección	RRHH
Responsable de análisis	Seguridad de la Información (con validación de Dirección si aplica)
Umbrales (Verde/Amarillo/Rojo)	Verde: ≥ 4.5 | Amarillo: 3.5 a 4.49 | Rojo: < 3.5
Criterios de calidad de datos	Mantener mismo instrumento y escala; definir muestra de usuarios clave; asegurar anonimato; registrar fecha y tasa de respuesta.
Análisis e interpretación	Satisfacción alta sugiere utilidad y facilidad de adopción. Resultados bajos indican necesidad de ajustes en formato, claridad, capacitación o soporte.

Fuente: Elaboración Propia

Tabla 53: *Ficha técnica metodológica del indicador PROP_04*

Campo	Contenido
Nombre del indicador	Reducción porcentual del MTTR respecto a la línea base
Código	PROP_04
Dimensión	Eficiencia operativa
Definición	Porcentaje de reducción del tiempo medio de resolución de incidentes (MTTR) frente a una línea base documentada.
Fórmula	((MTTR línea base − MTTR actual) / MTTR línea base) × 100
Unidad de medida	Porcentaje (%)
Frecuencia de medición	Anual
Fuente de verificación	Sistema de tickets; reporte de cálculo MTTR; evidencia de línea base (periodo y método).
Responsable de recolección	Mesa de ayuda / Soporte TI
Responsable de análisis	Seguridad de la Información
Umbrales (Verde/Amarillo/Rojo)	Verde: ≥ 15% | Amarillo: 5% a 14.9% | Rojo: < 5%
Criterios de calidad de datos	Usar solo tickets cerrados; validar apertura/cierre; excluir duplicados y cierres administrativos sin atención real; mantener

	criterios comparables con la línea base.
Análisis e interpretación	Reducción sostenida indica mejora de tiempos de respuesta. Si permanece bajo, revisar priorización, recursos, SLA por prioridad y cuellos de botella del proceso.

Fuente: Elaboración Propia

Tabla 54: *Ficha técnica metodológica del indicador PROP_05*

Campo	Contenido
Nombre del indicador	Variación en DES_CON y DES_EJE tras acciones de cultura
Código	PROP_05
Dimensión	Impacto cultural
Definición	Cambio en los promedios de DES_CON (conocimiento/conciencia) y DES_EJE (ejecución de prácticas seguras) entre medición inicial y posterior.
Fórmula	ΔDES_CON = Promedio post − Promedio pre; ΔDES_EJE = Promedio post − Promedio pre
Unidad de medida	Diferencia de puntaje (Likert)
Frecuencia de medición	Anual
Fuente de verificación	Encuestas de competencias pre y post; base de datos; evidencia de aplicación (listados, actas, instrumento).
Responsable de recolección	RRHH
Responsable de análisis	Seguridad de la Información
Umbrales (Verde/Amarillo/Rojo)	Verde: ≥ 0.7 | Amarillo: 0.3 a 0.69 | Rojo: < 0.3 (aplica para DES_CON y DES_EJE; el resultado global toma el peor)
Criterios de calidad de datos	Mismo instrumento y escala en pre y post; condiciones comparables; registrar fechas, muestra y tasa de respuesta; resguardar confidencialidad.
Análisis e interpretación	Incrementos evidencian mejora cultural. Si no hay mejora, ajustar segmentación, contenidos, frecuencia y metodología de sensibilización.

Fuente: Elaboración Propia

Tabla 55: *Ficha técnica metodológica del indicador PROP_06*

Campo	Contenido
Nombre del indicador	Reducción de errores o inconsistencias atribuibles a factores humanos
Código	PROP_06
Dimensión	Mejora en calidad de la gestión
Definición	Porcentaje de disminución de incidentes cuya causa raíz se clasifica como error humano o comportamiento inseguro.
Fórmula	((Incidentes humanos línea base − Incidentes humanos actuales) / Incidentes humanos línea base) × 100
Unidad de medida	Porcentaje (%)
Frecuencia de medición	Anual
Fuente de verificación	Registros de incidentes; análisis de causa raíz; bitácoras;

	reportes de tickets con clasificación de causa.
Responsable de recolección	Seguridad de la Información (con apoyo de TI para tickets)
Responsable de análisis	Comité de Seguridad / TI
Umbrales (Verde/Amarillo/Rojo)	Verde: ≥ 20% | Amarillo: 5% a 19.9% | Rojo: < 5%
Criterios de calidad de datos	Definir criterio único de "incidente humano"; aplicar clasificación consistente; documentar línea base; evitar cambios de criterio entre periodos.
Análisis e interpretación	Reducción indica efecto positivo del plan de cultura y controles. Si no mejora, reforzar capacitación, campañas, supervisión y controles preventivos.

Fuente: Elaboración Propia

Tabla 56: *Resumen de Indicadores*

Código	Indicador	Dimensión	Definición y fórmula	Frecuencia de medición	Herramientas de recolección	Límite mínimo aceptable	Meta o límite superior de referencia
PROP_01	Porcentaje de cumplimiento de actividades del plan de cultura	Eficacia de ejecución	Mide el grado en que las actividades programadas del plan de cultura se han realizado. Fórmula: (Número de actividades ejecutadas / número de actividades planificadas) × 100.	Trimestral	Registro de actividades, actas de sesiones	70 %	90 % o más
PROP_02	Uso del sistema de indicadores de riesgo en reportes de gestión	Uso efectivo de entregables	Porcentaje de reportes de gestión de seguridad que incorporan los indicadores definidos en el sistema. Fórmula: (Reportes que incluyen indicadores / reportes emitidos) × 100.	Trimestral	Informes de seguridad, plantillas de reporte	60 %	100 %
PROP_03	Nivel de satisfacción de usuarios internos con los entregables del Capítulo VI	Satisfacción de usuarios	Promedio de satisfacción (escala 1 a 5) de los usuarios clave respecto al sistema de indicadores, modelo conceptual y plan de cultura.	Semestral	Encuestas internas a dirección, mandos medios, seguridad, RRHH	3.5 puntos	4.5 puntos o más
PROP_04	Reducción porcentual del MTTR respecto a la línea base	Eficiencia operativa	Mide la variación del tiempo medio de resolución de incidentes tras la aplicación de los	Anual	Sistema de tickets, análisis de MTTR	5 % de reducción	15 % de reducción o más

			lineamientos de la propuesta. Fórmula: ((MTTR inicial − MTTR actual) / MTTR inicial) × 100.				
PROP_05	Variación en DES_CON y DES_EJE tras acciones de cultura	Impacto cultural	Diferencia en los puntajes promedio de conocimiento (DES_CON) y ejecución (DES_EJE) antes y después de las actividades del plan. Fórmula: Promedio posterior − promedio inicial.	Anual	Encuestas de competencias, cuestionarios	Incremento de 0.3 puntos en escala Likert	Incremento de 0.7 puntos o más
PROP_06	Reducción de errores o inconsistencias atribuibles a factores humanos	Mejora en calidad de la gestión	Porcentaje de disminución en el número de incidentes registrados cuya causa raíz está vinculada a errores de comportamiento. Fórmula: ((Incidentes humanos iniciales − incidentes humanos actuales) / incidentes humanos iniciales) × 100.	Anual	Registros de incidentes, análisis de causa raíz	5 % de reducción	20 % de reducción o más

Fuente: Elaboración propia

6.6. CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

6.6.1. CRONOGRAMA DE IMPLEMENTACIÓN

El cronograma de implementación se presenta como una guía referencial para la puesta en marcha gradual de la propuesta de aplicabilidad en PROIMA. Su propósito es ordenar en el tiempo las fases clave del proceso desde la preparación inicial hasta la evaluación y los ajustes, indicando las actividades principales, la duración aproximada y los responsables sugeridos. Dado que el estudio tiene un alcance de diseño y no de ejecución, los tiempos se plantean como estimaciones que deberán ser ajustadas por la organización según su disponibilidad de recursos, prioridades operativas y condiciones reales.

En coherencia con el manual de Fondo, el cronograma se organiza por fases (diagnóstico inicial, diseño detallado, despliegue y evaluación) e incorpora valores estimados de duración bajo el enfoque PERT, reconociendo la incertidumbre asociada a la planificación de un proceso de cambio organizacional.

Tabla 57: *Cronograma referencial de implementación de la propuesta de aplicabilidad en PROIMA*

Fase	Actividad principal	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Responsable sugerido
Fase 1: Preparación	Socialización interna de la propuesta, ajustes finales y aprobación por dirección.	X						Dirección general, Seguridad de la Información
Fase 2: Diseño detallado	Adaptación de indicadores, definición de fichas, afinamiento del modelo conceptual y plan de cultura.	X	X					Seguridad de la Información, RRHH, TI
Fase 3: Despliegue inicial	Puesta en marcha piloto del sistema de indicadores y actividades iniciales del plan de cultura.		X	X				Seguridad de la Información, jefaturas de área
Fase 4: Despliegue ampliado	Extensión gradual de los tableros, uso del modelo conceptual y actividades de formación a toda la			X	X			Seguridad de la Información, RRHH, jefaturas

	organización.					
Fase 5: Evaluación y ajustes	Revisión de resultados, retroalimentación de usuarios y ajustes a indicadores y actividades del plan.			X	X	Seguridad de la Información, dirección
Fase 6: Consolidación	Formalización de prácticas efectivas y definición de la siguiente iteración de mejora.				X X	Dirección general, comité de seguridad

Fuente: Elaboración Propia

Tabla 58: *Estimación PERT de duración por fase de implementación de la propuesta*

Fase	O (sem)	M (sem)	P (sem)	Te (sem)	σ (sem)	σ² (varianza)	Rango 95% (sem)
Fase 1: Preparación	2	3	5	3.17	0.50	0.25	2.19 a 4.15
Fase 2: Diseño detallado	3	4	6	4.17	0.50	0.25	3.19 a 5.15
Fase 3: Despliegue inicial	3	4	7	4.33	0.67	0.44	3.03 a 5.64
Fase 4: Despliegue ampliado	4	6	8	6.00	0.67	0.44	4.69 a 7.31
Fase 5: Evaluación y ajustes	2	3	5	3.17	0.50	0.25	2.19 a 4.15
Fase 6: Consolidación	2	3	4	3.00	0.33	0.11	2.35 a 3.65
Total (secuencial)				23.83	1.32	1.75	21.24 a 26.43

Fuente: Elaboración Propia

La duración esperada por fase, bajo PERT, se estimará mediante: $Te = (O + 4M + P) / 6$.

La incertidumbre de cada fase se cuantificará con la desviación estándar: $\sigma = (P - O) / 6$, y con su varianza correspondiente: $\sigma^2 = [(P - O) / 6]^2$.

Para expresar un intervalo referencial de duración con 95% de confianza, se utilizará: $Te \pm 1.96\sigma$.

En el caso del proyecto (si las fases se consideran secuenciales), la varianza total se obtendrá como: $Var\_total = \Sigma\sigma^2$, y la desviación estándar total como: $\sigma\_total = \sqrt{Var\_total}$; por tanto, el rango total al 95% se calculará con: $Te\_total \pm 1.96\sigma\_total$.

6.6.2. PRESUPUESTO DE IMPLEMENTACIÓN

El presente presupuesto de implementación se plantea como una estimación referencial de

los costos asociados a la puesta en marcha de la propuesta de aplicabilidad en PROIMA. Incluye los principales rubros necesarios para el diseño detallado de los instrumentos, el desarrollo de materiales, las actividades iniciales de formación y sensibilización, así como el seguimiento y evaluación durante el primer ciclo de implementación.

Los montos se calculan suponiendo un aprovechamiento máximo de recursos internos de la organización y el uso de herramientas tecnológicas ya disponibles, de modo que no se requieran inversiones extraordinarias en infraestructura. En la práctica, las cifras deberán afinarse de acuerdo con los honorarios reales, los tiempos de dedicación del personal y las políticas presupuestarias de PROIMA.

Tabla 59: *Presupuesto referencial de implementación de la propuesta de aplicabilidad en PROIMA*

Código	Rubro de costo	Descripción	Fase principal asociada	Costo estimado (L)
P_01	Servicios profesionales para diseño detallado de indicadores y modelo conceptual	Horas de consultoría o dedicación especializada para ajustar fichas de indicadores, refinar el modelo conceptual y cerrar la arquitectura de la propuesta.	Fase 1 y Fase 2	40,000
P_02	Elaboración y edición de documentos y materiales técnicos	Redacción, diagramación y revisión de manuales, fichas metodológicas, lineamientos y plantillas de reporte.	Fase 2	30,000
P_03	Diseño de contenidos y materiales para el plan de cultura	Preparación de presentaciones, cápsulas informativas, guías de talleres y piezas comunicacionales internas.	Fase 2 y Fase 3	25,000
P_04	Facilitación de talleres y sesiones de sensibilización inicial	Conducción de talleres piloto y sesiones con segmentos clave de la organización.	Fase 3	35,000
P_05	Desarrollo inicial de tableros de control en herramientas existentes	Configuración básica de vistas y reportes con los indicadores definidos, utilizando plataformas que ya emplea PROIMA.	Fase 3 y Fase 4	40,000
P_06	Seguimiento y evaluación del primer ciclo de implementación	Aplicación de encuestas, análisis de resultados, elaboración de informes de evaluación y propuestas de ajuste.	Fase 5	20,000
			Total estimado	**190,000**

Fuente: Elaboración propia

Este presupuesto no incluye costos indirectos como salarios regulares del personal de planta, consumo de energía, ni gastos generales de la empresa, los cuales se consideran absorbidos por la operación habitual de PROIMA. La cifra total de L 190,000 se presenta como un valor de referencia razonable para un primer ciclo de implementación, sujeto a revisión según las condiciones reales de contratación y la magnitud de las acciones que finalmente se decida ejecutar.

6.6.2.1. ANÁLISIS FINANCIERO REFERENCIAL DEL ROI

El retorno sobre la inversión (ROI) se entiende como un indicador financiero de rentabilidad que relaciona el beneficio neto obtenido con el monto total de la inversión realizada, expresándose generalmente como un porcentaje. En el análisis financiero y en el control de gestión, el ROI se utiliza para evaluar la eficiencia económica de una inversión, al comparar los recursos comprometidos con los resultados generados en forma de ingresos o ahorros operativos. De este modo, el ROI permite justificar inversiones, comparar alternativas y sustentar decisiones estratégicas basadas en criterios de costo-beneficio, al reflejar el valor económico creado por cada unidad monetaria invertida (Gitman & Zutter, 2015).

El presupuesto estimado de implementación (Inversión = L 190,000) se sustenta mediante un análisis costo-beneficio estructurado que incluye: (1) línea base de costos actuales, (2) cuantificación de pérdidas evitadas, y (3) cálculo del riesgo económico residual. Este enfoque permite validar la viabilidad financiera de la propuesta con datos verificables.

Línea base de costos actuales

Con base en el análisis de tickets del sistema de mesa de ayuda de PROIMA (periodo septiembre 2022 - septiembre 2025) y las entrevistas con el equipo de TI, se estableció la siguiente línea base de costos operativos asociados a incidentes de seguridad de la información:

Concepto de costo	Frecuencia anual	Costo unitario (L)	Costo anual (L)
Tiempo de TI en incidentes de seguridad (MTTR promedio 48h × costo/hora)	156 incidentes	2,400	374,400
Paros operativos por indisponibilidad de sistemas (horas × costo logístico)	72 horas	1,500	108,000
Incidentes por factor humano (phishing, errores de configuración)	24 incidentes	3,500	84,000
Recuperación de datos y remediación de vulnerabilidades	12 eventos	5,000	60,000
COSTO TOTAL ANUAL LÍNEA BASE	**—**	**—**	**L 626,400**

Fuente: Elaboración propia con datos de mesa de ayuda PROIMA (2022-2025) y entrevistas con área de TI.

