CULTURA DE CIBERSEGURIDAD EN LAS ORGANIZACIONES.

Prevención de Riesgos Digitales y Estandarización bajo ISO/IEC 27000.

Gustavo Eduardo Fernández Villacrés
Freddy Patricio Baño Naranjo
Marco Vinicio Rosillo Solano
Wilfrido Amilcar Trujillo Quinto

2026

ISBN 978- 9907-0-1046-6 doi 10.64584/

CULTURA DE CIBERSEGURIDAD EN LAS ORGANIZACIONES

Prevención de Riesgos Digitales y Estandarización bajo ISO/IEC 27000.

AUTORES

Gustavo Eduardo Fernández Villacrés
Instituto Superior Tecnológico España
Gustavo.fernandez@iste.edu.ec
Unidad de Ciencia y Tecnología
https://orcid.org/0000-0003-1028-1224

Freddy Patricio Baño Naranjo
Instituto Superior Tecnológico Mayor Pedro Traversari
freddy.bano@institutotraversari.edu.ec
Dirección Ejecutiva
https://orcid.org/0000-0001-9631-7595

Marco Vinicio Rosillo Solano
Universidad Estatal de Bolívar
mrosillo@ueb.edu.ec
Docente de la Carrera de Agronomía
https://orcid.org/0000-0002-2167-9492

Wilfrido Amilcar Trujillo Quinto
Instituto Superior Tecnológico Mayor Pedro Traversari
wilfrido.trujillo@istpet.edu.ec
Carrera de Desarrollo de Software
https://orcid.org/0000-0001-8580-1322

CULTURA DE CIBERSEGURIDAD EN LAS ORGANIZACIONES.
Prevención de Riesgos Digitales y Estandarización bajo ISO/IEC 27000.

CYBERSECURITY CULTURE IN ORGANIZATIONS: Digital Risk Prevention and Standardization under ISO/IEC 27000.

Primera edición, abril 5 del 2026

ISBN: 978- 9907-0-1046-6 (e-book)

DOI: 10.64584/

Editado por:
Marco Salazar C..
Telf. 096 067 7758
Ambato-Ecuador

Este libro ha sido sometido a un proceso de evaluación por pares externos con base a la normativa editorial. También dispone de revisión antiplagio.

Ver anexos

Diseño y diagramación.
Diseño, montaje y producción editorial.
Editorial MS

Hecho en Ambato, Ecuador
Made in Ambato, Ecuador.

PRÓLOGO

En el escenario contemporáneo, marcado por la acelerada transformación digital, la expansión de los ecosistemas interconectados y la creciente dependencia de infraestructuras tecnológicas en todos los sectores productivos, la ciberseguridad ha dejado de ser un asunto exclusivamente técnico para convertirse en un eje estratégico de gobernanza organizacional, sostenibilidad institucional y competitividad empresarial. En este contexto, las organizaciones enfrentan desafíos cada vez más complejos derivados de amenazas digitales sofisticadas, vulnerabilidades estructurales y riesgos asociados al comportamiento humano dentro de entornos altamente digitalizados.

La presente obra surge como una respuesta académica y profesional a la necesidad de comprender la ciberseguridad desde una perspectiva integral, articulando no solamente los componentes tecnológicos de protección, sino también los factores culturales, normativos, éticos y organizacionales que determinan la resiliencia digital de las instituciones. El libro propone una reflexión profunda sobre la construcción de una cultura preventiva en las organizaciones, entendiendo que la seguridad de la información no depende únicamente de herramientas técnicas avanzadas, sino de la consolidación de hábitos, responsabilidades compartidas y liderazgo institucional orientado a la protección sistemática de los activos digitales.

A lo largo de sus capítulos, esta obra desarrolla de manera estructurada los fundamentos conceptuales de la ciberseguridad, la identificación de

riesgos digitales, las principales amenazas contemporáneas, la relevancia de la cultura organizacional en la gestión preventiva y la aplicación de estándares internacionales como la familia ISO/IEC 27000, cuya adopción se ha convertido en un referente global para fortalecer sistemas de gestión de seguridad de la información en organizaciones públicas y privadas.

Uno de los aportes más significativos de este libro radica en situar el análisis de la ciberseguridad dentro de la realidad organizacional latinoamericana, donde muchas micro, pequeñas y medianas empresas aún enfrentan limitaciones estructurales para implementar políticas robustas de protección digital. En este sentido, la obra no solo presenta marcos teóricos actualizados, sino que también ofrece orientaciones aplicables para fortalecer capacidades institucionales, reducir la exposición a incidentes digitales y promover una cultura empresarial basada en la prevención, la concienciación y la mejora continua.

La relevancia de esta publicación se amplifica en un momento histórico donde los incidentes cibernéticos impactan no solamente en la continuidad operativa, sino también en la confianza social, la reputación institucional y la estabilidad económica de las organizaciones. Por ello, comprender la ciberseguridad como una dimensión transversal de la gestión moderna constituye una necesidad impostergable para directivos, académicos, investigadores, estudiantes y profesionales vinculados con la administración tecnológica, la innovación y la transformación digital.

Finalmente, esta obra representa una contribución valiosa al fortalecimiento del pensamiento académico sobre ciberseguridad organizacional, integrando enfoques internacionales con visión aplicada y rigor conceptual. Se espera que sus contenidos sirvan como base para la formación, la investigación y la toma de decisiones estratégicas orientadas a construir organizaciones más seguras, resilientes y preparadas frente a los desafíos del entorno digital contemporáneo.

Los autores.

INDICE

CAPÍTULO I

FUNDAMENTOS DE LA CIBERSEGURIDAD Y CULTURA ORGANIZACIONAL

1.1 Introducción a la ciberseguridad en el contexto organizacional

Hoy en día, la seguridad informática se ha convertido en un elemento estratégico imprescindible para la supervivencia y competitividad de las empresas en las nuevas tecnologías. La transformación digital, la migración a servicios en la nube, el uso masivo de dispositivos móviles y la interconectividad global han cambiado profundamente la forma en que las empresas operan, guarda la información y se relacionan con sus clientes. Este nuevo ecosistema tecnológico ha abierto oportunidades de crecimiento, pero también ha ampliado la exposición a riesgos digitales que pueden poner en riesgo activos críticos, procesos operativos y la reputación corporativa.

1.1.1 Evolución de la ciberseguridad en la era digital

En los últimos años, la ciberseguridad ha evolucionado considerablemente debido a que las organizaciones se han ido volviendo más dependientes de las tecnologías digitales. En los primeros tiempos de la informática, el objetivo de la seguridad era proteger el hardware y mecanismos muy básicos de autenticación. Sin embargo, la expansión de la red, la computación en la nube y la digitalización de procesos críticos aumentaron significativamente la superficie de ataque, lo que obligó a las empresas a adoptar enfoques más integrales y estratégicos. Según Von

Solms y Van Niekerk (2013), la ciberseguridad ha evolucionado de un problema estrictamente técnico a un fenómeno socio-organizacional que requiere la integración de las personas, los procesos y la tecnología.
Las amenazas digitales son hoy continuas, automatizadas y cada vez más sofisticadas. Al respecto, el National Institute of Standards and Technology (2018) señala que la gestión de la ciberseguridad moderna debe ser estructurada bajo funciones como identificar, proteger, detectar, responder y recuperar, lo que evidencia un enfoque basado en riesgo y resiliencia. Este marco evidencia que la ciberseguridad no se limita ya a una defensa reactiva, sino que forma parte de la planificación estratégica organizacional como elemento clave para la sostenibilidad digital.

1.1.2 Ciberseguridad vs Seguridad de la Información

En el lenguaje cotidiano los dos términos suelen utilizarse como si fuesen intercambiables, pero la seguridad de la información y la ciberseguridad son conceptos diferentes. La seguridad de la información se refiere a proteger los datos, ya sean digitales, físicos o verbales, para que se garanticen los principios de disponibilidad, integridad y confidencialidad. En contraste, la ciberseguridad se enfoca particularmente en proteger los sistemas, redes y activos digitales de posibles peligros en contextos interconectados (National Institute of Standards and Technology, 2018).

La norma ISO/IEC 27001, publicada por la Organización Internacional de Normalización, ofrece un marco para la gestión de la seguridad de la información que está basado en la identificación y el manejo de riesgos,

lo cual resulta importante ya que muestra que la seguridad de la información es un ámbito más amplio, por lo tanto, la ciberseguridad puede ser vista como un aspecto especializado de la seguridad de la información que se ha ido ajustando a los peligros del entorno digital contemporáneo. Para disponer de políticas coherentes a nivel institucional y repartir responsabilidades de forma clara, es indispensable esta distinción (International Organization for Standardization, 2019).

Figura No. #1. Ciberseguridad y Seguridad Informática

Nota. Fuente. Imagen creada con IA

1.1.3 Importancia de la ciberseguridad en la continuidad del negocio

La capacidad de la organización para mantener operaciones críticas cuando se producen sucesos disruptivos, incluyendo los cibernéticos, es lo que determina la continuidad del negocio. El hecho de que los sistemas

no estén disponibles en entornos muy digitalizados, puede dar lugar a que se detengan las actividades productivas, a que se afecte la reputación de la empresa y a importantes pérdidas económicas. Las Academias Nacionales de Ciencias, Ingeniería y Medicina (National Academies of Sciences, Engineering and Medicine, 2019) resaltan que la planificación anticipada, la documentación de procesos y los sistemas estructurados de recuperación son necesarios para lograr resiliencia digital.

La norma ISO 22301, bajo el aspecto regulatorio, exige que las organizaciones identifiquen amenazas posibles y desarrollen estrategias de reacción para asegurar la continuidad de las operaciones. Incorporar la seguridad digital a esos planes es admitir que los ataques cibernéticos constituyen amenazas estratégicas. Por lo tanto, la gestión preventiva hace crecer las posibilidades de recuperación y reduce las consecuencias económicas y de imagen de los incidentes (International Organization for Standardization, 2019).

1.1.4 Impacto de los incidentes digitales en micro, pequeñas y medianas empresas

Las MiPymes (micro, pequeñas y medianas empresas) están expuestas a un riesgo digital más alto porque no cuentan con estructuras formales para manejar la seguridad y tienen limitaciones en el presupuesto. La International Telecommunication Unión (2022) indica que numerosas empresas pequeñas no cuentan con políticas formales de ciberseguridad, lo cual aumenta su susceptibilidad ante ataques como el phishing y el ransomware.

Además, la Agencia de la Unión Europea para la Ciberseguridad (2025) señala que las empresas pequeñas tienden a tener más problemas para recuperarse después de incidentes serios, especialmente si no tienen protocolos de respuesta o planes de respaldo. En este escenario, aplicar prácticas elementales de seguridad y robustecer la cultura organizacional preventiva son elementos clave para que las empresas sean sostenibles.

1.2 Cultura organizacional y seguridad de la información

La cultura de una organización es uno de los elementos más influyentes en la manera en que ésta administra los riesgos, asume decisiones y reacciona ante circunstancias difíciles. En la seguridad de la información, la parte cultural es muy importante porque las medidas técnicas, por sí solas, no son suficientes si no van acompañadas de comportamientos coherentes y de una conciencia colectiva de la protección de los activos informativos. Diversos estudios han demostrado que el factor humano es uno de los principales puntos de vulnerabilidad de los sistemas organizacionales, lo que evidencia la necesidad de integrar la seguridad dentro de los valores y prácticas cotidianas de la empresa (Schneier, 2015).

Desde este punto de vista, la cultura organizacional no solo influye en el cumplimiento de las políticas, sino que determina la forma en que los colaboradores perciben el riesgo digital, priorizan la protección de datos y asumen responsabilidades ante los incidentes. Por eso la seguridad de

la información debe entenderse como un proceso cultural y no solo como una infraestructura tecnológica.

Figura No. #3. Cultura Organizacional

Nota. Fuente. Imagen creada con IA.

1.2.1 Concepto de cultura organizacional

La cultura organizacional puede entenderse como el conjunto de valores, creencias, normas y supuestos compartidos que orientan el comportamiento de los miembros de una organización. Schein (2010) dice que la cultura se expresa en tres niveles: los artefactos que se ven, los valores que se declaran y los supuestos básicos que están por debajo de la superficie, siendo estos últimos los que tienen un impacto más profundo en la toma de decisiones y el comportamiento cotidiano.

La cultura organizacional, aplicada al contexto de la seguridad de la información, determina la forma en la que los empleados interpretan las

políticas de seguridad, reaccionan ante controles establecidos y priorizan la protección de la información. Al integrar la seguridad como un valor organizacional, el cumplimiento ya no es visto como una obligación externa, sino que se convierte en una práctica incorporada que refuerza la resiliencia institucional.

1.2.2 Cultura de prevención y concienciación digital

La cultura de prevención en seguridad de la información consiste en adelantarse a los riesgos a través de prácticas continuas de formación, concienciación y supervisión. No es sólo reaccionar a los incidentes, sino desarrollar una mentalidad organizacional para identificar las amenazas antes de que ocurran. Según el National Institute of Standards and Technology (2018), la función “Identify” del marco de ciberseguridad es la base para una gestión preventiva eficaz.

La concienciación digital pasa, por tanto, a ser un componente estructural de la cultura organizacional. Según Parsons et al. (2014), programas de concienciación bien diseñados logran reducir significativamente comportamientos inseguros, particularmente ante ataques de ingeniería social. De este modo, la formación continua, las simulaciones de phishing y una comunicación interna clara contribuyen a la consolidación de hábitos digitales responsables y a la reducción de la exposición al riesgo humano.

1.2.3 Comportamiento humano como factor crítico de seguridad

Una de los eslabones más sensibles de la cadena de seguridad organizacional es el comportamiento humano. Diversos estudios en ciberseguridad coinciden en que buena parte de los incidentes tienen su origen en errores humanos, ya sea por negligencia o desconocimiento. Estas vulnerabilidades psicológicas son las que explota la ingeniería social, explica Hadnagy (2018), haciendo uso de la manipulación de emociones como la urgencia, el miedo o la confianza para tener acceso a sistemas de manera indebida.

Las National Academies of Sciences, Engineering, and Medicine (2019) también señalan que la confiabilidad de los sistemas depende tanto de la infraestructura tecnológica como de las prácticas humanas que operan los sistemas. Por lo tanto, fortalecer la cultura organizacional implica comprender factores cognitivos y conductuales, fomentando la responsabilidad individual, el pensamiento crítico y protocolos de acción claros ante situaciones sospechosas.

1.2.4 Responsabilidad compartida en la protección de la información

No puede recaer exclusivamente en el área de tecnologías de la información la protección de la información. Para que exista una cultura de seguridad sólida, es necesario que haya una responsabilidad compartida entre todos los niveles organizacionales, desde la alta dirección hasta el personal de operación. La International Organization

for Standardization (2019) en su norma ISO/IEC 27001 señala que la dirección debe dar ejemplo y demostrar su compromiso con el sistema de gestión de seguridad de la información asignando roles, recursos y responsabilidades claras.

Además, Von Solms y Van Niekerk (2013) afirman que la ciberseguridad organizacional es un fenómeno colectivo, que depende de la alineación entre las políticas formales y las prácticas reales. Si cada colaborador entiende cuál es su papel dentro del sistema de protección, la organización fortalece su resiliencia frente a las amenazas internas y externas. Por tanto, la responsabilidad compartida no es solamente un principio normativo, sino un componente esencial de la cultura organizacional moderna.

1.3 Principales riesgos digitales en las organizaciones

En el contexto actual, caracterizado por una digitalización intensiva de procesos, servicios y modelos de negocio, las organizaciones enfrentan un conjunto diverso y dinámico de riesgos digitales que pueden comprometer tanto su operatividad como su reputación institucional. La interconectividad global, el almacenamiento masivo de datos y la dependencia de infraestructuras tecnológicas han ampliado considerablemente la superficie de exposición frente a amenazas internas y externas. En este escenario, la gestión de riesgos digitales no puede limitarse a controles técnicos aislados, sino que debe integrarse en la planificación estratégica y en la cultura organizacional.

1.3.1 Amenazas internas y externas

Las amenazas digitales pueden clasificarse inicialmente en internas y externas, dependiendo de su origen. Las amenazas externas provienen de actores ajenos a la organización, tales como ciberdelincuentes, grupos organizados, activistas o incluso actores estatales. Estas amenazas suelen materializarse mediante ataques de ransomware, phishing, explotación de vulnerabilidades o denegación de servicio. Según ENISA (2025), el ransomware continúa siendo una de las principales amenazas en Europa, afectando tanto a grandes corporaciones como a pequeñas empresas.

Por otro lado, las amenazas internas se originan dentro de la propia organización y pueden ser intencionales o accidentales. Incluyen el uso indebido de credenciales, filtraciones de información por negligencia o sabotaje deliberado por parte de empleados descontentos. Greitzer y Frincke (Greitzer, 2010) destacan que las amenazas internas representan un desafío complejo debido a que el actor ya posee cierto nivel de acceso legítimo al sistema, lo que dificulta su detección temprana.

Desde una perspectiva organizacional, la distinción entre amenazas internas y externas permite diseñar controles diferenciados. Mientras que frente a amenazas externas predominan mecanismos técnicos como firewalls y sistemas de detección de intrusiones, ante amenazas internas resultan fundamentales las políticas de acceso basado en roles, auditorías periódicas y una cultura organizacional orientada a la ética y la responsabilidad compartida.

1.3.2 Riesgos tecnológicos, humanos y organizacionales.

Los riesgos digitales pueden analizarse también desde una clasificación estructural que distingue entre riesgos tecnológicos, humanos y organizacionales. Los riesgos tecnológicos se relacionan con fallas en software, configuraciones inadecuadas, vulnerabilidades no corregidas o infraestructuras obsoletas. El informe del National Institute of Standards and Technology (2018) enfatiza que la identificación de activos críticos y vulnerabilidades constituye un elemento esencial para mitigar este tipo de riesgos.

Los riesgos humanos, en cambio, están asociados a comportamientos inseguros, desconocimiento, exceso de confianza o manipulación mediante ingeniería social. Hadnagy (2018) explica que los atacantes suelen explotar debilidades psicológicas antes que fallas técnicas, lo que convierte al usuario en un objetivo estratégico. En este sentido, el error humano continúa siendo una de las principales causas de incidentes de seguridad a nivel global.

Finalmente, los riesgos organizacionales se vinculan con deficiencias estructurales como ausencia de políticas formales, falta de liderazgo en seguridad, escasa inversión en infraestructura o inexistencia de planes de continuidad. Von Solms y Van Niekerk (2013) sostienen que la seguridad no puede ser efectiva si no existe alineación entre la estrategia corporativa y las políticas de protección. Por ello, una gestión integral del riesgo digital requiere abordar simultáneamente dimensiones técnicas, humanas y administrativas.

