

Análisis de la Seguridad de la Información en la Era Digital
Un Enfoque Basado en la Gestión de Riesgos

Alumno: Ruppel, Yain Omar

Profesora de Trabajo Final: Dra. Marcela Samela.

Trabajo Final de Carrera presentado para obtener el título de

Lic. en Gestión de Tecnología informática

Julio 2025

Resumen

La presente investigación aborda el problema de la seguridad de la información en el contexto de una era digital marcada por la evolución constante de amenazas cibernéticas. Se adopta como eje central la gestión de riesgos, analizando cómo las organizaciones identifican, evalúan y tratan los riesgos que comprometen la confidencialidad, integridad y disponibilidad de sus activos informáticos. El estudio examina los factores que influyen en la efectividad de las estrategias de gestión de riesgos y su impacto en la reducción de incidentes, así como el nivel de confianza generado en los usuarios. Asimismo, se analiza el aporte de las herramientas basadas en inteligencia artificial en los procesos de detección, análisis y respuesta ante amenazas. Mediante un enfoque mixto, que combina encuestas y entrevistas a profesionales del área, se obtiene una visión integral del estado actual de la ciberseguridad en diversos sectores organizacionales, proponiendo recomendaciones para fortalecer las prácticas existentes y promover una cultura preventiva y resiliente frente a los riesgos digitales.

Palabras clave: activos de información, amenazas, ciberseguridad, controles de seguridad, evaluación de riesgos, gestión de riesgos, mitigación, vulnerabilidades.

Abstrac

This research addresses the issue of information security in the context of a digital era marked by the constant evolution of cyber threats. Risk management is adopted as the central axis, analyzing how organizations identify, assess, and treat the risks that compromise the confidentiality, integrity, and availability of their information assets. The study examines the factors that influence the effectiveness of risk management strategies and their impact on incident reduction, as well as the level of trust generated among users. Furthermore, it analyzes the contribution of artificial intelligence-based tools in the processes of threat detection, analysis, and response. Through a mixed-methods approach, combining surveys and interviews with cybersecurity professionals, the research provides a comprehensive view of the current state of cybersecurity in various organizational sectors, offering recommendations to strengthen existing practices and foster a preventive and resilient culture in the face of digital risks.

Keywords: artificial intelligence, cyber threats, cybersecurity, information assets, mitigation, risk assessment, risk management, security controls, vulnerabilities.

Dedicatoria

Dedico este trabajo con todo mi amor a mi querida novia, Sol. Gracias por tu incondicional apoyo, paciencia y amor a lo largo de todo este proceso.

A mis adorables gemelas Cata y Delfi, quienes llegaron a nuestras vidas en medio de la carrera y para cambiarlo todo. Ustedes han sido mi mayor inspiración y motivación. Sus sonrisas y alegrías me recuerdan diariamente el porqué de mis esfuerzos.

Índice General

Resumen 2

Abstrac 3

Dedicatoria 4

Índice General 5

Índice de Figuras 7

Índice de Tablas 8

CAPITULO 1 Introducción 9

1.1 Pregunta de la investigación 9

1.2 Hipótesis 9

1.2 Justificación de la propuesta 9

1.3 Objetivo general 10

1.3.1 Objetivos específicos 10

1.4 Contribuciones Principales 10

1.5 Estado del Arte 11

CAPITULO 2 Marco Teórico 16

2.1 Conceptos claves de seguridad de la información 16

2.2 La importancia de la seguridad de la información en las organizaciones 17

2.3 Gestión de Riesgos 18

2.4 Amenazas y vulnerabilidades en la seguridad de la información 20

2.5 Comprendiendo las Amenazas Cibernéticas 21

2.6 Integración de la Inteligencia Artificial en Seguridad de la Información 22

2.7 Fundamentos y Estrategias de Gestión de Riesgos en Seguridad Informática 24

2.8 Ciclo de vida de la gestión de riesgos: identificación, evaluación, mitigación y monitoreo de riesgos 26

2.9.1 ISO 27001: estándar internacional para la gestión de la seguridad de la información 30

2.9.2 COBIT: Marco de Gestión de TI y Seguridad de la Información 33

CAPITULO 3 Metodología 38

3.1 Enfoque de la Investigación 38

3.2 Métodos de Recolección de Datos 38

CAPITULO 4 Conclusiones 40

4.1 Contribuciones y limitaciones de la investigación 40

4.2 Informe final 41

4.2.1 Perfil general de los encuestados 41

4.2.2 Seguridad de la información en la organización 42

4.2.3 Gestión de riesgos en entornos digitales 43

4.2.4 Uso de inteligencia artificial y percepción personal 45

4.2.5 Análisis cualitativo: Entrevistas a profesionales de ciberseguridad 46

4.3 Conclusión 47

4.4 Direcciones futuras de investigación 49

4.5 Recomendaciones 50

4.6 Referencias bibliográficas 52

4.7 Anexos 53

4.7.1 Anexo 1 - Encuesta 53

4.7.2 Anexo 2 - Preguntas realizadas a los profesionales entrevistados 58

Índice de Figuras

Figura 1 Componentes de la información 17
Figura 2 Componentes de la Gestión de Riesgos..... 19
Figura 3 Interacción entre el Marco de gestión de Riesgos y el proceso de gestión de Riesgos. 25
Figura 4 Principios de COBIT 5 34
Figura 5 Componentes de la estructura 35
Figura 6 Tipos de organizaciones encuestadas 41

Índice de Tablas

Tabla 1 Activos organizacionales utilizados en sistemas 27
Tabla 2 Estrategias Principales para tratar los riesgos asociados a los activos de información 30
Tabla 3 Acciones específicas de ciclo PDCA 31
Tabla 4 Tamaño de la organización 42
Tabla 5 Tamaño de la organización 42
Tabla 6 Las prácticas de gestión de riesgos en las organizaciones 44
Tabla 7 Métodos o herramienta para evaluar riesgos 44
Tabla 8 Preferencia de uso de herramientas de IA 45

CAPITULO 1 Introducción

La seguridad de la información se ha transformado en un desafío crítico en el contexto actual, caracterizado por un entorno digital cada vez más interconectado. Según Whitman y Mattord (2022, p 122), el rápido avance tecnológico y la globalización de las comunicaciones han incrementado las amenazas cibernéticas, comprometiendo aspectos esenciales como la confidencialidad, la integridad y la disponibilidad de los datos. Aunque se implementan medidas como la autenticación de dos factores para garantizar la seguridad, estas pueden ser percibidas como incómodas por los usuarios, lo que genera tensiones entre la accesibilidad y la protección. Esto resalta la importancia de desarrollar estrategias sólidas que aseguren la protección de los activos de información y la continuidad de las operaciones.

Además, para aquellas organizaciones que dependen de sistemas de tecnología de la información, es esencial integrar la seguridad de la información y la gestión de riesgos en sus decisiones estratégicas. Whitman y Mattord (2022, p123) enfatizan que estas decisiones deben equilibrar los costos asociados con los controles de seguridad y los beneficios de operar en un entorno seguro, lo que permite construir una base económica sólida que respalde la viabilidad y disponibilidad.

1.1 Pregunta de la investigación

¿Cuáles son los factores determinantes para una implementación efectiva de estrategias de gestión de riesgos de seguridad de la información en entornos digitales?

1.2 Hipótesis

La implementación de la gestión de riesgos en la seguridad de la información, complementada con herramientas de inteligencia artificial, reduce los incidentes de seguridad y mejora la protección de la información crítica.

1.2 Justificación de la propuesta

La gestión de riesgos en la seguridad de la información representa un componente esencial en la protección de los activos informacionales frente a amenazas cibernéticas cada vez más sofisticadas. Como afirman Whitman y Mattord (2022, p. 123), esta disciplina permite gestionar eficazmente los riesgos asociados al uso de la información, mediante procesos estructurados y repetibles que identifican, evalúan y mitigan

vulnerabilidades. En un contexto digital marcado por la aceleración de los ataques y la criticidad de los datos, estas prácticas adquieren un rol estratégico en las políticas de ciberseguridad organizacional.

La presente investigación adquiere relevancia al proponer un abordaje que combina la gestión de riesgos con herramientas de inteligencia artificial, lo que permite optimizar la detección, análisis y respuesta frente a amenazas emergentes. Esta integración tecnológica mejora la capacidad predictiva de los sistemas de seguridad y fortalece la resiliencia organizacional. El estudio, además, aporta marcos teóricos y metodológicos que contribuyen al avance del conocimiento en materia de seguridad informacional, ofreciendo insumos valiosos tanto para el ámbito académico como para la implementación práctica en sectores clave como el empresarial, gubernamental, educativo y financiero.

1.4 Objetivo general

Evaluar el impacto de la gestión de riesgos en la seguridad de la información, incorporando el uso de inteligencia artificial, para determinar su efectividad en la reducción de incidentes y la protección de datos críticos en entornos organizacionales.

1.4.1 Objetivos específicos

Examinar las políticas de seguridad implementadas en entornos digitales para identificar fortalezas y debilidades en la gestión de riesgos.

Evaluar la influencia de las acciones de concientización y capacitación del personal en la prevención de incidentes de seguridad.

Analizar los riesgos y beneficios asociados al uso de inteligencia artificial en la gestión de la seguridad de la información.

1.5 Contribuciones Principales

La misión principal de cualquier programa de seguridad de la información es proteger los activos críticos de las organizaciones, asegurando que la información y los sistemas que la contienen se mantienen seguros y útiles. Según Whitman y Mattord (2022, p28), las organizaciones invierten considerables recursos financieros y humanos en cuidar estos activos. Sin embargo, la constante amenaza de ataques y la creciente

sofisticación de las técnicas utilizadas obligan a las organizaciones a priorizar la seguridad sobre la mejora exclusiva.

En este contexto, el presente trabajo aborda las demandas de un entorno digital marcado por amenazas avanzadas y la rápida adopción de tecnologías emergentes. A través de un análisis detallado de las políticas y procedimientos de seguridad, se identifican tanto fortalezas como debilidades en diversos entornos digitales. Además, se evalúan prácticas de concientización y capacitación del personal para medir su efectividad en la creación de una cultura de seguridad. Estas contribuciones están orientadas a fortalecer la capacidad de las organizaciones para proteger sus activos de información y asegurar la continuidad de sus operaciones en un entorno digital cada vez más complejo y cambiante.

1.6 Estado del Arte

Aguirre Sánchez (2023) llevó a cabo una investigación sobre la implementación de un sistema de gestión de riesgos de seguridad de la información en la Empresa Pública Mancomunidad de Tránsito de Tungurahua (EPMTT). Su hipótesis central sostiene que una gestión de riesgos adecuada, complementada con políticas, procedimientos y controles formales, mejora significativamente la protección de la información organizacional. El estudio parte del principio de que una gestión eficaz salvaguarda los tres pilares fundamentales de la seguridad de la información: integridad, confidencialidad y disponibilidad.

Para evaluar el grado de avance institucional, se utilizó un modelo de madurez, que permitió medir el progreso desde un nivel “Básico” hasta llegar a un nivel “Administrado”, con proyección a un estado “Óptimo”. La propuesta se fundamentó en las directrices de la norma ISO/IEC 27001, estableciendo criterios internacionales para la implementación de un sistema de gestión de seguridad de la información (SGSI).

En una evaluación inicial, se evidenció que las prácticas de gestión de riesgos en la EPMTT eran inconsistentes, descentralizadas y carentes de formalización, además de una escasa capacitación del personal. Sin embargo, tras la implementación de las recomendaciones planteadas, la organización logró alcanzar un nivel “Administrado”, incorporando un sistema formal y estructurado, con revisiones periódicas y documentación conforme a estándares internacionales (Aguirre Sánchez, 2023).

Villacorta Vidal (2023) desarrolló una investigación centrada en la incorporación de la inteligencia artificial (IA) en la seguridad de la información dentro de las organizaciones. Para ello, aplicó la metodología PRISMA, que le permitió realizar un análisis sistemático y fundamentado en evidencia de la literatura existente, abarcando tanto los aspectos técnicos como los dilemas éticos asociados al uso de IA en este ámbito.

El objetivo principal del estudio fue evaluar cómo la IA puede contribuir a optimizar la protección de la información a través de la automatización de respuestas ante incidentes, la prevención de pérdida de datos y la detección avanzada de amenazas. Asimismo, se consideraron cuestiones vinculadas a la privacidad y la ética digital. Los hallazgos revelan que la IA puede mejorar sustancialmente la eficiencia y la velocidad de respuesta ante incidentes de seguridad, al mismo tiempo que reduce los riesgos relacionados con la pérdida de datos sensibles y mejora la capacidad de anticiparse a posibles ataques

No obstante, el autor advierte sobre desafíos significativos, como el uso de IA por parte de ciberdelincuentes para desarrollar malware avanzado, la sofisticación de técnicas de ingeniería social y la aparición de nuevas vulnerabilidades en sistemas de autenticación. Estas amenazas exigen un enfoque regulado y estratégico en la adopción de soluciones basadas en IA.

Entre las limitaciones del estudio se destaca el acceso restringido a ciertos artículos científicos, lo cual podría haber reducido la profundidad del análisis. Además, algunos trabajos revisados presentan una tendencia a generalizar conclusiones sin tener en cuenta las particularidades contextuales de cada organización, e incluso a centrarse más en los riesgos que en los beneficios, lo que puede generar una percepción sesgada sobre el verdadero potencial de la IA. En definitiva, la investigación concluye que, aunque la inteligencia artificial representa un recurso valioso para fortalecer la seguridad de la información, su implementación debe estar cuidadosamente planificada y sujeta a marcos éticos y regulatorios adecuados (Villacorta Vidal, 2023).