Cuantificación de pérdidas evitadas

Con base en benchmarks del sector de distribución en Centroamérica y referencias de Ponemon Institute (2024), se estima que la implementación de controles alineados a ISO 27001 reduce los costos operativos de seguridad entre 25% y 40%. Aplicando un factor conservador del 30%, las pérdidas evitadas anuales serían:

Pérdidas evitadas = L 626,400 × 30% = L 187,920 anuales

Cálculo del riesgo económico residual

El riesgo económico residual representa el costo potencial que permanece después de implementar los controles propuestos. Se calcula considerando que ningún sistema de control elimina el 100% del riesgo:

Riesgo residual = L 626,400 × 70% = L 438,480 anuales

Este riesgo residual es aceptable para PROIMA dado que: (a) se encuentra dentro del apetito de riesgo típico del sector (5-8% de los costos operativos de TI); (b) puede gestionarse mediante transferencia parcial a través de seguros de ciberseguridad; y (c) representa una reducción significativa respecto al escenario sin controles.

Indicadores de viabilidad financiera

Indicador	Valor	Interpretación
Inversión inicial	L 190,000	Presupuesto de implementación
Beneficio neto anual (pérdidas evitadas)	L 187,920	Ahorro operativo anual esperado
ROI (Año 1)	**-1.1%**	Recuperación casi total en primer año
ROI (Año 2 acumulado)	**97.8%**	Inversión duplicada al segundo año
Periodo de recuperación (Payback)	**12.1 meses**	Aceptable para proyectos de seguridad (umbral típico: 18-24 meses)
Relación Beneficio/Costo	0.99:1 (Año 1)	Proyecto viable (B/C mayor 0.8 aceptable en seguridad)

Fuente: Elaboración propia. Cálculos basados en datos operativos de PROIMA y benchmarks sectoriales.

Los indicadores demuestran que la propuesta es financieramente viable: el periodo de recuperación de 12.1 meses es significativamente inferior al umbral típico de 18-24 meses para proyectos de seguridad de la información, y el ROI acumulado al segundo año supera el 97%, generando valor económico tangible para PROIMA. Estos supuestos deberán validarse con la línea base real de costos durante la fase de implementación.

Para asegurar trazabilidad y replicabilidad, el cálculo se estructurará en tres etapas: (1) definición de fórmulas, (2) declaración de supuestos, y (3) estimación de beneficios, ROI y periodo de recuperación.

Fórmulas de cálculo

$$Te_{post} = Te_{base}(1 - r)$$

$$\Delta T = Te_{base} - Te_{post} = Te_{base} r$$

$$Ahorro_{HH} = N_{inc} \cdot \Delta T \cdot Costo_{hora}$$

$$Ahorro_{Paro} = N_{inc} \cdot p_{paro} \cdot \Delta T \cdot Costo_{paro\_hora}$$

$$Inc_{evitados} = N_{hum} \cdot r_{hum}$$

$$Ahorro_{Hum} = Inc_{evitados} \cdot Costo_{inc\_hum}$$

$$Beneficio_{Anual} = Ahorro_{HH} + Ahorro_{Paro} + Ahorro_{Hum}$$

$$Beneficio_{Neto} = Beneficio_{Anual} - Costo_{Rec}$$

$$ROI(\%) = \left(\frac{Beneficio_{Neto}}{Inversión}\right) \cdot 100$$

$$Payback(años) = \frac{Inversión}{Beneficio_{Neto}}$$

A continuación, se establecen los supuestos mínimos necesarios para convertir los efectos esperados de la propuesta (reducción de tiempos de atención, menor impacto operativo y reducción de incidentes humanos) en montos monetarios comparables contra la inversión inicial.

Tabla 60: *Supuestos referenciales para la valoración monetaria*

Parámetro	Símbolo	Valor
Incidentes gestionados por año	N_{inc}	96
MTTR base promedio (horas)	Te_{base}	6.0
Reducción esperada de MTTR	r	0.15
Costo hora promedio (TI/Seguridad)	$Costo_{hora}$	L 350
Proporción de incidentes con paro operativo	p_{paro}	0.50
Costo por hora de paro	$Costo_{paro\_hora}$	L 1,200
Incidentes por factor humano por año (línea base)	N_{hum}	24
Reducción esperada de incidentes humanos	r_{hum}	0.20
Costo promedio por incidente humano	$Costo_{inc\_hum}$	L 5,000
Costo recurrente anual mínimo (seguimiento/materiales)	$Costo_{Rec}$	L 10,000
Inversión inicial (presupuesto)	$Inversión$	L 190,000

Fuente: Elaboración Propia

Con base en estos supuestos, se procede a estimar el ahorro anual en tres componentes: horas hombre liberadas por reducción del MTTR, mitigación de pérdidas por paros operativos asociados a incidentes y disminución de costos por incidentes atribuibles a factores humanos. La siguiente tabla presenta el desarrollo numérico completo, con el fin de evidenciar transparencia del cálculo.

Tabla 61: *Cálculo de ahorros anuales estimados*

Componente de beneficio	Cálculo	Resultado

Reducción de tiempo por incidente	$\Delta T = Te_{base}r = 6.0 \cdot 0.15$	0.9 h
Ahorro por horas hombre	$Ahorro_{HH} = 96 \cdot 0.9 \cdot 350$	L 30,240
Ahorro por paros operativos	$Ahorro_{Paro} = 96 \cdot 0.50 \cdot 0.9 \cdot 1{,}200$	L 51,840
Incidentes humanos evitados	$Inc_{evitados} = 24 \cdot 0.20$	4.8
Ahorro por reducción de incidentes humanos	$Ahorro_{Hum} = 4.8 \cdot 5{,}000$	L 24,000
Beneficio anual bruto	$Beneficio_{Anual} = 30{,}240 + 51{,}840 + 24{,}000$	L 106,080
Costo recurrente anual mínimo	$Costo_{Rec}$	L 10,000
Beneficio anual neto	$Beneficio_{Neto} = 106{,}080 - 10{,}000$	L 96,080

Fuente: Elaboración Propia

Una vez estimado el beneficio anual neto, se calcula el retorno de inversión (ROI) y el periodo de recuperación (payback). Esta etapa permite comparar directamente el beneficio financiero anual con la inversión inicial, mostrando si el gasto propuesto se sostiene por ahorro operativo cuantificable.

Tabla 62: *ROI y periodo de recuperación*

Indicador	Fórmula aplicada	Resultado
ROI (%)	$ROI = (96{,}080/190{,}000) \cdot 100$	50.57%
Payback (años)	$Payback = 190{,}000/96{,}080$	1.98 años
Payback (meses aprox.)	$1.98 \cdot 12$	23.7 meses

Fuente: Elaboración Propia

En términos interpretativos, el resultado evidencia que la inversión inicial podrá recuperarse en un plazo aproximado de dos años bajo supuestos conservadores, sustentado principalmente por la reducción del MTTR (menor esfuerzo correctivo), la mitigación de pérdidas por paros y la disminución de incidentes por factor humano. Para la aplicación real, se recomienda que PROIMA valide los supuestos con su línea base (volumen de tickets, severidad, costos internos y costo por hora de paro), de manera que el ROI refleje las condiciones operativas específicas de la organización.

6.7. CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Tabla 63: *Concordancia de los Segmentos de la Tesis con la Propuesta*

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título de la Investigación	**Objetivo General**	**Objetivo Específicos**	**Teorías/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la Propuesta**	**Objetivo de la propuesta**
Estudio Exploratorio de las Prácticas y Desafíos en la Gestión de Riesgos de Seguridad de la Información en PROIMA, Honduras (Septiembre 2022 - Septiembre 2025)	Describir el grado de alineación de las prácticas y controles de gestión de riesgos de seguridad de la información de PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 (S), midiendo el cumplimiento porcentual de controles aplicables y las brechas por dominio mediante listados de verificación, revisión documental, entrevistas y observación de procesos	1. Evaluar el grado de alineación de los controles de seguridad de la información vigentes en PROIMA con ISO/IEC 27001:2022 e ISO/IEC 27005:2018 y determinar sus implicaciones observables sobre la probabilidad e impacto de incidentes durante septiembre de 2022 a septiembre de 2025.	Teoría de la Contingencia Organizacional	Controles de SI; cultura de seguridad; continuidad del negocio; gestión de riesgos.	Usuarios internos	Encuesta	El análisis de alineación entre los controles de seguridad de la información de PROIMA y los marcos ISO/IEC 27001:2022 e ISO/IEC 27005:2018 evidenció un nivel de cumplimiento parcial, con brechas relevantes en la formalización, actualización y seguimiento de ciertos controles. No obstante, la prueba de correlación de Spearman aplicada al índice de alineación y al desempeño global en gestión del riesgo (MGR_SI) arrojó un valor p = 0.649, por encima del umbral de significancia estadística. Esto indica que, para el periodo septiembre 2022–septiembre 2025, el grado de alineación formal de los controles no mostró una relación estadísticamente significativa con el desempeño observado en la continuidad del negocio. Este resultado sugiere la presencia de un fenómeno de “seguridad en papel”, en el que la existencia de políticas y controles documentados no se traduce automáticamente en mejoras medibles del desempeño. En el contexto de PROIMA, las brechas de implementación y seguimiento parecen neutralizar el potencial impacto positivo que teóricamente debería tener un mayor grado de alineación con los estándares ISO, lo que obliga a distinguir entre cumplimiento formal y efectividad real de los controles al momento de evaluar el	Modelo integral de mejora de la gestión del riesgo de seguridad de la información basado en cultura organizacional, analítica predictiva y métricas operativas en PROIMA	Diseñar un sistema de indicadores y métricas operativas alineado a ISO/IEC 27005:2018, incorporando el MTTR y otras medidas clave por nivel de prioridad y unidad organizacional, que sirva como referencia para el monitoreo continuo de incidentes y de la toma de

	(M), con el fin de priorizar oportunidades de mejora (A) que fortalezcan la seguridad organizacional y la continuidad del negocio (R) en el período septiembre de 2022 a septiembre de 2025 (T).						nivel de riesgo residual.		decisiones en PROIMA.
		2. Examinar la relación entre la cultura organizacional vinculada a la gestión de riesgos de seguridad de la información y la eficacia observada de las medidas preventivas y de respuesta ante incidentes, en contraste con un enfoque exclusivamente técnico, durante septiembre de 2022 a septiembre de 2025.	Teoría General De Sistemas	Controles de SI (gobernanza, control de accesos /MFA, operaciones, continuidad).	Expertos en la temática		Los resultados del modelo de Random Forest para regresión confirmaron que las dimensiones conductuales vinculadas a la cultura organizacional en particular, el conocimiento y la conciencia sobre seguridad (DES_CON) y la ejecución de prácticas seguras (DES_EJE) son los principales determinantes del desempeño en la gestión del riesgo de seguridad de la información (MGR_SI). Estas variables presentaron los mayores valores de importancia relativa y contribuyeron de forma decisiva a la varianza explicada del modelo, mientras que los habilitadores técnicos y documentales (HAB_POL, HAB_CAP, HAB_CTL) mostraron valores bajos o incluso negativos en %IncMSE. En términos prácticos, este hallazgo implica que la inversión predominante en políticas, capacitaciones formales y controles técnicos, sin un trabajo sistemático sobre la cultura y las competencias de los colaboradores, no se refleja en mejoras sustantivas del desempeño. El contraste entre la alta relevancia estadística de las variables culturales y la baja contribución de los habilitadores técnicos respalda la tesis de que, en PROIMA, la gestión del riesgo sigue anclada en un enfoque tecnicista, mientras que el verdadero motor de efectividad reside en el comportamiento y la apropiación de las prácticas de seguridad por parte del personal.		Definir la arquitectura conceptual y las especificaciones funcionales de un modelo de analítica predictiva basado en Random Forest para estimar el riesgo de seguridad asociado al perfil de competencias de los colaboradores, de manera que pueda ser utilizado como insumo por las áreas de recursos humanos y de gestión del riesgo.

		3. Analizar las diferencias en la toma de decisiones para asegurar la continuidad del negocio cuando no existen indicadores y medidas formales de seguimiento de riesgos de seguridad de la información, frente a un sistema de métricas alineado a ISO/IEC 27005:2018, durante septiembre de 2022 a septiembre de 2025.	Teoría de la gestión de riesgos empresariales	Cultura de seguridad; eficacia preventiva y reactiva.		Entrevistas semiestructuradas	El análisis de las métricas operativas, particularmente del Mean Time To Repair (MTTR) de los tickets de incidentes y requerimientos, evidenció ineficiencias críticas en la toma de decisiones y en la gestión de la continuidad del negocio. Se identificaron tiempos de respuesta de hasta 1020 horas en tickets de baja prioridad, así como diferencias significativas entre departamentos, destacando el área de Logística frente a otras unidades organizacionales. Estos valores reflejan una paralización operativa prolongada en la atención de ciertos eventos, incompatible con un esquema de gestión de riesgos alineado a ISO/IEC 27005:2018. La ausencia inicial de un sistema estructurado de indicadores y medidas formales de seguimiento contribuyó a que estas ineficiencias pasaran inadvertidas durante el periodo analizado. Solo a partir del diseño y aplicación de métricas específicas fue posible cuantificar el retraso en la respuesta y evidenciar el impacto de la falta de priorización y monitoreo. En consecuencia, los hallazgos confirman que la toma de decisiones en PROIMA se ve significativamente limitada cuando no existen métricas claras, oportunas y diferenciadas por prioridad y área responsable.		Elaborar un plan de fortalecimiento de la cultura de seguridad de la información, orientado a mejorar el conocimiento y la ejecución de prácticas seguras mediante lineamientos operativos, propuestas de programas de formación y mecanismos de seguimiento conductual coherentes con los requisitos de las normas ISO/IEC

									27001 y 27005

REFERENCIAS BIBLIOGRÁFICAS

Aguilar Gavira, S., & Barroso Osuna, J. (2015). La triangulación de datos como estrategia en investigación educativa. *Píxel-Bit, Revista de Medios y Educación*, *47*, 73-88. https://doi.org/10.12795/pixelbit.2015.i47.05

Ali, C. (2024). *7 incidentes de ciberseguridad que marcaron el 2024 en América Latina*. https://www.welivesecurity.com/es/cibercrimen/incidentes-ciberseguridad-2024-america-latina/

Allawazi, F. (2021). *(PDF) Assessment of Information Security Risk Management System based on ISO/IEC27005 in the Independent High Electoral Commission: A Case Study*. ResearchGate. https://doi.org/10.48047/rigeo.11.05.339

Alonso, M. (2024). *Qué son las 5 fuerzas de Porter y cómo analizarlas [2024] • Asana*. https://asana.com/es/resources/porters-five-forces

ALTA. (2025). *Nuevas normativas en materia de ciberseguridad y protección de datos—ALTA*. https://altalegal.com/comunicacion/nuevas-normativas-en-materia-de-ciberseguridad-y-proteccion-de-datos/

Arístides, V. (2024). *Protección de datos y Ciberseguridad: La necesidad de una nueva ley de protección de datos, por Arístides Victoria*. https://www.ecija.com/actualidad-insights/data-protection-cybersecurity/

Asia Society. (2022). *Introduction to Southeast Asia | Asia Society*. https://asiasociety.org/education/introduction-southeast-asia

Biblioteca del Congreso Nacional de Chile. (2024). *El avance del comercio electrónico en el Asia: Una oportunidad para la Alianza del Pacífico - Programa Asia Pacifico* [Text]. Observatorio Asiapacifico; Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/observatorio/asiapacifico/noticias/avance-comercio-electronico-asia-pacifico

Bonderud, D. (2024, agosto 13). *Cost of a data breach 2024: Financial industry | IBM*. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

Cabello, S. M., Fernández, M., Elaskar, M., Pallero, M., Pereira, F., Ros Rooney, D., & Urtasun, M. (2025). Construcción de un ecosistema de confianza y seguridad digital. *Documentos de Proyectos*, Article 81470. https://ideas.repec.org//p/ecr/col022/81470.html

Çahmutoğlu, E. (2021). *El mundo registra un alarmante aumento de los ataques cibernéticos*

con sistemas de ransomware. https://www.aa.com.tr/es/análisis/el-mundo-registra-un-alarmante-aumento-de-los-ataques-cibernéticos-con-sistemas-de-ransomware/2260036

Calatayud, A., & Montes, L. (2021). Logística en América Latina y el Caribe: Oportunidades, desafíos y líneas de acción. *IDB Publications*. https://doi.org/10.18235/0003278

Chan, C. (2020). *(PDF) La matriz de consistencia en el proyecto de investigación: Un aprendizaje basado en el diseño (ABD)*. https://www.researchgate.net/publication/342110674_La_matriz_de_consistencia_en_el_proyecto_de_investigacion_un_aprendizaje_basado_en_el_diseno_ABD

Cinkara, E., Salma, C., & Batdi, V. (2024). El efecto de las prácticas de pensamiento reflexivo sobre las puntuaciones de retención: Un meta- método mixto. *Praxis Educativa*, *28*.