1.3.3 Ciberataques más comunes en el entorno empresarial

En el entorno empresarial contemporáneo, los ciberataques se han convertido en una amenaza constante que afecta a organizaciones de todos los tamaños y sectores. La creciente digitalización de procesos, la dependencia de servicios en la nube y la interconexión de sistemas han generado nuevas oportunidades para actores maliciosos. El European Unión Agency for Cybersecurity (2025) identifica como principales amenazas el ransomware, el phishing, los ataques de ingeniería social y la explotación de vulnerabilidades en software no actualizado.

El ransomware destaca como uno de los ataques más disruptivos, ya que cifra la información crítica de la organización y exige un rescate económico para su liberación. Este tipo de ataque no solo genera pérdidas financieras directas, sino que puede paralizar operaciones completas y afectar la confianza de clientes y socios comerciales. Según el informe del World Economic Forum (2023), el impacto del ransomware ha trascendido el ámbito tecnológico para convertirse en un riesgo estratégico que compromete la continuidad del negocio.

El phishing, por su parte, continúa siendo una de las técnicas más utilizadas debido a su bajo costo y alta efectividad. Mediante correos electrónicos fraudulentos o sitios web falsificados, los atacantes buscan obtener credenciales, datos bancarios o información sensible. Hadnagy (2018) explica que estas estrategias se apoyan en la manipulación psicológica y en la urgencia percibida por el usuario, lo que demuestra

que la vulnerabilidad no es exclusivamente técnica, sino también humana.

Además, los ataques de denegación de servicio distribuido (DDoS) y la explotación de fallas en aplicaciones web constituyen amenazas relevantes en sectores que dependen de servicios en línea. El National Institute of Standards and Technology (2018) enfatiza que la identificación temprana de vulnerabilidades y la implementación de mecanismos de detección y respuesta son esenciales para reducir el impacto de estos ataques. En conjunto, estos ciberataques evidencian la necesidad de una estrategia integral que combine tecnología, capacitación y gobernanza organizacional.

Figura No. #4. Ciberataques más comunes en el entorno empresarial

Nota. Fuente. Imagen creada por IA

1.3.4 Vulnerabilidades frecuentes en microempresas

Las microempresas presentan características estructurales que incrementan su exposición frente a riesgos digitales. La limitada disponibilidad de recursos financieros y humanos suele traducirse en ausencia de políticas formales de seguridad, falta de actualización de sistemas y carencia de planes de respaldo. La International Telecommunication Union (2022) señala que muchas pequeñas empresas no cuentan con personal especializado en ciberseguridad, lo que dificulta la implementación de controles preventivos adecuados.

Una vulnerabilidad frecuente en este tipo de organizaciones es el uso compartido de credenciales y contraseñas débiles, práctica que facilita accesos no autorizados. Asimismo, la inexistencia de copias de seguridad periódicas incrementa el riesgo de pérdida irreversible de información ante incidentes de ransomware o fallas técnicas. ENISA (2025) advierte que las pequeñas empresas suelen subestimar el impacto potencial de un ataque hasta que este ocurre, lo que limita su capacidad de reacción oportuna.

Desde una perspectiva organizacional, la principal debilidad radica en la ausencia de cultura preventiva. Von Solms y Van Niekerk (2013) sostienen que la seguridad efectiva requiere alineación entre políticas, liderazgo y comportamiento organizacional, elementos que a menudo no están formalizados en microempresas. La implementación de medidas básicas puede reducir significativamente la exposición al riesgo.

En consecuencia, fortalecer la resiliencia digital en microempresas no implica necesariamente grandes inversiones tecnológicas, sino el desarrollo progresivo de una cultura organizacional orientada a la prevención y a la responsabilidad compartida. Esta aproximación resulta coherente con los marcos internacionales de gestión de riesgos, que enfatizan la proporcionalidad y adaptación de controles según el tamaño y contexto de la organización (2018).

1.4 Marco ético, legal y normativo de la ciberseguridad

En el entorno digital contemporáneo, la ciberseguridad no puede abordarse exclusivamente desde una perspectiva técnica, sino que debe enmarcarse dentro de principios éticos, obligaciones legales y estándares normativos que orienten la conducta organizacional. La gestión responsable de la información implica reconocer que los datos representan no solo activos estratégicos, sino también derechos fundamentales vinculados a la privacidad, la dignidad y la autonomía de las personas. En este sentido, la ciberseguridad se integra dentro de un sistema más amplio de gobernanza corporativa y responsabilidad social empresarial.

El crecimiento de incidentes relacionados con filtraciones de datos, vigilancia indebida y uso inapropiado de información personal ha generado un fortalecimiento de marcos regulatorios y estándares internacionales. El World Economic Forum (2023) advierte que la confianza digital se ha convertido en un elemento central para la

estabilidad económica y social, lo que obliga a las organizaciones a adoptar políticas claras de cumplimiento y transparencia.

Por ello, comprender el marco ético, legal y normativo de la ciberseguridad resulta fundamental para asegurar no solo la protección técnica de los sistemas, sino también la legitimidad institucional y el respeto a los derechos de los usuarios.

1.4.1 Ética digital y responsabilidad empresarial

La ética digital se refiere al conjunto de principios que orientan el uso responsable de tecnologías y datos dentro de la sociedad y las organizaciones. En el contexto empresarial, implica actuar con transparencia, proporcionalidad y respeto por la privacidad en todas las operaciones que involucren información sensible. Floridi (2013) sostiene que la revolución digital ha transformado la naturaleza de la responsabilidad moral, ya que las decisiones tecnológicas pueden afectar de manera masiva y transfronteriza a individuos y comunidades.

Desde esta perspectiva, la responsabilidad empresarial no se limita al cumplimiento formal de la ley, sino que exige una conducta proactiva orientada a prevenir daños potenciales. La UNESCO (2021) establece que el uso de tecnologías digitales debe guiarse por principios de transparencia, rendición de cuentas y respeto a los derechos humanos, especialmente cuando se gestionan grandes volúmenes de datos.

En el ámbito organizacional, la ética digital se traduce en políticas internas claras, evaluación de riesgos antes de implementar nuevas tecnologías y mecanismos de supervisión que garanticen que los procesos digitales no vulneren derechos fundamentales. De esta manera, la ciberseguridad adquiere una dimensión ética que complementa su función técnica.

1.4.2 Legislación básica sobre protección de datos

El fortalecimiento de la regulación en materia de protección de datos ha sido una respuesta directa al aumento de incidentes de seguridad y al uso masivo de información personal en entornos digitales. Uno de los marcos normativos más influyentes a nivel internacional es el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, promulgado en 2016, el cual establece principios como licitud, transparencia, limitación de finalidad y minimización de datos.

El European Union (2016) determina que las organizaciones deben implementar medidas técnicas y organizativas apropiadas para garantizar la seguridad del tratamiento de datos personales. Este reglamento también reconoce derechos fundamentales de los titulares, como acceso, rectificación y supresión de datos, lo que refuerza el enfoque centrado en la persona dentro del ecosistema digital.

A nivel global, muchos países han adoptado legislaciones inspiradas en este modelo, lo que evidencia una tendencia hacia la armonización normativa en materia de privacidad. Para las organizaciones, esto implica

la necesidad de revisar continuamente sus prácticas de manejo de información, documentar procesos y establecer protocolos de respuesta ante incidentes que puedan comprometer datos personales.

Figura No. #5 Leyes de protección de datos personales.

Nota. Fuente. Imagen creada con IA.

1.4.3 Cumplimiento normativo y buenas prácticas

El cumplimiento normativo en materia de ciberseguridad implica la adopción sistemática de políticas, procedimientos y controles alineados con marcos regulatorios y estándares reconocidos internacionalmente. No se trata únicamente de evitar sanciones legales, sino de establecer un sistema estructurado de gestión que permita identificar riesgos, implementar controles y evaluar su efectividad de manera continua.

La norma ISO/IEC 27001, desarrollada por la International Organization for Standardization (2022), proporciona un marco para establecer, implementar y mejorar un sistema de gestión de seguridad de la información basado en riesgos. Este estándar promueve la documentación de procesos, la definición de responsabilidades y la evaluación periódica de controles, elementos fundamentales para garantizar coherencia organizacional.

Adicionalmente, el National Institute of Standards and Technology (2018) propone un marco flexible que permite a las organizaciones adaptar prácticas de ciberseguridad según su contexto y nivel de madurez. La combinación de estándares internacionales y regulaciones locales fortalece la gobernanza digital y contribuye a consolidar una cultura de cumplimiento y mejora continua.

1.4.4 Introducción a los estándares internacionales de seguridad

Los estándares internacionales de seguridad constituyen marcos de referencia diseñados para orientar a las organizaciones en la implementación de controles técnicos y organizacionales eficaces. Estos estándares buscan establecer criterios comunes que faciliten la interoperabilidad, la evaluación comparativa y la certificación de buenas prácticas en distintos sectores.

Entre los marcos más reconocidos se encuentran ISO/IEC 27001 y el Marco de Ciberseguridad del NIST, los cuales comparten un enfoque basado en la gestión de riesgos. Además, organismos como ISACA

desarrollan marcos como COBIT, orientados a la gobernanza y gestión de tecnologías de la información. ISACA (2019) enfatiza que la gobernanza efectiva de TI debe alinearse con los objetivos estratégicos del negocio, integrando seguridad y desempeño organizacional.

La adopción de estándares internacionales no solo fortalece la seguridad técnica, sino que también mejora la credibilidad institucional ante clientes, socios comerciales y entidades regulatorias. En este sentido, los estándares funcionan como herramientas de legitimación y como guías para estructurar una cultura organizacional orientada a la protección sistemática de la información.

1.5 Importancia de la cultura preventiva en la gestión empresarial

La cultura preventiva en ciberseguridad constituye uno de los pilares fundamentales para garantizar la estabilidad y sostenibilidad organizacional en entornos digitales altamente dinámicos. Más allá de la implementación de controles técnicos, la prevención implica integrar la gestión del riesgo como parte del pensamiento estratégico de la organización. En este contexto, anticiparse a los incidentes resulta más eficiente y menos costoso que reaccionar una vez que el daño ya se ha materializado.

El National Institute of Standards and Technology (2018) establece que la función “Identify” dentro del Marco de Ciberseguridad representa el punto de partida para cualquier estrategia sólida, ya que permite comprender activos, amenazas y vulnerabilidades antes de que generen

impactos significativos. Este enfoque demuestra que la prevención no es una acción aislada, sino un proceso continuo de evaluación y mejora.

Desde la perspectiva organizacional, consolidar una cultura preventiva implica alinear liderazgo, procesos y comportamientos individuales bajo una lógica de responsabilidad compartida. A continuación, se desarrollan los principales elementos estratégicos de esta cultura dentro de la gestión empresarial.

1.5.1 Prevención vs. Reacción ante incidentes

La diferencia entre prevención y reacción radica en el momento en que se actúa frente al riesgo. Un enfoque reactivo se centra en responder a incidentes una vez que estos han ocurrido, lo que generalmente implica mayores costos financieros, reputacionales y operativos. En cambio, la prevención busca anticipar amenazas mediante identificación temprana de vulnerabilidades, capacitación continua y establecimiento de controles estructurados.

El World Economic Forum (2023) advierte que los riesgos cibernéticos pueden generar efectos sistémicos en sectores completos cuando no se gestionan de manera anticipada. Esta afirmación evidencia que la reacción tardía no solo afecta a la organización individual, sino que puede comprometer cadenas de suministro y ecosistemas digitales más amplios.

Desde una perspectiva normativa, la norma ISO 22301 sobre continuidad del negocio subraya la importancia de la planificación preventiva para

reducir el tiempo de recuperación ante incidentes. En consecuencia, adoptar una cultura preventiva permite transformar la gestión de la ciberseguridad en un proceso estratégico de mitigación de riesgos y no únicamente en un mecanismo de respuesta a crisis.

1.5.2 Beneficios estratégicos de una cultura de ciberseguridad

La consolidación de una cultura organizacional orientada a la ciberseguridad genera beneficios que trascienden la reducción de incidentes técnicos. Entre estos beneficios se encuentran el fortalecimiento de la confianza de clientes y socios comerciales, la protección del capital intelectual y la mejora de la reputación corporativa. Según Von Solms y Van Niekerk (2013), la seguridad efectiva depende de la integración entre estrategia organizacional y prácticas operativas, lo que demuestra que la cultura constituye un factor estructural.

Además, el cumplimiento normativo se vuelve más eficiente cuando la cultura preventiva está internalizada en la organización. La norma ISO/IEC 27001 de la International Organization for Standardization (2022) enfatiza la mejora continua y el liderazgo como elementos esenciales dentro del sistema de gestión de seguridad de la información. Cuando estos principios se incorporan culturalmente, el cumplimiento deja de percibirse como una imposición externa y se convierte en parte del funcionamiento natural de la empresa.

Otro beneficio relevante es la reducción del riesgo financiero asociado a incidentes graves. Diversos estudios señalan que la inversión en

prevención resulta significativamente menor que los costos derivados de una brecha de seguridad. En consecuencia, la cultura de ciberseguridad se posiciona como una inversión estratégica y no como un gasto operativo.

1.5.3 Ciberseguridad como una ventaja competitiva

En mercados digitales altamente competitivos, la capacidad de demostrar altos estándares de protección de datos puede convertirse en un elemento diferenciador. Las organizaciones que garantizan seguridad, privacidad y transparencia generan mayor confianza, lo que influye positivamente en la percepción del cliente y en la fidelización. El World Economic Forum (2023) resalta que la confianza digital es un factor crítico para la sostenibilidad empresarial en economías interconectadas.

Desde una perspectiva estratégica, la ciberseguridad contribuye a la consolidación de alianzas comerciales y al acceso a mercados internacionales, especialmente cuando se requiere cumplir con estándares regulatorios estrictos. El European Union (2016) establece exigencias claras en materia de protección de datos que muchas empresas deben cumplir para operar dentro del mercado europeo. Esto demuestra que la seguridad puede convertirse en un habilitador de expansión comercial.

En este sentido, la cultura preventiva no solo protege activos, sino que fortalece la posición competitiva de la organización, proyectando una imagen de responsabilidad y profesionalismo ante el entorno global.

1.5.4 Rol de la alta dirección en la cultura de seguridad

La consolidación de una cultura preventiva depende en gran medida del compromiso de la alta dirección. El liderazgo organizacional tiene la responsabilidad de asignar recursos, definir políticas claras y establecer prioridades estratégicas que integren la ciberseguridad dentro del modelo de gestión empresarial. Sin este respaldo, las iniciativas técnicas tienden a fragmentarse y perder efectividad.

La norma ISO/IEC 27001 (2022) establece explícitamente que la dirección debe demostrar liderazgo y compromiso con el sistema de gestión de seguridad de la información, garantizando que las responsabilidades estén definidas y que exista mejora continua. Este enfoque confirma que la seguridad no puede delegarse completamente a departamentos técnicos, sino que requiere gobernanza institucional.

Asimismo, el National Institute of Standards and Technology (2018) señala que la gobernanza de la ciberseguridad debe integrarse con la estrategia organizacional, permitiendo que la gestión de riesgos forme parte del proceso de toma de decisiones ejecutivas. En consecuencia, el liderazgo activo constituye el motor principal para consolidar una cultura de seguridad sólida y sostenible en el tiempo.

CAPÍTULO II

PREVENCIÓN DE RIESGOS DIGITALES EN EL ENTORNO EMPRESARIAL

2.1 Identificación y clasificación de riesgos digitales

Las compañías, en la época digital, dependen más que nunca de datos, plataformas digitales y tecnología para funcionar. Esta dependencia incrementada no solo genera innovación y eficiencia, sino que también expone a riesgos digitales que tienen el potencial de comprometer la seguridad de la información, la confianza de los trabajadores y los clientes, así como la continuidad del negocio. Por lo tanto, la detección y clasificación de los riesgos digitales es un paso fundamental en la gestión preventiva, que posibilita identificar las amenazas presentes y analizarlas conforme a su procedencia, impacto y probabilidad.

2.1.1 Concepto de riesgo digital

El riesgo digital según Imbaquingo, D; Pusdá, M; Jácome, J (2016) es el grupo de posibles efectos negativos, daños o consecuencias adversas que pueden surgir del uso, la adopción o la dependencia creciente de tecnologías digitales y plataformas en línea a nivel individual, organizacional y social. Este riesgo incluye tanto peligros técnicos (como la violación de la seguridad, los ataques cibernéticos y la pérdida o corrupción de datos) como amenazas a la privacidad, el mal uso de información y la divulgación no autorizada de datos confidenciales. Adicionalmente, el riesgo digital puede provocar pérdidas monetarias, daños a la reputación, interrupciones en las operaciones y transgresiones

legales o regulatorias, sobre todo en sitios con leyes de seguridad de la información y protección de datos. Estos componentes, en su totalidad, evidencian que el riesgo digital no es únicamente de carácter tecnológico; también presenta efectos legales, éticos, organizacionales y sociales que necesitan ser administrados de forma integral y anticipada.

Las dimensiones del riesgo digital demuestran que es un riesgo de múltiples dimensiones, debido a que impacta simultáneamente en numerosas áreas. En el campo tecnológico se manifiesta a través de ataques cibernéticos, malware, fallas en los sistemas y la obsolescencia de las infraestructuras digitales. En el ámbito humano, el riesgo se incrementa debido a errores de los usuarios, analfabetismo digital y susceptibilidad frente a prácticas como la ingeniería social. A nivel organizacional, significa una mala administración de la información y la ausencia de protocolos y políticas de seguridad. El riesgo digital, desde el punto de vista legal y ético, alude a la violación de derechos, el mal manejo de datos personales y la falta de cumplimiento con las leyes. Por último, en el ámbito social se ve reflejado en la dependencia de la tecnología, la desinformación y la exclusión digital. Esto demuestra que el peligro digital trasciende lo tecnológico y debe ser tratado de forma completa. (Kiser, 2020)

2.1.2 Amenaza, vulnerabilidad e impacto

En el contexto de la prevención de riesgos digitales en las empresas, se entiende por amenaza todo acontecimiento, individuo o cosa (ya sea interno o externo) que tenga el potencial de dañar los activos de una

organización y comprometer la seguridad de su información, sus sistemas y la sostenibilidad del negocio. Las amenazas, en lo que respecta a la ciberseguridad de las organizaciones, pueden ser accidentales o intencionales e incluyen desde malware y ciberdelincuentes hasta errores técnicos u humanos, así como defectos en los procedimientos internos que aprovechan las debilidades de la infraestructura tecnológica. Estas amenazas, además, no solo incluyen las que son más comunes o conocidas (como el ransomware, el phishing y los ataques de día cero), sino también otras que son más avanzadas y complejas, como las amenazas persistentes avanzadas (APT) o la utilización de exploits sofisticados. Por lo tanto, para prever, identificar y reducir posibles incidentes de seguridad, las organizaciones deben estar en vigilancia constante y emplear estrategias preventivas completas. (Vega, 2021)

Para TN University Business School (2025) una vulnerabilidad es una carencia, error o hueco en las tecnologías, procesos, sistemas o prácticas de seguridad de una entidad que, si la amenaza lo quisiera, podría ser utilizada para provocar un incidente de seguridad y perjudicar sus activos digitales. En el ámbito empresarial, estas vulnerabilidades no están únicamente presentes en la tecnología (ya sea hardware o software), sino también en configuraciones de sistemas y redes que son inseguras y en el factor humano, cuando no se tiene conocimiento o capacitación sobre prácticas de ciberseguridad. Asimismo, las brechas de seguridad suelen aparecer debido a la falta de controles, actualizaciones o parches, configuraciones erróneas o un uso incorrecto de herramientas digitales. Esto incrementa el riesgo de que se produzcan interrupciones en la empresa, accesos no autorizados o pérdida de datos.