Guaña-Moya (2023) analiza la importancia de la seguridad informática en el ámbito educativo, destacando que la gestión de riesgos es esencial para identificar, evaluar y mitigar amenazas que puedan comprometer los sistemas institucionales. En este contexto, las auditorías de seguridad se presentan como herramientas fundamentales para detectar vulnerabilidades y aplicar controles eficaces que reduzcan los riesgos operativos. El autor subraya que los usuarios (tanto estudiantes como docentes y personal administrativo) constituyen el eslabón más débil en la cadena de seguridad, por lo que resulta

indispensable fomentar la concienciación y la capacitación en buenas prácticas, incluyendo el uso de contraseñas robustas y la prevención frente a ataques de phishing (Guaña-Moya, 2023).

Asimismo, se resalta la importancia de aplicar normas internacionales como la ISO/IEC 27002:2013, que proporciona lineamientos estandarizados para establecer controles efectivos en instituciones educativas. Estas normas promueven un enfoque integral que combina tecnologías, políticas institucionales y programas de formación para crear entornos más seguros (Guaña-Moya, 2023).

El autor también aborda problemáticas particulares como el ciberbullying, señalando que existen recursos digitales interactivos diseñados para sensibilizar a estudiantes y familias sobre sus efectos, y prevenir su ocurrencia. En relación con la evolución de las auditorías, se menciona la aplicación de metodologías como el Penetration Testing Execution Standard (PTES), que permite identificar vulnerabilidades críticas en los sistemas y proponer medidas concretas para fortalecer la seguridad en el entorno educativo (Guaña-Moya, 2023).

Torres Ramírez (2023) llevó a cabo una investigación cuyo objetivo principal fue demostrar cómo el uso de técnicas de hacking ético puede contribuir a mejorar la gestión de riesgos informáticos en la Clínica Americana Serfarmed de Pucallpa. El estudio partió de la necesidad crítica de proteger los datos sensibles de los pacientes y reforzar la infraestructura tecnológica, la cual había evidenciado vulnerabilidades ante amenazas como el phishing y los accesos no autorizados. La investigación se desarrolló bajo un enfoque cuantitativo y utilizó un diseño cuasiexperimental, dividido en distintas fases: planificación, descubrimiento, ataque y reporte. En la etapa de descubrimiento, se emplearon herramientas especializadas como Nmap, Nessus y OpenVAS para realizar actividades de escaneo y enumeración, con el fin de identificar servicios activos y posibles puntos débiles. Posteriormente, en la fase de ataque, se aplicaron técnicas de penetración controlada utilizando exploits y herramientas como Metasploit, incluso simulando ataques con elevación de privilegios para evaluar el impacto potencial de las amenazas reales. Finalmente, se elaboró un informe detallado que documentó las vulnerabilidades halladas y ofreció recomendaciones específicas para su mitigación.

Los resultados fueron contundentes: se identificaron 35 vulnerabilidades y 10 amenazas, clasificadas en distintos niveles de riesgo (alto, medio y bajo), lo cual permitió establecer prioridades en las acciones correctivas. El estudio concluyó que la implementación del hacking ético fortaleció significativamente la postura de seguridad de la clínica, mejorando su capacidad para prevenir y responder ante incidentes. Asimismo, se recomendó mantener programas de capacitación continua para el personal

de TI, realizar auditorías periódicas, y establecer un sistema de seguimiento que evalúe la efectividad de las medidas a lo largo del tiempo. En suma, el trabajo demuestra que el hacking ético puede ser una herramienta estratégica dentro de una política integral de gestión de riesgos (Torres Ramírez, 2023).

Custodio Chavarría, Arana Orrego y Valles Ríos (2025) desarrollaron una investigación orientada al diseño de un marco de referencia para mejorar la seguridad en entornos multi-cloud, en respuesta a la creciente exposición a brechas de seguridad en arquitecturas distribuidas. Los autores reportan que más del 80 % de las organizaciones encuestadas habían sufrido al menos un incidente de ciberseguridad, siendo las filtraciones de datos el tipo de amenaza más común. Esta situación se complica aún más en ambientes multi-nube, debido a la fragmentación de servicios, la dificultad de integración y la limitada visibilidad de los sistemas (Custodio Chavarría et al., 2025).

La propuesta metodológica combinó una revisión sistemática de literatura científica con un estudio de caso, aplicando matrices de evaluación de riesgos y priorización de amenazas. Además, se integraron marcos reconocidos internacionalmente como el NIST Cybersecurity Framework (CSF 2.0) y MITRE ATT&CK, orientando el diseño de controles a cinco funciones clave: gobernar, identificar, proteger, detectar y responder (Custodio Chavarría et al., 2025). Se incluyeron técnicas para mitigar amenazas como phishing, ransomware, accesos indebidos y errores de configuración.

A partir del diagnóstico, se implementó un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001, que permitió detectar riesgos como accesos no autorizados, pérdida de información y deficiencias en la gestión de contraseñas. Luego, se diseñaron controles específicos: políticas de acceso, procedimientos de respaldo, recuperación ante incidentes y capacitación del personal en buenas prácticas de seguridad (Custodio Chavarría et al., 2025).

Uno de los principales aportes fue establecer roles claros, definir responsabilidades y reforzar el compromiso de la alta dirección con la ciberseguridad. El trabajo demuestra que, incluso con recursos limitados, es posible establecer modelos sólidos de gestión de riesgos si se siguen buenas prácticas internacionales y se promueve una cultura organizacional orientada a la seguridad (Custodio Chavarría et al., 2025).

Morales Loayza, Neyra Montoya y Vidal Alegría (2021) propusieron un modelo cuantitativo de análisis de riesgos aplicable a la ciberseguridad en el sector financiero, como respuesta a las limitaciones de los enfoques cualitativos tradicionales. Su propuesta busca transformar variables abstractas como

amenazas y vulnerabilidades en valores medibles que faciliten decisiones basadas en evidencia (Morales Loayza et al., 2021).

El modelo permite la cuantificación de activos críticos, así como la estandarización de amenazas y su impacto. Se basa en el uso de matrices de riesgo y se alinea con los lineamientos de la norma ISO 31000:2018, lo que garantiza su aplicabilidad y replicabilidad en distintos contextos organizacionales (Morales Loayza et al., 2021). Esta metodología posibilita priorizar acciones correctivas e invertir con mayor precisión en medidas de seguridad.

Entre sus resultados, los autores aplicaron el modelo en entidades financieras reales, identificando accesos no autorizados a bases de datos como riesgo crítico. El análisis permitió estimar pérdidas potenciales asociadas a estos incidentes, tanto económicas como reputacionales, lo cual justificó la adopción de soluciones como la autenticación multifactor y el monitoreo avanzado (Morales Loayza et al., 2021). El modelo de Morales Loayza et al. (2021) aporta un enfoque riguroso y práctico que refuerza la gestión de riesgos mediante el uso de datos cuantificables y estándares internacionales.

CAPITULO 2 Marco Teórico

La seguridad de la información ha emergido como un pilar crítico en la era digital, impulsada por el vertiginoso crecimiento de la tecnología y la globalización de las comunicaciones. Este capítulo proporciona una visión exhaustiva de los elementos esenciales en la protección de los datos y sistemas de información de una organización, abarcando desde los conceptos fundamentales hasta las prácticas avanzadas de gestión de riesgos. Inicialmente, se detallan los principios básicos de la seguridad de la información, que incluyen la confidencialidad, integridad y disponibilidad, y su relevancia en la protección de los activos informáticos. Se exploran los componentes de la gestión de riesgos, un proceso esencial que comprende la identificación, evaluación y mitigación de riesgos, asegurando que las organizaciones estén preparadas para enfrentar y minimizar las amenazas. El capítulo también examina las diversas amenazas y vulnerabilidades que pueden comprometer la seguridad, destacando la necesidad de estrategias efectivas de defensa. Se describen los tipos comunes de ataques cibernéticos y las técnicas de compromiso que utilizan los actores maliciosos para explotar debilidades en los sistemas. Este capítulo ofrece un marco integral para entender y aplicar prácticas de seguridad de la información y gestión de riesgos, proporcionando a las organizaciones las herramientas necesarias para proteger sus activos en un entorno digital cada vez más complejo y desafiante.

2.1 Conceptos claves de seguridad de la información

La seguridad de la información ha adquirido una relevancia creciente en los últimos años, impulsada por el desarrollo acelerado de las tecnologías y la expansión global de las comunicaciones. Según Whitman y Mattord (2022, p 2), cualquier organización, sin importar su tamaño ni si es pública o privada posee información valiosa que necesita resguardar, como datos de clientes, productos, servicios o empleados. Proteger esa información es una responsabilidad institucional que involucra a todos los actores relacionados con la organización. En este sentido, la seguridad de la información busca garantizar que los datos y sistemas sean confidenciales, íntegros y estén disponibles cuando se los necesite. Comprender estos principios fundamentales es esencial para enfrentar los desafíos actuales en este ámbito. Tal como lo representa el triángulo de la seguridad de la información en la figura 1 se requiere un enfoque equilibrado para asegurar que los datos permanezcan protegidos, exactos y accesibles en todo momento.

Figura 1

Componentes de la información



Nota. (fuente: https://ticsalborada1.fandom.com/es/wiki/1._Principios_de_la_seguridad_inform%C3%A1tica:_Confidencialidad,_Integridad_y_Disponibilidad_de_la_informaci%C3%B3n)

La utilidad de la información depende de las cualidades que la definen, ya que estas determinan su valor en distintos contextos. Si alguna de esas propiedades se ve alterada, su valor puede cambiar considerablemente (Whitman & Mattord, 2022, p 11). La confidencialidad implica limitar el acceso solo a personas autorizadas, y para mantenerla es clave aplicar políticas claras de seguridad, resguardar adecuadamente los documentos y clasificarlos correctamente. Por su parte, la integridad se relaciona con la precisión y fiabilidad de los datos; si estos se alteran o destruyen, se pone en riesgo la operación de toda la organización. Para prevenirlo, se emplean mecanismos como algoritmos hash, copias redundantes o códigos de corrección. Finalmente, la disponibilidad asegura que la información esté accesible cuando se la necesite, aunque esto puede verse afectado por amenazas como ciberataques, errores técnicos o desastres. Por eso, es necesario contar con sistemas de respaldo y recuperación que mantengan el acceso constante a los datos.

2.2 La importancia de la seguridad de la información en las organizaciones

En el escenario actual de transformación digital, la seguridad de la información se ha consolidado como una prioridad estratégica para las organizaciones. El crecimiento sostenido de las amenazas cibernéticas exige que las empresas comprendan el entorno operativo de sus sistemas informáticos, de modo que puedan anticipar y gestionar tanto riesgos actuales como potenciales que comprometan la

continuidad del negocio. En este contexto, la gestión de riesgos adquiere un rol central, no solo en la protección de los activos de información, sino también en el sostenimiento de la confianza de los clientes y la reputación institucional. Asimismo, la incorporación de tecnologías basadas en inteligencia artificial ofrece nuevas posibilidades para optimizar los procesos de análisis, detección y respuesta frente a amenazas emergentes.

Según Whitman y Mattord (2011, p 41), la función principal de un programa de seguridad informática es preservar la integridad de los sistemas y de la información que resguardan. Para cumplir este objetivo, las organizaciones deben invertir importantes recursos económicos y humanos, dado que los ataques informáticos se han convertido en eventos cotidianos. Estas amenazas, cada vez más sofisticadas, exigen que los programas de seguridad evolucionen de forma constante y que se adapten a las particularidades del entorno tecnológico en el que se implementan.

Los autores identifican cuatro funciones esenciales que cumple la seguridad de la información en el ámbito organizacional. La primera es garantizar la operatividad de la organización, asegurando que sus procesos críticos puedan mantenerse activos incluso ante eventos disruptivos. La segunda función consiste en proteger el funcionamiento seguro de las aplicaciones utilizadas en los sistemas de tecnología de la información, lo cual implica mitigar vulnerabilidades que puedan comprometer la integridad y disponibilidad de los datos. En tercer lugar, se destaca la protección de los datos que la organización recopila y utiliza, tanto aquellos almacenados como los que se encuentran en tránsito. Para ello, Whitman y Mattord (2011, p 42) recomiendan la aplicación de mecanismos como el cifrado, los controles de acceso y las copias de seguridad, que permiten preservar la confidencialidad e integridad de la información. Por último, plantean la importancia de proteger los activos tecnológicos de la organización —incluyendo hardware, software y redes— mediante soluciones como firewalls, antivirus y sistemas de detección de intrusos, con el fin de mantener la estabilidad y seguridad de la infraestructura tecnológica.