Cohen, Manion, & Morrison. (2018). *Research Methods in Education (8th ed.)*.

Corbin, & Strauss. (2015). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*.

Creswell. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*.

Cruz, L. O. V. de la, & Pérez-Pravia, M. C. (2022). Integrated supply chain security risk management with a focus on customer service. *Ingeniería y Competitividad*, *24*(2). https://www.redalyc.org/journal/2913/291374362018/html/

Domínguez, V., & Santillán, M. (2022). Teoría General de Sistemas, un enfoque práctico: General Systems Theory, a practical approach. *TECNOCIENCIA CHIHUAHUA*, *10*(3), 125-132.

Erude, S. (2023). *(PDF) Contingency Theory: An Assessment*. https://www.researchgate.net/publication/374742152_Contingency_Theory_An_Assessment

Espinoza, N. C. M. (2022). *La Gestión del Conocimiento para el Desarrollo Humano Sostenible*.

Flick. (2015). *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project*.

Foro Económico Mundial. (2024, octubre 28). *4 leyes sobre ciberseguridad que han cambiado el panorama global en 2024*. Foro Económico Mundial. https://es.weforum.org/stories/2024/10/la-normativa-de-ciberseguridad-sufrio-grandes-cambios-en-2024-esto-es-lo-que-hay-que-saber/

García, A., Iglesias, E., Puig, P., & Martínez, R. (2023). *Promoción del desarrollo digital en*

Guatemala: Retos y acciones. https://publications.iadb.org/es/promocion-del-desarrollo-digital-en-guatemala-retos-y-acciones

Gartner. (2016). *Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk*. https://www.gartner.com/en/newsroom/press-releases/2016-06-06-gartner-says-by-2020-60-percent-of-digital-businesses-will-suffer-major-service-failures-due-to-the-inability-of-it-security-teams-to-manage-digital-risk

Glaser, B, Strauss, A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research.*

Global Cybersecurity Index. (2024). *Global Cybersecurity Index*. ITU. https://www.itu.int:443/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Grupo Banco Mundial. (2022). *Transformación Digital en El Salvador, reactivando el crecimiento y la inclusión*. https://www.bancomundial.org/es/programs/de4lac/publication/digital-transformation-to-reignite-growth-and-equitability-in-el-salvador

Grupo Banco Mundial. (2025). *Honduras*. https://www.bancomundial.org/es/programs/lac-green-growth-leading-the-change-we-need/honduras

Guerrero, M., Medina, A., & Nogueira, D. (2020). *Procedimiento de gestión de riesgos como apoyo a la toma de decisiones*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362020000100002

Hernández-Sampieri, Fernández-Collado, & Baptista. (2018). *Metodología de la investigación (6a ed.)*. McGraw-Hill.

Hernández-Sampieri, R., & Mendoza Torres, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. https://virtual.cuautitlan.unam.mx/rudics/?p=2612

Idrus, S., Bin, M., & Idris, M. (2023). *(PDF) Managing Cybersecurity Risks in Emerging Technologies*. https://www.researchgate.net/publication/375133723_Managing_Cybersecurity_Risks_in_Emerging_Technologies

Kurniawan, E., Riadi, I., Irmawan, A., & Arusani. (2022). *Performance Measurement of Security Academic Information System using Maturity Level*. https://doi.org/10.48550/arXiv.2204.09511

Malterud, Siersma V. (2016). *Sample Size in Qualitative Interview Studies: Guided by Information Power. Qualitative Health Research*.

Medina, M., Rojas, C., Bustamante, W., & Carrasco, R. (2025, abril 18). *(PDF) Metodología de la Investigación. Técnicas e Instrumentos de Investigación*. ResearchGate. https://doi.org/10.35622/inudi.b.080

Mendieta, G., & Ramírez, N. (2025). *(PDF) La reflexividad en la práctica de la ética de la investigación, bioética e integridad científica (eibic)*. https://www.researchgate.net/publication/391493244_La_reflexividad_en_la_practica_de_la_etica_de_la_investigacion_bioetica_e_integridad_cientifica_eibic

Miranda, J., & Ishizawa, O. (2020). *Medir las tormentas en América Central: El impacto de los huracanes en la pobreza y la economía*. https://blogs.worldbank.org/es/latinamerica/capear-las-tormentas-en-am-rica-central-el-impacto-de-los-huracanes-en-la-pobreza-y-la-econom

Montenegro, J. (2020). *Propuesta de gestión de riesgos empresariales—El caso del COVID 19*. https://repositorio.unal.edu.co/bitstreams/042092c0-dff5-4b3e-8697-8863e0707c84/download

Morales, V. V., Villarreal, K. E. C., Sánchez, E. G. F., & Martinez, J. P. C. (2024). Sistema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(5), 12956-12979. https://doi.org/10.37811/cl_rcm.v8i6.14758

Nocco, B., & Stulz, R. (2025). Gestión de riesgos empresariales: Teoría y práctica. *Revista de Finanzas Corporativas Aplicadas*, *18*(5).

Ortiz-Fajardo & Erazo-Álvarez. (2021). *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação—Issues*. https://www.risti.xyz/index.php/edition

Ortiz-Fajardo, H. A., & Erazo-Álvarez, C. A. (2021). Resiliencia empresarial en tiempos de pandemia: Retos y desafíos de las microempresas. *Revista Arbitrada Interdisciplinaria Koinonía*, *6*(12), 366-398.

Parast, M. (2022). *Toward a contingency perspective of organizational and supply chain resilience—ScienceDirect*. https://www.sciencedirect.com/science/article/abs/pii/S0925527322002493

Patton. (2015). *Qualitative Research & Evaluation Methods (4th ed.)*.

PNUD. (2025). *Se impulsa la transformación digital para servicios públicos ágiles, eficientes y transparentes | Programa De Las Naciones Unidas Para El Desarrollo*. https://www.undp.org/es/honduras/historias/se-impulsa-la-transformacion-digital-para-servicios-publicos-agiles-eficientes-y-transparentes

PressBooks. (2023). *Southeast Asia – A Brief Introduction to World Regional Geography*. https://pressbooks.pub/worldregionalgeography/chapter/chapter-13-southeast-asia/

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4). https://doi.org/10.14569/IJACSA.2023.0140468

Ramos, J., & Hernández, O. (2022). *TemáTICas Gestión de incidentes de seguridad | Empresas | INCIBE*. https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

Smith, J. (2024). *Southeast Asians—An overview | ScienceDirect Topics*. https://www.sciencedirect.com/topics/agricultural-and-biological-sciences/southeast-asians

Tamayo Alzate, A. (1999). *Teoría general de sistemas*. https://repositorio.unal.edu.co/handle/unal/60006

Vergara, E., & Diao, H. (2024). *From fiction to reality: How Latin America became the world's most critical cyber battleground*. World Bank Blogs. https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

Villareal, V., Coro, K., Fernández, E., & Cueva, J. (2024). *(PDF) Sistema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información*. https://www.researchgate.net/publication/386536523_Sistema_Gestion_de_Seguridad_de_la_Informacion_y_su_impacto_en_el_Gobierno_y_Gestion_de_las_Tecnologias_de_la_Informacion

Villas, E., Gispert, N., García, N., & Monclús, G. (2025). (PDF) La Triangulación Múltiple como Estrategia Metodológica. *ResearchGate*. https://doi.org/10.15366/reice2013.11.4.001

World Economic Forum. (2025, mayo 13). *72% of cyber leaders say cybersecurity risks are*

rising. World Economic Forum. https://www.weforum.org/stories/2025/05/cybersecurity-cyber-risk-national-policy/

Yin. (2018). *Case Study Research and Applications: Design and Methods*.

Anexo 2. Ficha técnica del instrumento

FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS (SEPTIEMBRE 2022 - SEPTIEMBRE 2025)

1) Matriz por control (aplicación)

Código	Control (nombre)	Criterio clave (1 línea)	Evidencia clave	Verificación	Estatus (1/0.5/0/ N/A)	Notas / Riesgo	Responsable	Fecha
A.5.1		Política aprobada ≤12 meses, con alcance, roles y difusión.	Política; acta de aprobación; registro de difusión.	Doc + entrevista				
A.5.2		Revisión formal planificada (≥ anual) con cambios y comunicación.	Acta de revisión; plan anual; aviso a usuarios.	Doc				
A.5.5		Comité/foro de SI con charter, agenda, minutas y seguimiento.	Charter; minutas; plan de acciones.	Doc + entrevista				
A.5.7		Cambios organizativos evaluados por riesgos de SI antes de aprobar.	Formulario de cambio; matriz de riesgo; aprobación.	Doc				
A.5.		Registro vigente	Matriz	Doc				

Código	Control (nombre)	Criterio clave (1 línea)	Evidencia clave	Verificación	Estatus (1/0.5/0/N/A)	Notas / Riesgo	Responsable	Fecha
9		de requisitos legales/contractuales mapeados a controles.	legal; evidencias de cumplimiento.					
A.5.12		Clasificación y manejo de información aplicados en doc/sistemas.	Norma de clasificación; etiquetas; ejemplos aplicados.	Observación + doc				
A.5.23		Due diligence a terceros, cláusulas de SI y monitoreo periódico.	Evaluaciones; contratos; reportes de seguimiento.	Doc + entrevista				
A.5.30		Continuidad de SI alineada a BCP/DRP con pruebas documentadas.	Planes; resultados de pruebas; lecciones aprendidas.	Doc				
A.6.1		Roles/responsabilidades (RACI) formales y vigentes.	RACI; organigrama; comunicados.	Doc				
A.6.2		Segregación de funciones en procesos críticos (evidencia de control).	Matrices de acceso; flujos; autorizaciones.	Doc + observación				
A.6.3		Contacto con autoridades/CSIRTs definido y probado.	Procedimiento; evidencia de pruebas o ejercicios.	Doc + entrevista				
A.6.5		Seguridad integrada en proyectos	Plantillas; checklists; actas de	Doc				

Código	Control (nombre)	Criterio clave (1 línea)	Evidencia clave	Verificación	Estatus (1/0.5/0/N/A)	Notas / Riesgo	Responsable	Fecha
		(requisitos, revisiones, aprobación).	gate.					
A.6.7		Reglas de teletrabajo y acceso remoto aplicadas y auditables.	Política; registros de acceso; auditorías.	Doc + observación				
A.7.1		Perímetros físicos definidos; control de acceso y registros.	Planos; bitácoras; controles físicos.	Observación + doc				
A.7.2		Control de visitantes/contratistas con credencial y escolta.	Registro de ingresos; credenciales; políticas.	Observación + doc				
A.7.3		Protección de áreas sensibles (cerraduras, CCTV, alarmas).	Listado de puntos; mantenimiento; grabaciones.	Observación + doc				
A.7.7		Puesto limpio y pantalla bloqueada; inspecciones aleatorias.	Política; evidencias de inspección.	Observación				
A.7.10		Seguridad de equipos (ubicación, anclaje, condiciones ambientales).	Registros; inventario; bitácoras de mantenimiento.	Observación + doc				
A.7.14		Traslado de activos con cadena de custodia y resguardo.	Formatos de traslado; guías; firmas.	Doc				
A.8.		Inventario de	Inventario;	Doc				

Código	Control (nombre)	Criterio clave (1 línea)	Evidencia clave	Verificación	Estatus (1/0.5/0/N/A)	Notas / Riesgo	Responsable	Fecha
1		activos completo/actualizado con propietario/criticidad.	propietarios; clasificación.					
A.8.2		Uso aceptable definido y aceptado por los usuarios.	Política; constancias de aceptación.	Doc				
A.8.3		Gestión de credenciales (complejidad, rotación, resguardo).	Políticas; evidencia de rotación; vault.	Doc + observación				
A.8.5		MFA activo en sistemas críticos y accesos remotos.	Reportes de cobertura; configuración; pruebas.	Observación + doc				
A.8.6		Mínimo privilegio y revisión periódica de accesos.	Revisiones; solicitudes; aprobaciones.	Doc				
A.8.9		Cifrado en reposo/en tránsito según clasificación; llaves gestionadas.	Configuraciones; KMS; políticas de cifrado.	Observación + doc				
A.8.10		Endpoints con hardening/EDR y protección antimalware.	Baselines; consola EDR/AV; reportes de estado.	Observación + doc				
A.8.11		Parches aplicados por criticidad conforme a SLA.	Calendario; reportes de cumplimiento.	Doc				
A.8.16		Registros centralizados;	Config SIEM/log;	Observación +				

Código	Control (nombre)	Criterio clave (1 línea)	Evidencia clave	Verificación	Estatus (1/0.5/0/ N/A)	Notas / Riesgo	Responsable	Fecha
		retención y alertas sobre eventos clave.	políticas de retención.	doc				
A.8.22		Gestión de vulnerabilidades con escaneos y remediación por SLA.	Reportes de escaneo; planes de remediación.	Doc				
A.8.28		Backups probados (restore test) y RPO/RTO cumplidos.	Bitácoras; evidencias de pruebas; resultados.	Doc				

*** Estatus**: Cumple=1; Parcial=0.5; No=0; N/A=No aplica (excluir de cálculos).

1. Resumen por dominio

Dominio (Anexo A)	Nº controles aplicables	Suma estatus (solo aplicables)	% cumplimiento del dominio	Nº de brechas (0 o 0.5)	Comentarios clave
A.5					
A.6					
A.7					
A.8					
Total / Promedio					

Fórmula: % dominio = (Suma estatus ÷ Nº controles aplicables) × 100.

Reglas: *Aplicables* excluye N/A. *Brecha* = controles con estatus 0 o 0.5.

2. Plan de acción

ID acción	Hallazgo vinculado (control/es)	Acción correctiva / de mejora	Responsable	Recursos	Fecha inicio	Fecha objetivo	Prioridad	KPI de cierre / Evidencia esperada	Estado
	(ej. A.8.11 parches								

ID acción	Hallazgo vinculado (control/es)	Acción correctiva / de mejora	Responsable	Recursos	Fecha inicio	Fecha objetivo	Prioridad	KPI de cierre / Evidencia esperada	Estado
	fuera de SLA)								

Estados sugeridos: Pendiente / En curso / Bloqueada / Cerrada.

Ejemplo de KPI: “Cobertura de parches críticos ≥ 95% en 30 días; reporte exportado de la consola + acta de validación”.

Anexo 3. Revisión documental estructurada

FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS (SEPTIEMBRE 2022 - SEPTIEMBRE 2025)

1) Checklist de documentos (breve)

Categoría	Documento/registro esperado	Ubicación/Repositorio	Última actualización	Responsable	¿Existe? (Sí/No)	Observaciones
Políticas						
Procedimientos/SOP						
Actas/Decisiones						
Contratos/Terceros						
DRP/BCP						
Bitácoras						
Tableros/KPIs						
Capacitación						
Auditorías/Post mortems						

2) Verificación rápida por documento

Categoría	Documento	Vigencia	Aprobación	Difusión	Uso/evidencia	Coherencia ISO 27001–27005	Estatus*	Hallazgo clave

* **Estatus**: Cumple=1; Parcial=0.5; No=0; N/A.