Y por último el impacto, en el contexto de la prevención de los riesgos digitales en el entorno corporativo, se refiere al resultado tangible y cuantificable que tiene lugar cuando una amenaza explota una vulnerabilidad y ocurre un incidente de seguridad asegura. Este es el perjuicio que la organización experimenta, y puede presentarse de varias formas, desde daños en la infraestructura tecnológica hasta deterioros en el funcionamiento del negocio. El efecto se presenta a nivel técnico en la indisponibilidad, la pérdida de confidencialidad o integridad de los sistemas y los datos. Esto puede resultar en accesos sin autorización, manipulación de información o el cese del funcionamiento de sistemas fundamentales. En la realidad, las consecuencias se presentan frecuentemente como interrupciones de procesos esenciales, pérdida de servicios digitales o incapacidad para realizar las operaciones normales de la empresa. Todo esto afecta tanto la atención al cliente como la productividad.

En términos económicos, el resultado puede ser una pérdida monetaria inmediata, como el desembolso de rescates, multas, costos de recuperación, reparación de sistemas o inversión en medidas correctivas. Los incidentes de seguridad pueden afectar la reputación, al tener el potencial de perjudicar la imagen corporativa y provocar que los clientes, socios y proveedores pierdan confianza. (Vega, 2021)

2.1.3 Clasificación de riesgos informáticos

Las amenazas y las vulnerabilidades informáticas son riesgos que impactan a la empresa en todos los sentidos. Las consecuencias pueden

ser muy severas en cuanto a la información que se está gestionando. Muñoz,H (2019) creen que "la terna de activo, amenaza y vulnerabilidad, vinculadas a través de la fórmula" constituyen el riesgo para un sistema informático, "riesgo = vulnerabilidad + amenaza", lo que implica que las compañías cuentan con un conjunto de elementos que funcionan como medio para la protección y conservación de la información, o sea, los activos, que diariamente están expuestos a ciertos riesgos asociados con amenazas y vulnerabilidades. Se puede afirmar que una cosa conduce a la otra, porque si un ordenador no cuenta con las protecciones mínimas que deben tener, como las actualizaciones del sistema operativo, los antivirus y demás elementos. En otras palabras: que ese equipo tiene vulnerabilidades que podrían hacerse efectivas, lo que provocaría el acceso no conseguir autorización de un atacante para acceder al servidor contable de una compañía y, por lo tanto, ejercer control absoluto sobre la información.

La categorización de riesgos de TI clasifica las amenazas más significativas que pueden impactar la tecnología de una empresa en categorías concretas (por función o tipo de activo afectado), como los riesgos relacionados con sistemas (interrupciones, fallos de software o hardware), los riesgos asociados a datos (accesos insuficientes, seguridad o uso inapropiado), los riesgos en comunicaciones online (caídas o interrupciones en la red) y los riesgos operativos (equivocaciones, fraudes internos/exteriores). Este proceso permite determinar dónde se encuentran las vulnerabilidades y priorizar mitigaciones y controles. Algunos de los tipos más comunes de riesgos informáticos incluyen los riesgos cibernéticos (APT, DDoS, malware y phishing), que roban o

bloquean información mediante la explotación de vulnerabilidades; los riesgos de infraestructura y sistemas (hardware, software, redes y desastres naturales), que obstaculizan el acceso a los datos; y los riesgos humanos (manipulación insegura, equivocaciones en la configuración y uso indebido de herramientas), que ponen en riesgo activos críticos y provocan incidentes relacionados con la seguridad. (Kiser, 2020).

2.1.4 Evaluación inicial del nivel de exposición.

El proceso de evaluación inicial de la exposición en ciberseguridad es un procedimiento organizado que permite establecer el grado de vulnerabilidad de una organización frente a las amenazas cibernéticas, ya sean internas o externas.

Figura No. #6 Ataque cibernético

Nota. Fuente: Imagen creada con IA

Esta auditoría consiste en elaborar un inventario de todos los activos tecnológicos (como bases de datos, servidores, redes, aplicaciones, cuentas de usuario y nubes) y averiguar si presentan vulnerabilidades, fallos en la configuración, permisos excesivos o controles de seguridad inadecuados. Asimismo, no se restringe solo a elementos técnicos; tiene en cuenta también los procedimientos de reacción ante incidentes, las políticas de seguridad, los niveles de capacitación del personal y factores humanos.

Después de identificar las vulnerabilidades, se evalúa el grado de riesgo que cada una representa, considerando la probabilidad de explotación y el efecto que tendría en la confidencialidad, integridad y disponibilidad de los datos. Se establece un plan de acción para mitigar las vulnerabilidades más críticas de forma efectiva después. Esta evaluación es el primer paso para consolidar la posición de seguridad, reducir el área de ataque, prevenir incidentes y garantizar la continuidad del negocio. En resumen, presenta una representación del estado de la ciberseguridad en la organización y ayuda a tomar decisiones que permitan implementar adecuadas mejoras y controles. (Morales, 2025)

2.2 Principales amenazas cibernéticas actuales

Cuanto más dependen las empresas de su infraestructura, mayor es el riesgo que tienen frente a las amenazas cibernéticas. La aparición de dispositivos móviles, la computación en la nube, el internet de las cosas y otros equipos ha generado muchos vectores potenciales a través de los cuales un agente de amenazas cibernéticas tiene la posibilidad de atacar

a una entidad. En consecuencia, el panorama de amenazas ha crecido de manera significativa. Los ataques de intermediario, los de denegación de servicio, los que ocurren a la cadena de suministro, los exploits de aplicaciones web y el malware son las principales formas de amenazas cibernéticas con las que lidian hoy en día las compañías.

2.2.1 Malware, ransomware y phishing

Los medios de comunicación y los usuarios frecuentes de computadoras utilizan el término virus como una expresión general para aludir a cualquier tipo de malware que se mencione en los encabezados. Sin embargo, no es justo afirmar que el malware sea un virus afirma Kiser, Q (2020). Un virus informático se adhiere a los archivos en su sistema o apunta a dichos archivos y se activan cuando el usuario los ejecuta. Un usuario, por ejemplo, puede abrir un archivo PDF normal y el virus puede haberse infiltrado mediante un código incrustado.

El dominio digital no suele tener virus en la actualidad, pues estos constituyen menos del diez por ciento de los programas maliciosos. Esto es algo positivo. El virus es el único subgénero de malware que está contenido en un archivo y se propaga a otros. Limpiar los virus se convierte en una tarea complicada debido a que, por su naturaleza, siguen propagándose. Aún las soluciones antivirus más efectivas enfrentan retos para eliminar virus, lo que siempre ha sido un proceso difícil. Detectar y poner en cuarentena archivos infectados es la única capacidad de la mayoría de las soluciones antivirus. No son capaces de limpiarlos, así que solamente acaban borrando esos archivos como último recurso. Es

posible que uno se pregunte cuál es el daño de borrar archivos, pero si esos archivos son esenciales para el funcionamiento de su aplicación o aplicación web, eliminarlos ocasionará un mal desempeño de la misma.
Malware es una palabra que se refiere a varios tipos de software dañino, incluyendo programas espía, virus y ransomware. El malware es un código que los atacantes crean con el propósito de atacar un sistema y la información vinculada a él, o para entrar en la red de otra persona. El correo electrónico es normalmente el medio que se usa para liberar malware. El correo electrónico incluye vínculos o archivos adjuntos que, al hacer clic en ellos o descargarlos, causan la ejecución de un código malicioso.

El malware surgió en la última parte de los años setenta, cuando se introdujo el virus Creeper, que ponía en peligro tanto a las organizaciones como a los usuarios individuales. Desde ese momento, se han observado miles de variantes de malware en todo el mundo, todas con el mismo objetivo: desactivar y destruir servicios. El malware contiene cargas que son distribuidas en los sistemas de destino de diversas maneras. Las razones del atacante van desde exigir dinero hasta robar información, y sus métodos de ataque están empezando a ser más sofisticados. En la actualidad conviven diferentes clases de malware. (Kiser, 2020)

El malware que existe hoy en día es una mezcla híbrida de virus, software malicioso y troyanos. Aunque el malware puede asemejarse a un troyano al principio, su ejecución acabará por atacar a todos los usuarios de una red; esta característica es propia de los gusanos. Hoy en día, los programas de malware son considerados por lo general programas

ocultos o rootkits. Esto quiere decir que la meta primordial del malware hoy en día es hacerse con el control del sistema operativo de la computadora y manejarlo de modo que no sean detectados ni por los programas antimalware. La única forma de eliminar un malware de esta clase es desconectando el componente de memoria que controla el sistema. Una combinación híbrida más de gusanos y troyanos son los bots, que se aprovechan de un sistema y tratan de incorporarlo a un ataque contra una infraestructura mayor. Los bots se encuentran en sistemas informáticos individuales y posteriormente obtienen órdenes de los botmasters, que son servidores de control y comando para la red de bots.

Las botnets, o redes de bots, tienen la capacidad de infestarse desde centenares hasta miles de servidores a través de Internet, todos controlados por un único botmaster. Con frecuencia, los botmasters rentan estas redes de bots a otros criminales que las emplean para sus propias necesidades. (Astudillo, 2025)

El ransomware es, como indica su nombre, un "malware muy interesante que, tras infectar el sistema, cierra ciertos recursos relevantes y populares del sistema de computación y posteriormente solicita dinero para reestablecer el acceso". Usualmente, los ransomwares emplean tecnologías de cifrado para retener la información como evidencia. El 12 de mayo de 2017, el mundo empresarial pasó por un día muy difícil debido a un ciberataque que sucedió a escala mundial. Inicialmente, se indicó que los atacantes generaron cerca de 80.000 incidentes que impactaron a individuos y entidades jurídicas en más de setenta naciones. Después, los medios de comunicación informaron que en realidad habían

sucedido 130.000 ataques y que se llevaron a cabo en un centenar de naciones. El ransomware, al principio creado para atacar a las organizaciones, ahora tiene distintas versiones que pueden impactar a individuos comunes en múltiples dispositivos y plataformas. (Ávila, 2023)

Uno de los ataques más elegidos por los cibercriminales es el ransomware. Esta forma de criminalidad, con la que "Se roba información de un usuario, una empresa o el gobierno para cobrar un rescate, mantiene en alerta al continente americano frente a una serie de ataques que ha examinado la madurez de sus sistemas cibernéticos, que son relativamente nuevos. Según Ávila, F (Ávila, 2023) se ha demostrado que se puede conseguir grandes beneficios si el ataque logra impactar a empresas o entidades gubernamentales que no tienen aún planes de contingencia o contramedidas para este tipo de ataques cibernéticos, siendo la única alternativa en este caso abonar el rescate de los datos. Se habla a menudo del ransomware y de las precauciones que se deben tomar para no ser blanco de esta clase de ataque; sin embargo, aún continúan surgiendo casos y nuevas versiones de este malware siguen siendo producidas.

El ransomware ha revelado que las entidades todavía no perciben la relevancia de aplicar políticas de seguridad, administrar copias de seguridad y seguir prácticas óptimas en el manejo de información. Los atacantes han puesto atención a esta circunstancia en Latinoamérica.

Puede ser difícil conforme aparecen nuevas variantes hacer un seguimiento de las distintas cepas. Aunque cada una de estas variantes de malware es distinta, pero a menudo se fundamentan en métodos parecidos para sacar provecho de los usuarios y mantener los datos cifrados como prenda.

Algunos de los tipos de ransomware más habituales son:

- Ransomware de encriptación. Esta clase cifra todos los archivos del equipo, archivos de documentos, hojas de cálculo, PDF, fotografías y videos y así sucesivamente. CryptoLocker es un caso ejemplar de esto. La captura de pantalla que se presenta a continuación corresponde a un dispositivo afectado por esta clase de malware.
- Ransomware de bloqueo de pantalla: impide el acceso a la pantalla del dispositivo de la víctima y exige un pago. En otras palabras, limita el acceso a archivos o la sesión de inicio mientras requiere el pago para remover la limitación. Por lo general, se pone en práctica a nivel de sistema operativo, lo cual implica que no podrá utilizar el ordenador o el aparato infectado.
- Ransomware que cifra servidores web. Está destinado a los servidores web con el objetivo de encriptar sus archivos. La amenaza cifra los archivos que tienen extensiones conocidas o comunes que se utilizan para crear un sitio web, solo funciona adecuadamente si se ejecuta con privilegios de root.

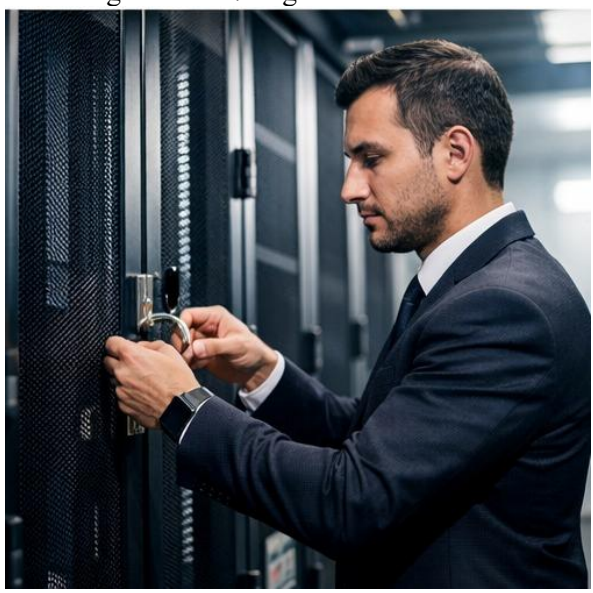
Afirma Castellano, L (2015) que el phishing es un concepto informático que engloba a una clase de delito encuadrada en el campo de las estafas, la cual consiste en tratar de obtener información confidencial de manera fraudulenta (como podría ser una contraseña o datos específicos sobre tarjetas bancarias, por ejemplo). El phisher, o estafador, se presenta como alguien de confianza (una persona o empresa) mediante una comunicación electrónica que parece oficial; frecuentemente es un correo electrónico, aunque también puede ser a través de sistemas de mensajería instantánea o incluso por llamadas telefónicas. El término proviene del inglés "fishing" (pesca), ya que sugiere la idea de "pescar" víctimas incautas con señuelos. Es verdad que Kevin Mitnick se volvió célebre gracias a su phishing telefónico, a través del cual logró acceder a datos sensibles de muchos usuarios, mediante llamadas telefónicas.

El fraude africano o nigeriano tradicional, en el que una supuesta autoridad bancaria, petrolera o gubernamental de África pide al destinatario la información de su cuenta bancaria para poder transferirle grandes cantidades de dinero que necesitan retirar del país, a cambio de una sustancial comisión. En caso de aceptar, luego de varios contactos por correo electrónico e incluso por fax o teléfono, se le pide a la persona incauta en un momento determinado que haga algún desembolso para cubrir gastos imprevistos y hasta sobornos. Por supuesto, ni las cantidades anticipadas serán devueltas, ni los beneficios prometidos se recibirán nunca.

El Tío de América es un mensaje de correo electrónico en el que se informa al destinatario que ha sido nombrado como beneficiario del

testamento de un pariente desconocido y rico, cuyo fallecimiento acaba de ser anunciado por los supuestos albaceas. Como en los demás casos, en algún punto del proceso, los estafadores pedirán que la víctima pague por alguna cosa. Cabe destacar que en este caso se emplean métodos de ingeniería social, pues el apellido del fallecido es igual al del receptor.

Figura No. #7 Seguridad Cibernética



Nota .Fuente: Imagen creada con IA

A través de correos electrónicos, chats, IRC y otros medios, compañías falsas contratan trabajadores a distancia para ofrecerles no solo laborar desde casa, sino también otros beneficios atractivos. Los individuos que aceptan la oferta se vuelven automáticamente víctimas de un delito grave: el blanqueo de dinero adquirido mediante el acto fraudulento del phishing, sin ser conscientes de ello. Para registrarse con este tipo de compañías, una persona debe completar un formulario que incluye su número de cuenta bancaria, entre otra información. Esto tiene como

objetivo depositar en la cuenta del trabajador-víctima el dinero obtenido de estafas bancarias que se llevaron a cabo mediante phishing. Cuando es contratada, la víctima pasa a ser automáticamente lo que se llama comúnmente mulero. La víctima recibe el ingreso sustancial en su cuenta bancaria con cada acto de phishing fraudulento, y la empresa le informa de la situación. Después de que la víctima reciba este ingreso, se quedará con un porcentaje del total, que podrá estar entre el 10% y el 20%, como comisión de trabajo. El resto lo enviará utilizando sistemas para transferir dinero a las cuentas designadas por la pseudoempresa. (Castellano, 2015).

2.2.2 Ingeniería social y fraude digital

La ingeniería social, en realidad, no es una nueva disciplina ni nada por el estilo. Desde el comienzo de la humanidad, ha existido y se ha estado llevando a cabo menciona Castellano, L (2015). En los lugares donde hay engañadores y estafadores, así como también personas inocentes y crédulas, existe Ingeniería Social. Se escucha mucho la frase "Todos los días sale a la calle un tonto". "El que lo atrape es suyo." El propósito de estos párrafos es brindar una perspectiva sobre qué es la Ingeniería Social, describir cómo se realiza, cómo prevenir los ataques por medio de dicha ingeniería, cuáles son las consecuencias de la aparición de las llamadas Redes Sociales y debatir acerca del límite ético de hacer Ingeniería Social. Una de las tácticas más eficaces para contrarrestar las acciones de la Ingeniería Social es el saber. Por ende, a mayor conocimiento, mejor se estará preparado para evitar ser víctima de los ingenieros sociales.