2.3 Gestión de Riesgos

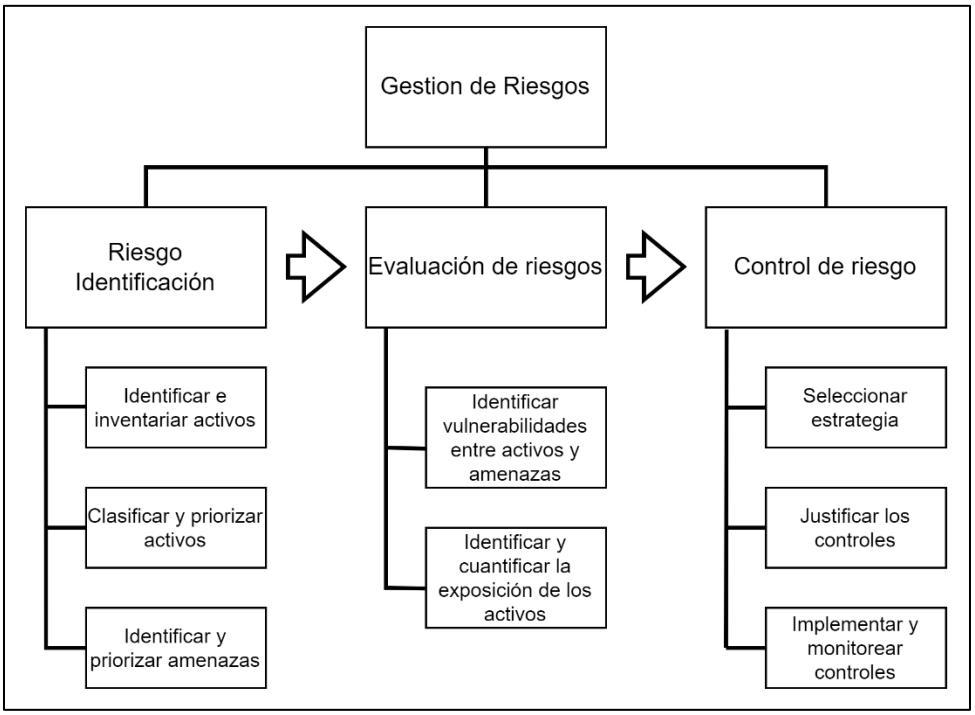
La gestión de riesgos en el ámbito de la seguridad de la información constituye un proceso estructurado que se compone de tres etapas principales: identificación, evaluación y control de riesgos (Whitman & Mattord, 2011, p 120). Estas fases se desarrollan de forma sistemática e iterativa, permitiendo

que las organizaciones ajusten continuamente sus estrategias frente a nuevas amenazas, y así garantizar la protección efectiva de sus activos informacionales.

Tal como se presenta en la Figura 2, “Componentes de la Gestión de Riesgos”, este proceso se organiza en un flujo continuo que conecta cada una de las etapas a través de actividades específicas. Este enfoque dinámico refleja la necesidad de retroalimentar y actualizar las medidas de protección en función de los cambios en el entorno tecnológico y de seguridad. La gestión de riesgos, en este sentido, no es un proceso estático, sino un ciclo de mejora constante.

Figura 2

Componentes de la Gestión de Riesgos



Nota. (Fuente: Course Technology/ Cengage Learnig)

La primera etapa del proceso es la identificación de riesgos, que comienza con el reconocimiento y clasificación de los activos de información más relevantes para la organización. Estos pueden incluir datos, aplicaciones, dispositivos, procedimientos y personas que participan en el procesamiento de la información. Una vez identificados, se procede a registrar y describir las amenazas potenciales que puedan comprometer la confidencialidad, integridad o disponibilidad de dichos activos (Whitman & Mattord, 2011, p 121). Para facilitar este análisis, los autores definen un “activo de información” como cualquier

recurso que recopila, almacena, procesa o transmite información de valor para la organización (Whitman & Mattord, 2022, p130). Con el fin de valorar adecuadamente estos activos, es necesario considerar ciertos criterios estratégicos. Entre ellos, se incluyen preguntas como:

- ¿qué activo es fundamental para el funcionamiento del negocio?
- ¿cuál contribuye más a la rentabilidad?
- ¿cuál sería más costoso de reemplazar o de proteger?
- ¿qué activo podría implicar mayores consecuencias legales o reputacionales si se ve comprometido?

Estas preguntas permiten estimar la criticidad de cada activo y priorizar su protección dentro del esquema general de seguridad (Whitman & Mattord, 2011, p 131). La siguiente fase corresponde a la evaluación de riesgos, donde se identifican las vulnerabilidades que afectan a los activos previamente analizados y se cuantifica su exposición ante las amenazas detectadas. Este paso proporciona una visión clara del nivel de riesgo existente y facilita la toma de decisiones sobre los recursos que deben asignarse a la mitigación. Por último, la fase de control de riesgos se enfoca en la selección e implementación de medidas de seguridad orientadas a reducir los riesgos identificados. Esto implica justificar las estrategias elegidas, aplicar los controles correspondientes, y monitorear de manera constante su eficacia. Esta etapa es esencial para asegurar que las soluciones implementadas sean sostenibles, escalables y alineadas con los objetivos operativos de la organización.

2.4 Amenazas y vulnerabilidades en la seguridad de la información

En el ámbito de la seguridad de la información, comprender la relación entre amenazas, vulnerabilidades y ataques resulta fundamental para proteger los activos críticos de una organización. Según Whitman y Mattord (2011, p 65), un ataque se produce cuando un agente externo, conocido como agente de amenaza, logra explotar una vulnerabilidad presente en un sistema controlado, con el objetivo de causar daño o sustraer información. Esta acción puede dirigirse tanto a activos digitales como físicos.

Las vulnerabilidades son debilidades identificadas en los sistemas, las cuales surgen cuando los controles de seguridad no existen, han sido eliminados o ya no son efectivos. Estas fallas crean oportunidades para que las amenazas puedan materializarse. A diferencia de las amenazas, que están presentes de manera constante como potenciales peligros para la integridad de los sistemas, los ataques

solo ocurren cuando un evento específico logra aprovechar dichas debilidades, generando una pérdida concreta para la organización (Whitman & Mattord, 2011).

Comprender cómo interactúan estos elementos —la presencia constante de amenazas, la existencia de vulnerabilidades y la ejecución eventual de ataques— es clave para diseñar mecanismos eficaces de prevención, detección y respuesta. Una estrategia de seguridad robusta debe enfocarse tanto en la reducción de vulnerabilidades como en la vigilancia activa de las amenazas, con el fin de mitigar los riesgos antes de que se materialicen en daños reales.

2.5 Comprendiendo las Amenazas Cibernéticas

La seguridad de la información enfrenta actualmente un panorama de amenazas cada vez más sofisticadas, donde los ataques cibernéticos representan riesgos considerables para individuos, organizaciones y gobiernos. Comprender las tipologías de ataques y las técnicas de compromiso de sistemas resulta fundamental para el diseño de estrategias de defensa eficaces. Diversos autores han estudiado en profundidad los métodos utilizados por los agentes de amenaza y sus motivaciones, proporcionando marcos teóricos valiosos para su prevención y mitigación.

De acuerdo con Whitman y Mattord (2011, p 65), los ataques cibernéticos pueden clasificarse en categorías que comprenden tanto técnicas tecnológicas como de manipulación psicológica. Entre los ataques de naturaleza tecnológica se encuentra el software espía (spyware), un tipo de programa malicioso destinado a recolectar información del usuario de manera encubierta, sin su consentimiento, enviando los datos a terceros para su explotación. Asimismo, destacan las denominadas puertas traseras (backdoors), accesos ocultos creados originalmente por desarrolladores legítimos, que pueden ser posteriormente aprovechados por atacantes para mantener el control persistente sobre un sistema comprometido.

Otra técnica mencionada es el ataque de fuerza bruta (brute force), en el cual los atacantes prueban sistemáticamente todas las combinaciones posibles de contraseñas hasta lograr acceso. Aunque este método puede considerarse rudimentario, continúa siendo efectivo especialmente contra sistemas que carecen de mecanismos de autenticación robustos (Whitman & Mattord, 2011, p 65). Por su parte, los ataques de denegación de servicio (DoS) y los ataques de denegación de servicio distribuido (DDoS) consisten en saturar redes o servidores mediante tráfico malicioso, provocando interrupciones que afectan la disponibilidad de servicios críticos y generan pérdidas económicas significativas.

En cuanto a ataques que afectan directamente a personas, Whitman y Mattord (2011, p 68) describen la suplantación de identidad (identity theft), que implica el robo de información personal con el fin de cometer fraudes o acceder ilícitamente a sistemas protegidos. También destacan los ataques de intermediario (man-in-the-middle), en los cuales los atacantes interceptan la comunicación entre dos partes, pudiendo leer o modificar los datos sin que los usuarios legítimos lo detecten.

Los autores subrayan la importancia de la ingeniería social como una técnica que explota la manipulación psicológica para obtener acceso no autorizado a información confidencial. Dentro de esta categoría, los ataques de phishing son particularmente peligrosos: se presentan como comunicaciones legítimas (correos electrónicos, mensajes de texto) que engañan a los usuarios para que revelen credenciales de acceso, datos bancarios u otra información sensible (Whitman & Mattord, 2011, p 72).

Respecto a las técnicas específicas obligatorias que debe tener un sistema, Whitman y Mattord (2011, p 76) detallan distintos métodos que aprovechan vulnerabilidades técnicas. Entre ellos se encuentran los desbordamientos de búfer (buffer overruns), donde se sobrecarga una aplicación con datos para ejecutar código malicioso; las inyecciones de comandos y de SQL (SQL injection), que permiten a los atacantes introducir instrucciones no autorizadas en bases de datos o sistemas de gestión; y el envenenamiento de caché DNS (DNS cache poisoning), que manipula respuestas de servidores DNS para redirigir a usuarios hacia sitios maliciosos.

Finalmente, también mencionan los errores de números enteros (integer overflow/underflow), que explotan fallos de cálculo en los sistemas para obtener accesos indebidos o alterar el comportamiento de aplicaciones críticas. Estas técnicas, combinadas con errores humanos en la configuración de los sistemas, evidencian la complejidad de mantener una infraestructura tecnológica completamente segura en un entorno de amenazas dinámico y en constante evolución.

2.6 Integración de la Inteligencia Artificial en Seguridad de la Información

En un contexto donde las amenazas cibernéticas evolucionan constantemente y la superficie de ataque se expande de manera acelerada, la inteligencia artificial (IA) se ha consolidado como un componente estratégico en la protección de los activos digitales. Tal como señala Microsoft (s.f.), la IA permite procesar grandes volúmenes de datos en tiempo real, lo que resulta fundamental para transformar esa información en acciones concretas orientadas a la detección temprana y la respuesta automatizada frente a incidentes de seguridad.

Una de las capacidades más relevantes de la IA en este ámbito radica en su habilidad para aprender y adaptarse al comportamiento habitual de los usuarios. A través del análisis continuo de patrones de inicio de sesión, tráfico de red y uso de servicios en la nube, es posible identificar desviaciones que podrían evidenciar una amenaza. Este enfoque basado en la detección de anomalías contribuye a anticipar actividades maliciosas antes de que generen daños significativos (Microsoft, s.f.).

Además de su función preventiva, la IA permite combinar datos locales con inteligencia de amenazas a escala global, sin comprometer la privacidad entre organizaciones. Esta capacidad de generalización y contextualización enriquece los modelos predictivos sin infringir principios de confidencialidad, fortaleciendo la capacidad de respuesta de los equipos de seguridad (Microsoft, s.f.).

A partir de los avances recientes, destaca el papel de la IA generativa como herramienta de apoyo a los analistas. Esta tecnología no solo automatiza tareas complejas, sino que también es capaz de sintetizar grandes volúmenes de información técnica en lenguaje natural, facilitando la elaboración de informes, la generación de respuestas contextualizadas y la toma de decisiones informadas (Microsoft, s.f.). De este modo, se convierte en un recurso que amplifica las capacidades humanas en la gestión de incidentes.

Asimismo, la IA potencia diversas soluciones tecnológicas ya existentes, como los sistemas de prevención de intrusos (IPS), los firewalls de nueva generación, las plataformas de seguridad para endpoints y los sistemas de gestión de eventos e información de seguridad (SIEM). En todos estos casos, el valor agregado radica en la capacidad de correlacionar datos, identificar patrones sospechosos y actuar con rapidez ante posibles ataques (Microsoft, s.f.).

Desde una perspectiva técnica, la implementación de la IA en seguridad se apoya en métodos como el aprendizaje supervisado y no supervisado, el análisis de comportamiento de usuarios y entidades (UEBA), y el procesamiento de lenguaje natural (NLP). Estos enfoques permiten no solo detectar amenazas previamente conocidas, sino también anticipar actividades inusuales o interpretar señales ocultas en datos no estructurados, como foros o redes sociales (Microsoft, s.f.).

Por otra parte, la incorporación responsable de estas tecnologías exige una gobernanza adecuada. Microsoft (s.f.) enfatiza la necesidad de definir una estrategia clara para la integración de la IA, asegurando su interoperabilidad con sistemas existentes como XDR y SIEM. Además, se subraya la importancia de mantener la calidad de los datos utilizados, garantizar su privacidad y realizar pruebas continuas que permitan evitar sesgos o errores en la toma de decisiones.

El panorama futuro apunta hacia una mayor automatización y eficiencia en la gestión de la ciberseguridad, con detecciones más precisas y menos falsos positivos. Sin embargo, también se advierte que los actores maliciosos están comenzando a utilizar IA para perfeccionar sus ataques, lo que obliga a las organizaciones a invertir con urgencia en estas tecnologías para preservar la integridad de sus sistemas (Microsoft, s.f.).