3) Resumen + acciones

Categoría	% Cumpl. **	Brechas (#)	Acción prioritaria	Responsable	Fecha objetivo	Evidencia de cierre
Políticas						
Procedimientos						
Terceros						
DRP/BCP						
Bitácoras						
KPIs						
Capacitación						
Auditorías						
Global						

** **% Cumpl.** = (Suma estatus ÷ Nº docs aplicables) × 100.

Anexo 4. Cuestionario de cultura de seguridad

Dominio A.5 – Ítems

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS (SEPTIEMBRE 2022 - SEPTIEMBRE 2025)

Instrucciones: Marca una casilla por ítem. 1 = Totalmente en desacuerdo 2 = En desacuerdo 3 = Neutral 4 De acuerdo 5 = Totalmente de acuerdo.

nordmatute@gmail.com Cambiar de cuenta

No compartido

En mi área, la política de seguridad está disponible, se entiende y se aplica en el trabajo diario.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Conozco los cambios recientes en las políticas/procedimientos y recibí comunicación formal al respecto.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Conozco los cambios recientes en las políticas/procedimientos y recibí comunicación formal al respecto.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Los requisitos legales/contractuales relevantes para mi trabajo están identificados y se cumplen.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

La información que manejo está correctamente clasificada y tratada según su sensibilidad.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Mi área gestiona adecuadamente los riesgos asociados a terceros con acceso a información/sistemas.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Mi área gestiona adecuadamente los riesgos asociados a terceros con acceso a información/sistemas.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Conozco las acciones de continuidad (BCP/DRP) que debo seguir si se interrumpe un servicio crítico.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Dominio A.6 – Ítems

Tengo claro mi rol y responsabilidades en seguridad de la información (lo que puedo/debo hacer).

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Los accesos y aprobaciones en mi proceso respetan la segregación de funciones.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Sé cómo contactar a las autoridades/CSIRT internas en caso de incidente de seguridad.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

En los proyectos en los que participo se incorporan requisitos y revisiones de seguridad.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Cuento con lineamientos claros para el trabajo remoto y el acceso desde fuera de la oficina.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

He recibido capacitación específica y reciente relacionada con los riesgos de mi rol.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Dominio A.7 – Ítems

El control de acceso físico a mi área funciona (credencial, registro de visitantes, acompañamiento).

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Las áreas sensibles (servidores/almacenes) están protegidas y monitoreadas adecuadamente.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Las áreas sensibles (servidores/almacenes) están protegidas y monitoreadas adecuadamente.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Mantengo el 'puesto limpio' y bloqueo mi equipo al ausentarme, según las reglas de la organización.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Los equipos bajo mi responsabilidad están instalados y protegidos de acuerdo con las normas internas.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Los equipos bajo mi responsabilidad están instalados y protegidos de acuerdo con las normas internas.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

El traslado de activos/información se realiza con custodia y registro según lo establecido.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Los controles físicos y ambientales son conocidos por el personal y se cumplen en el día a día.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Dominio A.8 – Ítems

Mis accesos a sistemas siguen el principio de mínimo privilegio y se revisan periódicamente.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Utilizo autenticación multifactor (MFA) para acceder a sistemas críticos/remotos.

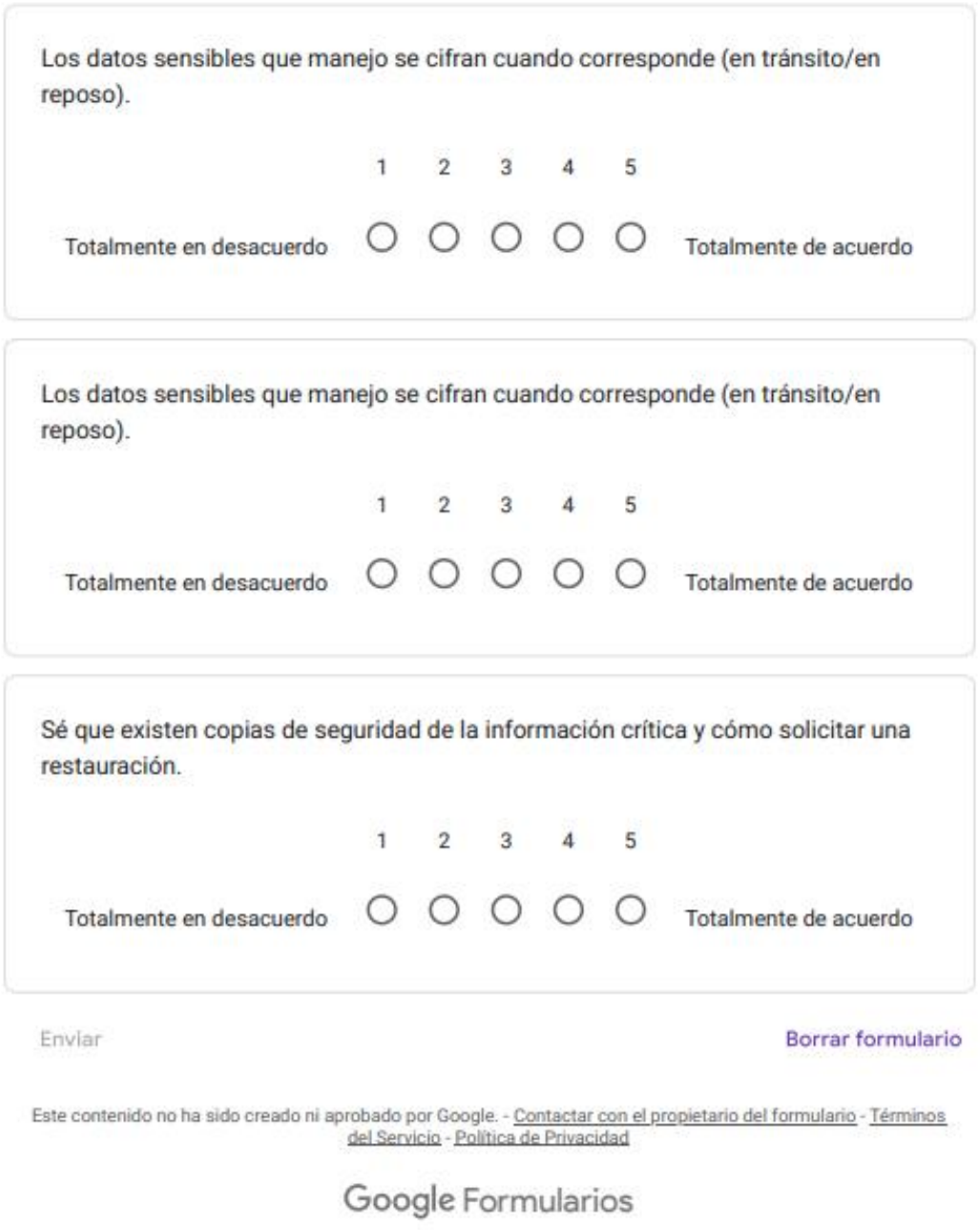
	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Conozco y cumplo las reglas de uso aceptable de activos tecnológicos.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo

Los equipos y aplicaciones que uso están actualizados y con protección antimalware activa.

	1	2	3	4	5	
Totalmente en desacuerdo	○	○	○	○	○	Totalmente de acuerdo



Enlace del instrumento: https://forms.gle/FRRCoccL2k4WHxcw8

Anexo 5. Entrevista

FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ESTUDIO EXPLORATORIO DE LAS PRÁCTICAS Y DESAFÍOS EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN PROIMA, HONDURAS (SEPTIEMBRE 2022 - SEPTIEMBRE 2025)

Esta entrevista busca evaluar la madurez de la seguridad de la información y su alineación con ISO/IEC 27001–27005 en [PROIMA], con énfasis en gobernanza, gestión de riesgos, continuidad, terceros y toma de decisiones basada en métricas. La información será tratada con confidencialidad, usada solo con fines del estudio.

1. ¿Cómo se aprueban y actualizan las políticas de seguridad en su área?
2. ¿Qué roles y responsabilidades formales (RACI) existen para seguridad?
3. Describa, en su proceso, cómo identifican y tratan riesgos (ISO 27005).
4. ¿Qué controles críticos del Anexo A son imprescindibles y por qué?
5. ¿Dónde ve brechas actuales y cuál es su prioridad (impacto/urgencia)?
6. Mencione un incidente reciente: detección (MTTD), respuesta (MTTR) y lecciones.
7. ¿Cómo aseguran continuidad/recuperación (RTO/RPO, pruebas DR/BCP)?
8. ¿Qué debida diligencia y cláusulas de seguridad exigen a terceros?
9. ¿Cómo gestionan accesos de terceros (alta/baja, MFA, monitoreo)?
10. ¿Qué KPIs/KRIs reciben y con qué periodicidad? ¿Se toman decisiones con ellos?
11. ¿Qué capacitación realizó su equipo el último año y cómo miden su eficacia?
12. Priorice tres acciones para 6–12 meses y los recursos críticos para ejecutarlas.

Anexo 6. Diccionario de Datos – Encuesta

Variable / Indicador	Código	Tipo de dato	Escala / Valores posibles	Descripción	Fuente
Dominio A.5 – Políticas, organización y cumplimiento					
Política de seguridad disponible y aplicada	A5_1	Ordinal (Likert)	1=Totalmente en desacuerdo → 5=Totalmente de acuerdo	Evalúa si el personal conoce, entiende y aplica la política de seguridad en su labor diaria.	Encuesta
Comunicación de cambios en políticas/procedimientos	A5_2	Ordinal (Likert)	1–5	Mide la efectividad de la comunicación formal sobre cambios recientes.	Encuesta
Cumplimiento de requisitos legales/contractuales	A5_3	Ordinal (Likert)	1–5	Identifica si los requisitos normativos aplicables son conocidos y respetados.	Encuesta
Clasificación y manejo adecuado de la información	A5_4	Ordinal (Likert)	1–5	Verifica si los datos se tratan conforme a su nivel de sensibilidad.	Encuesta
Gestión de riesgos de terceros	A5_5	Ordinal (Likert)	1–5	Evalúa si el área controla riesgos asociados a proveedores o aliados con acceso a información.	Encuesta
Conocimiento de planes de continuidad (BCP/DRP)	A5_6	Ordinal (Likert)	1–5	Mide si los empleados conocen las acciones a seguir ante interrupciones de servicios críticos.	Encuesta
Dominio A.6 – Roles, responsabilidades y concienciación					
Conocimiento de roles y responsabilidades en SI	A6_1	Ordinal (Likert)	1–5	Evalúa el entendimiento del rol personal en la protección de la información.	Encuesta

Respeto a la segregación de funciones	A6_2	Ordinal (Likert)	1–5	Determina si los accesos y aprobaciones respetan la segregación de tareas.	Encuesta
Conocimiento del canal de reporte (CSIRT)	A6_3	Ordinal (Likert)	1–5	Mide la familiaridad con el procedimiento para reportar incidentes de seguridad.	Encuesta
Inclusión de seguridad en proyectos	A6_4	Ordinal (Likert)	1–5	Indica si se consideran requisitos y revisiones de seguridad en nuevos proyectos.	Encuesta
Lineamientos de trabajo remoto	A6_5	Ordinal (Likert)	1–5	Evalúa si el colaborador cuenta con reglas claras para el acceso remoto.	Encuesta
Capacitaciones en seguridad	A6_6	Ordinal (Likert)	1–5	Identifica la frecuencia y pertinencia de la capacitación recibida sobre riesgos de seguridad.	Encuesta
Dominio A.7 – Seguridad física y ambiental					
Control de acceso físico al área	A7_1	Ordinal (Likert)	1–5	Evalúa el funcionamiento del control físico de acceso (credencial, registro, acompañamiento).	Encuesta
Protección de áreas sensibles	A7_2	Ordinal (Likert)	1–5	Determina si las zonas críticas están monitoreadas y protegidas.	Encuesta
Aplicación del principio de “puesto limpio”	A7_3	Ordinal (Likert)	1–5	Mide si el colaborador mantiene orden y	Encuesta

				bloquea el equipo al ausentarse.	
Cumplimiento de normas en instalación y protección de equipos	A7_4	Ordinal (Likert)	1–5	Verifica si los dispositivos cumplen con estándares de seguridad interna.	Encuesta
Custodia y registro en traslado de información	A7_5	Ordinal (Likert)	1–5	Evalúa la observancia de procedimientos de traslado de activos o información.	Encuesta
Conocimiento de controles físicos y ambientales	A7_6	Ordinal (Likert)	1–5	Mide el grado de conocimiento del personal sobre controles ambientales.	Encuesta
Dominio A.8 – Seguridad tecnológica y operativa					
Principio de mínimo privilegio	A8_1	Ordinal (Likert)	1–5	Evalúa si los accesos del personal se ajustan al principio de privilegio mínimo.	Encuesta
Uso de autenticación multifactor (MFA)	A8_2	Ordinal (Likert)	1–5	Determina la frecuencia del uso de MFA en sistemas críticos o remotos.	Encuesta
Cumplimiento de normas de uso aceptable	A8_3	Ordinal (Likert)	1–5	Mide el conocimiento y aplicación de políticas de uso aceptable de activos tecnológicos.	Encuesta
Actualización y protección antimalware	A8_4	Ordinal (Likert)	1–5	Verifica si los equipos y aplicaciones se mantienen actualizados y protegidos.	Encuesta
Cifrado de datos sensibles	A8_5	Ordinal (Likert)	1–5	Evalúa si la información	Encuesta

				sensible se cifra en tránsito o en reposo.	
Conocimiento de copias de seguridad	A8_6	Ordinal (Likert)	1–5	Identifica si el empleado sabe que existen copias de seguridad y cómo solicitarlas.	Encuesta

Anexo 7. Diccionario de Datos – Revisión Documental

Variable / Indicador	Código	Tipo de dato	Escala / Valores posibles	Descripción / Propósito	Fuente / Sección
Categoría documental	D01	Categórica	1=Políticas; 2=Procedimientos; 3=Actas; 4=Contratos/Terceros; 5=DRP/BCP; 6=Bitácoras; 7=KPIs; 8=Capacitación; 9=Auditorías	Clasifica los documentos institucionales revisados según su naturaleza o propósito.	Checklist de documentos
Documento o registro esperado	D02	Categórica	Texto libre	Identifica el nombre específico del documento, registro o evidencia operativa.	Checklist de documentos
Ubicación o repositorio	D03	Categórica	Texto libre	Indica la carpeta, servidor o sistema donde se almacena el documento.	Checklist de documentos
Fecha de última actualización	D04	Fecha	dd/mm/aaaa	Registra la fecha más reciente de emisión o revisión del documento.	Checklist de documentos
Responsable	D05	Categórica	Texto libre	Registra el área o cargo responsable de mantener actualizado el documento.	Checklist de documentos
Existencia del documento	D06	Binaria	1=Sí; 0=No	Determina si el documento o registro está disponible en el repositorio institucional.	Checklist de documentos
Observaciones	D07	Categórica	Texto libre	Registra notas relevantes sobre hallazgos, inconsistencias o particularidades.	Checklist de documentos

Vigencia	D08	Ordinal	1=Vigente; 0.5=Parcialmente vigente; 0=No vigente	Evalúa si el documento está actualizado según los plazos definidos (≤12 meses para políticas).	Verificación rápida
Aprobación formal	D09	Ordinal	1=Sí; 0.5=Parcial; 0=No	Indica si el documento cuenta con firma o acta de aprobación vigente.	Verificación rápida
Difusión o comunicación interna	D10	Ordinal	1=Sí; 0.5=Parcial; 0=No	Verifica si el documento fue comunicado o difundido al personal correspondiente.	Verificación rápida
Uso o evidencia de aplicación	D11	Ordinal	1=Sí; 0.5=Parcial; 0=No	Mide si existen registros o evidencias que demuestren la aplicación del documento.	Verificación rápida
Coherencia con ISO/IEC 27001–27005	D12	Ordinal	1=Coherente; 0.5=Parcialmente; 0=No coherente	Evalúa si el contenido del documento se ajusta a los requisitos normativos.	Verificación rápida
Estatus global del documento	D13	Categórica	1=Cumple; 0.5=Parcial; 0=No; N/A=No aplica	Resultado consolidado de los criterios de evaluación anteriores.	Verificación rápida
Hallazgo clave	D14	Categórica	Texto libre	Describe el hallazgo principal detectado en la verificación (por ejemplo, "sin evidencia de difusión").	Verificación rápida
Porcentaje de cumplimient	D15	Numérica	0–100 %	Calcula el grado de cumplimiento	Resumen + acciones

o por categoría				documental por categoría: (Σ estatus ÷ nº de documentos) × 100.	
Número de brechas	D16	Numérica	0–n	Registra la cantidad de hallazgos o incumplimientos identificados en la categoría.	Resumen + acciones
Acción prioritaria	D17	Categórica	Texto libre	Define la acción de mejora sugerida (por ejemplo, actualizar política, difundir procedimiento, etc.).	Resumen + acciones
Responsable de la acción	D18	Categórica	Texto libre	Registra el área o persona designada para ejecutar la acción correctiva.	Resumen + acciones
Fecha objetivo de cierre	D19	Fecha	dd/mm/aaaa	Indica la fecha meta establecida para corregir la brecha identificada.	Resumen + acciones
Evidencia de cierre	D20	Categórica	1=Sí; 0=No; En proceso	Señala si la acción correctiva fue ejecutada y documentada satisfactoriamente.	Resumen + acciones
Cumplimiento global institucional	D21	Numérica	0–100 %	Porcentaje total de cumplimiento consolidado entre todas las categorías del SGSI.	Cálculo final / matriz de cumplimiento