Según (Walker) La ingeniería social debe ser discutida para que cualquier tema sobre la recopilación de información esté completo. Esta técnica consiste en explotar las debilidades humanas que todos los negocios y organizaciones tienen. La intención es manipular a un trabajador mediante la ingeniería social hasta que divulgue información importante que de otra forma no se revelaría. Visualice una situación en la que está haciendo un examen de penetración en su objetivo. En la etapa de investigación inicial, podrá encontrar los datos de contacto de un empleado del departamento de ventas. Es razonable pensar que una persona que trabaja en ventas probablemente responda a correos electrónicos o incluso llamadas telefónicas. Por lo tanto, les envías un correo electrónico haciéndoles creer que eres una persona interesada en sus productos o servicios. Pide más información y recibe una respuesta.

La información que contiene el correo electrónico no es relevante. Lo que estás buscando es el correo electrónico en sí. Es posible que lo revise, implemente diversas herramientas para obtener información de él y recopile datos sobre los servidores de correo electrónico de la entidad**.** Nunca infravalores el potencial de la ingeniería social. La gente siempre comete errores, y en ocasiones muchos de ellos son excesivamente confiados, creyendo que la información que divulgan no es útil para nadie. Solo asegúrese de que tiene permiso para recolectar información de esta forma.

¿Cuántas personas conocemos que nos han contado que les "hackearon" su cuenta de correo electrónico? ¿O que alguien llevó a cabo "operaciones fraudulentas" con su cuenta de usuario en una compañía?

¿O que simplemente alguien "entró" en su Banco Virtual y le "borró" la cuenta? ¿A cuántas personas no les han "clonado" su tarjeta de crédito o débito? ¿Cuántas personas han recibido el "paquete chileno"? Porque esas personas han sido víctimas de lo que se conoce como "ingeniería social". Alvin Toffler (en sus libros "La Tercera Ola" o "The Third Wave", y "Cambio de Poder" o "Powershift", lanzados en 1980 y 1990, respectivamente) menciona las "Olas" o "Eras" humanas, iniciando con la primera ola, en la que el poder es poseído por quien tiene fuerza (o ejércitos grandes). La segunda ola, que se produce con la llegada de la Revolución Industrial, establece que el dinero otorga poder. En la tercera ola, también conocida como la época moderna, se sostiene que el que tiene información es quien ostenta el poder. (Castellano, 2015)

Lo primordial es distinguir entre el fraude digital y el tradicional. El fraude convencional consiste en hábiles engaños o trucos para que tú proporciones información sin darte cuenta, o también en robar documentos de identificación físicos. Un fraude clásico, por ejemplo, consiste en que te roben el INE o el pasaporte y usen esos documentos para sacar un crédito o teléfono a tu nombre. Además de eso, es frecuente falsificar firmas y emitir cheques sin fondos. Estos métodos consisten en engaños o robo de identidad para que se entregue dinero y normalmente tardan un tiempo en materializarse.

No obstante, el fraude cibernético en México es mucho más rápido; puede ocurrirte de un solo momento por una distracción y los criminales se enfocan solamente en robar información que ya está disponible en plataformas digitales. Algunas de las maneras de estafa en Internet están

vinculadas con: La duplicación de tarjetas, el pirateo de cuentas, el engaño por phishing, el vishing, el smishing. Si no te percatas de inmediato de todos estos engaños, los criminales pueden actuar muy rápidamente para apropiarse del dinero que tienes en tus cuentas y en tus tarjetas de crédito; por lo tanto, son peligrosos. Una vez que se tiene conocimiento de qué consiste el fraude digital, es necesario reconocerlo y actuar rápidamente si se tienen dudas o si se percibe alguna irregularidad en tus cuentas. (BBVA, 2026).

El fraude digital consiste en servirse de víctimas mediante el empleo de software y servicios en línea que tienen acceso a la red. El concepto de "fraude en Internet" normalmente abarca las acciones del cibercrimen que se realizan por medio de Internet o del correo electrónico, incluyendo crímenes como el robo e imitación de la identidad y otras actividades de piratería informática con el propósito de engañar a la gente para que entregue dinero. Cada año, las estafas en línea dirigidas a las víctimas por medio de servicios en Internet suponen la actividad fraudulenta de millones de dólares. Y los números siguen creciendo a medida que se extiende la utilización de Internet y las estrategias de los ciberdelincuentes se vuelven más complejas.

Los delincuentes cibernéticos emplean una diversidad de tácticas y vectores de ataque para perpetrar fraudes en la red. Esto abarca el correo electrónico, los servicios de mensajería instantánea y el software malicioso para diseminar malware, así como las estafas de suplantación de identidad sofisticadas y extensas, además de las páginas web fraudulentas que roban información personal. (Fortinet, 2025)

2.2.3 Riesgos asociados al uso de la nube y dispositivos móviles

Internet está compuesto por nubes, aunque no las que se encuentran en el cielo. La computación en la nube es una tecnología que posibilita que los usuarios consulten sus archivos desde cualquier lugar del planeta. La nube es una red de computadoras que guarda información a la cual se puede acceder de manera remota mediante un dispositivo inteligente. Los correos electrónicos son la manifestación más común de una nube. Desde cualquier lugar, siempre que cuente con las credenciales requeridas, se puede acceder a ellos; están guardados en un grupo de computadoras repartidas por Internet. Otro caso sería una lista de reproducción de Spotify que elaboró con su teléfono móvil, pero también tiene la posibilidad de acceder a ella desde otro dispositivo, como un computador portátil, al iniciar sesión con la misma cuenta. (Kiser, 2020).

Numerosas amenazas de seguridad que afrontan los centros de datos convencionales se propagan hacia los entornos de computación en la nube. Los ciberdelincuentes intentan, en los dos casos, aprovecharse de las debilidades de hardware y software. No obstante, la computación en la nube plantea un nuevo elemento: los atacantes tienen la posibilidad de explotar tanto los procedimientos y tecnologías controlados por el proveedor como por el cliente de la nube. Las dos partes comparten el deber de tratar y reducir estos riesgos. Para salvaguardar la nube, es esencial entender esta relación. En el modelo de responsabilidad compartida (modelo de infraestructura de nube pública), es necesario que los datos sensibles, las aplicaciones, los usuarios y las cargas laborales sean salvaguardados por el cliente de la nube. Las herramientas de CSPM

colaboran en la detección y solución de vulnerabilidades de seguridad. CSPM lo asiste para identificar equivocaciones y configuraciones erróneas, entender las infracciones de políticas y de seguridad a través de la detección de amenazas, así como para solucionar problemas y aplicar parches antes de que ocurran ciberataques.

Las soluciones CSPM operan de forma automática para detectar de manera constante fallos en la configuración que pueden causar filtraciones y fugas de datos. Cuando las organizaciones utilizan la detección automatizada de errores en la configuración, pueden hacer las correcciones necesarias con regularidad. Ofrece visibilidad de la infraestructura de nube pública, un ambiente que suele ser limitado a los usuarios de la nube. Las organizaciones pueden, gracias a CSPM, detectar finalmente errores de configuración en la nube y corregirlos a tiempo. (Fuks, 2024)

Los dispositivos móviles han sido parte del día a día de la mayoría de las organizaciones durante años. Los smartphones y las tabletas se emplean para obtener acceso a aplicaciones de negocios, información fundamental, herramientas colaborativas e incluso el correo corporativo. La movilidad no es más un fenómeno nuevo. Y precisamente por esa razón, muchos de sus riesgos son inadvertidos. Hay una percepción generalizada de que los dispositivos móviles "ya están más o menos bajo control". No obstante, en la práctica, no siempre esa percepción coincide con lo que es real. El hecho de tener teléfonos móviles en uso no implica necesariamente que se estén administrando de manera estructurada, y es

precisamente ahí donde surgen los riesgos ocultos. (Bromwich & Bromwich, 2016)

Según el escrito de la Universidad Veracruzana (2025) los dispositivos portátiles, tabletas y móviles, por su tamaño pequeño y por su capacidad para manejar información del negocio, conllevan riesgos adicionales. En el teletrabajo, además de emplear aparatos móviles y conectarnos fuera de la red universitaria, usamos servicios para compartir documentos y enfrentamos riesgos relacionados con ambientes laborales menos controlados. El hurto o el extravío de dispositivos móviles, computadoras portátiles, tabletas y de almacenamiento, como son los discos duros externos y las memorias USB. Este puede ser el peligro más relevante al que se enfrentan estos dispositivos por su tamaño y, en gran parte de los casos, por su alto precio. Siempre es un peligro a considerar la infección por malware, ya que el software malicioso tiene el potencial de hurtar datos confidenciales de la compañía y credenciales de acceso a diversos recursos.

Con frecuencia, pasamos por alto la protección contra malware en equipos pequeños. El uso de redes wifi-inseguras podría amenazar la privacidad de las comunicaciones, dado que los cibercriminales tienen la posibilidad de "escuchar" todo lo que se envía y recibe. Además, tenemos la posibilidad de conectarnos a redes wifi que se hacen pasar por otras redes wifi-legítimas.

La utilización de dispositivos móviles ha brindado a los médicos métodos nuevos de comunicación profesional, una manera más fácil de acceder a

ayuda para la toma de decisiones y consultas especializadas eficaces y rápidas. No obstante, entre los peligros vinculados al empleo de teléfonos inteligentes para almacenar y crear imágenes médicas se encuentran la falta de seguridad en el almacenamiento de datos, las infracciones a la privacidad y que el médico o la entidad sean responsables por no haber conseguido el consentimiento del paciente. Las apps móviles para documentar fotos no satisfacen los estándares de atención que se prevén razonablemente para asegurar la privacidad del paciente y el resguardo seguro de la documentación médica. Hay dos demandas judiciales en curso en los tribunales de Canadá que tratan sobre las infracciones a la privacidad en el cuidado de la salud. (Bromwich & Bromwich, 2016)

2.3 Estrategias de prevención y control de riesgos

2.3.1 Controles técnicos, administrativos y físicos.

Las acciones de prevención y control de riesgos en ciberseguridad constituyen un conjunto de medidas integrales, sistemáticas y persistentes que buscan prever, reducir y gestionar las amenazas que pueden poner en riesgo los activos informáticos de una entidad. No solamente implementan herramientas tecnológicas, sino que, a fin de proteger la confidencialidad, integridad y disponibilidad de la información, fusionan procesos, personas y tecnología. Desde un enfoque administrativo y técnico, estas estrategias forman parte del manejo de riesgos, el cual es el procedimiento mediante el cual una entidad identifica sus activos esenciales, detecta las amenazas y

debilidades que los impactan, estima el riesgo y aplica las medidas de tratamiento adecuadas. (Vega, 2021)

Los controles técnicos de ciberseguridad son el agrupamiento de procedimientos tecnológicos que resguardan la infraestructura digital de una entidad ante peligros internos y externos. Se implementan de manera directa en redes, sistemas informáticos, servidores, aplicaciones y dispositivos finales con el objetivo de prevenir accesos no autorizados, identificar conductas sospechosas y reducir incidentes de seguridad automáticamente o semiautomáticamente. Los controles técnicos se llevan a cabo por medio de configuraciones de software y hardware, así como herramientas que permiten la supervisión en tiempo real del ambiente digital, a diferencia de los controles administrativos, que dependen de políticas y procedimientos.

Estos controles incluyen sistemas de gestión de identidades y accesos (IAM) para implementar el principio de privilegio mínimo, antivirus y antimalware para protegerse contra software malicioso, cifrado de datos para asegurar la información tanto en tránsito como en reposo, autenticación multifactor (MFA) para reforzar la verificación de identidad, así como firewalls con el fin de filtrar el tráfico de red e IDS/IPS (sistemas de detección y prevención de intrusiones) para detectar actividades sospechosas. Asimismo, las soluciones SIEM ayudan a determinar incidentes de manera anticipada, ya que recopilan, correlacionan y examinan sucesos de seguridad en tiempo real. (Seguridad 360, 2024)

Según Juca,F (2025) los controles administrativos de ciberseguridad en cambio son las políticas, normas, procedimientos y directrices organizacionales que rigen el comportamiento del personal y definen el marco de gestión de seguridad de la información de una organización.

Figura No. # 8 Ciberseguridad

Nota. Fuente: Imagen creada con IA

Mientras que los controles técnicos utilizan la tecnología como base, los controles administrativos implican la planificación, organización y supervisión de las prácticas de seguridad, garantizando que existan políticas y procedimientos establecidos para proteger los activos digitales. Estos controles abarcan políticas de seguridad de la información, normas internas de uso aceptable de sistemas, clasificación y manejo de datos, gestión de contraseñas, planes de respuesta a incidentes, planes de continuidad de negocio, auditorías internas,

evaluaciones periódicas de riesgos y programas de capacitación y concienciación del personal. También incluyen la designación de roles y responsabilidades, la separación de funciones y la gestión de proveedores externos, para minimizar errores humanos y prevenir vulnerabilidades en la organización.

Las medidas de seguridad que se implementan con el fin de proteger los recursos, las instalaciones y los equipos tecnológicos contra robos, accesos no autorizados, daños maliciosos o desastres naturales constituyen los controles físicos de ciberseguridad. Estos controles tienen un impacto en el entorno donde funcionan los sistemas de información, asegurando que servidores, estaciones de trabajo y dispositivos de red no puedan ser manipulados físicamente por personas no autorizadas.

Sistemas de control de acceso biométrico o con tarjeta, vigilancia por video (CCTV), guardias, registro de visitantes, sistemas contra incendios, cerraduras seguras y generadores eléctricos de respaldo son algunos ejemplos. Busca garantizar la disponibilidad y continuidad operativa, así como agregar controles administrativos y técnicos, porque incluso la infraestructura digital más segura puede estar en riesgo si no se dispone de seguridad física para proteger los activos tecnológicos. (Castellano, 2015).

2.3.2 Políticas básicas de seguridad de la información

La ciberseguridad es una de las inquietudes más relevantes para cualquier empresa en el actual entorno digital, que avanza velozmente, sin importar su magnitud. Cuando las amenazas cibernéticas son más avanzadas cada

día, proteger la información confidencial, mantener la confianza y cumplir con los requerimientos legales y normativos se han vuelto de gran relevancia. El establecimiento de una política de seguridad clara y efectiva debe ser el núcleo central de este esfuerzo. La estrategia de ciberseguridad de una organización se fundamenta en una política de seguridad. Ofrece una estructura clara que constituirá la base para que la organización proteja sus sistemas de información y prevenga el acceso no autorizado, las violaciones de datos y otros incidentes cibernéticos.

Una política de seguridad asegura que todos los integrantes de la organización comprendan su rol en el mantenimiento de la seguridad cuando se les proporcionan directrices claras. (Sentineloen, 2025)

Las políticas de seguridad de la información son el conjunto de normas, directrices y procesos que determinan los lineamientos para salvaguardar la información de una entidad. Estas políticas establecen qué requisitos de seguridad tiene la información, determinan cuáles son los roles y las responsabilidades de los individuos que participan en la administración de la seguridad de dicha información y ofrecen estrategias para defenderla frente a potenciales peligros. Para cualquier entidad que gestione información confidencial, las políticas de seguridad de la información son fundamentales, porque ofrecen una orientación para garantizar el resguardo apropiado de la información. Al determinar estas normas, se define un punto de partida y un marco de referencia para gestionar la seguridad de la información en la organización. Hay que considerar que las políticas de seguridad de la información no son una respuesta universal. Deben ajustarse a las necesidades particulares de

cada organización y a sus requisitos exclusivos de seguridad. Las políticas de seguridad de la información deben actualizarse con regularidad para asegurar que continúen siendo eficaces.

Las políticas de seguridad de la información pueden englobar algunos de los siguientes ámbitos: El Control de Acceso: Determinando las prerrogativas y derechos de cada usuario en cuanto a la información. La seguridad física: implementando medidas de protección para salvaguardar la información en el ámbito físico de la empresa. La gestión de activos: garantizando que la información está resguardada en todo momento y que se emplean métodos apropiados para almacenar y usar dicha información. La política de gestión de contraseñas: se establecen procedimientos y normas para la administración y uso de las contraseñas. Numerosas organizaciones implementan sus políticas de seguridad de la información hoy en día utilizando normas como las de CIS Controls, NIST SP 800-53 o ISO 27001. (Castellano, 2015)

2.3.3 Gestión de accesos y contraseñas

La gestión de accesos es el campo de la ciberseguridad que se ocupa de administrar los derechos que tienen los usuarios para acceder a recursos digitales. Los procesos y las herramientas para gestionar accesos aseguran que únicamente los usuarios con autorización puedan acceder a los recursos requeridos, impidiendo el acceso de individuos externos con malas intenciones y de usuarios internos. La administración de accesos y la administración de identidades son los dos fundamentos de una rama más amplia de ciberseguridad: la gestión de identidades y accesos (IAM).

La IAM se encarga de proteger y proporcionar las identidades digitales y los permisos de los usuarios en un sistema informático.

La administración de identidades implica formar y conservar las identidades de todos los usuarios de un sistema, incluyendo seres humanos (como empleados, clientes o contratistas) y no humanos (como dispositivos IoT, agentes de IA y cargas de trabajo automatizadas o puntos finales). La gestión de acceso implica proporcionar a estos usuarios un acceso seguro a los activos basados en la nube, así como a las aplicaciones, los datos y los recursos locales de una organización. La gestión de acceso tiene como funciones primordiales la autorización para que los usuarios realicen ciertas acciones en un sistema, la autenticación de su identidad y la administración de las políticas de acceso. (Holdsworth & Kosinski, 2025)

Para Mishra, A (2025) las contraseñas son la llave de nuestro mundo digital. Sirven como claves secretas para liberar nuestro email, cuentas de banco y sistemas de empresa. La administración de contraseñas en términos de ciberseguridad es crucial para salvaguardar la información confidencial y prevenir el acceso no autorizado. Supone guardar, crear y actualizar de manera segura a través de herramientas especializadas que facilitan nuestras interacciones digitales cotidianas y optimizan la seguridad. Cuando discutimos la gestión de contraseñas, nos referimos a la práctica de guardar, acceder y proteger sus contraseñas de manera segura con el fin de aumentar la privacidad y seguridad en su vida digital. Conforme se incrementa la cantidad de cuentas en línea, se hace difícil recordar una contraseña secreta única para cada una. Los administradores

de contraseñas especializados protegen y consolidan la información de inicio de sesión en un cofre cifrado, producen alternativas sólidas y le recuerdan que necesita actualizarlas, disminuyendo de este modo el peligro de acceso no autorizado. Para las entidades, esto supone la centralización del almacenamiento de todas las credenciales, lo que simplifica el seguimiento del acceso por parte de los equipos de TI y el mantenimiento de los estándares de seguridad en diversos sistemas y usuarios.