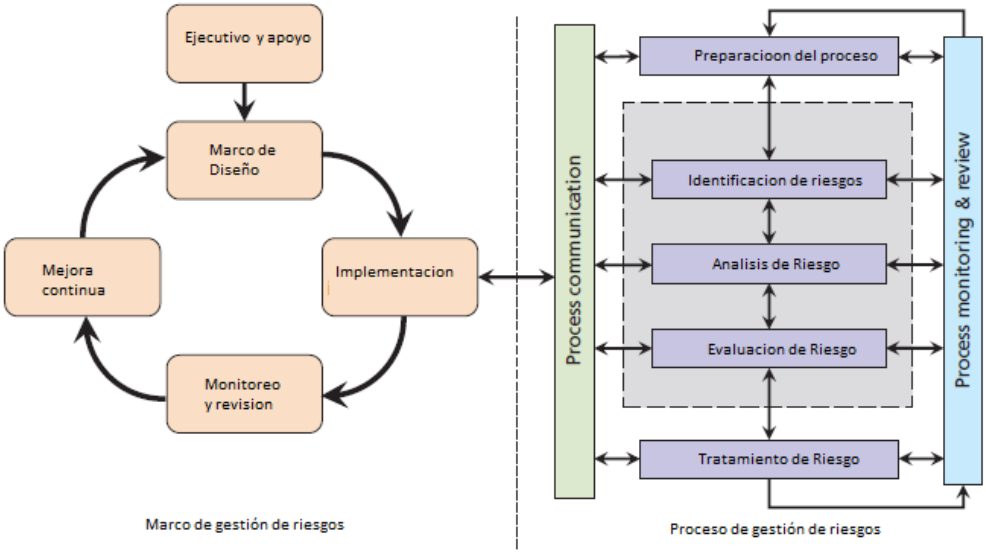
2.7 Fundamentos y Estrategias de Gestión de Riesgos en Seguridad Informática

La gestión de riesgos en seguridad informática constituye un componente esencial para preservar la integridad, disponibilidad y confidencialidad de los activos de información dentro de una organización. Abordar eficazmente esta labor requiere responder a cuestiones clave relacionadas con la identificación, evaluación y mitigación de amenazas potenciales. En esta línea, Whitman y Mattord (2022, p 123) ofrecen un enfoque integral que permite enfrentar dichos desafíos mediante la implementación articulada de un marco estratégico y un proceso operativo.

Según los autores, la gestión de riesgos se estructura a partir de dos componentes interrelacionados: el marco de gestión de riesgos y el proceso de gestión de riesgos. La figura 3 ilustra cómo ambos elementos se conectan de forma dinámica, destacando que el proceso alimenta de manera continua al marco estratégico a través de la comunicación de resultados, el monitoreo y la retroalimentación constante.

Figura 3

Interacción entre el Marco de gestión de Riesgos y el proceso de gestión de Riesgos.



Nota.(Fuente: Principles of Information Security, Whitman y Mattord, 2022, p.124)

Whitman y Mattord (2022, p. 124) subrayan que las organizaciones que ya cuentan con programas consolidados pueden integrar esta metodología con un impacto mínimo en sus estructuras existentes. No obstante, aquellas sin una gestión formal o con esquemas ineficientes deberán iniciar el proceso desde sus cimientos, lo que exige un compromiso institucional sostenido. El marco de gestión de riesgos actúa como la estructura general que guía las decisiones estratégicas en torno a la seguridad de la información. Este define cinco pasos fundamentales: gobernanza ejecutiva y apoyo institucional, diseño del marco, implementación, monitoreo y revisión, y mejora continua. Estas etapas buscan asegurar que el proceso esté alineado con los objetivos organizacionales y sea susceptible de ser optimizado en función de los resultados obtenidos. Por su parte, el proceso de gestión de riesgos constituye la dimensión operativa del marco. Comprende actividades específicas tales como la identificación de riesgos, la evaluación de su probabilidad e impacto, la selección de controles adecuados y su aplicación, así como el monitoreo constante para verificar la eficacia de las medidas adoptadas. Este enfoque sistemático permite gestionar riesgos de forma proactiva y adaptativa, manteniendo la protección de los activos informáticos como un proceso en evolución.

Un aspecto clave señalado por los autores es el papel de los grupos de interés o comunidades involucradas en la gestión de riesgos. La colaboración entre los equipos de ciberseguridad, tecnología de la información y alta dirección resulta indispensable para cubrir todas las dimensiones del riesgo, desde eventos catastróficos hasta errores operativos menores. Como indican Whitman y Mattord (2022, p 125), los profesionales con conocimientos especializados en amenazas y ataques suelen liderar este proceso, mientras que los usuarios y gerentes, si están adecuadamente formados, contribuyen a la detección temprana de incidentes y a la asignación efectiva de recursos.

La dirección general tiene la responsabilidad de proporcionar el respaldo necesario —en términos de tiempo, presupuesto, personal y tecnologías— para que las áreas técnicas puedan implementar y mantener los controles requeridos. De este modo, la participación activa y coordinada de estas tres comunidades permite una respuesta más integral y efectiva frente a los diversos niveles de riesgo que enfrenta la organización.

2.8 Ciclo de vida de la gestión de riesgos: identificación, evaluación, mitigación y monitoreo de riesgos

La identificación del riesgo, primera fase operativa del proceso de gestión de riesgos comienza con un autoexamen de la organización, siguiendo el consejo de Sun Tzu de "conocerse a sí misma" para comprender los riesgos que enfrentan sus activos de información. Lo que afirman Whitman y Mattord (2022, p 130), los gerentes deben identificar, clasificar, categorizar y priorizar estos activos, tarea compleja pero esencial para detectar debilidades y amenazas. Este proceso implica la catalogación de personas, procedimientos, datos, software, hardware y elementos de red, sin prejuzgar su valor. Un activo de información es cualquier elemento que recopila, almacena, procesa o transmite información, siendo cruciales los datos y aplicaciones sobre hardware estándar. La separación de componentes reemplazables facilita la gestión, enfocándose en activos críticos. Algunas organizaciones comienzan con datos y aplicaciones centrales, añadiendo otros activos en iteraciones posteriores. Los activos se clasifican en personas (internas y externas), procedimientos (estándar y sensibles) y datos en todos los estados.

Tabla 1

Activos organizacionales utilizados en sistemas

Componentes de sistemas de Información	Componentes de la Gestión de Riesgos	Ejemplos de componentes de Riesgos
Gente	Personal interno y externo	Empleados de confianza Otros miembros del personal Personas en las que confiamos fuera de nuestra organización extraños
Procedimientos	Procedimientos	Procedimientos estándar de TI y de negocios Procedimientos TI y sensibles al negocio
Datos	Datos/Información	Transmisión / procesamiento / Almacenamiento
Software	Software	Aplicaciones Sistemas operativos Utilidades Componentes de seguridad
Hardware	Hardware	Sistemas y periféricos Dispositivos de seguridad Dispositivos de control de procesos conectados a la red y otros Sistemas embebidos (Internet de las cosas)
Redes	Redes	Componentes de la red de área local Componentes de intranet Componentes de Internet o extranet Componentes basados en la nube

Nota. La Tabla 1 categoriza los activos de información que una organización puede incluir en su gestión de riesgos. Este esquema asegura que todos los recursos de información se identifiquen, evalúen y gestionen adecuadamente para mitigar riesgos. (Fuente: Principles of Information Security, Whitman y Mattord, 2022, p.131)

La evaluación de riesgos incluye el análisis de riesgos, que asigna una calificación a cada vulnerabilidad específica. Este proceso afirma Whitman y Mattord (2022, p 145) aunque no es una ciencia exacta, permite comparar el riesgo relativo entre activos de información vulnerables, facilitando la creación de calificaciones comparativas para el tratamiento de riesgos. El enfoque del NIST para la evaluación de riesgos integra el análisis con la comprensión de las amenazas, buscando desarrollar un método repetible para evaluar el riesgo relativo de cada vulnerabilidad identificada. La mitigación de

controles implica determinar si una vulnerabilidad está total o parcialmente gestionada por controles existentes. La probabilidad de un evento de amenaza se evalúa mediante un valor numérico que indica la probabilidad de que una vulnerabilidad específica sea explotada. El impacto potencial de un ataque se evalúa en términos de la pérdida de valor del activo, considerando las consecuencias de la divulgación no autorizada, modificación, destrucción o pérdida de disponibilidad de la información. Las organizaciones suelen crear escenarios de ataque para comprender mejor el impacto potencial y prepararse para la respuesta a incidentes, recuperación ante desastres y continuidad del negocio. La creación de estos escenarios en la etapa de evaluación y su transmisión al equipo de planificación de contingencias ahorra tiempo y esfuerzo a la organización.

En la agregación de riesgos afirman Whitman y Mattord (2022, p 147) que este proceso se vuelve abrumador para una pequeña o mediana empresa, el equipo de gestión de riesgos puede comenzar a agrupar activos, amenazas y sus riesgos asociados en categorías más generales. La agregación de riesgos permite a las organizaciones manejar de manera eficiente la evaluación de riesgos que involucran múltiples sistemas de información y procesos de negocio interrelacionados. Este enfoque ayuda a consolidar varios riesgos específicos o de nivel inferior en un riesgo más general o de nivel superior, estableciendo un límite superior para el riesgo global de las operaciones y activos organizacionales. Incertidumbre en la Evaluación de Riesgos, es un factor esencial Whitman y Mattord (2022, p 147) afirman que en la evaluación de riesgos, debido a la imposibilidad de conocer completamente cada vulnerabilidad, como la probabilidad de un ataque o el impacto exacto que tendría un ataque exitoso en la organización, destaca que es crucial considerar siempre un factor de incertidumbre, basado en la estimación y juicio del gestor, debido a limitaciones como: diferencias entre el pasado y el futuro, conocimiento incompleto de las amenazas, vulnerabilidades desconocidas en tecnologías o productos, y dependencias no reconocidas que pueden causar impactos imprevistos. La incertidumbre también puede deberse a la fase del ciclo de vida del desarrollo del sistema en la que se realiza la evaluación de riesgos, ya que la efectividad de los controles de seguridad puede ser desconocida en las fases tempranas y costosa de evaluar en las fases posteriores.

En la determinación de riesgos Whitman y Mattord (2022, p 147) sugieren que una vez conocidos la probabilidad y el impacto de un ataque, la organización puede realizar la determinación de riesgos usando una fórmula que busca cuantificar ciertos elementos de riesgo: riesgo igual a la probabilidad de ocurrencia del evento de amenaza multiplicada por el impacto, más o menos un elemento de

incertidumbre. Por ejemplo, si un activo de información enfrenta una amenaza con una probabilidad asignada de 3 y un impacto de 5, y se estima que los datos son 90% precisos, el valor de riesgo resultante es 15 ± 1.5 en una escala de 25 puntos. Lo que afirma Whitman Mattord (2022, p 148) que la mayoría de las organizaciones aceptan el factor de incertidumbre y utilizan una fórmula más sencilla: Probabilidad × Impacto. Los resultados proporcionan una gama de calificaciones de riesgo, que pueden resumirse en una hoja de cálculo de calificación de riesgos, mostrando solo los activos y las vulnerabilidades relevantes. Este documento ayuda a identificar las vulnerabilidades más urgentes y priorizar las medidas correctivas.

Whitman y Mattord (2022, p 149) destacan que el principal desafío al utilizar un enfoque cuantitativo más complejo es la gran cantidad de estimaciones necesarias para desarrollar valores precisos, debido a la falta de ejemplos concretos que proporcionen la probabilidad de un ataque específico y el impacto exacto en el valor de un activo tras un ataque exitoso. Por esta razón, muchas organizaciones están optando por evaluaciones cualitativas o semi-cualitativas, lo que permite tomar decisiones de manera relativa y más manejable.

Después de que el equipo de gestión de riesgos ha identificado, analizado y evaluado el nivel de riesgo inherente en sus activos de información (evaluación de riesgos), debe tratar los riesgos que se consideran inaceptables, es decir, aquellos que superan el apetito de riesgo de la organización. Este proceso se conoce como respuesta a riesgos o control de riesgos.

Al iniciar el tratamiento de riesgos, la organización tiene una lista de activos de información con niveles de riesgo inaceptables. Es crucial seleccionar y aplicar la estrategia adecuada para cada activo. Whitman y Mattord (2022, p 152) describen cuatro estrategias principales en la Tabla 2, para tratar los riesgos asociados a los activos de información. Estas estrategias permiten a las organizaciones manejar los riesgos de manera efectiva, alineándolos con su apetito de riesgo. A continuación, se presentan las estrategias junto con su uso específico:

Tabla 2

Estrategias Principales para tratar los riesgos asociados a los activos de información

Estrategia	Uso
Mitigación	Aplicar controles y salvaguardas para eliminar o reducir el riesgo residual no controlado, intentando prevenir la explotación de vulnerabilidades.
Transferencia	Desplazar los riesgos a otras áreas o a entidades externas.
Aceptación	Entender y aceptar las consecuencias de mantener la vulnerabilidad de un activo de información en su nivel de riesgo actual, tras una evaluación formal y un reconocimiento intencional de esta decisión.
Terminación	Eliminar o discontinuar el activo de información del entorno operativo de la organización.

Nota. elaboración propia de tabla (Fuente : Whitman y Mattord, 2022, p 152)

2.9.1 ISO 27001: estándar internacional para la gestión de la seguridad de la información

Las normas ISO 27000 e ISO 27001 son fundamentales para la gestión de la seguridad de la información en las organizaciones modernas. Estas normas, desarrolladas por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), proporcionan un marco estructurado para proteger los activos de información contra una amplia gama de amenazas.

Definición de SGSI según (ISO 27001:2013), un sistema de gestión para la Seguridad de la información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización.