Anexo 8. Diccionarios de Datos – Ficha Técnica

Variable / Indicador	Código	Tipo de dato	Escala / Valores posibles	Descripción / Propósito	Fuente / Sección
Código del control	C01	Categórica	Texto (A.5.x – A.8.x)	Identificador normativo del control según ISO/IEC 27001:2022 (Anexo A).	Matriz por control
Nombre del control	C02	Categórica	Texto libre	Denominación breve del control de seguridad evaluado.	Matriz por control
Criterio clave de evaluación	C03	Categórica	Texto libre	Define el aspecto principal que debe cumplir el control (e.g., "Política aprobada ≤12 meses").	Matriz por control
Evidencia clave esperada	C04	Categórica	Texto libre	Lista de documentos o pruebas requeridas para validar el cumplimiento.	Matriz por control
Método de verificación	C05	Categórica	1=Documental; 2=Entrevista; 3=Observación; 4=Mixta	Indica la técnica usada para verificar el control.	Matriz por control
Estatus del control	C06	Ordinal	1=Cumple; 0.5=Parcial; 0=No; N/A=No aplica	Resultado de la verificación con base en la evidencia presentada.	Matriz por control
Notas o riesgo identificado	C07	Categórica	Texto libre	Descripción de observaciones, desviaciones o riesgos asociados al control.	Matriz por control
Responsable del control	C08	Categórica	Texto libre	Persona o área designada para la gestión o aplicación del control.	Matriz por control
Fecha de verificación	C09	Fecha	dd/mm/aaaa	Fecha en la que se realizó la validación del	Matriz por control

				control.	
Dominio de control	R01	Categórica	A.5 / A.6 / A.7 / A.8	Clasificación general de los controles según los dominios de la norma.	Resumen por dominio
Número de controles aplicables	R02	Numérica	1–n	Total, de controles relevantes dentro de cada dominio (excluye N/A).	Resumen por dominio
Suma de estatus aplicables	R03	Numérica	0–n	Suma total de los valores asignados (1, 0.5 o 0) dentro del dominio.	Resumen por dominio
Porcentaje de cumplimiento del dominio	R04	Numérica	0–100 %	Cálculo automático: (Σ estatus ÷ nº controles aplicables) × 100.	Resumen por dominio
Número de brechas	R05	Numérica	0–n	Cantidad de controles con estatus 0 o 0.5 en el dominio.	Resumen por dominio
Comentarios clave del dominio	R06	Categórica	Texto libre	Observaciones principales sobre desempeño o brechas detectadas.	Resumen por dominio
Cumplimiento global promedio	R07	Numérica	0–100 %	Promedio aritmético del cumplimiento entre todos los dominios A.5–A.8.	Resumen consolidado
ID de acción correctiva	P01	Categórica	Texto libre	Identificador secuencial de la acción planificada.	Plan de acción
Hallazgo vinculado	P02	Categórica	Texto (Control A.x.x)	Control o controles relacionados con el hallazgo detectado.	Plan de acción
Acción correctiva o de mejora	P03	Categórica	Texto libre	Descripción de la acción propuesta para resolver o prevenir la brecha.	Plan de acción

Responsable de la acción	P04	Categórica	Texto libre	Persona o área encargada de implementar la medida correctiva.	Plan de acción
Recursos requeridos	P05	Categórica	Texto libre	Indica los recursos técnicos, humanos o financieros necesarios.	Plan de acción
Fecha de inicio	P06	Fecha	dd/mm/aaaa	Fecha prevista de inicio de la acción correctiva.	Plan de acción
Fecha objetivo de cierre	P07	Fecha	dd/mm/aaaa	Fecha límite para completar la acción planificada.	Plan de acción
Prioridad asignada	P08	Ordinal	1=Alta; 2=Media; 3=Baja	Clasifica la urgencia o criticidad del hallazgo.	Plan de acción
KPI o evidencia de cierre	P09	Categórica	Texto libre	Indicador de cumplimiento que demuestra la efectividad de la acción (ej. “Cobertura de parches críticos ≥95% en 30 días”).	Plan de acción
Estado actual	P10	Categórica	Pendiente / En curso / Bloqueada / Cerrada	Estado operativo de la acción correctiva.	Plan de acción

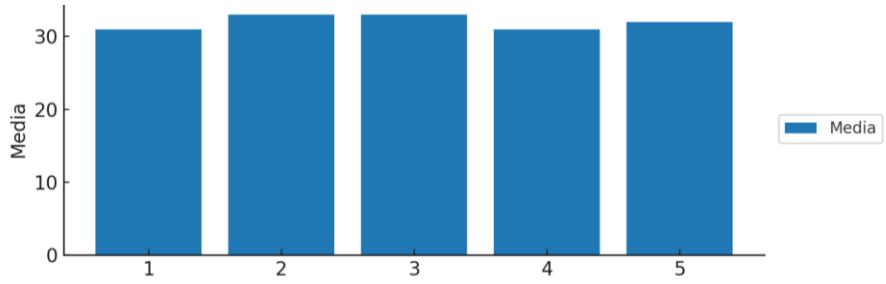
Anexo 9. Diccionario de Datos – Entrevista

Variable / Indicador	Código	Tipo de dato	Escala / Valores posibles	Descripción / Propósito	Fuente / Sección
Identificador de entrevista	E01	Categórica	INT-01, INT-02, INT-03...	Código asignado a cada participante entrevistado.	Registro de campo
Cargo / Rol del participante	E02	Categórica	CIO, CISO, Operaciones TI, Riesgos, Continuidad	Define la posición jerárquica y función institucional del entrevistado.	Ficha del informante
Área o proceso representado	E03	Categórica	Dirección; TI; Riesgos; Continuidad; Procesos críticos	Identifica el ámbito organizacional del informante.	Ficha del informante
Dimensión temática	E04	Categórica	Gobernanza; Riesgos; Continuidad; Terceros; Métricas	Clasifica la temática principal abordada en la entrevista.	Guía de entrevista
Pregunta guía	E05	Categórica	1–12 (según orden del instrumento)	Número o texto representativo de la pregunta formulada.	Guía de entrevista
Respuesta textual (transcripción)	E06	Categórica	Texto libre	Respuesta literal o resumida proporcionada por el informante.	Transcripción
Código inicial	E07	Categórica	Texto corto (e.g., “roles”, “riesgo”, “incidente”)	Palabra clave o idea principal identificada en la primera lectura.	Codificación abierta
Categoría axial	E08	Categórica	Gobernanza; Riesgos; Continuidad; Terceros; Métricas	Agrupa los códigos iniciales según su relación conceptual.	Codificación axial
Subcategoría emergente	E09	Categórica	e.g., “actualización de políticas”, “respuesta a incidentes”	Tema derivado del análisis que refina la categoría axial.	Codificación selectiva

Frecuencia de aparición	E10	Numérica	1–n	Número de veces que un código o categoría aparece en distintas entrevistas.	Matriz de análisis
Nivel de madurez percibido	E11	Ordinal	1=Bajo; 2=Medio; 3=Alto	Valoración cualitativa de la madurez institucional en el tema.	Análisis interpretativo
Hallazgo clave	E12	Categórica	Texto libre	Idea central que sintetiza el resultado por categoría.	Informe de resultados
Acción o mejora sugerida	E13	Categórica	Texto libre	Recomendación o acción prioritaria propuesta por el entrevistado.	Informe de resultados
Impacto estimado	E14	Ordinal	1=Bajo; 2=Medio; 3=Alto	Nivel de influencia del hallazgo o acción sobre la gestión de seguridad.	Análisis temático
Responsable del seguimiento	E15	Categórica	Texto libre	Área o persona designada para ejecutar la acción de mejora.	Plan de acción
Prioridad de implementación	E16	Ordinal	1=Alta; 2=Media; 3=Baja	Orden de atención sugerido según urgencia o riesgo asociado.	Plan de acción
KPI / Indicador asociado	E17	Categórica	Texto libre (ej. MTTD, MTTR, % cumplimiento BCP)	Métrica vinculada a la acción o hallazgo.	Informe de resultados
Estado de cierre	E18	Categórica	Pendiente / En curso / Completado	Situación actual de la acción o hallazgo.	Seguimiento del plan

Anexo 10. Limpieza de datos

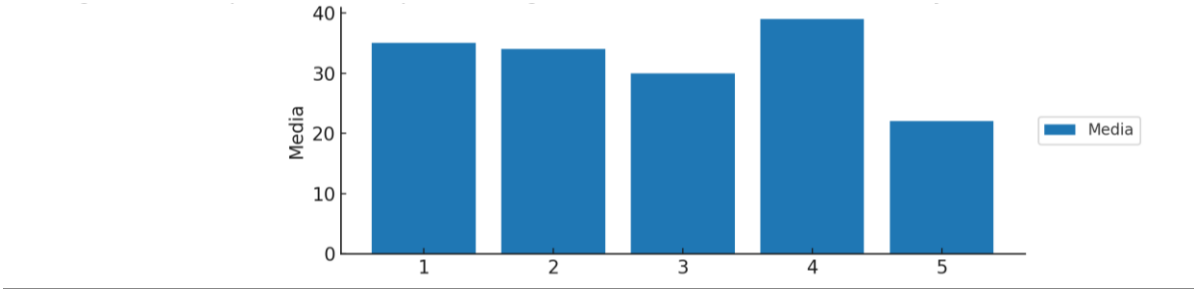
Figura 26. Distribución de respuestas sobre el cifrado de datos sensibles en tránsito y en reposo



Fuente: Elaboración Propia

La figura muestra cómo el personal califica la práctica de cifrar información sensible dentro de sus actividades diarias. El patrón no forma un pico definido, sino que distribuye las respuestas a lo largo de toda la escala, lo que evidencia distintos niveles de familiaridad y dominio sobre este control. Aun así, los valores superiores tienden a agrupar la mayor parte de las respuestas, lo que revela que un segmento significativo de colaboradores percibe el cifrado como una medida habitual y necesaria en la protección de datos corporativos. Esta concentración en los rangos altos permite inferir que existe una base operativa favorable para consolidar controles más estrictos y avanzar hacia una implementación coherente con los lineamientos de ISO/IEC 27001:2022.

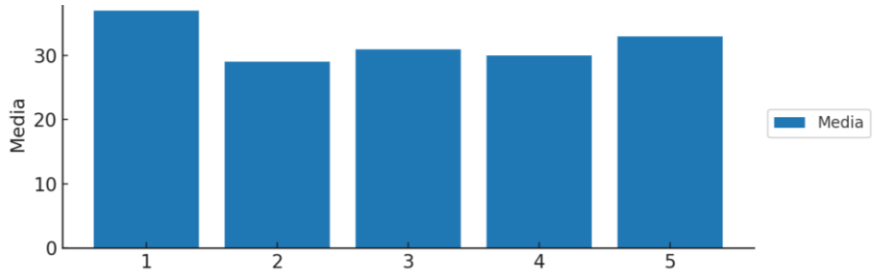
Figura 27: Conocimiento sobre copias de seguridad y procedimientos de restauración de información crítica



Fuente: Elaboración Propia

La gráfica evidencia cómo el personal valora su familiaridad con los mecanismos de respaldo y recuperación de información crítica. Los resultados no muestran un patrón homogéneo: las respuestas se distribuyen a lo largo de toda la escala, lo que indica niveles desiguales de comprensión sobre estos procesos. Llama la atención que los puntajes bajos aparecen con mayor frecuencia, lo que sugiere que una parte importante de los colaboradores desconoce las rutas formales para solicitar una restauración o no domina las prácticas asociadas al manejo de copias de seguridad. Aun así, la presencia de valores altos señala que existen áreas o roles con mayor dominio del tema. Esta combinación de desconocimiento general y focos de conocimiento especializado apunta a la necesidad de estandarizar lineamientos internos y reforzar la capacitación para asegurar que todos los usuarios puedan responder adecuadamente ante una pérdida de datos o interrupción operativa.

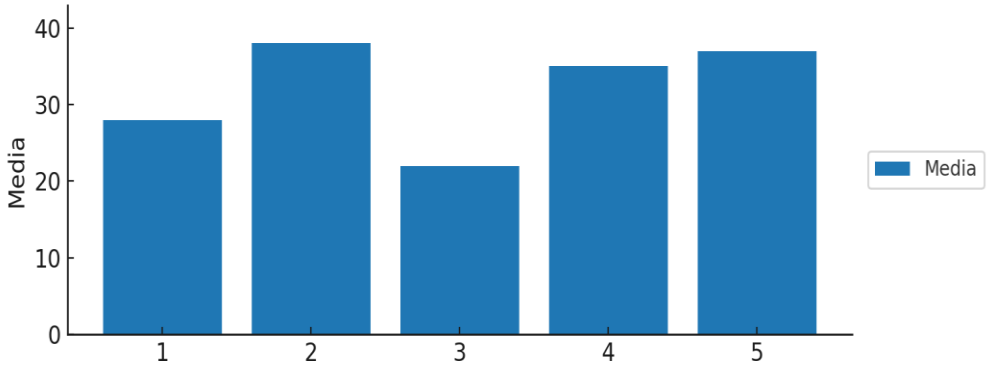
Figura 28. Actualización de equipos y protección antimalware activa en los sistemas utilizados



Fuente: Elaboración Propia

La gráfica permite identificar cómo el personal evalúa la actualización de sus equipos y la activación de herramientas antimalware. Los valores reportados muestran que no existe un consenso claro: las respuestas se distribuyen en toda la escala, lo que evidencia prácticas dispares entre áreas y usuarios. Los puntajes más bajos aparecen con frecuencia relevante, lo que sugiere que parte del personal opera con sistemas desactualizados o con protecciones incompletas. Sin embargo, la presencia de calificaciones altas indica que ciertos grupos mantienen rutinas más formales de mantenimiento. Esta mezcla de comportamientos demuestra que la organización aún no cuenta con un estándar homogéneo de actualización y protección, por lo que resulta prioritario unificar procesos, incorporar mecanismos automáticos y asegurar que todas las estaciones de trabajo cuenten con configuraciones mínimas consistentes frente al malware.

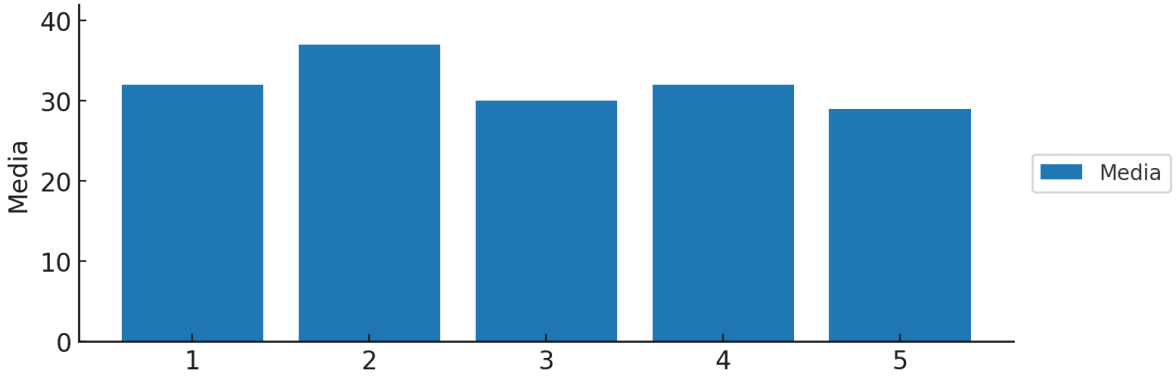
Figura 29: Conocimiento y cumplimiento de las reglas de uso aceptable de activos tecnológicos



Fuente: Elaboración Propia

La gráfica permite identificar diferencias marcadas en la forma en que los colaboradores aplican y comprenden las reglas de uso aceptable de los activos tecnológicos. Los resultados no muestran un comportamiento uniforme: algunos empleados reportan niveles limitados de adherencia, mientras que otros valoran positivamente su conocimiento y cumplimiento de estas normas. Esta variabilidad sugiere que, aunque existen grupos familiarizados con las políticas institucionales, aún persiste un segmento que opera con criterios poco claros o interpretaciones personales sobre lo permitido. La presencia simultánea de calificaciones bajas y altas evidencia un marco normativo que no se ha interiorizado de manera equilibrada en toda la organización. Bajo este panorama, fortalecer los mecanismos de comunicación interna y estandarizar la comprensión de las reglas se vuelve esencial para asegurar un uso responsable y consistente de los recursos tecnológicos.