2.3.4 Copias de seguridad y planes de contingencia

Si todos estos datos están almacenados en un solo lugar digital, como una computadora, tableta o teléfono inteligente, existe el riesgo de que se pierdan. Hay muchas formas en que los datos pueden perderse. Quizás tu computadora se moje o una actualización de software no funcione como debería. Un dispositivo tiene el potencial de extraviarse en un desastre natural o en un incendio. Un virus tiene la capacidad de hurtar todos tus datos o de arruinar tu computadora. Un atacante malicioso podría atacarte con ransomware, un tipo de ataque en el que los datos de un dispositivo se mantienen secuestrados a menos que se pague una tarifa. Para prevenir la pérdida de documentos, datos y archivos importantes, haz copia de seguridad de tus archivos con frecuencia y regularidad. Incluso podrías pensar en respaldar tus archivos todos los días, o más a menudo. (National Cybersecurity Alliance, 2024)

La descripción más básica de una copia de seguridad de datos es el proceso de crear y almacenar copias de sus datos para que puedan

restaurarse si el original se pierde, se corrompe o es robado. La copia de seguridad es a menudo considerada como su segunda línea de defensa, o la red de seguridad que lo ampara si todos sus métodos para prevenir ataques cibernéticos se desploman. La dura realidad es que, incluso los sistemas más seguros, pueden perder datos. No se requiere mucho: basta con un clic incorrecto, una fuga de datos o una avería del hardware que no se esperaba. Cualquiera de estas variables puede causar una pérdida importante de datos. Si no tiene un proceso confiable de copias de seguridad, esa pérdida podría interrumpir el funcionamiento de su empresa. Con seguridad, existen bastantes noticias en los medios sobre estas interrupciones y ataques, así que tratemos de evitarlos si podemos.

La buena noticia es que, si tiene una copia de seguridad sólida, podrá recuperar sus datos y recuperarse con rapidez. No solo se trata de almacenar los datos en otro lugar, sino de asegurar que continúen siendo accesibles y estén protegidos. En el campo de la ciberseguridad, es crucial reconocer cuán relevantes son las copias de seguridad de datos. ¿A qué se refieren? Con regularidad, son parte de un Plan de Recuperación ante Desastres (DRP) o del Plan de Continuidad de Negocios (BCP). Ambos generalmente incluyen un conjunto de procedimientos que se refieren a los procesos de copia de seguridad y recuperación, los cuales están incluidos en los planes. (Security Everywhere, 2025)

Es malo pensar que podemos preverlo todo, ya que la seguridad total y la ausencia absoluta de riesgos no existen. Creernos inmunes a los peligros puede causarnos la realización de errores graves Ochoa, M (2025). Uno

de ellos es no contar con un plan de contingencia para actuar si una amenaza imprevista resulta en un ataque. El plan de ciberseguridad de tu empresa debe incluir un plan de contingencia que garantice la continuidad de la actividad, mantenga viva a la compañía y, sobre todo, tenga la capacidad de reducir los daños provocados por el ataque. Un plan de contingencia frente a una filtración de datos es una serie de acciones estructuradas para reaccionar con rapidez ante sucesos de ciberseguridad y disminuir su efecto negativo en la reputación y el funcionamiento de la compañía también se compone de preparación, detección, respuesta y recuperación. Estas cuatro fases son vistas como partes del ciclo de gestión de riesgos, no como tareas independientes.

2.4 Concienciación y capacitación del talento humano

2.4.1 Importancia de la formación continua

Para las organizaciones que aspiran a salvaguardar sus activos digitales de forma eficaz, la capacitación constante en ciberseguridad se vuelve una necesidad en un mundo con un progreso tecnológico acelerado y donde los delincuentes cibernéticos no dejan de innovar sus tácticas de ataque. La ciberseguridad es un área en permanente cambio. Los ataques cibernéticos se tornan más complejos y difíciles de anticipar, mientras que cada día emergen nuevas vulnerabilidades. La capacitación permanente posibilita que los expertos en ciberseguridad se mantengan al día con las amenazas y tecnologías más recientes para protegerse de ellas. Incluso los sistemas que parecen seguros pueden volverse obsoletos y estar expuestos a riesgos importantes si no se actualizan regularmente.

Numerosos sectores industriales están sometidos a regulaciones rigurosas que requieren la protección de datos personales y el aseguramiento de la seguridad de la información. Para acatar estas regulaciones, es esencial la capacitación permanente en ciberseguridad. Ofrece a los trabajadores el conocimiento requerido para aplicar y sostener prácticas que se ajusten a estándares como HIPAA, GDPR, etc. No acatar estas normas no solo pone en peligro la seguridad de los datos, sino que puede también conllevar castigos legales graves. (Linkedin, 2024)

2.4.2 Programas de sensibilización en ciberseguridad

Los programas de sensibilización en ciberseguridad son planes diseñados para robustecer la cultura de seguridad de una entidad mediante la educación, la conciencia y el cambio en las actitudes del personal. Su propósito es reducir el riesgo vinculado al factor humano, que es una de las principales razones por las que ocurren incidentes de seguridad informática. Estos programas no solamente enseñan conocimientos técnicos básicos, sino que tratan de fomentar una actitud de responsabilidad y prevención en la gestión de la información y el empleo de las herramientas tecnológicas.

La capacitación y la toma de conciencia son componentes fundamentales en un sistema de gestión de seguridad de la información, según organismos internacionales como el NIST (National Institute of Standards and Technology) (2024) y la ISO (International Organization for Standardization), particularmente en lo que respecta a la norma

ISO/IEC 27001. Esto quiere decir que las empresas tienen que poner en marcha programas formales de capacitación, revisiones regulares y registros que evidencien la competencia del personal en términos de seguridad.

Figura No. #9 Prevención de ataques cibernéticos

Nota. Fuente: Imagen creada con IA

Un programa de concienciación efectivo supone capacitaciones periódicas, ejercicios prácticos, campañas de comunicación interna, simulacros de ataques (como las pruebas de phishing), boletines informativos y evaluaciones del aprendizaje. Además, debe adecuarse a los diversos tipos de colaboradores, desde el personal operativo hasta el gerencial, y actualizarse para enfrentar nuevas amenazas como la suplantación de identidad, ransomware o fraudes digitales. No solo se trata de informar, sino también de modificar la conducta diaria en materia de seguridad de los usuarios.

2.4.3 Buenas prácticas digitales para colaboradores

Para Barnes, T (2025) la ciberseguridad es esencial para compañías de cualquier tamaño, y los trabajadores son clave para proteger la información confidencial frente a las amenazas digitales. Lo siguiente son algunas de las prácticas sugeridas que los trabajadores pueden adoptar para incrementar su conocimiento sobre ciberseguridad:

- Utilice contraseñas seguras: Es obligatorio que los trabajadores utilicen contraseñas únicas y complejas en todas sus cuentas, además de modificarlas con regularidad. Las contraseñas tienen que tener entre 8 y 12 caracteres, incluyendo cifras, mayúsculas y minúsculas, así como símbolos.
- Preste atención a los emails sospechosos: Los correos electrónicos de phishing son bastante frecuentes y los delincuentes cibernéticos los emplean con frecuencia para estafar a la gente y lograr que divulguen información privada. Los trabajadores no deben brindar información personal hasta que verifiquen la identidad del emisor y deben tener cuidado con correos electrónicos de remitentes desconocidos, así como con enlaces o archivos adjuntos inesperados.
- Emplee redes seguras: los trabajadores deben hacer uso de una red privada virtual (VPN) para asegurar que su conexión esté encriptada y sea segura al conectarse a Internet mediante redes Wi-Fi públicas.
- Dispositivos físicos seguros: Todos los dispositivos que son de la compañía, incluyendo computadoras portátiles, tabletas y teléfonos inteligentes, tienen que estar asegurados con métodos como cifrado, contraseñas o autenticación biométrica.

- Reportar incidentes de seguridad: Los trabajadores tienen la obligación de notificar al departamento de TI, sin demora, cualquier incidente de seguridad, ya sea un correo electrónico que despierte sospechas o un intento no autorizado de acceder a los sistemas corporativos.

2.4.4 Cultura de reporte de incidentes

Para reducir los perjuicios y asegurar una rápida recuperación, es esencial gestionar e informar de manera efectiva sobre los incidentes de ciberseguridad. Es necesario que las organizaciones implementen protocolos precisos para detectar, analizar y reaccionar ante los incidentes. Estos protocolos deben incorporar estrategias de comunicación, documentación exhaustiva y acciones de contención inmediata. Los reportes de incidentes tienen que ser puntuales y exactos, brindando información fundamental tanto a los organismos reguladores como a las partes interesadas. La formación y los ensayos regulares optimizan la preparación y aseguran que cada uno de los integrantes del equipo entienda sus responsabilidades y funciones. El empleo de tecnologías y herramientas avanzadas tiene el potencial de mejorar la gestión de incidentes, posibilitando así una respuesta y detección más veloces. El análisis posterior a los incidentes contribuye a perfeccionar las estrategias y a evitar que ocurran incidentes en el futuro. La resiliencia y la confianza se refuerzan cuando estas prácticas se incorporan a la cultura de la organización, lo que protege tanto los datos como la reputación. (Astudillo, 2025).

2.5 Gestión de incidentes y continuidad del negocio

2.5.1 Identificación y respuesta ante incidentes

La respuesta a incidentes (RI) alude a los procedimientos y sistemas de una institución para detectar y reaccionar ante las brechas y amenazas cibernéticas. El propósito de la IR es identificar, investigar y contener los ataques en una organización. Las enseñanzas adquiridas de las actividades de IR también contribuyen a las estrategias posteriores de mitigación y prevención, con el objetivo de optimizar la posición general de seguridad dentro de una organización. No se puede evitar que ocurran incidentes de ciberseguridad. Tener un robusto programa de respuesta a incidentes puede marcar la diferencia entre hundirse o nadar. La sofisticación, la gravedad y la frecuencia de las tácticas de ataque continúan creciendo. Por lo tanto, es fundamental que un centro de operaciones de seguridad (SOC) disponga de respuestas documentadas y verificadas para los peligros a los que se verá expuesto.

El proceso de IR contribuye a responder preguntas clave acerca de un ataque, por ejemplo: cómo accedió el atacante, qué acciones realizó y si la información sensible se vio comprometida. No solo mejorará la posición de seguridad de una organización, sino que también contribuirá a evaluar las responsabilidades regulatorias o legales potenciales si se responde con confianza a estas preguntas.

Asimismo, una estrategia de IR efectiva tiene la capacidad de disminuir las consecuencias económicas que suelen acompañar a los incidentes o

infracciones de la ciberseguridad. Si una organización no está bien preparada para reaccionar, los métodos de ataque como el robo de credenciales, DDoS y los brotes de malware (que incluyen el ransomware y el spyware) pueden ser perturbadores y costosos. (Paloaltonetwork, 2025)

2.5.2 Procedimientos básicos de actuación

Los procedimientos fundamentales de respuesta a incidentes cibernéticos son las etapas sistemáticas que una organización aplica para reaccionar eficazmente ante un ataque o amenaza de este tipo. Estos procesos comienzan con la preparación, que consiste en establecer herramientas de seguimiento, roles y políticas; luego se prosigue con la identificación del incidente por medio de la detección de alertas de seguridad o conductas anormales; posteriormente se lleva a cabo la contención para evitar su diseminación; después ocurre la eliminación de la causa, por ejemplo cuando se quita malware o se corrigen vulnerabilidades; y finalmente concluyen con la recuperación de los sistemas afectados para restablecer las operaciones normales. Después del incidente, se lleva a cabo un repaso de las lecciones aprendidas con el fin de fortalecer los controles y prevenir su repetición. En total, estos pasos garantizan una respuesta coordinada que reduce al mínimo los efectos, salvaguarda la información y sostiene la continuidad de las operaciones comerciales. (cyberhaven, 2025)

2.5.3 Continuidad operativa y recuperación ante desastres

El proceso que asiste a las empresas en la reanudación de sus actividades comerciales normales después de un desastre se conoce como recuperación ante desastres y continuidad del negocio (BCDR). Aunque la continuidad del negocio y la recuperación frente a catástrofes están íntimamente vinculadas, representan dos maneras levemente distintas de gestionar crisis que las compañías tienen la posibilidad de implementar. A medida que se hace más caro prevenir la pérdida de datos y el tiempo de inactividad, varias organizaciones están incrementando su inversión en la administración de emergencias. Las compañías de todo el mundo planeaban invertir 219 000 millones de dólares en ciberseguridad durante el año 2023, lo que representa un incremento del 12 % respecto al año anterior.

Un plan de recuperación ante desastres (DRP) es un proyecto que describe cómo una compañía se recuperará de un acontecimiento imprevisto. Los DRP asisten a las compañías en la administración de una variedad de situaciones catastróficas, incluyendo interrupciones masivas, ataques de ransomware y malware, desastres naturales y más. Los planes de continuidad del negocio (BCP), como los DRP, tienen un rol fundamental en la recuperación después de desastres y asisten a las empresas para que retornen a sus actividades comerciales habituales cuando se presenta un desastre. A diferencia de un DRP, que se enfoca concretamente en los sistemas de TI, la gestión de la continuidad del negocio abarca más ampliamente varios elementos de la preparación. (Flinders & Smalley, 2024)

2.5.4 Lecciones aprendidas y mejora continua

La última etapa y una de las más relevantes en la gestión de incidentes cibernéticos es la mejora continua y las lecciones aprendidas. En esta etapa se investiga lo que ocurrió luego de un incidente, con el objetivo de identificar qué salió mal, qué fue bien y cómo se puede mejorar para evitar que vuelva a suceder. Para reforzar la resiliencia organizacional, no es suficiente con resolver el problema; también es necesario aprender de él. El periodo de respuesta, la eficacia de las medidas de seguridad, la colaboración del equipo, la comunicación interna y externa y el verdadero efecto del incidente en las operaciones son analizados en esta etapa.

A partir de este análisis, se ponen al día los procedimientos, las políticas, los planes de continuidad, los controles técnicos y los programas de capacitación. Asimismo, se registra oficialmente el suceso para establecer un historial de referencia frente a futuros acontecimientos. La mejora continua implica que la organización no debe considerar la seguridad como un proceso inalterable, sino como un ciclo constante de evaluación, ajuste y fortalecimiento. De este modo, cada evento es una oportunidad para optimizar la postura de seguridad, reducir las vulnerabilidades y estar más listo frente a nuevas amenazas.

CAPÍTULO III

LA FAMILIA ISO/IEC 27000 Y LA ESTANDARIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1 Introducción a la familia de normas ISO/IEC 27000

3.1.1 Origen y evolución de la norma

ISO es un acrónimo que significa "Organización Internacional para la Normalización" (International Standardization Organization, en inglés), cuyo domicilio se ubica en Suiza. Fundada después de la Segunda Guerra Mundial (23 de febrero de 1947), se trata del ente responsable de fomentar el progreso de estándares internacionales en cuanto a comunicación, fabricación y comercio para todos los sectores industriales, salvo el sector electrónico y eléctrico. Su tarea fundamental es procurar que las empresas u organizaciones del mundo entero estandaricen las normas de seguridad y productos. La ISO es una red compuesta por las entidades de normas nacionales de 163 naciones, con un miembro por país.

La coordinación del sistema se lleva a cabo desde la Secretaría Central, situada en Ginebra (Suiza). La Organización Internacional de Normalización (ISO), cuyo centro está en Ginebra, está formada por delegaciones gubernamentales y no gubernamentales que se dividen en varios subcomités, los cuales tienen la responsabilidad de crear guías para mejorar el medio ambiente. (Castellano, 2015)

La norma ISO 27000 es una norma internacional y de acceso libre, que busca definir los requisitos mínimos que debe satisfacer un Sistema de Gestión de Seguridad de la Información (SGSI) en una entidad. La mejora del SGSI dentro de la organización se fundamenta en la implementación del ciclo PDCA (Plan – Do – Check - Act, Planifica – Ejecuta – Supervisa - Actúa), como ocurre con muchas otras normas ISO. Al implementar y certificar la norma ISO 27000 para el SGSI de la organización, se puede probar de forma independiente que la entidad satisface los requerimientos mínimos necesarios para garantizar que la información esté segura.

La familia ISO 27000 es el desarrollo de normas internacionales con el propósito de robustecer la administración de seguridad informativa en las entidades. El comienzo de su desarrollo se fundamentó en la norma británica BS 7799, que fue establecida en los años 90 y que definía las prácticas adecuadas para proteger la información. Con posterioridad, la Organización Internacional de Normalización adoptó esta norma como ISO/IEC 27001, un estándar que se puede certificar y que determina lo necesario para crear un Sistema de Gestión de Seguridad de la Información (SGSI). A medida que pasó el tiempo, la familia ISO 27000 se expandió para incluir normas relacionadas. Por ejemplo, la ISO/IEC 27002 proporciona una guía sobre controles de seguridad, y existen otras orientadas a áreas específicas como gestión de riesgos, auditoría, continuidad del negocio y seguridad en la nube.

El hecho de que la serie ISO 27000 continúe siendo un marco integral y al día para mantener la confidencialidad, integridad y disponibilidad de

la información en cualquier organización es una evidencia de que están adaptándose a las nuevas amenazas cibernéticas y a los cambios tecnológicos. (Castellano, 2015)

3.1.2 Enfoque de gestión basado en riesgos

La aproximación de la gestión de riesgos es la piedra angular del Sistema de Gestión de Seguridad de la Información (SGSI) de la familia ISO/IEC 27000, en particular de la ISO/IEC 27001. Este enfoque define que la seguridad de la información se debe de gestionar en base al análisis de riesgos que puedan impactar a los activos de la organización, en vez de aplicar controles de forma homogénea o por cumplimiento normativo. Para ello, la organización debe de definir sus activos críticos (información, sistemas, infraestructura tecnológica, procesos, personal, etc.) y determinar las amenazas y vulnerabilidades que pudieran comprometerlos. El propósito es conocer de qué manera estos elementos pueden afectar la confidencialidad, integridad y disponibilidad de la información en el entorno particular de la organización.