Un aspecto clave que resalta ISOtools.org (s.f.) que la norma 27001 es un sistema basado en enfoque basado en el ciclo de mejora continua ciclo consiste, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act), en la tabla 3, cada fase del ciclo asegura que el sistema sea evaluado y ajustado constantemente, lo que contribuye a una mejora continua en la protección de la información de la organización.

Tabla 3

Acciones específicas de ciclo PDCA

PDCA	Acción
PLANIFICAR	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades
HACER	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles
CONTROLAR	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
ACTUAR	Adoptar acciones correctivas Adoptar acciones de mejora

Nota. (Fuente: ISOtools.org)

Lo que afirma (ISOtools.org, s.f.) es que el propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática y estructurada (s.f.).

En base a este sistema PDCA, la norma ISO 27001 establece una serie de fases para elaborar un SGSI (ISOtools.org, s.f.). El análisis y evaluación de riesgos en un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 se centra en identificar amenazas que puedan afectar los activos de información, incluyendo ataques informáticos, desastres naturales, fallas técnicas y errores humanos. Este proceso implica asociar estas amenazas con activos específicos, determinar vulnerabilidades y evaluar el impacto potencial en la confidencialidad, integridad y disponibilidad de la información. Se utiliza una metodología estructurada que incluye la recogida de información, la clasificación de activos y amenazas, la estimación de vulnerabilidades y la valoración de impactos.

Luego se recomienda según ISOtools (s.f.), analizar las consecuencias potenciales de los riesgos, distinguiendo entre riesgo aceptable, donde se minimizan las consecuencias a niveles manejables, y riesgo

residual, que persiste aún con medidas de mitigación implementadas. La norma ISO 27001 resalta el liderazgo en la seguridad de la información, estableciendo roles como el dueño del riesgo para supervisar las actividades de control, asegurando una implementación efectiva del SGSI adaptada a la estructura organizacional y necesidades específicas de cada entidad. Continua con la segunda fase del sistema SGSI, es la implementación de controles según la norma ISO 27001 se centra en asegurar que cada riesgo identificado sea adecuadamente cubierto y auditado. La norma específica hasta 113 puntos de control en su versión actual, divididos en áreas como políticas de seguridad de la información y controles operacionales.

El proceso de definición de un plan de tratamiento de riesgos según la norma ISO 27001 y ISOtools.org(s.f.), implica identificar inicialmente las amenazas y evaluar sus posibles consecuencias, asignándoles una criticidad para una evaluación objetiva. Las organizaciones pueden enfrentar el riesgo eliminándolo, mitigándolo o trasladándolo. La eliminación total del riesgo es preferible en situaciones críticas que amenacen la continuidad del negocio, aunque en la mayoría de los casos se opta por la mitigación, implementando medidas preventivas o correctivas para reducir la probabilidad de ocurrencia o el impacto del riesgo. La opción de trasladar el riesgo implica la contratación de seguros que cubran las pérdidas económicas derivadas de incidentes. Es crucial que cada control establecido sea clasificado y evaluado según su efectividad preventiva, siendo preferibles aquellos que previenen los problemas antes de que ocurran, como ilustra el ejemplo de un sistema de monitoreo de temperatura frente a un sistema de detección de incendios. Este enfoque está integrado en un ciclo de mejora continua, evaluando la efectividad de los controles y ajustándolos según sea necesario.

En la planificación de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), resulta fundamental delimitar con precisión el alcance dentro de la organización. Esto implica considerar diversos factores como el tamaño de la empresa, el volumen de datos manejados, el número de sedes y otros elementos relevantes (ISOtool.org, s.f.). Normalmente, la definición del alcance se realiza según las líneas de negocio o los macroprocesos, dando prioridad a las áreas que son más críticas o vulnerables en términos de seguridad de la información y que tienen un impacto directo en el cumplimiento de la misión institucional.

ISOtool.org (s.f.), especifica que “la organización debe preocuparse, y por tanto determinar, que cuestiones o aspectos internos y externos están involucrados en el propósito de la misma y puedan afectar a la capacidad de alcanzar los resultados previstos para su SGSI”.

En el contexto del Sistema de Gestión de Seguridad de la Información (SGSI), el análisis del contexto organizacional es crucial, ya que permite identificar y evaluar tanto problemas internos como externos, junto con las debilidades, amenazas, fortalezas y oportunidades que podrían influir en la organización. Aunque la norma ISO no prescribe un método específico para este análisis, el análisis DAFO es uno de los enfoques más utilizados y reconocidos.

2.9.2 COBIT: Marco de Gestión de TI y Seguridad de la Información

El framework COBIT (Control Objectives for Information and Related Technology) emerge como una herramienta crucial para la gobernanza y gestión de IT, destacándose por su capacidad para alinear la estrategia tecnológica con los objetivos empresariales y por su robustez en la gestión de riesgos y cumplimiento normativo. Introducido por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) en 1996, COBIT ha evolucionado considerablemente, comenzando como un método para integrar los aspectos financieros con la tecnología de la información, y transformándose en un framework holístico que abarca todos los aspectos de IT dentro de una organización, facilitando la gobernanza efectiva y la optimización de la gestión de servicios de IT (ITSM). La evolución de COBIT refleja su adaptación continua a las necesidades cambiantes de las organizaciones, incorporando en su versión COBIT 5 de 2012 aspectos esenciales de seguridad de la información y datos, y finalmente adoptando un modelo de código abierto con COBIT 2019, que aprovecha tanto las aportaciones de expertos en dirección como de la comunidad para actualizarse de manera dinámica. En la figura 4, se muestran los principios que buscan proporcionar una estructura coherente y eficiente que permita a las organizaciones maximizar el valor de sus inversiones en IT, gestionar mejor sus riesgos, cumplir con las normativas y regulaciones aplicables, y asegurar una alineación constante entre la estrategia de IT y los objetivos del negocio.

Figura 4

Principios de COBIT 5



Nota.. (Fuente: https://forum.huawei.com/enterprise/es/%C2%BFqu%C3%A9-es-cobit/thread/667234586171686912-667212881550258176)

Steve Manjaly (2022), fundamenta los cinco principios rectores:

- Satisfacer las necesidades de las partes interesadas, garantiza que todas las actividades y procesos de IT estén orientados a cumplir con los objetivos y expectativas de los stakeholders.
- Cubrir la organización de forma integral, aplicar el framework a todos los aspectos de la organización, más allá del departamento de IT, integrando todos los recursos y funciones empresariales.
- Aplicar un solo marco integrado, utilizar un marco unificado que esté alineado con otros estándares y prácticas (como ITIL e ISO), evitando la fragmentación y facilitando una gestión coherente.
- Garantizar un enfoque holístico en la toma de decisiones empresariales, considerar la organización en su totalidad para tomar decisiones integradas que promuevan el rendimiento global, utilizando habilitadores que permitan la implementación eficiente de políticas y prácticas.
- Separar la dirección de la gestión, distinguir claramente entre las funciones de dirección estratégica y las de gestión operativa de IT, estableciendo estructuras y responsabilidades diferenciadas para cada una.

Estos principios aseguran que las decisiones estratégicas se reflejen en acciones operativas, proporcionando una estructura que facilita la cohesión entre la visión de los ejecutivos y las actividades del departamento de IT, abordando áreas críticas como la disponibilidad, eficacia, eficiencia, integridad, cumplimiento, fiabilidad y confidencialidad de los sistemas y datos. En términos de componentes, COBIT se organiza en una estructura de tres niveles: requisitos del negocio, recursos de IT y procesos de IT. La Figura 5 ilustra el enfoque del marco de trabajo COBIT para alinear las necesidades de negocio con los recursos y procesos de TI. Este modelo está compuesto por tres elementos clave: Recursos de TI, Procesos de Trabajo y Requerimientos de Negocio.

Figura 5

Componentes de la estructura



Nota(Fuente: https://es.slideshare.net/slideshow/cobit-2/3788930)

Requerimientos de Negocio, representan los objetivos y necesidades que la organización espera alcanzar a través de su infraestructura y servicios de TI. Estos requerimientos están centrados en aspectos como la efectividad, eficiencia, confidencialidad, cumplimiento y confiabilidad de la información. Estos criterios son esenciales para asegurar que la TI no solo apoya las metas de la organización, sino que también cumple con los estándares de seguridad y control de calidad necesarios para mantener la competitividad y reputación del negocio.

Los recursos de TI, comprenden los elementos fundamentales que permiten a la TI cumplir con los procesos y objetivos de la organización. Estos recursos incluyen los datos (información que debe ser protegida y utilizada adecuadamente), sistemas de información (plataformas y aplicaciones que procesan y gestionan datos), tecnología (equipamiento y software necesarios para el funcionamiento), instalaciones (infraestructura física), y recursos humanos (personal con las competencias necesarias). Estos componentes proporcionan la base sobre la cual se construyen y soportan los procesos de TI. Procesos de Trabajo, estos procesos definen las actividades y prácticas que utilizan los recursos de TI para cumplir con los requerimientos del negocio. Incluyen áreas clave como la planeación y organización (establecimiento de estrategias y políticas), adquisición e implementación (incorporación de nuevas tecnologías y sistemas), prestación de servicios y soporte (garantía de que los sistemas operan adecuadamente), y monitoreo (evaluación continua de los procesos de TI). Estos procesos operativos permiten una gestión estructurada y consistente de los recursos de TI, alineando las acciones diarias con las metas estratégicas.

El marco COBIT facilita la clasificación de los objetivos de TI dentro de procesos y dominios específicos, permitiendo que las decisiones estratégicas se reflejen directamente en el trabajo diario del equipo de TI (Manjaly, 2022). Esto es esencial para asegurar la sincronización entre los objetivos organizacionales y las actividades de TI, promoviendo un lenguaje y un modelo de referencia comunes que facilitan la planificación, ejecución y monitoreo de los procesos. Esta alineación es clave para que la organización funcione de manera eficiente y para minimizar malentendidos y ambigüedades en la gestión de TI.

El framework de COBIT proporciona un esquema para clasificar los objetivos de IT en procesos y dominios específicos, conectando las decisiones estratégicas con el trabajo operativo del equipo de IT (Steve Manjaly, 2022), lo cual es esencial para mantener la sincronización entre los objetivos organizacionales y las actividades de IT. Las descripciones de procesos crean un lenguaje común a lo largo de la organización, unificando la terminología y las descripciones de los procesos, lo que reduce la confusión y proporciona un modelo de referencia claro para la planificación, ejecución y monitoreo de los procesos de IT.

Los objetivos de control para Steve Manjaly (2022) son esenciales para supervisar los procesos de IT, estableciendo un conjunto completo de requisitos de alto nivel que aseguran que los procesos se gestionen de manera efectiva. Las directrices de gestión asignan responsabilidades, definen conexiones

entre procesos, y establecen métricas de rendimiento, facilitando la integración de COBIT con otros frameworks existentes en la organización, como ITIL e ISO, mientras que los modelos de madurez miden la capacidad y madurez de los procesos, actividades y dominios en una escala de cero a cinco, ayudando a identificar áreas de mejora y a evaluar el progreso de la implementación de COBIT.

Steve Manjaly (2022) hace una comparación con ITIL, otro popular framework para la gestión de servicios de IT, COBIT se destaca por su enfoque en la gobernanza y el control. Mientras que ITIL se centra en la prestación de servicios IT y en garantizar una comunicación clara entre el proveedor de servicios y el cliente, COBIT adopta un enfoque normativo y basado en reglas, orientado a establecer controles bien definidos y asegurarse de que se implementen de manera consistente en toda la organización. Este enfoque es particularmente relevante para el cumplimiento de normas y regulaciones del sector, así como para lograr los objetivos de las partes interesadas, proporcionando un modelo robusto para la gestión de riesgos y la conformidad normativa, esenciales en la ciberseguridad.

El modelo de madurez de COBIT, revisado en COBIT 2019 para integrar el CMMI (Capability Maturity Model Integration), proporciona un marco detallado para evaluar la capacidad de los procesos en términos de madurez, ofreciendo una evaluación clara desde un nivel cero, donde el proceso carece de capacidad básica, hasta un nivel cinco, donde el proceso está bien definido, se logra su propósito, y se implementan la medición y mejora continua del rendimiento. Sugiere Steve Manjaly (2022) que este modelo permite a las organizaciones identificar áreas de mejora en sus procesos IT y establecer objetivos medibles e indicadores claros de éxito, lo cual es crucial para la planificación estratégica y la gestión de la seguridad de la información.

COBIT ofrece numerosos beneficios clave para las organizaciones. Facilita la estandarización de procesos IT, mejora la eficiencia de la infraestructura tecnológica, y ayuda a organizar y maximizar el uso de recursos de IT. Uno de sus beneficios más destacados es su capacidad para ayudar a las organizaciones a cumplir con los requisitos legales del sector, así como con los acuerdos contractuales con los clientes. COBIT es conocido por su eficacia en la gestión de riesgos de cumplimiento, financieros y de ciberseguridad, proporcionando un framework integral para que las partes interesadas y los ejecutivos de la empresa controlen las operaciones de IT con una visión holística, alineando cada proceso IT con los objetivos organizacionales. Además, el framework permite a los ejecutivos ejecutar su visión estratégica a todos los niveles de la organización, facilitando una conexión directa entre la estrategia y las operaciones,

y ofreciendo herramientas para implementar y medir la efectividad de las políticas y controles de seguridad de la información.