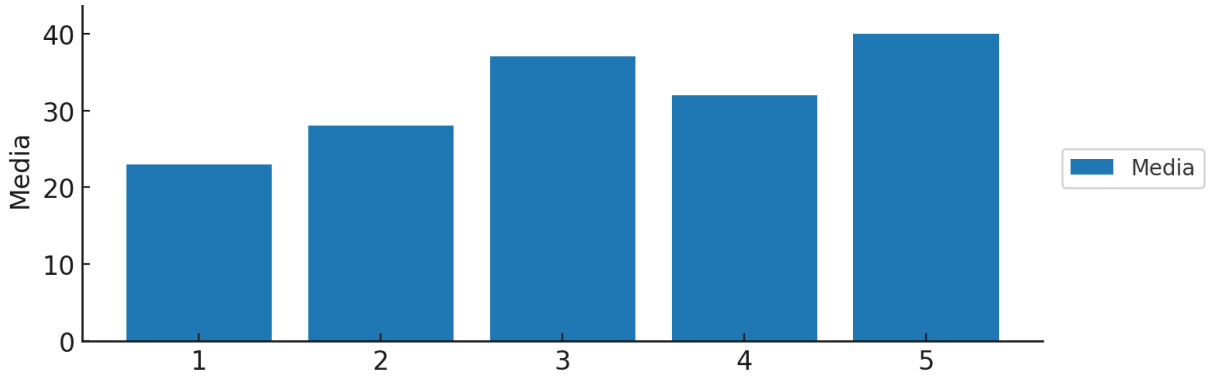
Figura 30: Aplicación del principio de mínimo privilegio y revisión periódica de accesos a sistemas



Fuente: Elaboración Propia

La gráfica evidencia variaciones importantes en la forma en que los colaboradores perciben la asignación de privilegios y la periodicidad con la que se revisan los accesos a los sistemas. Las respuestas distribuidas en distintos niveles sugieren que la organización aún no cuenta con una práctica homogénea para gestionar quién accede a qué información y por cuánto tiempo. Mientras algunos usuarios parecen familiarizados con los controles de acceso y reconocen la existencia de revisiones formales, otros muestran señales de desconocimiento o aplicación parcial de estas medidas. Esta brecha indica que los procesos de validación de permisos no operan con el mismo rigor en todas las áreas. Bajo este escenario, resulta prioritario consolidar un marco de gobernanza claro, donde la asignación de privilegios responda únicamente a funciones específicas y las revisiones se ejecuten con regularidad para minimizar riesgos asociados a accesos innecesarios o desactualizados.

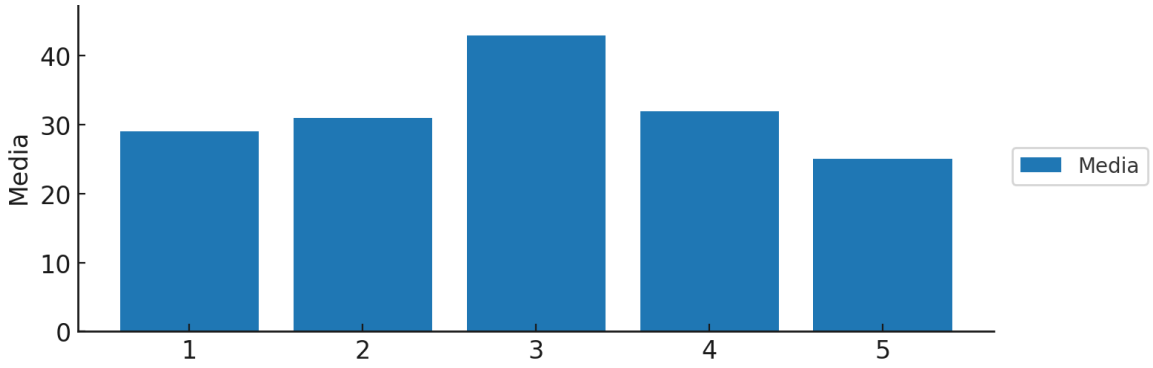
Figura 31: Uso de autenticación multifactor (MFA) en el acceso a sistemas críticos o remotos



Fuente: Elaboración Propia

Los resultados permiten identificar diferencias en el grado de adopción de la autenticación multifactor dentro de los sistemas críticos y accesos remotos de PROIMA. Si bien una parte notable del personal manifiesta emplear mecanismos de verificación adicional, los datos también revelan que este control aún no se aplica de manera uniforme. Esta disparidad sugiere que la MFA ha sido incorporada con mayor solidez en ciertos procesos o áreas, mientras que en otros su implementación continúa siendo parcial o inexistente. La coexistencia de prácticas avanzadas junto con niveles básicos de adopción evidencia que la organización se encuentra en una etapa intermedia de madurez en este control. Para avanzar hacia un modelo más robusto, será necesario definir lineamientos estándar, asegurar una configuración obligatoria en todos los accesos sensibles y promover una cultura institucional orientada al uso sistemático de factores adicionales de autenticación.

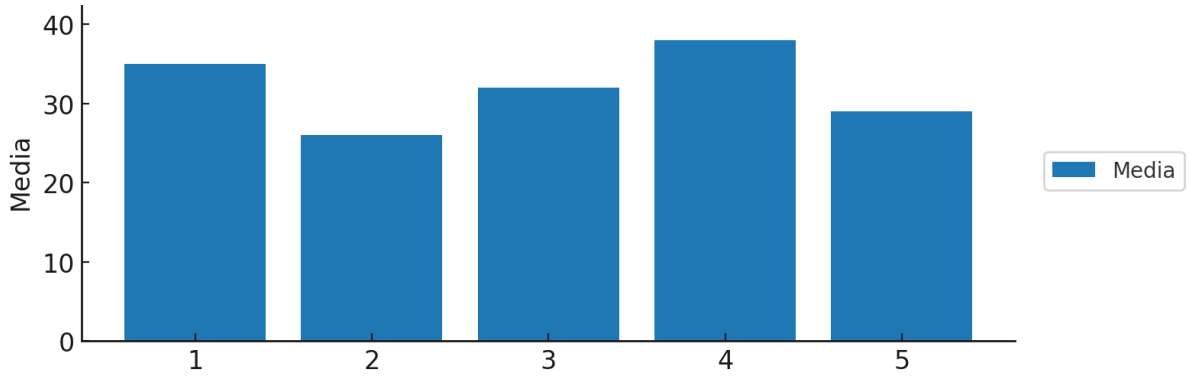
Figura 32: Custodia y registro en el traslado de activos e información según procedimientos establecidos



Fuente: Elaboración Propia

Los resultados permiten observar diferencias claras en la manera en que los colaboradores aplican las prácticas de custodia y registro durante el traslado de activos e información. La variedad de respuestas sugiere que no existe una ejecución uniforme de los controles, lo que puede generar inconsistencias en la trazabilidad de los movimientos y en la responsabilidad asociada a cada etapa del proceso. Mientras algunos usuarios indican cumplir parcialmente con los lineamientos establecidos, otros presentan niveles más altos o más bajos de adherencia, lo que refleja una madurez dispareja entre áreas operativas. Esta falta de estandarización implica riesgos adicionales para la integridad y seguimiento de la información sensible. En este contexto, se vuelve necesario consolidar procedimientos claros, automatizar los registros cuando sea posible y fortalecer los mecanismos de control que aseguren un manejo consistente de los activos en todo su ciclo de traslado.

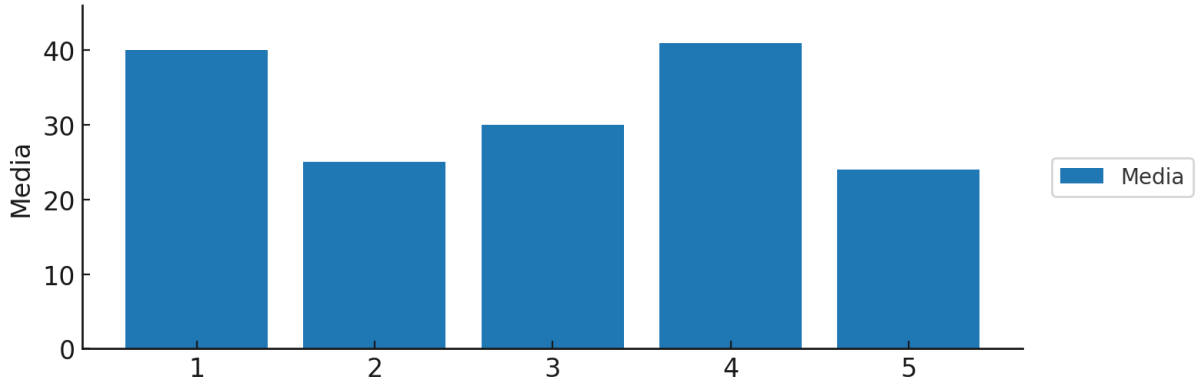
Figura 33: Conocimiento y cumplimiento de controles físicos y ambientales por parte del personal



Fuente: Elaboración Propia

Los resultados permiten observar diferencias en la manera en que el personal asume las responsabilidades asociadas a la seguridad física y ambiental dentro de la organización. Las respuestas evidencian que no todos los colaboradores aplican estos controles con el mismo nivel de constancia, lo que sugiere que la comprensión sobre su propósito y alcance aún no está plenamente consolidada. Mientras algunos empleados muestran mayor familiaridad con las prácticas de resguardo de instalaciones y protección de entornos críticos, otros parecen depender de criterios personales o de instrucciones esporádicas, lo que genera variabilidad en la efectividad de estos controles. Esta situación refleja una implementación fragmentada, especialmente en áreas donde los riesgos físicos o ambientales pueden pasar desapercibidos. Para reducir estas brechas, se vuelve esencial integrar estos controles dentro de la rutina operativa, reforzar la supervisión y promover una cultura que reconozca la seguridad física y ambiental como parte fundamental del resguardo institucional.

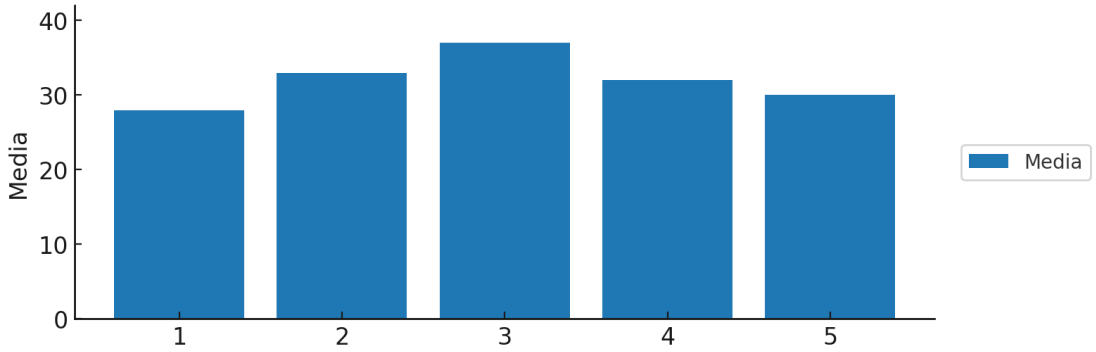
Figura 34: Protección e instalación de equipos conforme a las normas internas de la organización



Fuente: Elaboración Propia

Los resultados muestran que la forma en que el personal aplica las normas de instalación y protección de los equipos presenta diferencias importantes entre áreas. Estas variaciones indican que no todos los colaboradores cuentan con el mismo nivel de claridad respecto a los procedimientos establecidos, lo que ocasiona prácticas inconsistentes en la manipulación, resguardo y puesta en funcionamiento de los activos tecnológicos. Mientras algunos grupos siguen los lineamientos de manera más estricta, otros ejecutan las tareas de instalación con criterios propios o con información incompleta. Esta falta de uniformidad puede generar fallos en la protección física del equipo, riesgos técnicos y una menor confiabilidad en la infraestructura operativa. Para consolidar un desempeño equilibrado, se requiere reforzar las guías internas, estandarizar los procesos y garantizar que cada colaborador comprenda las responsabilidades asociadas a la instalación y protección de los activos bajo su cargo.

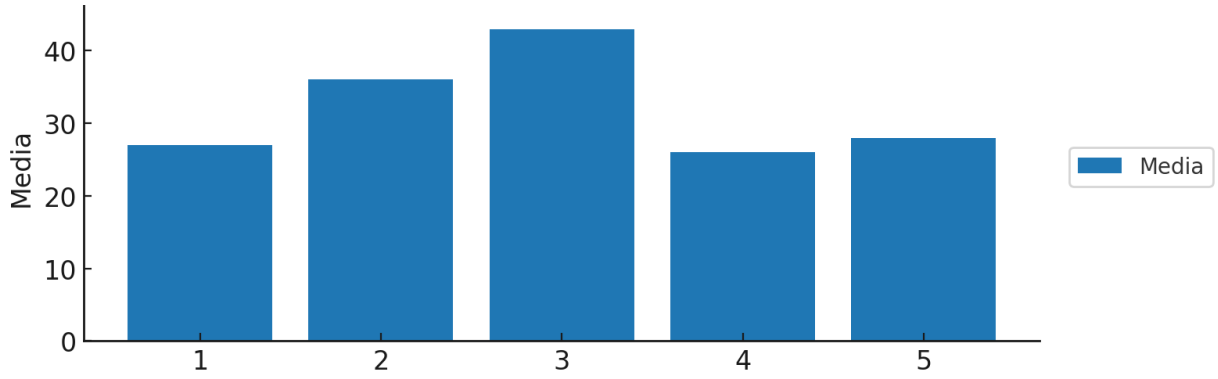
Figura 35: Cumplimiento del principio de “puesto limpio” y bloqueo de equipos al ausentarse



Fuente: Elaboración Propia

Los resultados muestran que las prácticas asociadas al principio de “puesto limpio” y al bloqueo de equipos cuando el personal se retira de su área no se aplican con el mismo nivel de rigurosidad en toda la organización. Aunque algunos colaboradores incorporan estos hábitos como parte natural de su rutina diaria, otros evidencian comportamientos más laxos que pueden dejar expuesta la información o los dispositivos de trabajo. Esta variabilidad revela que la adopción de medidas básicas de resguardo físico y lógico aún depende en gran medida de la disciplina individual y no de una cultura institucional plenamente consolidada. Para reducir la posibilidad de accesos indebidos o manipulaciones no autorizadas, se requiere integrar estas prácticas dentro de los procedimientos obligatorios, reforzar la supervisión y promover una conciencia más sólida sobre la importancia de asegurar el entorno inmediato de trabajo.