Este modelo implica un ciclo continuo de identificación, análisis, valoración y tratamiento del riesgo, ampliamente desarrollado en ISO/IEC 27005. En el análisis se calcula la probabilidad de que ocurra y el daño que podría causar cada riesgo, y en la evaluación se decide si el nivel de riesgo es aceptable o necesita ser tratado. Luego, la organización elige la mejor manera de manejar el riesgo, la cual puede ser mitigarlo con controles técnicos, administrativos o físicos, transferirlo a otros, evitar la actividad que lo causa o aceptarlo formalmente bajo criterios

establecidos. Este enfoque permite asignar prioridades, dirigir las inversiones en seguridad y asegurar que las medidas adoptadas se ajusten a los objetivos estratégicos y de continuidad de negocio, fomentando una cultura organizacional orientada a la prevención y la mejora continua. (hichex, 2024)

3.1.3 Beneficios de la estandarización

La implementación de la norma ISO 27000 posibilita que las organizaciones evidencien que cuentan con los procesos y controles apropiados para garantizar el manejo seguro de la información y los datos con los que trabajan. Asimismo, dispone de un ciclo PDCA que garantiza la mejora incesante en los controles de seguridad implementados en la organización. Asimismo, al implementar la norma ISO 27000 dentro de la organización, se logra un elemento diferenciador significativo que, a un coste reducido, posibilita sobresalir frente a la competencia en el momento de hacer una puja sobre una oferta.

Por lo tanto, la puesta en práctica de las normas ISO 27000 ofrece a las organizaciones múltiples ventajas, entre las que sobresalen: el perfeccionamiento de la seguridad Babilonia, G (2023). Estas pautas nos ofrecen un esquema de referencia para la gestión de la seguridad de los datos; nos fijan requisitos y nos brindan sugerencias. Para aplicar controles de seguridad de la información (SI) que sean eficaces y que resulten óptimos para preservar la confidencialidad, la integridad y la disponibilidad de la información, además señala que los estándares ISO 27000 proponen una perspectiva sistemática; esta optimiza el manejo de

la seguridad de nuestra información, lo que hace posible que las distintas organizaciones reconozcan y manejen correctamente los riesgos de la SI. Esta implementación ofrece ventajas a largo plazo, como es la optimización de la eficiencia y la disminución de los costos, lo que resulta en un aumento de la reputación de las organizaciones y, por ende, una mejora en la confianza de los clientes y de las partes implicadas en la seguridad.

La puesta en marcha de esas normas ha posibilitado que las organizaciones establezcan una relación entre el costo y el beneficio al implementar controles de seguridad de la información y en definir cómo contribuye a estos procedimientos, facilito la identificación de los activos de información y de procesos para una gestión apropiada de los riesgos latentes. Las Normas ISO 27000 constituyen un ciclo de mejora continua en la gestión de la seguridad de la información, lo que permite a las organizaciones mantenerse al día y adaptarse constantemente a los cambios ambientales, ya sean internos o externos. La ventaja es que garantizan el cuidado adecuado de la información. Las normas ISO 27000 ofrecen muchos beneficios en términos de seguridad y gestión procesal para las organizaciones y pueden implementarse en cualquier tipo de entidad, independientemente de su tamaño o naturaleza. (Babilonia, 2023)

3.1.4 Aplicabilidad en distintos tipos de organizaciones

Según Brown, C (2024) las empresas que gestionan información delicada y que están obligadas a cumplir con regulaciones internacionales deben

tener en cuenta las normas ISO 27000. No es obligatorio cumplir con la normativa ISO 27001 o seguir su familia más extensa. No obstante, acatar las regulaciones puede asistir a las compañías en la toma de decisiones complicadas acerca de datos y ciberseguridad. Por ejemplo, los dueños de empresas que pueden no estar familiarizados con las maneras más efectivas de proteger su información podrían restringir las medidas de seguridad óptimas a sus configuraciones particulares. Cumplir con las normas ISO 27000 podría facilitar a los dueños de las compañías la toma de decisiones en cuanto a los servicios de pruebas de penetración y la inversión en hardware.

Para las PYMES, un SGSI basado en ISO/IEC 27001 significa transformar prácticas informales o reactivas en un enfoque estructurado, documentado y en línea con el enfoque de gestión de riesgos. Muchas pymes manejan información sensible (bases de datos de clientes, información financiera, estrategias de negocio, propiedad intelectual, etc.) sin políticas ni controles establecidos, lo que aumenta su vulnerabilidad ante incidentes de seguridad.

La certificación facilita la identificación de vulnerabilidades, la priorización de riesgos y la implementación de controles apropiados, reforzando la confianza de clientes y socios comerciales, mejorando la imagen corporativa y aumentando la competitividad, especialmente al competir en cadenas de suministro que exigen estándares internacionales. Mientras que, en el sector financiero, donde bancos, cooperativas y aseguradoras manejan información altamente sensible y transacciones de alto riesgo, la certificación ISO 27001 se convierte en una necesidad

estratégica y de cumplimiento normativo. En este contexto, la certificación no solo avala el cumplimiento de regulaciones y auditorías externas, sino que también minimiza riesgos relacionados con fraude online, ciberataques, fuga de datos y errores operativos, asegurando la continuidad del servicio y reforzando la confianza del cliente en un sector donde la seguridad y la confianza son esenciales. (Orozco, 2018)

Figura No. #10 Normas ISO

Nota. Fuente: Imagen creada con IA

En el ámbito sanitario es de vital importancia la aplicabilidad de la familia de normas ISO/IEC 27000, por la sensibilidad de la información médica que manejan hospitales, clínicas y laboratorios Disterer, G (2013). Estas instituciones gestionan historiales clínicos, resultados de laboratorio, diagnósticos, información personal, sistemas de atención, los cuales deben ser confidenciales y estar disponibles en todo momento. La certificación ISO 27000 de un SGSI permite definir políticas, procedimientos y controles basados en la gestión de riesgos para proteger la confidencialidad del paciente, evitar accesos no autorizados, prevenir

ciberataques como ransomware y garantizar la continuidad de los servicios de salud. Para las instituciones educativas también aplica la norma en su totalidad, ya que las universidades y centros educativos manejan bases de datos académicas, información personal de estudiantes y profesores, datos de investigación, propiedad intelectual. A través de un SGSI basado en ISO 27000, estas instituciones pueden reconocer amenazas, mejorar sus controles tecnológicos y administrativos, y asegurar la integridad, confidencialidad y disponibilidad de la información en un mundo cada vez más digitalizado, ayudando a proteger a la comunidad educativa y la sostenibilidad institucional.

3.2 ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI)

3.2.1 Principios y estructura del SGSI

La norma ISO 27001 es una norma internacional que garantiza la confidencialidad, la integridad y la seguridad de los datos e información, además de los sistemas que se encargan de su procesamiento. El estándar ISO 27001:2022 para los Sistemas de Gestión de Seguridad de la Información posibilita a las entidades evaluar los riesgos y aplicar las medidas necesarias para aminorarlos o erradicarlos. Este mismo estándar determina lo que se necesita para implementar, conservar y optimizar un Sistema de Gestión de Seguridad de la Información (SG-SI). La meta principal es asistir a las empresas en la conservación de su integridad y confidencialidad, además de garantizar que la información y los activos asociados estén disponibles. La norma ISO 27001:2022 ofrece un marco para la administración de los riesgos relacionados con la seguridad de la

información. Asiste a todas las compañías en la identificación y valoración de los potenciales riesgos para la seguridad de la información. Asimismo, posibilita la aplicación de medidas de seguridad y controles necesarios para una gestión y mitigación efectivas. (Iso Tools, 2024)
Los principios de la ISO/IEC 27001 (2022) se enfocan en administrar la seguridad de la información de manera integral y sirven como guía para establecer el Sistema de Gestión de Seguridad de la Información (SGSI).

Los más importantes son:

- **Confidencialidad**: Garantizar que la información solo esté disponible para individuos autorizados.
- **Integridad:** Mantener la precisión y la integridad de los medios para procesar la información y de la información misma.
- **Disponibilidad:** Asegurarse de que la información esté accesible para los usuarios autorizados cuando se requiera.
- **Perspectiva fundamentada en riesgos:** Reconocer, examinar y abordar los peligros que puedan amenazar la seguridad de la información.
- **Compromiso y liderazgo:** Compromiso de la alta dirección con la protección.
- **Perfeccionamiento constante:** Empleo del ciclo Planificar-Hacer-Verificar-Actuar (PHVA) para perfeccionar el SGSI de manera constante.

3.2.2 Requisitos de la norma

La ISO 27001 (2022) tiene como fundamento garantizar un manejo eficiente y sistemático de la seguridad de la información dentro de las entidades. La protección de la confidencialidad, la integridad y la disponibilidad de los datos como metas primordiales; el enfoque de gestión de riesgos para detectar y atender peligros; el liderazgo y compromiso del nivel superior; así como el perfeccionamiento constante a través del ciclo Planificar-Hacer-Verificar-Actuar (PHVA) son algunos de ellos:

- **Contexto:** Las diversas entidades de sectores variados están potencialmente expuestas a una serie de factores, internos y externos, que pueden representar un peligro para sus métodos de gestión de la información. En este caso, entre otros aspectos, se consideran las características técnicas de los sistemas de información, las expectativas de los interesados, las exigencias legales, las obligaciones contractuales y la información que es especialmente delicada.
- **Alcance del SGSI:** Un Sistema de Gestión de la Seguridad de la Información (SGSI) debe ser diseñado considerando su campo de aplicación, lo cual significa establecer los métodos y las tareas involucradas, así como las clases de información que deben ser monitoreadas y protegidas. Además, es necesario determinar sus límites, ya sean técnicos o no. El SGSI debe incorporar los procesos y sistemas de gestión existentes en la organización para ser más eficaz.

- **Liderazgo:** La administración de la organización desempeña un rol crucial en el establecimiento y la conservación de este sistema de gestión. Los líderes jerárquicos son los encargados de crear una política de seguridad de la información, integrarla en los procesos organizacionales y comunicar sus principios a lo largo de la cadena jerárquica. Además, deben promover este tema constantemente al interior de su organización, lo que incluye ofrecer formación apropiada a su personal.
- **Planificación:** Planear es esencial, especialmente en lo que concierne a la definición de procesos de gestión de oportunidades y riesgos dentro del SGSI. Esto incluye: criterios de riesgo, identificación de amenazas, evaluación de los peligros asociados con cada riesgo, medidas para mitigar y controlar (los planes para tratar los riesgos también están incluidos), así como el establecimiento de objetivos para asegurar la información.
- **Soporte:** La obtención y distribución de todos los recursos requeridos para la implementación eficaz del sistema de gestión se denomina soporte. En este caso, se pueden tener en cuenta la infraestructura (como servidores y software), los recursos humanos (por ejemplo, trabajadores calificados o proveedores externos) y el conocimiento técnico (por ejemplo, acciones de formación o concienciación).
- **Operación:** En esta etapa se realiza la implementación completa de los procesos y planes que se definieron previamente. Es importante señalar que la etapa de explotación debe estar respaldada por un desarrollo meticuloso y bien estructurado de la documentación, capaz de describir detalladamente todas las acciones llevadas a cabo. Solo

de esta manera se podrá, en una etapa posterior, analizar el trabajo hecho y encontrar los problemas y riesgos que necesitan ser solucionados.

- **Evaluación de Resultados:** Como es natural, la etapa de evaluación del rendimiento tiene como objetivo garantizar la calidad del trabajo realizado. Esta fase respalda la eficacia del SGSI y fomenta la implementación de mejoras en el futuro, al tiempo que reduce los problemas encontrados y nutre los procesos de auditoría interna**.**
- **Mejora:** Cualquier disconformidad o inconveniente que se identifique en la etapa de evaluación debe ser abordado rápidamente, ya sea para reducir el daño y las pérdidas potenciales, o para impedir su futura repetición. Cualquier debilidad en la seguridad de la información puede tener grandes repercusiones legales y reputacionales, las cuales pueden afectar el marco del RGPD, que determina las multas según el volumen de ventas anuales de una entidad.

3.2.3 Política de seguridad de la información

Una política de seguridad de la información, frecuentemente llamada infosec policy, es un grupo de reglas que se han creado con atención para controlar el acceso, la utilización y la conservación de información crucial para la empresa. 27001:2022, ISO/IEC (2022). Estas políticas establecen un robusto conjunto de procedimientos y herramientas para asegurar una protección total contra el acceso no autorizado, protegiendo de esta manera los activos de información confidencial de una entidad.

Las políticas de seguridad informática se rigen por una estructura y un formato estándar son:

- Una declaración que detalle las clases de actividades protegidas por la póliza
- Una declaración de compromiso emitida por la gerencia, que muestra que se han destinado los recursos necesarios para garantizar el sostenido cumplimiento de la política.
- Un conjunto de obligaciones particulares para los trabajadores en cuanto a la utilización y salvaguarda de la información de la empresa. Es importante señalar que la mayor parte de las organizaciones deberían tener un delegado de protección de datos, cuyo rol es sostener e implementar estas modificaciones y proponer soluciones a los inconvenientes relacionados con la protección de datos.

Los principios, los requerimientos y las recomendaciones relacionados con las políticas de seguridad de la información se especifican en el anexo A5. Su propósito es describir las políticas de seguridad de la información junto con los requisitos, ideas y recomendaciones que estén vinculados a estas. Conlleva la elaboración, implementación y valoración de políticas. El Anexo A.5 no solamente proporciona orientación sobre cómo aplicar las políticas de seguridad de la información, sino que también aborda la forma en que se comunican estas políticas y cómo se relacionan con otras políticas corporativas. El establecimiento de políticas para la protección de la información es un proceso continuo. Es extremadamente importante renovar las políticas de seguridad de la información de forma periódica, conforme surgen nuevas tecnologías, se

desarrollan amenazas y las operaciones comerciales cambian. También el gobierno impone de manera continua nuevos requisitos que las organizaciones deben cumplir para protegerse frente a la pérdida de datos, y no hacerlo puede conllevar sanciones importantes.

Una política de seguridad de la información asiste a su entidad en la clasificación de sus datos privados. Esto depende parcialmente de la regulación vigente, pero también tiene que tener en cuenta cualquier elemento externo que pueda influir en cómo se percibe el riesgo, como la competencia sectorial o las alteraciones geopolíticas relacionadas con el clima. La categorización de la información puede oscilar entre baja (confidencial), media (secreta), alta (alto secreto) y hasta alta plus o superior. Los términos exactos empleados pueden tener ligeras variaciones dependiendo de la agencia o compañía que las elabore. No obstante, es necesario que todas las organizaciones tengan un buen entendimiento de la norma ISO 27001 para que los que la ponen en práctica puedan entender el significado de cada control. Esto se vuelve más importante cuando se sabe que entre el 70 % y el 90 % de los ataques cibernéticos involucran algún tipo de ingeniería social. (DataGuard, 2026)

3.2.4 Liderazgo y compromiso organizacional

La ISO 27001 (anexo 5.1) requiere que la alta dirección demuestre liderazgo y compromiso con el SGSI. Esto implica que la dirección no puede delegar por completo la seguridad de la información al departamento de TI o a un equipo técnico, sino que debe participar en la

gobernanza del sistema. La alta gerencia debe hacer que la política y los objetivos de seguridad de la información sean consistentes con la dirección estratégica de la empresa; es decir, que la seguridad sirva para alcanzar los objetivos generales de la organización y no sea una función aislada. Además, el compromiso organizacional significa que la alta dirección destine los recursos humanos, financieros y tecnológicos para establecer y mantener el SGSI. Esto implica disponer de personal capacitado, tecnología apropiada y recursos presupuestarios para que el SGSI funcione. Este respaldo debe estar explícito y registrado como evidencia para auditorías y para demostrar que la seguridad es una prioridad corporativa. (Holloway, 2025).

Otra área fundamental del liderazgo es comunicar y defender la seguridad de la información en toda la organización. Los líderes deben explicar de forma transparente y repetida por qué la seguridad es importante, cómo apoya al negocio y cómo todos contribuyen a ella. Esta comunicación crea una cultura organizacional en donde la seguridad es apreciada por todos. Finalmente, el liderazgo y el compromiso se demuestran con acciones tales como participar en las revisiones del SGSI, apoyar las mejoras continuas y garantizar que el SGSI logre los objetivos establecidos. La alta gerencia también debe apoyar y desarrollar a otros roles de liderazgo en la organización para que también sean líderes en sus propias áreas. Estas acciones no solo refuerzan la seguridad, sino que demuestran que el sistema se administra de manera estratégica y continua, no solo por cumplimiento. (27001, 2022)

Según Holloway, D (2025) si los líderes no están activamente involucrados, como al no participar en las revisiones de la gestión o al no poder mostrarle a un auditor externo que hay un representante del liderazgo que se toma la auditoría en serio, es muy probable que la organización fracase. Los auditores afirman que el espíritu de ISO 27001 se origina desde arriba y si no lo ven, es probable que durante la auditoría examinen con mayor profundidad y escepticismo. La administración de la seguridad de la información es una filosofía esencial para el negocio, como se ha mencionado en numerosas ocasiones. Para que sea efectiva en la práctica, tiene que estar alineada con los procesos y metas comerciales de una organización. Si no hay respaldo de los líderes, o si se tiene que completar 25 tareas antes de realizar el trabajo que realmente se desea hacer, será complicado iniciar el camino hacia la ISO 27001.

3.3 ISO/IEC 27002: Controles de seguridad de la información

3.3.1 Estructura y dominios de control

La norma ISO 27002 es un estándar global que ofrece lineamientos para la puesta en práctica de controles de seguridad de la información. La norma ISO 27002, a diferencia de la norma ISO 27001, que se enfoca en los requerimientos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), funciona como un suplemento a la primera. Un estándar que proporciona un grupo minucioso de recomendaciones y prácticas óptimas para aplicar los controles de seguridad que se encuentran en el Anexo A de la norma ISO 27001. Es una norma fundamental como recurso exhaustivo para las entidades que desean obtener orientación acerca de las prácticas óptimas para asegurar la

información**.** La norma ISO 27002 se puede aplicar a cualquier organización, sin importar su tipo, tamaño o sector. Su objetivo es asistir a las organizaciones en la elección y aplicación de los controles de seguridad apropiados, conforme a los riesgos que afrontan. (Suits, 2025)

La forma en que se organiza la ISO/IEC 27002 según Holloway, D (2025) Su diseño apoya la orientación para establecer controles de seguridad de la información. En su estructura, la norma inicia con las secciones preliminares que establecen el propósito y alcance, las referencias normativas y los términos y definiciones, proporcionando la base conceptual para su aplicación. El cuerpo de la norma lo constituye la cláusula 4, donde se proporciona un listado de 93 controles de seguridad agrupados en cuatro bloques: organizacionales, de personal, físicas y tecnológicas.