CAPITULO 3 Metodología

3.1 Enfoque de la Investigación

La presente investigación adopta un enfoque mixto de tipo concurrente, en el cual se integran técnicas cuantitativas y cualitativas de manera complementaria. Esta estrategia permite no solo describir patrones generales, sino también profundizar en los significados y experiencias que los participantes atribuyen a la gestión de riesgos y al uso de inteligencia artificial (IA) en la seguridad de la información.

De acuerdo con Sampieri et al. (2014, p 569), este enfoque es particularmente adecuado cuando se busca obtener una comprensión integral del fenómeno, ya que combina la objetividad del análisis estadístico con la riqueza interpretativa de los datos cualitativos. Mientras que el componente cuantitativo permite medir variables como el nivel de madurez en la gestión de riesgos, la adopción de herramientas de IA, la frecuencia de incidentes o la implementación de políticas formales de seguridad, el enfoque cualitativo aporta contexto, profundidad y sentido, revelando percepciones, barreras culturales y buenas prácticas que no suelen captarse mediante respuestas estructuradas.

El diseño de la investigación fue no experimental y de tipo transversal, lo cual implica que los datos fueron recolectados en un único momento en el tiempo, sin manipulación de variables, con el fin de observar y describir el estado actual del fenómeno en estudio.

3.2 Métodos de Recolección de Datos

En coherencia con el enfoque mixto adoptado, se utilizaron dos instrumentos complementarios: una encuesta estructurada y entrevistas semiestructuradas.

La encuesta fue aplicada a aproximadamente 300 personas pertenecientes a diversas áreas organizacionales. Se diseñó con preguntas cerradas y abiertas, lo que permitió captar tanto información cuantificable como aspectos cualitativos vinculados a la percepción institucional sobre la seguridad informacional. La muestra fue intencionalmente diversa, incluyendo personal técnico y no técnico, con el objetivo de relevar múltiples perspectivas sobre la implementación, uso y supervisión de políticas de

seguridad en entornos reales de trabajo, los datos fueron recolectados en un único momento, sin intervención sobre las variables analizadas.

El cuestionario se estructuró en tres bloques temáticos, alineados con los objetivos específicos del estudio:

- Bloque 1: Políticas y gestión de la seguridad de la información (existencia, aplicación, revisión y control de normativas).
- Bloque 2: Capacitación y cultura organizacional (formación del personal, periodicidad de acciones y percepción de efectividad).
- Bloque 3: Uso de inteligencia artificial en seguridad (grado de adopción, áreas de aplicación, beneficios y obstáculos).

Como complemento a la encuesta, se realizaron entrevistas a dos profesionales que se desempeñan en el área de ciberseguridad. La finalidad de estas entrevistas fue obtener una visión más concreta y cercana sobre cómo se gestionan los riesgos y cómo se aplican herramientas de inteligencia artificial en entornos reales de trabajo. Los entrevistados compartieron su mirada sobre el nivel de madurez de las prácticas de seguridad, las principales dificultades que enfrentan en su implementación, y el grado de confianza en la automatización de ciertos procesos mediante IA.

CAPITULO 4 Conclusiones

4.1 Contribuciones y limitaciones de la investigación

La presente investigación representa un aporte significativo al estudio de la seguridad de la información en entornos organizacionales, al integrar de manera innovadora el análisis de la gestión de riesgos con la aplicación de herramientas basadas en inteligencia artificial (IA). Su principal fortaleza radica en la adopción de un enfoque mixto de tipo concurrente, que permitió complementar el análisis cuantitativo —obtenido a través de encuestas estructuradas— con una perspectiva cualitativa enriquecida por entrevistas a profesionales del área, aportando así una mirada integral y situada sobre la problemática abordada.

Desde un plano empírico, el trabajo ofrece evidencia actualizada sobre las prácticas implementadas en distintos sectores estratégicos del país, tales como el financiero, telecomunicaciones, educativo, salud y comercio electrónico. Entre los principales hallazgos se destacan el grado de madurez institucional en materia de seguridad, la implementación de políticas formales, la capacitación del personal frente a amenazas cibernéticas, y el nivel de adopción de tecnologías emergentes como la IA. Esta diversidad sectorial y funcional otorga al estudio una validez contextual robusta y lo posiciona como una herramienta útil tanto para el ámbito académico como para tomadores de decisiones en materia de ciberseguridad.

En el plano conceptual, los resultados permiten afirmar que existe una relación consistente entre la implementación sistemática de prácticas de gestión de riesgos y una mayor capacidad institucional para anticipar, detectar y responder a incidentes de seguridad. Asimismo, el uso de herramientas basadas en IA se asocia a una mejora en los tiempos de respuesta y a una percepción positiva de preparación frente a amenazas emergentes. El estudio también permite identificar buenas prácticas, desafíos recurrentes y oportunidades de mejora que pueden orientar el diseño de estrategias más eficaces en contextos digitales complejos.

Como todo estudio empírico, este trabajo presenta ciertos márgenes de alcance. El diseño transversal aplicado permite identificar tendencias y asociaciones relevantes en un momento determinado, aunque no pretende establecer relaciones de causalidad estricta. Por otro lado, si bien la muestra fue amplia y heterogénea en cuanto a sectores y perfiles laborales, los resultados deben interpretarse en función de las características del universo consultado. En cuanto al componente cualitativo, las entrevistas seleccionadas ofrecieron información valiosa y profunda, representando casos relevantes en sectores

altamente expuestos a ciber amenazas. Su aporte cualitativo enriquece la interpretación general, sin pretender extrapolación estadística.

4.2 Informe final

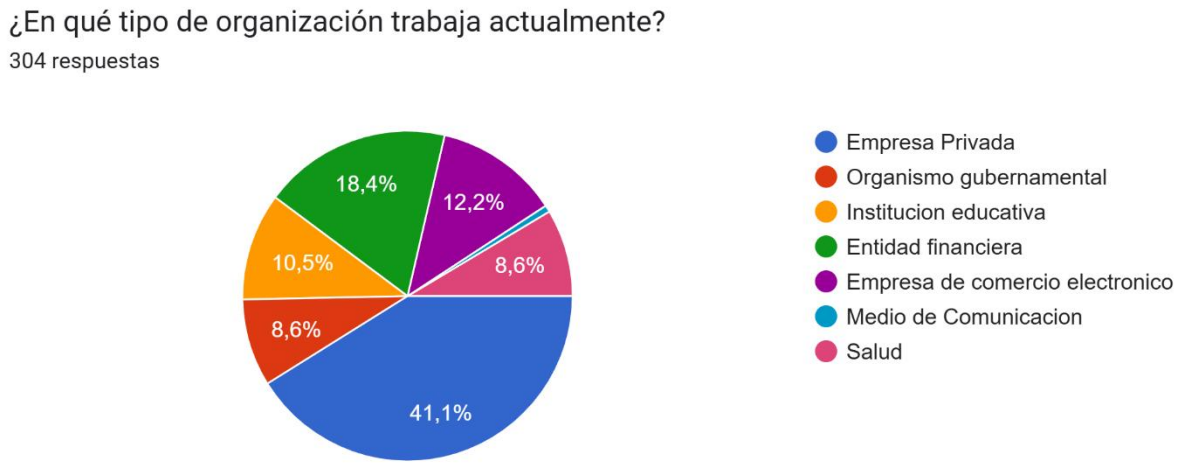
Con el propósito de obtener un diagnóstico general sobre el estado de la seguridad de la información, la gestión de riesgos y la incorporación de inteligencia artificial en las organizaciones, se aplicó una encuesta estructurada a aproximadamente 300 personas de diversos sectores y funciones laborales. El instrumento, compuesto por tres bloques temáticos, permitió relevar información tanto organizacional como perceptual, enfocándose en aspectos clave del ecosistema de ciberseguridad actual.

4.2.1 Perfil general de los encuestados

En cuanto al tipo de organización, se observa en la figura 6, una mayor representación del sector privado (41,1 %), seguido por el financiero (18,4 %) y el de comercio electrónico (12,2 %), lo que evidencia una participación activa de sectores que manejan datos sensibles o críticos para su operatividad. También se incluyó personal de instituciones educativas (10,5 %), organismos gubernamentales (8,6 %) y del sector salud (8,6 %), ampliando la heterogeneidad del análisis.

Figura 6

Tipos de organizaciones encuestadas



Respecto al tamaño organizacional tabla 4, predominan las pequeñas empresas (43,4 %), aunque también se relevaron grandes empresas (26,3 %) y medianas (25 %), lo que permite observar prácticas en estructuras de distinta complejidad. Solo un 5,3 % de los encuestados indicó pertenecer a microempresas.

Tabla 4

Tamaño de la organización

Organización	**%**
Microempresa (menos de 10 empleados)	5.3 %
Pequeña empresa (11 a 50 empleados)	43.3 %
Mediana empresa (51 a 200 empleados)	25 %
Gran empresa (más de 200 empleados)	26,3 %

En relación con el área de desempeño, el 25,7 % pertenece al sector Tecnología / IT, seguido por Administración / Finanzas (20,7 %), Recursos Humanos (19,1 %) y Operaciones (20,1 %). Este dato es relevante ya que permite contrastar la visión de áreas técnicas con la de funciones administrativas y de gestión del talento, esenciales en la construcción de una cultura organizacional de seguridad.

4.2.2 Seguridad de la información en la organización

Este primer segmento abordó aspectos estructurales y culturales vinculados a la seguridad informacional. A la hora de identificar las áreas más involucradas en este tema, la mayoría de los encuestados indicó que todas las áreas están igualmente comprometidas (36,6 %), lo que podría interpretarse como una visión institucional transversal. No obstante, también se destacan Tecnología/Sistemas/IT (25,1 %) y Alta Dirección (24,5 %), lo cual indica que los aspectos técnicos y estratégicos continúan teniendo un rol protagónico en la gestión de la seguridad.

Sobre la actualización de políticas, el 42,4 % manifestó que estas se modifican solo ante incidentes, mientras que un 41,8 % señaló que se actualizan anualmente. Esta información revela una tendencia mayoritaria a la reactividad, en lugar de a la actualización preventiva o periódica.

Tabla 5

Frecuencia se actualizan las políticas de seguridad

Frecuencia	%
Cuando ocurre un incidente	42.4 %
Anualmente	41.8 %
No se actualizan	6.9 %
Cada 6 meses	3.9 %
No sabe/No aplica	4.5 %

Al consultar sobre la importancia de las prácticas de seguridad en el área de trabajo, el 45,1 % eligió el valor “4” y el 11,2 % “5” en la escala Likert, reflejando una valoración alta. En contraste, solo el 2,6 % consideró que no son importantes. Esto demuestra que, en términos generales, la seguridad de la información es percibida como un tema relevante en el entorno laboral.

Finalmente, ante la pregunta sobre si las organizaciones cuentan con mecanismos adecuados para gestionar incidentes de seguridad, el 50,7 % respondió afirmativamente, mientras que el 41,4 % lo negó. Este resultado muestra una división significativa en la percepción de preparación institucional, que deberá observarse en conjunto con los hallazgos del segundo bloque de la encuesta.

4.2.3 Gestión de riesgos en entornos digitales

Este bloque tuvo como propósito indagar sobre la existencia de prácticas formales de gestión de riesgos y la percepción sobre la preparación organizacional ante eventos de ciberseguridad.

El 42,2 % de los encuestados señaló que su organización cuenta con un área o responsable específico de gestión de riesgos, mientras que el 34,2 % indicó que no, y un 23,4 % respondió que lo desconoce. Este dato muestra que aún persiste una falta de visibilidad o formalización en muchas estructuras.

Entre las prácticas más aplicadas se encuentran el registro de incidentes (28,2 %), la evaluación de vulnerabilidades (20,5 %) y la revisión periódica de controles (22,1 %). En cambio, los simulacros o pruebas de contingencia tienen una presencia baja (7,9 %), lo que evidencia una debilidad en la preparación proactiva ante eventos críticos.

Tabla 6

Las prácticas de gestión de riesgos en las organizaciones

Practica aplicada	%
Identificación de amenazas	18,9 %
Evaluación de vulnerabilidades	20,5 %
Registro de incidentes	28,2 %
Revisión periódica de controles	22,1 %
Simulacros / pruebas de contingencia	7,9 %
Ninguna / No sabe	2,3 %

Respecto a la frecuencia de evaluación de riesgos, el 37,5 % indicó una revisión semestral, el 31,9 % anual y solo el 9,9 % de forma trimestral. Un pequeño grupo (5,3 %) manifestó que nunca se realiza este proceso, lo cual es preocupante en términos de gestión anticipada.

Entre los métodos y herramientas más utilizados para evaluar o mitigar riesgos tabla 6, se destacan el uso de software especializado (23,9 %), auditorías internas (20,7 %) y la aplicación de estándares ISO (18,7 %), lo que evidencia cierto grado de profesionalización en las organizaciones encuestadas. Además, un 16,5 % mencionó el uso de matrices de riesgos o mapas de calor, fundamentales para priorizar amenazas.

Tabla 7

Métodos o herramienta para evaluar riesgos

Método o herramienta	%
Software especializado	23,9 %
Auditorías internas	20,7 %
Estándares ISO (ej. ISO 27001)	18,7 %
Matriz de riesgos / mapa de calor	16,5 %
Planes de contingencia / continuidad operativa	15,3 %
No se utilizan métodos formales	3,1 %
No sabe / No aplica	1,9 %

Al consultar sobre la preparación del equipo para enfrentar incidentes de ciberseguridad, el 54,9 % optó por un valor “4” y el 6,9 % por “5”, lo cual indica que una mayoría se considera moderadamente o altamente preparada. Esto se ve reforzado por el dato de que el 82,2 % recibió capacitaciones sobre ciberseguridad en el último año, lo cual resulta alentador y muestra una creciente conciencia institucional.