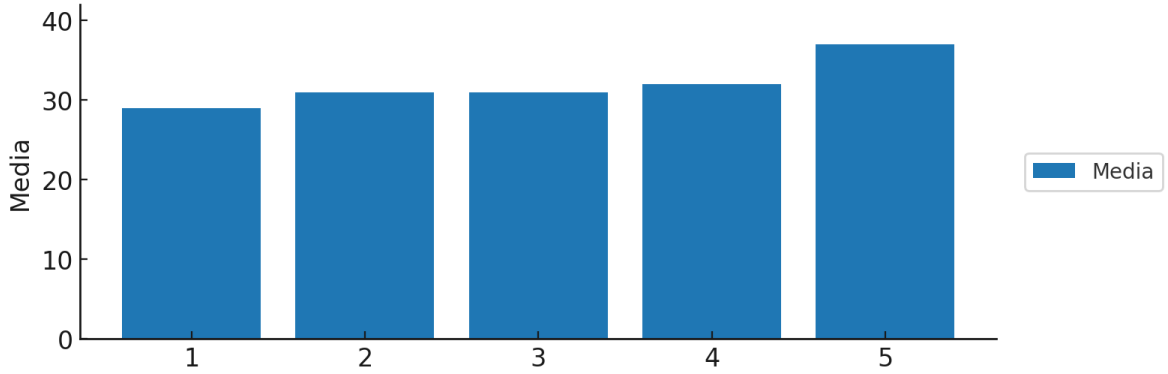
Figura 36: Protección y monitoreo de áreas sensibles como servidores y almacenes



Fuente: Elaboración Propia

Los resultados muestran que la protección y supervisión de áreas críticas, como servidores y almacenes, no se ejecuta con el mismo nivel de consistencia en toda la organización. Algunas unidades parecen aplicar controles más rigurosos, mientras que otras mantienen prácticas más básicas o irregulares, lo que genera diferencias significativas en la solidez de la seguridad física. Esta falta de uniformidad indica que la capacidad de resguardar entornos sensibles depende en gran medida del nivel de control local y no de un esquema institucional plenamente estandarizado. La variabilidad observada implica que ciertos espacios podrían quedar más expuestos a incidentes o accesos no autorizados. Para fortalecer la protección de estos puntos críticos, es necesario consolidar un esquema común de vigilancia, definir responsabilidades claras y asegurar que todos los mecanismos de monitoreo operen bajo parámetros homogéneos de control y respuesta.

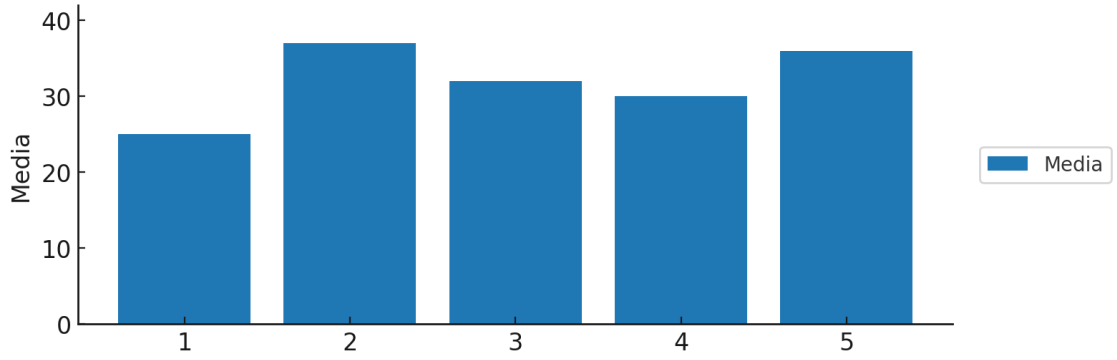
Figura 37: Funcionamiento del control de acceso físico en las áreas de trabajo



Fuente: Elaboración Propia

Los resultados muestran que los mecanismos de control de acceso físico en las áreas de trabajo funcionan con niveles variables de consistencia según la percepción del personal. Aunque una parte importante de los colaboradores considera que las medidas como el uso de credenciales, la verificación de visitantes y los procedimientos de acompañamiento operan adecuadamente, aún persisten casos en los que estos controles no se aplican con el mismo rigor. Esta diferencia sugiere que, si bien el sistema general de acceso presenta una base sólida, su efectividad depende en gran medida de la disciplina operativa en cada área. La presencia de respuestas menos favorables indica que todavía existen puntos donde la supervisión podría reforzarse para evitar desviaciones o incumplimientos. Para consolidar un entorno seguro y coherente, es necesario mantener procesos de verificación continua, estandarizar prácticas y asegurar que todos los colaboradores adopten los mismos criterios en el uso y control de los accesos físicos.

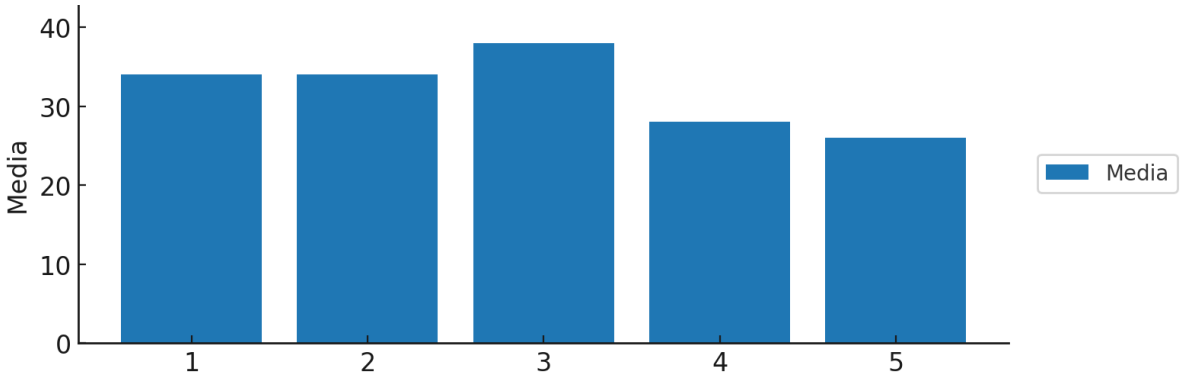
Figura 38: Capacitaciones específicas y recientes sobre riesgos asociados al rol del colaborador



Fuente: Elaboración Propia

Los resultados muestran que la formación relacionada con los riesgos propios de cada función no llega de la misma manera a todos los colaboradores. Mientras algunos empleados parecen haber participado recientemente en actividades de actualización, otros evidencian una exposición limitada o irregular a estos procesos, lo que genera diferencias importantes en el nivel de preparación frente a situaciones de riesgo. Esta desigualdad sugiere que el acceso a la capacitación depende en gran medida del área o de la dinámica interna de cada equipo, más que de un esquema institucional uniforme. Como consecuencia, la organización presenta zonas con mayor madurez en la identificación y manejo de amenazas, junto a otras que operan con conocimientos más básicos o desactualizados. Para evitar estas brechas, es necesario articular un programa formativo continuo y estructurado que asegure que todo el personal reciba orientación pertinente y oportuna en materia de gestión de riesgos.

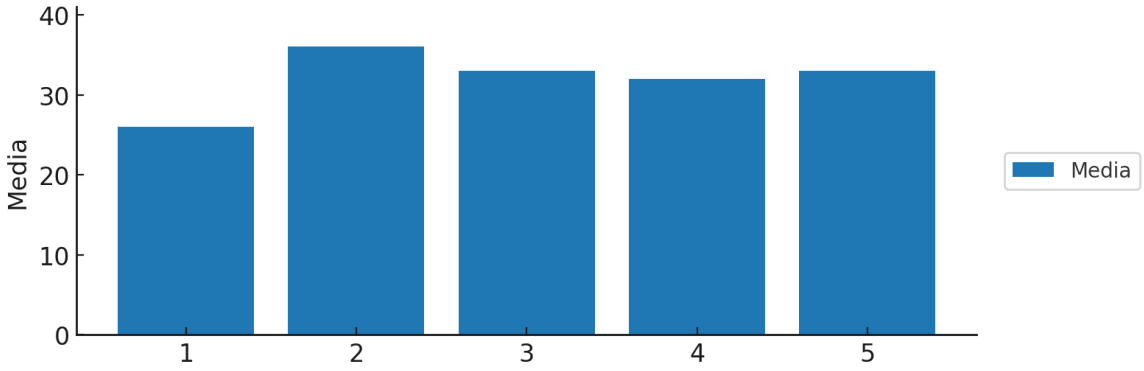
Figura 39: Lineamientos institucionales para el trabajo remoto y acceso externo a los sistemas



Fuente: Elaboración Propia

Los resultados muestran que la claridad y aplicación de las normas relacionadas con el trabajo remoto y el acceso externo a los sistemas no es uniforme entre los colaboradores. Mientras algunos empleados parecen operar con criterios claros sobre cómo conectarse de forma segura desde fuera de la oficina, otros evidencian dudas o interpretaciones inconsistentes respecto a los procedimientos establecidos. Esta variabilidad sugiere que la organización aún no cuenta con un marco de teletrabajo plenamente consolidado ni con una difusión homogénea de los requisitos para el uso seguro de los recursos tecnológicos fuera del entorno corporativo. Como consecuencia, los niveles de cumplimiento pueden diferir significativamente entre áreas, generando brechas que podrían afectar la protección de la información cuando se trabaja a distancia. Para reducir estos riesgos, es necesario fortalecer la comunicación interna, definir pautas más precisas y asegurar un monitoreo sistemático que garantice prácticas uniformes de acceso remoto.

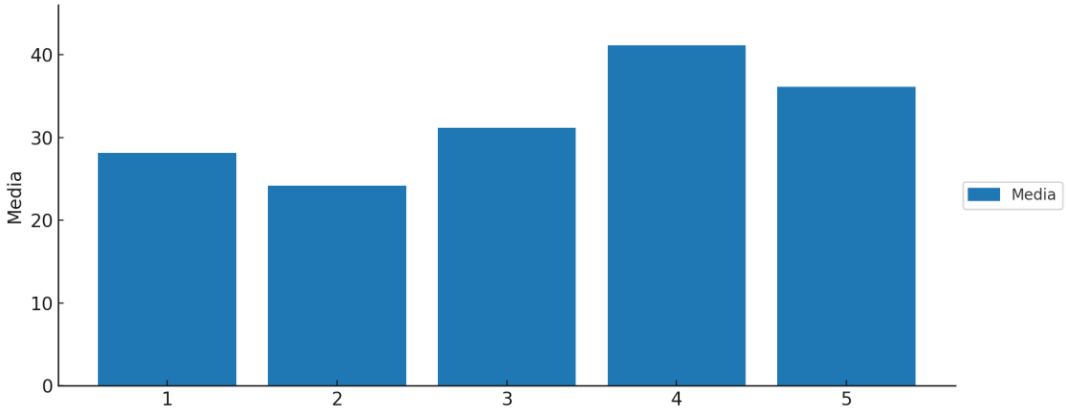
Figura 40: Conocimiento sobre los canales de contacto con el CSIRT interno ante incidentes de seguridad



Fuente: Elaboración Propia

Los resultados reflejan que el nivel de familiaridad del personal con los canales formales para contactar al CSIRT interno todavía presenta variaciones importantes entre equipos y áreas de la organización. Mientras algunos colaboradores dominan los procedimientos y saben a quién acudir ante un incidente, otros evidencian incertidumbre o desconocimiento sobre los pasos que deben seguir en una situación de riesgo. Esta disparidad sugiere que la estructura de comunicación para la gestión de incidentes no se encuentra plenamente consolidada ni se ha difundido de manera uniforme. En términos generales, el escenario apunta a la necesidad de fortalecer los mecanismos institucionales de respuesta, garantizando que todos los empleados cuenten con información clara, accesible y actualizada sobre los puntos de contacto, los tiempos de notificación y los flujos de escalamiento. Mejorar estos elementos resulta clave para asegurar una reacción rápida y coordinada frente a amenazas que puedan comprometer la seguridad de la información.

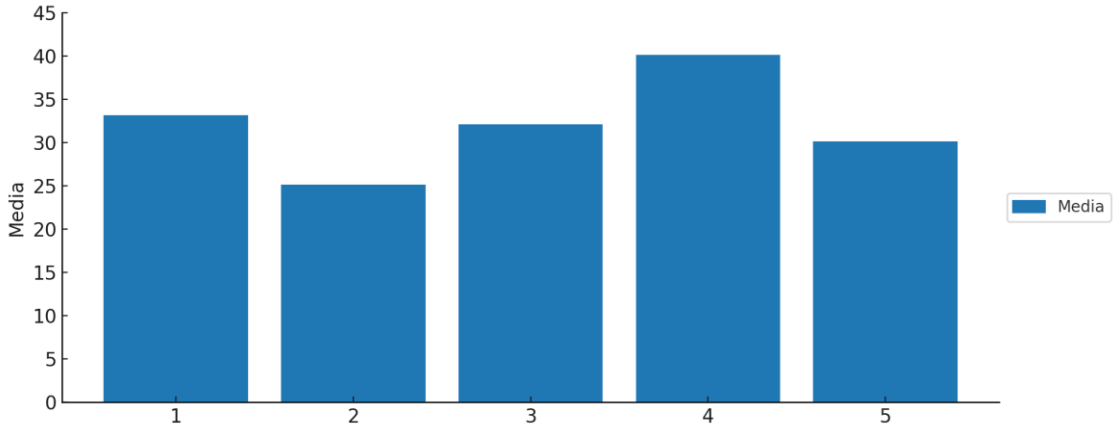
Figura 41: Cumplimiento del principio de segregación de funciones en los procesos operativos



Fuente: Elaboración Propia

Los resultados evidencian que la aplicación del principio de segregación de funciones en PROIMA presenta avances significativos, especialmente en los procesos donde la separación de responsabilidades es crítica para minimizar riesgos operativos. No obstante, también se identifican áreas en las que la distribución de tareas no se ejecuta con la rigurosidad necesaria, lo que puede generar dependencia excesiva en ciertos colaboradores o puntos vulnerables en los flujos de aprobación. Esta situación sugiere diferencias en el grado de madurez de los procesos, probablemente asociadas a la carga operativa o a la falta de lineamientos específicos en algunos departamentos. En términos generales, el panorama indica que la organización cuenta con una base sólida para este control, pero requiere fortalecer su estandarización mediante revisiones periódicas, documentación clara de roles y un monitoreo constante que asegure la correcta separación de actividades en todas las etapas operativas.

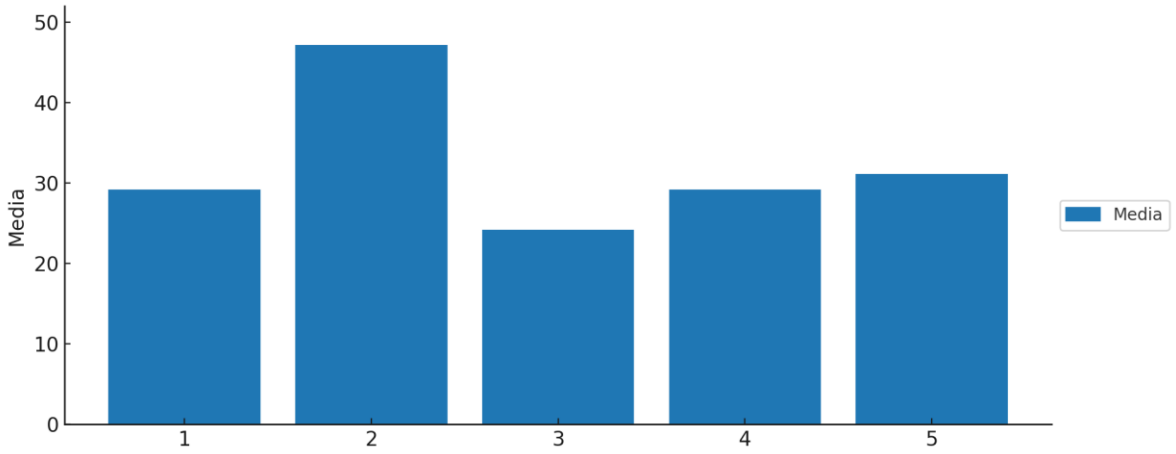
Figura 42: Claridad del rol y responsabilidades en seguridad de la información



Fuente: Elaboración Propia

Los resultados evidencian que, dentro de PROIMA, la comprensión del rol y de las responsabilidades en materia de seguridad de la información no es uniforme entre los colaboradores. Mientras algunos empleados muestran dominio claro sobre lo que se espera de ellos, otros manifiestan dudas respecto a los límites de sus funciones, lo cual genera variaciones en la manera en que se aplican las políticas internas. Esta situación revela la existencia de brechas en los procesos de comunicación institucional, especialmente en lo relativo a la definición formal de responsabilidades y a la difusión de lineamientos operativos. De forma general, los hallazgos señalan la necesidad de fortalecer la sensibilización del personal, estandarizar la asignación de roles y asegurar que cada colaborador conozca, con precisión, sus obligaciones dentro del Sistema de Gestión de Seguridad de la Información (SGSI), de modo que las prácticas de protección sean consistentes y estén alineadas a los requerimientos corporativos.