Esta nueva estructura sustituye el antiguo modelo de 14 dominios por uno más ágil y alineado con las prácticas actuales de gestión de riesgos. Cada control en estos bloques sigue la misma estructura: nombre, propósito, directrices de implementación y, en algunos casos, notas adicionales. Además, la norma ofrece un esquema de atributos para clasificar los controles por tipo, las propiedades de seguridad que abordan (confidencialidad, integridad y disponibilidad), su asociación con conceptos de ciberseguridad y las capacidades operativas que implican, para alinearlos con ISO/IEC 27001 y otras normas de la industria. Finalmente, se adjuntan anexos informativos para relacionar con versiones anteriores y con la norma de requisitos, permitiendo a las

organizaciones incorporar estos controles de forma integrada en su Sistema de Gestión de Seguridad de la Información (SGSI).

Figura No.#11 Controles de la seguridad de la información

Nota. Fuente: Imagen creada con IA

3.3.2 Controles organizativos, humanos y tecnológicos

La revisión de 2022 es un avance importante, pues reestructura los controles de 14 categorías (114 en la versión de 2013) a un esquema simplificado con solo 4 temas y 93 controles. Esta reestructuración disminuye la redundancia, mejora la usabilidad y trata los peligros emergentes de ciberseguridad, como lo son: la seguridad de la nube, las arquitecturas de confianza nula, los riesgos de seguridad en el suministro, la seguridad del trabajo a distancia, la inteligencia sobre amenazas y la seguridad de la base de datos CMDB (Gestión de Configuración). Los cuatro controles son:

- **Controles Organizacionales/ 37 controles:** Esta área de control establece la forma en que se gestionará la seguridad de la información dentro de la organización. Implica la identificación de riesgos, la formulación de políticas, la asignación de roles y responsabilidades, la gestión adecuada y clasificación de la información y la relación con proveedores y terceros. Además, abarca la planificación de continuidad de negocio y la gestión de incidentes de seguridad. En definitiva, estos controles aseguran que la seguridad esté integrada en la estructura estratégica y de gestión de la organización, proporcionando dirección, supervisión y mejora continua al Sistema de Gestión de Seguridad de la Información (SGSI).

- **Controles de personas /8 controles:** Hacen énfasis en el factor humano como un elemento de seguridad para proteger la información. Entre ellas se encuentran la firma de acuerdos de confidencialidad, la verificación antes de la contratación, la definición clara de las responsabilidades de seguridad, la capacitación y concienciación continuas, y los procedimientos de finalización de la relación laboral. Estos controles buscan reducir los riesgos asociados con errores humanos, negligencia o actos maliciosos, fortaleciendo la cultura de seguridad de la organización.

- **Controles físicos/14 controles:** Este control resguarda las instalaciones, equipos físicos y la infraestructura en donde se procesa o almacena información. Entre ellas se encuentran el control de acceso a edificios y zonas restringidas, sistemas de vigilancia, protección contra amenazas ambientales (incendios, inundaciones),

seguridad del cableado y políticas de escritorio y pantalla limpia. Busca prevenir accesos no autorizados, daños o interrupciones a la información o sistemas críticos.

- **Controles tecnológicos /34 controles:** Reúnen las acciones técnicas para proteger los sistemas de información y las redes. Incluyen defensa contra malware, control de accesos lógicos, autenticación multifactor, gestión de identidades, registro y auditoría de eventos, gestión de vulnerabilidades, cifrado de datos y copias de seguridad. Para mantener la confidencialidad, integridad y disponibilidad de la información en los mundos digitales cada vez más complejos, estos controles son necesarios.

3.3.3 Selección e implementación de controles

Afirma Pescadilla,J (2025) que dentro de la ISO/IEC 27002, la elección e implantación de controles es el proceso por el cual una organización define qué medidas de seguridad debe implementar para proteger su información de los riesgos identificados. La norma no exige controles obligatorios, sino que ofrece un listado de 93 controles agrupados en cuatro categorías (organizacionales, de personas, físicas y tecnológicas) antes mencionados para abordar los riesgos identificados.

La elección de controles se hace una vez analizados los riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. En esta fase, la organización determina qué controles son apropiados para disminuir el riesgo a un nivel aceptable. La elección dependerá del entorno organizacional, los requisitos legales,

contractuales, normativos y la viabilidad técnica y económica de su implementación. No todos los controles serán necesarios; la necesidad de los mismos dependerá del resultado del tratamiento de riesgos. Implementar los controles significa poner en práctica las medidas seleccionadas. Esto implica crear o modificar políticas internas, configurar soluciones tecnológicas como sistemas de autenticación o cifrado, capacitar al personal, mejorar la seguridad física, establecer procedimientos operativos. Debe documentarse y ajustarse al SGSI.

Una vez implementados, estos controles deben ser monitoreados y analizados de forma continua para verificar su efectividad y permitir una optimización continua. De esta manera, la selección e implementación de controles se convierte en un proceso dinámico, en línea con la gestión de riesgos y el panorama de amenazas en constante cambio. (Romo & Valarezo, 2015).

3.3.4 Adaptación de controles a microempresas

La flexibilidad es uno de los beneficios más significativos de la ISO 27002. Está concebida para que sea utilizada por cualquier tipo de empresa, desde un startup hasta una multinacional. No obstante, su aplicación cambia dependiendo del contexto.

Ajustar los controles de la ISO/IEC 27002 a una microempresa es, en esencia, usar el sentido común: tomar esas buenas prácticas de seguridad y adaptarlas al día a día de una empresa pequeña, con pocos empleados y pocos recursos. En ese sentido, querer aplicar los 93 controles de la

norma sería como querer vestir a un equipo de fútbol sala con el uniforme de una selección absoluta: no tiene sentido. Lo mejor es hacer un ejercicio sencillo de evaluación para detectar qué riesgos realmente pueden causar daño (pérdida de información, ataque ransomware que te deje fuera de juego, robo de contraseñas, intrusión donde no debes). Con eso en mente, lo que sigue es seleccionar un par de controles, pero los críticos: los que protegen la información crítica para el negocio (datos de clientes, cuentas, contratos etc.) sin tener que montar una estructura de oficina que termine paralizando el trabajo en vez de agilizarlo.

En la práctica, esto significa apostar por acciones simples, fáciles de mantener y que no cuesten un ojo de la cara, pero que prevengan los problemas serios. Hablamos de cosas como tener unas normas de uso de los equipos, contraseñas fuertes y doble autenticación donde se pueda, copias de seguridad automáticas para no tener que acordarse cuando ya es tarde, mantener los programas y sistemas actualizados, ayudar al equipo a desarrollar buenos hábitos digitales sin manuales de mil páginas. Y ojo, tampoco hace falta descuidar lo físico: desde que no todo el mundo pueda acceder al ordenador donde se guardan los datos confidenciales hasta los archivadores donde se guardan los contratos. Y así, con estos pasos, la microempresa va haciéndose segura poco a poco, sin enloquecer ni gastar de más, y en cumplimiento de la norma sin que esto se convierta en un problema más. (Rueda, 2026).

3.4 ISO/IEC 27005: Gestión del riesgo de seguridad de la información

3.4.1 Proceso de gestión de riesgos

Para Whiting, J (2025) la norma ISO 27005 es una regulación global que establece los métodos para llevar a cabo una evaluación de riesgos de seguridad informática en concordancia con la norma ISO 27001. Como se indicó antes, las evaluaciones de riesgos constituyen un elemento clave en la iniciativa de cumplimiento de la norma ISO 27001 de una entidad. La gestión de riesgos de seguridad de la información (ISRM, por sus siglas en inglés) es el procedimiento para detectar y reducir los riesgos asociados con el uso de las tecnologías informáticas. Supone la identificación, valoración y reducción de los peligros que amenazan la privacidad, el prestigio y la disponibilidad de los bienes de una entidad. El resultado final consiste en administrar los riesgos de acuerdo con la tolerancia al riesgo general de la organización. Las compañías no se proponen eliminar todos los riesgos; en cambio, necesitan trabajar para establecer y sostener un nivel de riesgo apropiado para su negocio.

Aunque las prácticas de gestión de riesgos más efectivas han progresado a lo largo del tiempo para atender las necesidades individuales en distintos sectores e industrias a través de la aplicación de diversos métodos, establecer procesos coherentes dentro de un marco general puede contribuir a asegurar que los riesgos se manejen con fiabilidad, exactitud y claridad en la organización. Estos marcos estandarizados están definidos en la norma ISO 27005. La norma ISO 27005 establece las prácticas óptimas para gestionar riesgos, orientadas sobre todo a la

administración de los riesgos de seguridad de la información y poniendo énfasis en la observancia de los estándares de un Sistema de Gestión de Seguridad de la Información (SGSI), tal como lo estipula la norma ISO/IEC 27001.

El proceso se inicia con la contextualización, definiendo el alcance, los criterios de evaluación y el apetito al riesgo de la organización, para que la gestión se ajuste a la estrategia de negocio. Luego, se realiza la identificación de riesgos, identificando activos, amenazas y vulnerabilidades, para luego pasar al análisis de riesgos, el cual define la magnitud de cada riesgo en términos de sus consecuencias y probabilidad. Luego, la evaluación de riesgos compara estos resultados con los criterios establecidos para priorizar los riesgos que necesitan atención inmediata. Finalmente, el tratamiento de riesgos aplica controles (como los del Anexo A de ISO 27001) para alterar, retener, evitar o transferir los riesgos inaceptables, documentando la aceptación de los riesgos residuales.

Es importante saber que este flujo no finaliza, sino que se apoya en un proceso de seguimiento y revisión continua que permite su adaptación a los cambios del entorno y la mejora continua de la postura de seguridad de la información. (Whiting, 2025)

3.4.2 Identificación, análisis y tratamiento del riesgo

Según Bonnie, E (2026) pensar en riesgos es, básicamente, sentarse a responder a la pregunta más incómoda: ¿Qué es lo que puede fallar? Esta fase es la base del proceso entero, ya que no podemos protegernos de lo

que no sabemos que existe. Es hacer un inventario honesto de todo lo que podría dañar nuestra información. Así que lo primero es saber qué tenemos (nuestros activos), desde lo más valioso, una base de datos de clientes, hasta las herramientas que lo sostienen, un servidor o una aplicación. Luego, hay que pensar en quién o qué les puede hacer daño (las amenazas). Puede ser un hacker, un error sin maldad de un compañero o incluso una inundación. Pero no solo hay que mirar fuera, sino también mirarse al ombligo y reconocer las vulnerabilidades, las pequeñas (o grandes) debilidades que tenemos y que facilitarían el desastre. Claro que también hay que tener en cuenta las medidas de seguridad que ya tenemos por si nos sirven de paraguas. En fin, es un ejercicio de sinceridad el dar respuesta a tres preguntas claves: ¿Qué puede fallar?, ¿cuáles son nuestros puntos débiles? y ¿de cuánta gravedad sería el golpe si esto llegara a ocurrir?

Una vez que hemos identificado todo lo que podría salir mal, es el momento de ponerle números y contexto a esos miedos: esto es el análisis de riesgos. La fase anterior era la del ¿qué puede pasar? y ésta es la del ¿y qué tan grave es? Se trata de poner bajo la lupa cada riesgo para entender su verdadera dimensión. Para ello, valoramos dos factores clave: la probabilidad de que ocurra (¿es algo remoto o puede pasar mañana?) y el impacto que tendría en el negocio si finalmente se materializa (¿sería un disgusto menor o un golpe del que sea difícil recuperarse?). Al sumar ambos factores obtenemos el nivel de riesgo, y así podemos separar los problemas que son graves de los que no merecen desvelos. En el fondo, esta etapa nos ayuda a pasar de la intuición a la

claridad, nos da una visión objetiva para luego decidir qué incendios apagar primero.

Disterer, G (2013) menciona que, aunque la norma ISO 27005:2022 no establece opciones para el tratamiento de riesgos, la versión previa del año 2018 sí lo hacía y proporcionaba cuatro alternativas:

- Mitigación de riesgos: Implementar controles de seguridad de la información con el objetivo de disminuir la posibilidad o el efecto del riesgo.
- Evitar el riesgo: prevenir las situaciones en las que podría ocurrir para evitar el riesgo.
- Transferencia de riesgo: Consiste en compartir o traspasar el riesgo a un tercero, por ejemplo, al adquirir un seguro.
- Aceptación del riesgo: aceptar el riesgo porque el daño potencial es menor que los costos asociados.

Por otro lado, la norma ISO 27005:2022 resalta que los encargados de los riesgos son responsables de la elaboración y aprobación del plan de tratamiento de riesgos, además de aceptar cualquier riesgo residual. Los encargados de los riesgos tienen que ser participantes en la determinación de las medidas de control que se usarán para administrar los riesgos. Asimismo, la actualización de 2022, al incorporar la Declaración de Aplicabilidad, establece una relación más cercana entre las normas ISO/IEC 27005 y las normas ISO/IEC 27001 e ISO/IEC 27002. En el proceso de tratamiento de riesgos, todos los controles de seguridad que

se empleen para modificar el riesgo deben contrastarse con aquellos que aparecen en la lista del Anexo A de la norma ISO 27001.

Figura No. #12 ISO/Gestión de riesgos de seguridad informática

Nota. Fuente: Imagen creada con IA

3.4.3 Aceptación y monitoreo del riesgo

El monitoreo del riesgo, por último y no menos importante, no es una tarea que se realiza una sola vez, se guarda en un archivo y se olvida; es más bien un compromiso continuo que requiere una constante supervisión, ya que los riesgos son como organismos vivos: pueden mutar de forma repentina y sin previo aviso. Lo que ayer era un riesgo menor, hoy puede convertirse en una amenaza crítica por la aparición de una nueva vulnerabilidad o un cambio en el negocio. Este seguimiento es la única forma de detectar a tiempo cualquier novedad, como la incorporación de nuevos activos tecnológicos, cambios en el valor de la información que manejamos (quizás ahora es más sensible o estratégica), la irrupción de amenazas inesperadas como un nuevo tipo de malware o

un cambio en la legislación o los incidentes de seguridad que van ocurriendo y que nos dan pistas sobre dónde estamos fallando. Siempre que estemos alerta, podemos ir cambiando el plan de tratamiento a medida que pasen las cosas, a medida que la realidad vaya cambiando, y de paso comprobar si las medidas que tomamos en su día siguen funcionando o se han quedado obsoletas. Después de todo, un plan que no se revisa es como un mapa que no se actualiza: acaba llevándote por caminos que ya no existen. (DataGuard, 2026).

3.4.4 Relación con ISO 27001

La ISO 27005 fue creada con el propósito de respaldar y complementar la puesta en marcha de un sistema de gestión de seguridad de la información (SGSI) fundamentado en la norma ISO 27001. La ISO 27001 define los requisitos para la creación, puesta en marcha, conservación y optimización de un SGSI; por su parte, la ISO 27005 ofrece pautas concretas para gestionar los riesgos relacionados con la seguridad de la información. Este último es un elemento fundamental del sistema de gestión de seguridad de la información.

La armonía entre las dos normas se consigue por medio de diferentes elementos: para empezar, la ISO 27005 contribuye a que las entidades acaten con el requerimiento de la cláusula 6.1.2 de la ISO 27001, que manda identificar, examinar y evaluar riesgos para establecer los controles que se necesitan. Asimismo, la ISO 27005 proporciona una perspectiva detallada y estructurada para el procedimiento de gestión de riesgos, lo cual simplifica la elección y aplicación de controles de

seguridad (Anexo A de la ISO 27001). Las dos normas tienen un enfoque que se basa en el contexto organizacional, la mejora continua y la implicación de los altos mandos; esto garantiza que la gestión de riesgos esté incorporada en la estrategia general de seguridad de la organización. En síntesis, la ISO 27005 funciona como una guía práctica para poner en marcha el componente de gestión de riesgos en un SGSI que cumple con la norma ISO 27001, garantizando así una protección de la información coherente y eficaz. (Guarin, 2025)

3.5 Otras normas complementarias de la familia ISO/IEC 27000

3.5.1 ISO/IEC 27003, 27004 y 27017

La ISO 27003, también llamada ISO/IEC 27003, es un documento que orienta y asiste a las organizaciones para que puedan poner en marcha de forma eficaz y exitosa un Sistema de Gestión de Seguridad de la Información (SGSI). Esta regulación es más que simples instrucciones; se presenta como un mapa minucioso que guía a las organizaciones en la defensa de sus activos informativos. La finalidad central es ofrecer un manual pormenorizado para la puesta en marcha de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001, posibilitando que el procedimiento para diseñar y poner en práctica un SGSI sea más sencillo y claro.

La norma ISO 27003 es una herramienta esencial para las compañías que desean robustecer sus sistemas de seguridad, en el contexto de la administración de la seguridad de la información. Esta norma es un componente de la serie ISO 27000, que se ocupa de los sistemas de

gestión de seguridad de la información (SGSI), que es un elemento esencial para entender y llevar a cabo de manera eficaz las directrices establecidas en ISO 27001. La norma ISO/IEC 27003:2017, que fue publicada por primera vez el 1 de febrero del año 2010 y luego actualizada el 12 de abril del año 2017, es un documento general que puede ser utilizado por cualquier organización, sin importar su tamaño o sector. Esto destaca su adaptabilidad y pertinencia en un entorno empresarial variado. Es importante subrayar que, a pesar de que la norma no es certificable en sí misma, juega un papel fundamental en la certificación de un SGSI conforme a la ISO/IEC 27001. (/IEC, 2017)

La norma ISO27004 ofrece la posibilidad de aplicar diferentes prácticas óptimas para medir los resultados de un Sistema de Gestión de la Seguridad de la Información (SGSI) en ISO 27001. Este estándar determina la manera de estructurar el sistema de medición, los parámetros que se deben medir, así como cuándo y cómo hacerlo. Asimismo, contribuye a las compañías al definir metas vinculadas con el desempeño y los estándares de éxito. Los métodos necesarios que propone la norma ISO 27004 estarán determinados por el tamaño y la complejidad de la organización, así como por la relación entre el costo y el beneficio, y el grado de integración de la seguridad de la información en los procesos que realice esta. Esta norma detalla cómo se deben establecer estos métodos y cómo los datos obtenidos en el SGSI tienen que integrarse y documentarse. (ISOTools, 2026)

La norma ISO 27017 propone un grupo de controles adicionales a la ISO 27002 que se enfocan directamente en los servicios brindados en la nube

y sus proveedores, sugiriendo controles particulares relacionados con la administración y el suministro de servicios seguros en la nube. Tengamos presente que la ISO 27001 establece un grupo de 114 controles de seguridad, distribuidos en 14 dominios, que se utilizan dentro del ámbito que cada empresa determine al implementar su Sistema de Gestión de Seguridad de la Información.