4.2.4 Uso de inteligencia artificial y percepción personal

Este último bloque permitió relevar el grado de conocimiento, adopción y confianza respecto al uso de IA en entornos de seguridad informática.

El 66,4 % de los encuestados conoce herramientas de IA aplicadas a la seguridad, lo que refleja un nivel importante de familiaridad con estas tecnologías. Entre los beneficios percibidos, se destacan la automatización de respuestas (32,9 %) y el monitoreo continuo (30,3 %), lo que evidencia una valorización de su eficiencia operativa. En menor medida se menciona el ahorro de costos (17,8 %) y la detección temprana de amenazas (15,8 %).

Tabla 8

Preferencia de uso de herramientas de IA

Practica aplicada	**%**
Automatización de respuestas	32,9 %
Monitoreo continuo	30,3 %
Ahorro de costos	17,8 %
Detección temprana de amenazas	15,8 %
No sabe	3,3 %

En cuanto a la adopción institucional, el 46,4 % afirma que en su organización ya se utilizan herramientas con componentes de IA, mientras que el 42,8 % sostiene que no, lo que muestra niveles dispares de implementación según el tipo de organización.

Respecto a la confianza en la IA para proteger datos, el 50,7 % marcó un nivel de 4 sobre 5, mientras que un 24 % eligió un valor medio (3), lo que permite inferir una actitud mayormente favorable pero aún cautelosa frente al uso de estas tecnologías.

Finalmente, al consultar sobre la posibilidad de que la IA reemplace parcialmente al personal humano en tareas de ciberseguridad, las opiniones estuvieron divididas: el 44,1 % cree que no, el 43,4 % que sí, y el resto se mostró indeciso. Este resultado sugiere una percepción ambigua y abierta al debate, que refleja tanto la expectativa de eficiencia como la preocupación por el reemplazo laboral.

4.2.5 Análisis cualitativo: Entrevistas a profesionales de ciberseguridad

Como complemento al análisis cuantitativo, se llevaron a cabo entrevistas a dos profesionales del área de ciberseguridad que se desempeñan en organizaciones altamente expuestas a amenazas digitales: una empresa de telecomunicaciones con alcance nacional y una plataforma de compraventa de criptomonedas. El objetivo fue obtener una visión práctica y detallada sobre la gestión de riesgos y la aplicación de herramientas basadas en inteligencia artificial (IA), considerando contextos organizacionales distintos, pero igualmente críticos en cuanto a la protección de la información.

El primer entrevistado Profesional del sector de telecomunicaciones relató que uno de los desafíos más relevantes en la gestión de riesgos ha sido la diversidad del personal y los distintos niveles de sensibilización frente a amenazas cibernéticas. A comienzos del año 2025, la organización implementó una estrategia de concientización mediante el envío de un correo electrónico simulado de phishing a todo el personal, con el objetivo de identificar a quienes interactuaran con el mensaje. Esta acción permitió detectar perfiles vulnerables y asignarles de manera inmediata un curso obligatorio de ciberseguridad. Dado el éxito de la experiencia, la capacitación fue posteriormente extendida a toda la empresa, estableciendo una base de conocimiento común que mejoró significativamente la postura de seguridad organizacional.

En términos de monitoreo, la organización emplea herramientas SIEM como Splunk y Wazuh, complementadas por soluciones de detección y respuesta en endpoints (EDR) y escaneos automatizados de vulnerabilidades. Se indicó además que el marco normativo adoptado está alineado con ISO/IEC 27001 e ISO/IEC 27002, y que se realizan auditorías internas con frecuencia semestral. La estructura de gestión de incidentes también considera recomendaciones del NIST Cybersecurity Framework, especialmente en lo que respecta a la identificación y protección de activos críticos.

Respecto a experiencias recientes, se mencionó un intento de ataque de denegación de servicio (DDoS), que fue contenido mediante un protocolo de respuesta previamente establecido, articulando

acciones del equipo de seguridad, el área de redes y los proveedores de infraestructura. Este tipo de incidentes refuerzan la necesidad de una postura preventiva, sostenida en la vigilancia permanente y la formación continua del personal.

El segundo entrevistado se desempeña en una plataforma fintech servicios financieros basados en tecnología Blockchain, un entorno altamente dinámico y vulnerable a intentos de fraude, ataques de ingeniería social y accesos no autorizados. Desde sus inicios, la organización adoptó como pilar fundamental la implementación de estándares como ISO/IEC 27001, además de lineamientos específicos del proyecto OWASP para el aseguramiento de aplicaciones web y móviles. Las revisiones de seguridad incluyen análisis de código estático, pruebas de penetración y monitoreo automatizado.

En relación con el uso de IA, el entrevistado destacó la implementación de tecnologías de User and Entity Behavior Analytics (UEBA), con motores de correlación capaces de detectar patrones anómalos en tiempo real. Herramientas como CrowdStrike Falcon y Darktrace permiten automatizar respuestas ante eventos sospechosos, como el bloqueo inmediato de una cuenta o la suspensión de transacciones no autorizadas. Estas soluciones no solo mejoran la capacidad de respuesta, sino que reducen significativamente el tiempo medio de detección y contención de amenazas.

Un caso puntual relatado fue la detección de un intento de acceso mediante credenciales comprometidas, mitigado automáticamente gracias a la identificación de un comportamiento atípico en la sesión. Aunque el evento no generó pérdidas, sirvió como validación del sistema de defensa basado en IA y como justificación de futuras inversiones en automatización.

El entrevistado también subrayó la importancia de mantener una cultura organizacional orientada a la seguridad, respaldada por programas continuos de concientización, capacitaciones breves y simulaciones frecuentes. La seguridad, en este tipo de organizaciones, no se percibe como un área aislada, sino como un eje estratégico que impacta directamente en la confianza del usuario y en la sostenibilidad del negocio.

4.3 Conclusión

Los resultados de este estudio permiten comprender en profundidad las dinámicas actuales en torno a la seguridad de la información en entornos organizacionales, especialmente en lo que respecta a la gestión de riesgos y la incorporación de inteligencia artificial. Si bien se constatan avances significativos

en algunos sectores, el análisis evidencia una serie de desafíos estructurales y operativos que condicionan la efectividad de las estrategias implementadas.

Respecto al primer objetivo específico, que planteaba describir las políticas y medidas adoptadas en materia de seguridad, se evidenció que, aunque muchas organizaciones declaran contar con políticas formalizadas, su actualización responde mayoritariamente a eventos adversos. Más del 42 % de los encuestados indicó que dichas políticas se revisan solo tras la ocurrencia de un incidente, lo que revela una estrategia de tipo reactivo. Esta postura, si bien responde a necesidades inmediatas, amplía la ventana de exposición ante amenazas prevenibles. A ello se suma que casi un 7 % declaró que las políticas no se actualizan en absoluto, y un 4,5 % indicó desconocer estos procesos, lo que sugiere fallas en la gobernanza y la comunicación interna.

El segundo objetivo, centrado en identificar el nivel de preparación del personal ante incidentes, los datos reflejan una brecha preocupante entre el conocimiento teórico y la capacitación práctica. Si bien el 82,2 % de los participantes afirmó haber recibido alguna formación en ciberseguridad durante el último año, solo un 7,9 % participó en simulacros o pruebas de contingencia. Esta diferencia pone en evidencia que muchas organizaciones limitan su preparación a instancias formales o genéricas, sin proporcionar experiencias que fortalezcan la toma de decisiones en escenarios reales. Las entrevistas confirmaron esta situación, al señalar que los entrenamientos prácticos —cuando se aplican— generan mejoras sustanciales en el comportamiento de los usuarios y en la capacidad de respuesta frente a amenazas comunes como el phishing.

En relación con el tercer objetivo específico, enfocado en analizar los riesgos y beneficios del uso de inteligencia artificial en la gestión de la seguridad, se observa un avance importante en términos de familiarización y confianza en estas herramientas. Sin embargo, su implementación aún no es homogénea: cerca de la mitad de las organizaciones encuestadas no las ha incorporado. Aquellas que sí lo hicieron destacaron beneficios concretos, como la automatización de respuestas y el monitoreo continuo. No obstante, la adopción de tecnologías basadas en IA parece estar condicionada por el nivel de madurez organizacional, el acceso a recursos y la existencia de una estrategia clara de transformación digital. Los casos analizados en las entrevistas ilustran cómo la IA puede actuar como un refuerzo clave en la detección de anomalías, pero también advierten sobre la necesidad de integrarla dentro de marcos de gestión sólidos, donde lo humano y lo tecnológico trabajen de forma complementaria

En función del objetivo general —evaluar el impacto de la gestión de riesgos en la seguridad de la información incorporando la inteligencia artificial como variable de análisis—, los hallazgos sugieren que su cumplimiento es parcial. Las organizaciones que implementan políticas claras, capacitan regularmente a su personal y adoptan tecnologías avanzadas muestran mejores indicadores de preparación y respuesta ante incidentes. Sin embargo, muchas otras aún operan con prácticas mínimas, sin una estrategia integral de gestión del riesgo ni criterios definidos para adoptar soluciones innovadoras.

La hipótesis del estudio, que sostenía que una adecuada gestión de riesgos complementada con herramientas basadas en inteligencia artificial contribuye a reducir los incidentes y proteger la información crítica, se confirma parcialmente. Los resultados respaldan su validez, pero también muestran que su cumplimiento está condicionado por factores como el presupuesto, la cultura institucional, la claridad en la asignación de responsabilidades y el nivel de madurez de los procesos internos.

Finalmente, la pregunta de investigación —¿cuáles son los factores clave para implementar con éxito estrategias de gestión de riesgos apoyadas en IA?— encuentra respuesta en una serie de elementos comunes a las organizaciones más avanzadas: la existencia de políticas actualizadas y conocidas por el personal, la asignación de roles y responsabilidades claras, la capacitación continua orientada a la práctica, la adopción progresiva de estándares reconocidos (como ISO 27001) y el uso estratégico de herramientas tecnológicas. La ausencia de alguno de estos factores compromete la efectividad del sistema en su conjunto.

En síntesis, esta investigación permite concluir que la resiliencia digital organizacional no se logra exclusivamente a través de la tecnología, sino a partir de una cultura organizacional comprometida, con políticas claras, personas entrenadas y procesos integrados. Tanto los datos de la encuesta como los relatos de las entrevistas muestran que la articulación entre estrategia, tecnología y formación es clave para enfrentar las amenazas actuales y futuras en el entorno digital

4.4 Direcciones futuras de investigación

A partir de los hallazgos obtenidos en este estudio, se identifican diversas líneas que podrían ser exploradas en investigaciones futuras para profundizar el conocimiento sobre la seguridad de la información, la gestión de riesgos y el uso de inteligencia artificial en entornos organizacionales.

En primer lugar, sería pertinente avanzar hacia estudios longitudinales que permitan observar la evolución de las prácticas de ciberseguridad en el tiempo, especialmente en relación con la eficacia de los

programas de capacitación, la maduración de políticas internas y la adopción progresiva de herramientas basadas en IA. Este enfoque facilitaría la evaluación del impacto sostenido de las estrategias de gestión de riesgos y su relación con la reducción efectiva de incidentes.

Asimismo, resulta valioso ampliar el alcance del análisis cualitativo mediante un mayor número de entrevistas en profundidad con profesionales del sector. Incorporar diferentes perfiles como responsables de compliance, líderes de TI, desarrolladores de software seguro y auditores permitiría capturar una visión más completa sobre las tensiones, obstáculos y oportunidades en la implementación de marcos normativos como ISO/IEC 27001, COBIT o NIST CSF en diversas industrias.

Otra línea de investigación recomendable es el análisis comparativo entre sectores (por ejemplo, financiero, salud, educación, telecomunicaciones y administración pública), con el objetivo de identificar buenas prácticas, brechas y niveles de madurez diferenciados en materia de ciberseguridad. Este tipo de estudios podría dar lugar al desarrollo de modelos de madurez sectoriales, adaptados a los riesgos y necesidades específicos de cada dominio.

En cuanto al uso de inteligencia artificial, se abre una agenda emergente centrada en la evaluación ética, legal y técnica de estas tecnologías. Futuros trabajos podrían enfocarse en analizar los riesgos derivados de decisiones automatizadas, el sesgo algorítmico, la privacidad de los datos analizados por los motores de IA y la relación entre automatización y desplazamiento de funciones humanas en el ámbito de la seguridad.

Finalmente, considerando el contexto regional, sería de gran utilidad fomentar investigaciones con foco en la realidad latinoamericana, que contemplen limitaciones presupuestarias, niveles desiguales de digitalización, marco normativo local y cultura organizacional. El desarrollo de políticas públicas y estrategias de gobernanza que fortalezcan la seguridad de la información requiere evidencias sólidas adaptadas al entorno en el que se aplicarán.

4.5 Recomendaciones

Con base en los hallazgos obtenidos en esta investigación, se presentan las siguientes recomendaciones dirigidas a organizaciones, responsables de seguridad, formuladores de políticas y futuros investigadores interesados en fortalecer la gestión de la seguridad informacional mediante enfoques innovadores y sostenibles:

1. Fortalecer la formalización y actualización de políticas de seguridad:

   Se recomienda establecer procedimientos formales de revisión periódica (al menos semestral) de las políticas de seguridad de la información. Las organizaciones deben evitar una gestión meramente reactiva y avanzar hacia esquemas proactivos, alineados con estándares internacionales como ISO/IEC 27001 y COBIT 2019.