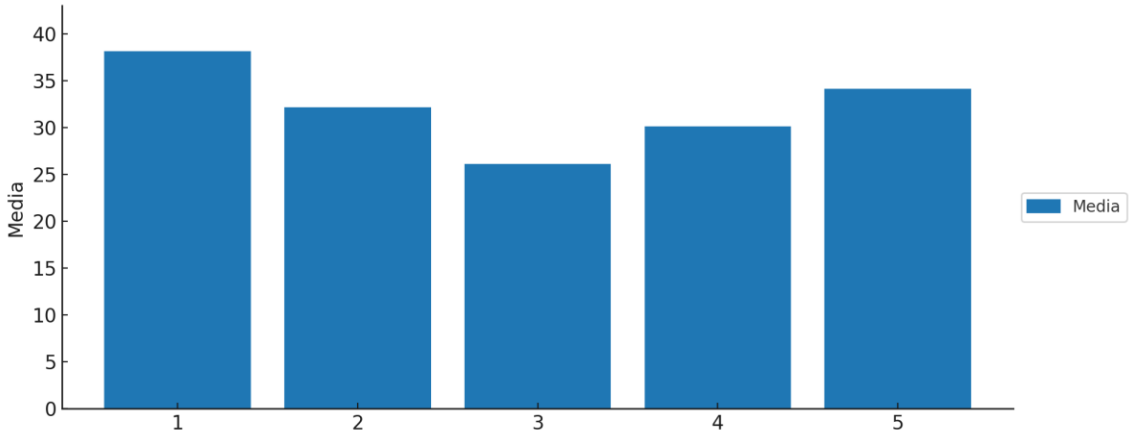
Figura 43: Conocimiento de las acciones de continuidad operativa ante la interrupción de servicios críticos (BCP/DRP)



Fuente: Elaboración Propia

Los resultados evidencian que el nivel de preparación del personal de PROIMA frente a posibles interrupciones de servicios críticos aún presenta importantes desigualdades. Una parte de los colaboradores demuestra conocimiento adecuado sobre los procedimientos de continuidad operativa y recuperación ante contingencias; sin embargo, otro grupo significativo revela limitaciones para identificar con claridad las acciones que deben ejecutarse en situaciones de emergencia. Esta brecha sugiere que los lineamientos relacionados con BCP/DRP no han sido interiorizados de manera uniforme en toda la organización. En términos generales, los hallazgos resaltan la importancia de reforzar los procesos de capacitación, documentación y socialización de los protocolos, de modo que cada empleado tenga claridad sobre su rol y sobre las medidas que garantizan la estabilidad de los servicios esenciales ante incidentes que afecten la operación.

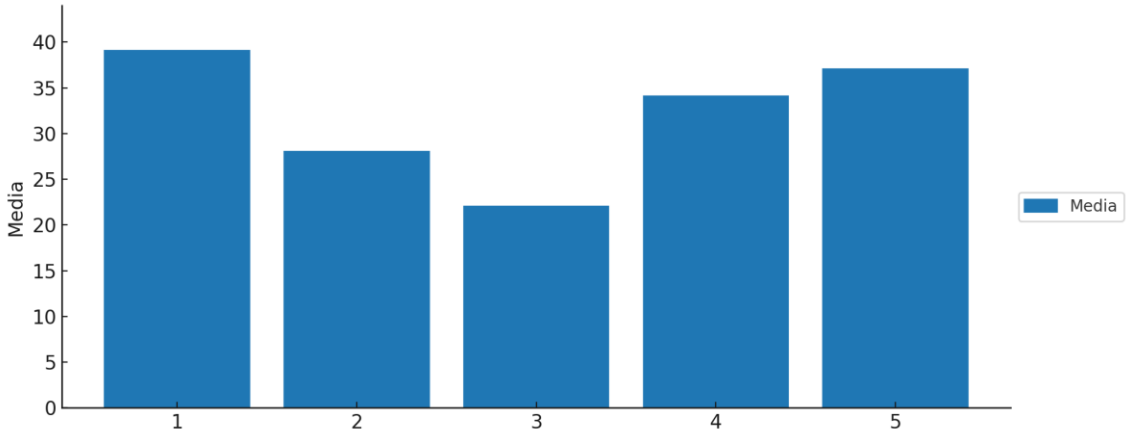
Figura 44: Gestión de riesgos asociados a terceros con acceso a información o sistemas



Fuente: Elaboración Propia

Los resultados evidencian que la percepción del personal acerca de la gestión de riesgos asociados a terceros con acceso a información o sistemas es heterogénea, lo que refleja diferencias en la forma en que estas relaciones son administradas dentro de PROIMA. El análisis sugiere que, aunque existen prácticas y controles aplicados a proveedores, socios tecnológicos y otros actores externos, su implementación no es uniforme entre las distintas áreas operativas. Esta falta de estandarización puede derivar en brechas de seguridad que expongan información sensible o procesos críticos. En términos generales, los hallazgos subrayan la necesidad de consolidar un marco integral para la gestión de terceros, que incluya evaluaciones sistemáticas, requisitos de seguridad claramente definidos y mecanismos de verificación continua, garantizando que todos los colaboradores externos se alineen con los estándares internos de protección de la información.

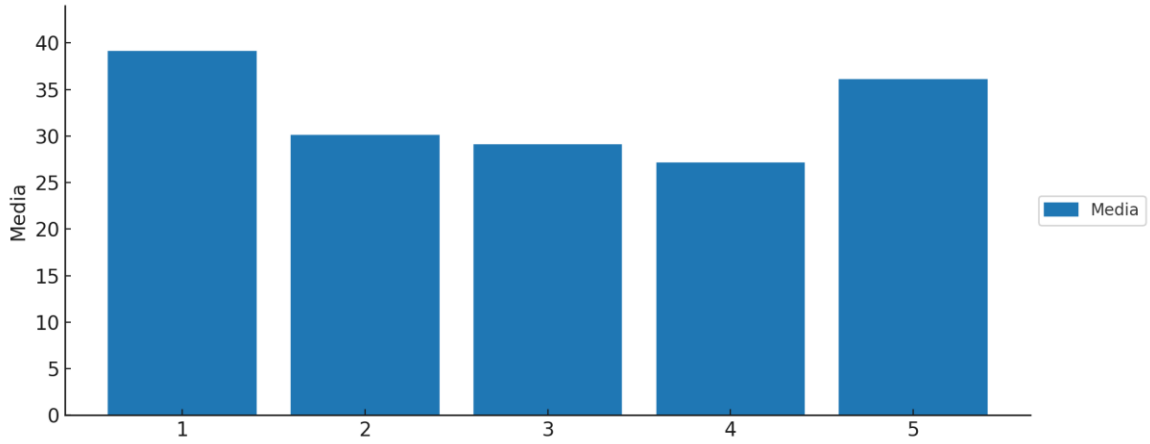
Figura 45: Clasificación y tratamiento de la información según su nivel de sensibilidad



Fuente: Elaboración Propia

Los resultados evidencian que la forma en que se clasifica y trata la información según su nivel de sensibilidad no es uniforme en toda la organización. Mientras algunas áreas parecen contar con procesos claros y aplicados de forma consistente, en otras persiste incertidumbre respecto a los criterios que determinan la categoría de la información y las medidas de protección asociadas. Esta variabilidad refleja que los lineamientos de clasificación no han sido interiorizados de manera homogénea por el personal, lo cual puede generar riesgos en el manejo de datos sensibles. En términos generales, los hallazgos resaltan la necesidad de fortalecer la cultura organizacional en torno al ciclo de vida de la información, estandarizando procedimientos, asegurando la correcta identificación de los niveles de sensibilidad y promoviendo la adopción de prácticas alineadas al Sistema de Gestión de Seguridad de la Información.

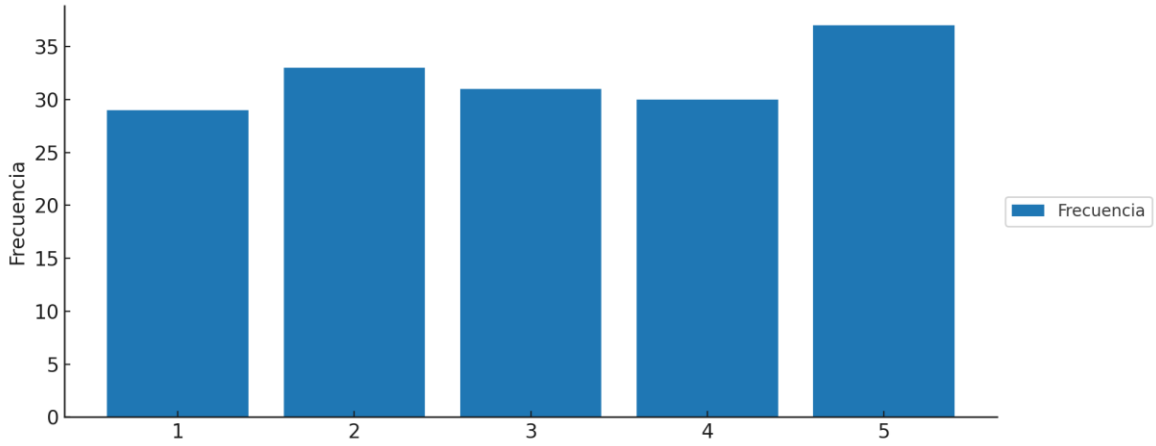
Figura 46: Identificación y cumplimiento de los requisitos legales y contractuales aplicables al puesto de trabajo



Fuente: Elaboración Propia

Los resultados evidencian que el nivel de comprensión y aplicación de los requisitos legales y contractuales asociados a las funciones del personal no es homogéneo dentro de la organización. Mientras parte del equipo demuestra familiaridad con las obligaciones normativas que regulan su labor, otro grupo refleja dudas o desconocimiento sobre los compromisos que deben observarse en el ejercicio de sus responsabilidades. Esta variabilidad apunta a que la comunicación institucional sobre los marcos legales aplicables no llega con la misma claridad a todas las áreas, lo que puede generar inconsistencias en el cumplimiento. En conjunto, los hallazgos subrayan la necesidad de fortalecer los mecanismos de orientación y formación en materia regulatoria, garantizando que todo el personal cuente con criterios claros para el manejo adecuado de la información, el cumplimiento corporativo y la alineación con las obligaciones vigentes.

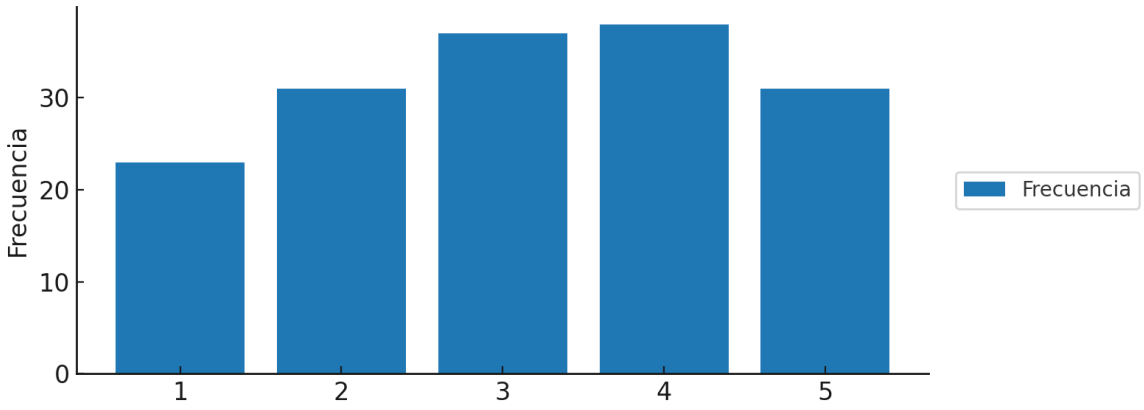
Figura 47: Conocimiento de los cambios recientes en políticas y procedimientos internos



Fuente: Elaboración Propia

El histograma revela niveles heterogéneos de conocimiento entre el personal respecto a las modificaciones recientes en políticas y procedimientos internos. Mientras un grupo significativo manifiesta claridad sobre los cambios implementados, otro sector indica no haber recibido información suficiente oportuna, lo que evidencia un desfase en la transmisión de comunicados oficiales. Esta variación sugiere que los procesos de divulgación institucional no están llegando de manera consistente a todas las unidades operativas. En términos generales, los resultados apuntan a la necesidad de reforzar los mecanismos formales de notificación y seguimiento, de modo que toda la organización reciba, comprenda y adopte de forma uniforme las actualizaciones normativas que impactan el desempeño de sus funciones.

Figura 48: Disponibilidad, comprensión y aplicación de la política de seguridad en el entorno laboral



Fuente: Elaboración Propia

El histograma evidencia que el nivel de conocimiento y uso de la política de seguridad de la información varía entre las diferentes áreas de PROIMA. La concentración de respuestas en los puntos intermedios sugiere que, si bien una parte significativa del personal reconoce la existencia de estas directrices y las aplica en cierta medida, todavía persisten inconsistencias en su comprensión y uso cotidiano. Las respuestas más bajas muestran que algunos colaboradores no cuentan con la claridad necesaria para incorporar estas políticas en sus labores diarias, lo que podría generar brechas en la gestión de la seguridad. En términos globales, los hallazgos resaltan la importancia de consolidar mecanismos de difusión y formación continua que faciliten una apropiación plena de las políticas, promoviendo su adopción transversal y fortaleciendo la cultura institucional de protección de la información.

Anexo 11. Acta de Validación por Juicio de Expertos

ACTA DE VALIDACIÓN DE INSTRUMENTO DE INVESTIGACIÓN

En la ciudad de Tegucigalpa, M.D.C., se reunió el panel de expertos convocado para evaluar el instrumento de investigación correspondiente al estudio titulado: "Estudio Exploratorio de las Prácticas y Desafíos en la Gestión de Riesgos de Seguridad de la Información en PROIMA, Honduras".

Panel de Expertos Evaluadores:

1. Asesor con especialización en gestión de TI
2. Especialista interno de PROIMA (ISO 27001 Lead Implementer, 8 años de experiencia)
3. Consultor externo en ciberseguridad (CISM, CISSP, 10+ años en auditorías)

Resultados de la Evaluación:

Criterios evaluados (escala 1-4): Claridad (IVC=0.92), Pertinencia (IVC=0.97), Coherencia (IVC=0.90), Suficiencia (IVC=0.88). Índice de Validez de Contenido Global: IVC = 0.92 (supera umbral de 0.80).

Decisiones sobre ítems:

- Ítems reformulados (3): P07, P12, P18 por ambigüedad o términos técnicos.
- Ítems eliminados (1): P23 por redundancia con P05.

Dictamen: APROBADO para aplicación con modificaciones incorporadas.

Tegucigalpa, M.D.C., 2025

Anexo 12. Análisis de Fiabilidad - Salida SPSS

ANÁLISIS DE FIABILIDAD - PRUEBA PILOTO (n=25)

```
RELIABILITY ANALYSIS - SCALE (ALPHA)
Escala: Instrumento completo (24 ítems)
Resumen de procesamiento de casos:
  Casos válidos:      25    100.0%
  Casos excluidos:     0      0.0%
  Total:              25    100.0%
Estadísticas de fiabilidad:
+-----------------------------------------+
| Alfa de Cronbach | N de elementos    |
|       .890       |        24         |
+-----------------------------------------+
Estadísticas por dominio:
  A.5 Políticas (4 ítems):      α = .840
  A.6 Organización (5 ítems):   α = .812
  A.7 Controles físicos (6):    α = .791
  A.8 Tecnológicos (9 ítems):   α = .858
```

Interpretación: Todos los dominios superan α ≥ 0.70

```
Decisión: Instrumento APTO para aplicación definitiva.
```

Fuente: Salida IBM SPSS Statistics v.27, prueba piloto mayo 2025.