2. Implementar simulacros de incidentes y ejercicios prácticos:

   Más allá de la capacitación teórica, se sugiere institucionalizar simulacros de ataques controlados (como campañas de phishing o escenarios de contingencia), con el fin de evaluar en tiempo real la preparación del personal y mejorar la capacidad de respuesta ante amenazas reales.

3. Promover una cultura organizacional de seguridad:

   Es fundamental que la seguridad deje de percibirse como una tarea exclusiva del área técnica. Se recomienda integrar acciones de concientización dirigidas a todas las áreas y niveles jerárquicos, fomentando una cultura de corresponsabilidad en la protección de los activos informacionales.

4. Incrementar la adopción de herramientas de inteligencia artificial:

   Las organizaciones que aún no han incorporado tecnologías con IA deberían explorar su implementación progresiva, especialmente en funciones como monitoreo de comportamientos anómalos, detección de amenazas en tiempo real y automatización de respuestas. Esto puede realizarse mediante soluciones escalables y compatibles con sus capacidades técnicas y presupuestarias.

5. Establecer estructuras claras de gobernanza y gestión de riesgos:

   Se recomienda designar responsables formales para la gestión de riesgos y dotarles de recursos adecuados para aplicar metodologías estructuradas de identificación, evaluación, tratamiento y monitoreo continuo. La utilización de mapas de calor, matrices de riesgos y software especializado debería formar parte del enfoque sistemático de prevención.

6. Incentivar la inversión en talento humano y formación continua:

Dada la velocidad con la que evolucionan las amenazas, es clave que las organizaciones inviertan en la actualización permanente de sus equipos de ciberseguridad, así como en programas internos de formación adaptados a distintos perfiles, niveles de conocimiento y generaciones.

7. Fomentar alianzas sectoriales y marcos de colaboración:

Se recomienda la creación de redes de cooperación entre empresas, cámaras sectoriales, universidades y organismos públicos, que permitan compartir buenas prácticas, amenazas emergentes y recursos para la mejora colectiva de la ciberseguridad a nivel nacional y regional.

4.6 Referencias bibliográficas

Alonso, C.(s.f.) *ISO 27000 y el conjunto de estándares de Seguridad de la Información (Recuperado 01 junio de 2024).* https://www.globalsuitesolutions.com/es/la-familia- de-normas-iso-27000/

Business Intelligent. (s.f.). *ISO 27000*. (Recuperado 01 junio de 2024). http://www.business-intelligent.com/iso27000.pdf

Custodio Chavarria, Gianpaul Jesus, Arana Orrego, Carlos Alberto, Valles Rios, Lenin Ruben. (2025). *Marco Referencial de Ciberseguridad para la Filtración de Datos en Arquitecturas Multi-cloud.* *https://repositorioacademico.upc.edu.pe/handle/10757/684597*

Estevez, J. (2025). *Estrategias Disruptivas de Ciberseguridad: Abordando las Amenazas Informáticas Emergentes en el Ámbito Empresarial, Educativo y Gubernamental*. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/66386

Guaña-Moya, J. (2023). *La importancia de la seguridad informática en la educación digital retos y soluciones*.https://dialnet.unirioja.es/servlet/articulo?codigo=8977055

ISOtools.org (s.f.) – *Norma ISO 27001* (Recuperado 01 junio de 2024). De https://www.isotools.us/pdfs/norma-iso-27001.pdf

Lenin Alexis Aguirre Sánchez, *Gestión de riesgos de seguridad de la información a través de normas internacionales en la empresa pública*. Noviembre 2023 https://repositorio.uta.edu.ec/server/api/core/bitstreams/0f5a3f61-bcdc-4ab2-a898-ce6e44dd5539/content

Microsoft (s.f.). *Aplicaciones de la Inteligencia Artificial en Seguridad de la Información*. (Recuperado 04/06/2024) https://www.microsoft.com/es-ar/security/business/security-101/what-is-ai-for-cybersecurity

Morales Loayza Jorge Luis, Neyra Montoya Arnaldo, Vidal Alegria Alberto. *Método de análisis cuantitativo de riesgos de ciberseguridad enfocado a la seguridad de datos en entidades financieras.* *https://repositorioacademico.upc.edu.pe/handle/10757/660721*

Normas ISO-27001.es (s.f.). *Norma ISO270001*" (Recuperado 01 junio de 2024) https://normaiso27001.es/

Steve Manjaly (2022) *COBIT: una visión diferente de la gestión de servicios. (*Recuperado 14-06-2024) https://blog.invgate.com/es/cobit

Guillermo Wilfredo, Torres Ramirez. (2023) *Implementación de Ethical Hacking para mejorar la gestión de riesgos informaticos de la Clinica Americana SERFARMED – Pucallpa* (https://apirepositorio.unu.edu.pe/server/api/core/bitstreams/72fc92a7-a8cc-441c-8e19-a152d2954ef6/content)

Villacorta Vidal, C. A., Ortiz Centurion, E. S., & Mendoza de los Santos, A. C. (2023). *Inteligencia artificial en la seguridad de la información en una organización*. Investigación Universitaria UNU, 13(2), 1046 –.http://revistas.unu.edu.pe/index.php/iu/article/view/120/142

Whitman M. y Mattord H. (2011). *Principles of Information Security*. Edición N°4. http://almuhammadi.com/sultan/sec_books/Whitman.pdf

Whitman M. y Mattord H. (2022). *Principles of Information Security*. Edición N°7. https://dokumen.pub/principles-of-information-security-7nbsped-2021909680-9780357506431.html

Sampieri Roberto .(2014). *Metodología de la investigación científica*. Edicion N°6

4.7 Anexos

4.7.1 Anexo 1 - Encuesta

Link encuesta: (https://docs.google.com/spreadsheets/d/1CERJtWnk8uUeAz-sgaC-MrQ7lZAFZCg7HU1lYn71g_E/edit?usp=sharing)

Resultados del instrumento de recolección de datos

El siguiente anexo presenta los resultados obtenidos a partir de la encuesta estructurada aplicada a una muestra de más de 300 personas provenientes de distintos sectores. La encuesta se organizó en cuatro secciones: datos generales del encuestado, seguridad de la información, gestión de riesgos e inteligencia artificial.

Sección A. Datos generales del contexto organizacional

1. ¿En qué tipo de organización trabaja actualmente?

- Empresa privada: 41,1 %
- Entidad financiera: 18,4 %
- Empresa de comercio electrónico: 12,2 %
- Institución educativa: 10,5 %
- Organismo gubernamental: 8,6 %
- Sector salud: 8,6 %
- Medio de comunicación: 0,2 %

2. ¿Cuál es el tamaño aproximado de la organización?

- Pequeña empresa (11 a 50 empleados): 43,4 %
- Gran empresa (más de 200 empleados): 26,3 %
- Mediana empresa (51 a 200 empleados): 25,0 %
- Microempresa (menos de 10 empleados): 5,3 %

3. ¿En qué área o sector se desempeña

- Tecnología / IT: 25,7 %
- Operaciones: 20,1 %
- Administración / Finanzas: 20,7 %
- Recursos Humanos: 19,1 %
- Marketing / Comercial: 11,2 %
- Dirección / Alta gerencia: 3,3 %

Sección B. Seguridad de la información en la organización

4. ¿Qué áreas considera que están más involucradas en la seguridad de la información en su organización? (respuesta múltiple)

- Todas las áreas por igual: 36,6 %
- Tecnología / Sistemas / IT: 25,1 %
- Alta Dirección: 24,5 %
- Recursos Humanos: 7,7 %
- Legal / Compliance: 4,8 %
- Ninguna / No aplica: 1,3 %

5. ¿Con qué frecuencia se actualizan las políticas de seguridad en su organización?

- Cuando ocurre un incidente: 42,4 %
- Anualmente: 41,8 %
- No se actualizan: 6,9 %
- Cada 6 meses: 3,9 %
- No sabe / No aplica: 4,5 %

6. En una escala del 1 al 5, ¿cuán importantes considera que son las prácticas de seguridad de la información en su área de trabajo?

- 5 (Muy alta): 11,2 %
- 4 (Alta importancia): 45,1 %
- (Moderada): 25,0 %
- (Baja): 16,1 %
- 1 (Nada importante): 2,6 %

7. ¿Considera que su organización cuenta con mecanismos adecuados para gestionar incidentes de seguridad de la información?

- Sí: 50,7 %
- No: 41,4 %
- No sabe: 7,9 %

Sección C. Gestión de riesgos en entornos digitales

8. ¿Su organización cuenta con un área o responsable específico para la gestión de riesgos?

- Sí: 42,2 %
- No: 34,2 %
- No sabe: 23,4 %

9. ¿Qué prácticas de gestión de riesgos se aplican en su organización? (respuesta múltiple)

- Registro de incidentes: 28,2 %
- Evaluación de vulnerabilidades: 20,5 %
- Revisión periódica de controles: 22,1 %
- Identificación de amenazas: 18,9 %
- Simulacros / pruebas de contingencia: 7,9 %
- Ninguna / No sabe: 2,3 %

10. ¿Con qué frecuencia se realizan evaluaciones de riesgos de seguridad informática en su organización?

- Semestral: 37,5 %
- Anual: 31,9 %
- Trimestral: 9,9 %
- Nunca / No se realiza: 5,3 %
- No sabe: 15,5 %

11. ¿Qué métodos o herramientas utiliza su organización para evaluar o mitigar riesgos de seguridad? (respuesta múltiple)

- Software especializado: 23,9 %
- Auditorías internas: 20,7 %
- Estándares ISO (ej. ISO/IEC 27001): 18,7 %
- Matriz de riesgos / mapa de calor: 16,5 %
- Planes de contingencia / continuidad operativa: 15,3 %
- No se utilizan métodos formales: 3,1 %
- No sabe / No aplica: 1,9 %

12. En una escala del 1 al 5, ¿cuán preparado considera que está su equipo para enfrentar un incidente de ciberseguridad?

- 5 (Muy preparado): 6,9 %
- 4 (Bastante preparado): 54,9 %
- (Moderadamente preparado): 22,4 %
- 2: 14,1 %
- 1 (Nada preparado): 1,6 %

13. ¿Ha recibido alguna capacitación sobre riesgos informáticos o ciberseguridad en los últimos 12 meses?

- Sí: 82,2 %
- No: 17,8 %

Sección D. Uso de inteligencia artificial (IA) y percepción personal

14. ¿Conoce alguna herramienta de inteligencia artificial aplicada a la seguridad de la información?

- Sí: 66,4 %
- No: 28,0 %
- Tal vez: 5,6 %

15. ¿Cuál cree que podría ser la principal ventaja del uso de IA en seguridad informática?

- Automatización de respuestas: 32,9 %
- Monitoreo continuo: 30,3 %
- Ahorro de costos: 17,8 %
- Detección temprana de amenazas: 15,8 %
- No sabe: 3,3 %

16. ¿En su organización se utilizan herramientas con componentes de IA para seguridad informática?

- Sí: 46,4 %
- No: 42,8 %
- Tal vez: 10,9 %

17. ¿Qué nivel de confianza le genera el uso de inteligencia artificial en la protección de datos?

- 5 (Máxima confianza): 9,5 %
- 4 (Alta confianza): 50,7 %
- 3 (Moderada): 24,0 %
- 2 (Baja): 13,5 %
- 1 (Nula confianza): 2,3 %

18. ¿Considera que el uso de IA podría reemplazar parcialmente al personal humano en tareas de ciberseguridad?

- No: 44,1 %
- Sí: 43,4 %
- Tal vez: 12,5 %

4.7.2 Anexo 2 - Preguntas realizadas a los profesionales entrevistados

Dado que ciertos aspectos de la gestión de riesgos y el uso de inteligencia artificial en seguridad de la información son difíciles de cuantificar mediante encuestas estructuradas, se decidió complementar el enfoque cuantitativo con entrevistas semiestructuradas a profesionales del sector. Las siguientes preguntas fueron diseñadas para obtener una visión más profunda y contextualizada sobre las prácticas, desafíos y percepciones que enfrentan las organizaciones en escenarios reales.

¿Cómo evaluaría el nivel de madurez actual en la gestión de la seguridad de la información dentro de su organización?

- (Se buscó explorar la existencia de políticas formales, cumplimiento de normativas, prácticas sistemáticas y cultura organizacional.)

¿Cuáles son los principales desafíos o barreras que enfrentan para implementar o mantener medidas efectivas de ciberseguridad?

- (Se indagó sobre factores técnicos, culturales, presupuestarios o de formación del personal.)

¿Qué herramientas, normativas o marcos utilizan para monitorear, detectar y responder a incidentes de seguridad?

- (Ejemplos mencionados incluyeron SIEM, EDR, frameworks como ISO/IEC 27001 o NIST CSF.)

¿Utilizan soluciones basadas en inteligencia artificial en sus procesos de seguridad? Si es así, ¿para qué casos específicos?

- (Se orientó a conocer casos reales de automatización, monitoreo, detección de anomalías o correlación de eventos.)

¿Considera que la IA puede reemplazar parcial o completamente tareas críticas en ciberseguridad sin comprometer la fiabilidad? ¿Por qué?

- (Esta pregunta buscó captar el grado de confianza, límites percibidos y expectativas sobre el futuro del trabajo en el área.)