Se establecen pautas para la identificación y mitigación de riesgos particulares relacionados con los entornos en la nube, de modo que puedan ser abordados correctamente. La implementación de la ISO 27017, además, exige que se tenga antes la norma ISO 27001 y brinda a los proveedores de servicios en la nube una imagen coherente y comprometida con la administración de seguridad ante sus clientes. El propósito primordial es administrar de manera segura los datos guardados por los clientes, fortaleciendo así la confianza en el manejo y procesamiento de la información. (Domingo, 2024)

3.5.2 Protección de datos y privacidad (ISO/IEC 27001)

La ISO 27001 es como el esqueleto de la seguridad en una empresa, y la **ISO/IEC 27701** viene a ser esa capa extra que se preocupa específicamente por tus datos personales. Es una norma internacional pensada para ayudar a las organizaciones a gestionar la privacidad con el mismo rigor con el que cuidan su seguridad. Su objetivo es que la empresa tenga claro en todo momento qué datos tuyos tiene, para qué los usa, cómo los guarda y con quién los comparte, algo fundamental en un mundo donde regulaciones como el GDPR exigen cada vez más

transparencia. Define quién es responsable de cada cosa dentro del proceso y establece controles específicos para que tanto quienes deciden cómo se usan los datos como quienes los procesan lo hagan con todas las garantías. Al final, lo que busca esta norma es que la organización no solo cumpla la ley, sino que además genere confianza. Porque cuando una empresa se toma en serio tu privacidad, te lo demuestra con hechos, no solo con palabras.

3.5.3 Seguridad en la nube y servicios digitales

En la actualidad, las organizaciones almacenan y ejecutan grandes volúmenes de datos y software en la nube. Todo esto debe estar protegido frente a ataques externos y amenazas internas. Holdsworth, J; Kosinski, M (2025). No existe una única cosa que pueda ser denominada "la nube". El término hace referencia a las arquitecturas de computación en la nube que fusionan los recursos de diversos entornos informáticos para guardar información y alojar aplicaciones de software, bases de datos y otros servicios. Los cuatro tipos fundamentales de entornos en la nube son los siguientes: nubes públicas, que pueden ser utilizadas por cualquiera; nubes privadas, diseñadas específicamente para empresas, grupos u organizaciones concretas; nubes comunitarias, compartidas por múltiples compañías vinculadas entre sí, organismos gubernamentales u otras entidades; y nubes híbridas, que integran dos o más de las características mencionadas. Como los entornos en la nube son "distribuidos" (es decir, sus elementos se distribuyen, pero están integrados entre sí), requieren métodos específicos para garantizar su seguridad.

3.5.4 Integración con otros sistemas de gestión (ISO 9001, ISO 22301)

La integración de la ISO 27001 con otras normas como la ISO 9001 o la ISO 22301 no es solo una cuestión técnica, es sobre todo una decisión práctica. Muchas organizaciones encuentran que el manejo independiente de la calidad, la seguridad de la información y la continuidad del negocio genera duplicidades, esfuerzos dispersos y con frecuencia cierta confusión interna. Lo bueno es que estas normas comparten una estructura base, la conocida High Level Structure, lo cual hace que su integración sea mucho más sencilla de lo que parece. En vez de tener sistemas paralelos que no se comunican entre sí, se puede crear un único Sistema Integrado de Gestión donde las políticas, los procedimientos y las auditorías fluyan de forma coherente.

Cada una de estas normas tiene su valor y se complementan entre sí. La norma ISO 9001 pone el acento en la calidad y en la satisfacción del cliente. Lo que hace la ISO 27001 es proteger la información y evitar que los riesgos de seguridad nos pongan en apuros. La ISO 22301 garantiza que la organización no se paralice ante cualquier imprevisto grave. La integración de estas tres perspectivas permite abordar de manera conjunta los riesgos operativos, tecnológicos o de crisis desde una visión más completa y menos fragmentada. Con esto se consigue algo que va más allá del ahorro de recursos o de la simplificación de procesos. Se gana en resiliencia, en capacidad de reacción ante lo inesperado y, sobre todo, en la confianza de los que confían en la organización: clientes, socios y otras partes interesadas. Finalmente, la integración de estos sistemas no solo

es una buena decisión administrativa, sino también una forma de construir una cultura organizacional más sólida, coherente y orientada a mejorar cada día. (ISO, 2015).

CAPÍTULO IV

IMPLEMENTACION DE UNA CULTURA DE CIBERSEGURIDAD BASADA EN ISO/IEC 27000

4.1 Diagnóstico del nivel de madurez en ciberseguridad

La implementación de una cultura organizacional de ciberseguridad requiere, como punto de partida, comprender el estado actual de la organización respecto a la gestión de riesgos digitales. Este proceso de diagnóstico permite identificar fortalezas, debilidades y áreas de mejora en relación con las políticas, procesos y controles existentes. En el marco de los sistemas de gestión de seguridad de la información, esta etapa inicial es fundamental para establecer una base objetiva sobre la cual diseñar estrategias de mejora y adaptación.

La familia de normas desarrolladas por la International Organization for Standardization proporciona directrices claras para evaluar la madurez de los sistemas de seguridad de la información dentro de las organizaciones. En particular, la norma ISO/IEC 27001 establece que antes de implementar o mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), es necesario identificar el contexto organizacional, las partes interesadas y los riesgos asociados al manejo de la información.

En este sentido, el diagnóstico del nivel de madurez permite analizar no solo los aspectos tecnológicos de la seguridad, sino también los factores organizacionales, humanos y estratégicos que influyen en la gestión de la información. A través de herramientas como evaluaciones iniciales,

análisis de brechas y priorización de riesgos, las organizaciones pueden establecer un plan de acción alineado con estándares internacionales y adaptado a su realidad operativa.

4.1.1 Evaluación inicial de la organización

La evaluación inicial constituye el primer paso para comprender el estado real de la seguridad de la información dentro de una organización. Este proceso implica revisar las prácticas actuales relacionadas con el manejo de datos, la infraestructura tecnológica, las políticas internas y el nivel de conocimiento del personal respecto a los riesgos digitales. De acuerdo con la norma ISO/IEC 27001, el análisis del contexto organizacional permite identificar factores internos y externos que influyen en la seguridad de la información (International Organization for Standarization, 2022).

Durante esta fase también se analizan los recursos tecnológicos disponibles, tales como servidores, redes, sistemas de almacenamiento y herramientas de seguridad existentes. El National Institute of Standards and Technology (2018) destaca que comprender el entorno tecnológico es esencial para establecer controles adecuados y evitar vulnerabilidades derivadas de configuraciones inadecuadas o sistemas obsoletos.

Además, la evaluación inicial incluye el análisis de la cultura organizacional y del nivel de concienciación del personal en materia de ciberseguridad. Von Solms y Van Niekerk (2013) sostienen que muchas brechas de seguridad no se originan exclusivamente en fallas

tecnológicas, sino en comportamientos humanos inseguros o en la falta de políticas organizacionales claras. Por ello, una evaluación integral debe considerar tanto los aspectos técnicos como los organizacionales.

4.1.2 Análisis de brechas (GAP Analysis)

El análisis de brechas, conocido comúnmente como GAP Analysis, es una herramienta utilizada para comparar el estado actual de la organización con los requisitos establecidos por un estándar o marco de referencia. En el contexto de la ciberseguridad, este análisis permite identificar diferencias entre las prácticas existentes y los controles recomendados por normas internacionales como ISO/IEC 27001.

Según la International Organization for Standardization (2022), el análisis de brechas facilita la identificación de áreas donde los controles de seguridad no están implementados o son insuficientes. Esta comparación permite establecer prioridades de mejora y diseñar un plan estructurado para alcanzar los niveles de seguridad requeridos por el estándar.

Adicionalmente, el GAP Analysis contribuye a optimizar el uso de recursos organizacionales, ya que permite concentrar esfuerzos en los controles que realmente generan mayor impacto en la reducción del riesgo. El ISACA (2019) destaca que esta metodología es ampliamente utilizada en procesos de auditoría y certificación debido a su capacidad para proporcionar una visión clara del nivel de cumplimiento normativo de la organización.

Figura No. #13 Análisis de Brechas (GAP Analysis)

Nota. Fuente. Imagen creada con IA.

4.1.3 Identificación de activos críticos

La identificación de activos críticos es un paso esencial dentro del proceso de gestión de riesgos en ciberseguridad. Los activos de información incluyen no solo datos digitales, sino también sistemas informáticos, infraestructura tecnológica, procesos organizacionales y conocimiento estratégico. La correcta identificación de estos elementos permite comprender qué recursos deben recibir mayor nivel de protección.

El National Institute of Standards and Technology (2018) establece que la gestión efectiva de la seguridad comienza con la identificación de activos que son fundamentales para el funcionamiento de la

organización. Esto incluye bases de datos de clientes, sistemas financieros, plataformas digitales y documentos estratégicos que podrían generar impactos significativos en caso de ser comprometidos.

En el caso de las microempresas, la identificación de activos críticos suele ser un proceso simplificado, pero igualmente relevante. A menudo, la información financiera, las bases de datos de clientes y los sistemas de facturación representan activos clave cuya pérdida o exposición podría afectar gravemente la continuidad del negocio. Por esta razón, el inventario de activos constituye una herramienta fundamental para orientar las estrategias de protección y asignación de recursos.

4.1.4 Priorización de riesgos

La priorización de riesgos permite determinar cuáles amenazas requieren atención inmediata dentro del proceso de gestión de la seguridad de la información. Dado que las organizaciones poseen recursos limitados, resulta necesario establecer criterios que permitan clasificar los riesgos según su probabilidad de ocurrencia y el impacto potencial que podrían generar.

El enfoque basado en riesgos promovido por la norma ISO/IEC 27001 de la International Organization for Standardization establece que los controles de seguridad deben seleccionarse de acuerdo con la criticidad de los riesgos identificados. Este enfoque permite adaptar el sistema de gestión de seguridad a las características específicas de cada organización.

Asimismo, el National Institute of Standards and Technology (2018) señala que la priorización de riesgos facilita la toma de decisiones estratégicas al proporcionar una base objetiva para asignar recursos y establecer planes de mitigación. En consecuencia, este proceso se convierte en un elemento clave para garantizar que las medidas de seguridad implementadas generen el mayor beneficio posible en términos de reducción del riesgo organizacional.

4.2 Diseño de un modelo de ciberseguridad organizacional

Una vez realizado el diagnóstico del nivel de madurez en ciberseguridad, el siguiente paso consiste en diseñar un modelo organizacional que permita gestionar de manera estructurada la protección de la información. Este modelo debe integrarse con la estrategia general de la organización, considerando sus objetivos, recursos disponibles y nivel de riesgo aceptable. El diseño de un modelo de ciberseguridad no implica únicamente la implementación de herramientas tecnológicas, sino la definición de estructuras de gobernanza, responsabilidades y procedimientos que orienten el comportamiento organizacional.

La familia de normas desarrollada por la International Organization for Standardization establece que un Sistema de Gestión de Seguridad de la Información (SGSI) debe construirse sobre un enfoque basado en riesgos y mejora continua. En este sentido, el modelo organizacional debe contemplar la planificación de controles, la asignación de responsabilidades y la evaluación periódica de su efectividad (International Organization for Standarization, 2022).

4.2.1 Definición de roles y responsabilidades

La definición clara de roles y responsabilidades es un elemento fundamental dentro de cualquier sistema de gestión de seguridad de la información. Sin una distribución adecuada de funciones, las iniciativas de ciberseguridad pueden volverse fragmentadas o carecer de coordinación, lo que incrementa el riesgo de incidentes y debilita la efectividad de los controles implementados.

La norma ISO/IEC 27001 de la International Organization for Standardization (2022) establece que la dirección de la organización debe asignar responsabilidades específicas relacionadas con la seguridad de la información y garantizar que estas sean comunicadas adecuadamente dentro de la estructura organizacional. Este principio busca asegurar que cada miembro de la organización comprenda su papel en la protección de los activos de información.

En el caso de microempresas, la estructura organizacional suele ser más reducida, lo que implica que una misma persona puede asumir múltiples responsabilidades relacionadas con la gestión tecnológica y la seguridad. No obstante, incluso en estos contextos es necesario definir claramente quién se encarga de la administración de sistemas, la supervisión de controles de seguridad y la gestión de incidentes.

Asimismo, el ISACA (2019) destaca que la gobernanza efectiva de la seguridad requiere la participación activa de la alta dirección, los responsables de tecnología y los usuarios finales. Esta distribución de

responsabilidades fortalece la cultura organizacional de ciberseguridad y promueve la colaboración entre las distintas áreas de la empresa.

4.2.2 Políticas y procedimientos de seguridad

Las políticas de seguridad representan el marco normativo interno que orienta el comportamiento de los miembros de la organización respecto al uso de los recursos tecnológicos y la gestión de la información. Estas políticas establecen principios, reglas y lineamientos que deben cumplirse para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Según la International Organization for Standardization (2022), las organizaciones deben documentar políticas de seguridad que sean coherentes con sus objetivos estratégicos y que estén alineadas con los requisitos del sistema de gestión de seguridad de la información. Estas políticas deben ser comunicadas a todo el personal y revisadas periódicamente para asegurar su vigencia frente a nuevos riesgos tecnológicos.

Los procedimientos de seguridad complementan estas políticas al describir de manera detallada cómo deben ejecutarse las actividades relacionadas con la protección de la información. Entre los procedimientos más comunes se encuentran la gestión de contraseñas, el control de accesos, la realización de copias de seguridad y la respuesta ante incidentes de seguridad.

El National Institute of Standards and Technology (2018) señala que la formalización de políticas y procedimientos contribuye a reducir la improvisación en la gestión de incidentes, ya que proporciona directrices claras que pueden ser aplicadas por el personal de la organización. En consecuencia, estos documentos constituyen la base operativa del modelo de ciberseguridad organizacional.

4.2.3 Integración de la ciberseguridad en la gestión empresarial

La ciberseguridad debe integrarse dentro del sistema general de gestión empresarial para garantizar su sostenibilidad y efectividad. Cuando la seguridad se trata como un elemento aislado del resto de procesos organizacionales, es más probable que las iniciativas pierdan continuidad o no reciban los recursos necesarios para su implementación.

El World Economic Forum (2023) destaca que los riesgos cibernéticos se han convertido en uno de los principales desafíos para las organizaciones modernas, por lo que su gestión debe formar parte de las decisiones estratégicas de la alta dirección. Esta integración permite considerar la seguridad como un componente clave del gobierno corporativo.

Desde una perspectiva operativa, integrar la ciberseguridad en la gestión empresarial implica incluir controles de seguridad en procesos como la gestión de proyectos, la administración de recursos humanos y la adquisición de tecnología. De esta manera, cada área de la organización contribuye a la protección de la información.

4.2.4 Enfoque progresivo y escalable

La implementación de un modelo de ciberseguridad debe realizarse de manera progresiva y escalable, especialmente en organizaciones con recursos limitados como las microempresas. Un enfoque gradual permite priorizar controles esenciales y ampliar el sistema de seguridad conforme aumentan las capacidades organizacionales.

El National Institute of Standards and Technology (2018) propone un modelo flexible que permite adaptar los controles de seguridad al nivel de madurez de cada organización. Este enfoque reconoce que no todas las empresas poseen los mismos recursos tecnológicos ni enfrentan los mismos niveles de riesgo.

Asimismo, la norma ISO/IEC 27001 enfatiza la importancia del ciclo de mejora continua basado en el modelo PDCA (Plan-Do-Check-Act), el cual permite implementar cambios graduales y evaluar continuamente la efectividad de las medidas adoptadas (International Organization for Standarization, 2022).

4.3 Implementación práctica del SGSI en microempresas

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) representa un paso fundamental para fortalecer la protección de los activos digitales dentro de una organización. En el caso de las microempresas, este proceso adquiere características particulares debido a las limitaciones de recursos financieros, tecnológicos y

humanos. Sin embargo, estas organizaciones también enfrentan riesgos significativos asociados al manejo de información, por lo que adoptar prácticas estructuradas de ciberseguridad resulta cada vez más necesario.

La familia de normas desarrollada por la International Organization for Standardization establece un marco de referencia para implementar sistemas de gestión orientados a la protección de la información. En particular, la norma ISO/IEC 27001 propone un enfoque basado en riesgos que permite adaptar los controles de seguridad a las características específicas de cada organización (International Organization for Standarization, 2022).

Además, el National Institute of Standards and Technology (2018) destaca que incluso las organizaciones de menor tamaño pueden implementar prácticas efectivas de seguridad mediante un enfoque progresivo, priorizando controles esenciales y fortaleciendo gradualmente su nivel de madurez en ciberseguridad. En este sentido, la implementación de un SGSI en microempresas debe orientarse a soluciones prácticas, sostenibles y alineadas con las capacidades organizacionales.

4.3.1 Fases de Implementación

La implementación de un SGSI generalmente se estructura en varias fases que permiten planificar, ejecutar y evaluar las medidas de seguridad dentro de la organización. Estas fases suelen basarse en el ciclo de mejora

continua conocido como PDCA (Plan-Do-Check-Act), el cual constituye uno de los principios fundamentales de la norma ISO/IEC 27001.

Durante la fase de planificación (Plan), la organización identifica sus activos de información, evalúa riesgos y define los controles necesarios para protegerlos. Posteriormente, en la fase de ejecución (Do), se implementan las políticas, procedimientos y medidas técnicas diseñadas durante la planificación. Este proceso incluye la capacitación del personal, la configuración de sistemas de seguridad y la documentación de los procesos operativos.

Figura No. #14 Ciclo PDCA

Nota. Fuente. Imagen creada con IA.

En la etapa de verificación (Check), la organización evalúa la efectividad de los controles implementados mediante auditorías internas, revisiones de desempeño e indicadores de seguridad. Finalmente, en la fase de mejora (Act), se realizan ajustes y mejoras basadas en los resultados

obtenidos. Este enfoque permite que el sistema de seguridad evolucione continuamente frente a nuevos riesgos y cambios tecnológicos (International Organization for Standarization, 2022).

4.3.2 Recursos mínimos necesarios

La implementación de un SGSI en microempresas no requiere necesariamente grandes inversiones tecnológicas. En muchos casos, es posible establecer un nivel adecuado de protección mediante el uso de herramientas básicas, buenas prácticas organizacionales y capacitación del personal.

El European Union Agency for Cybersecurity (2021) señala que las pequeñas empresas pueden mejorar significativamente su seguridad mediante medidas simples como la actualización periódica de software, el uso de contraseñas robustas, la implementación de copias de seguridad y la instalación de soluciones antivirus. Estas medidas constituyen la base de una estrategia de protección efectiva.

Además de los recursos tecnológicos, es fundamental contar con compromiso organizacional y liderazgo directivo. La alta dirección debe apoyar las iniciativas de ciberseguridad y garantizar que se asignen los recursos necesarios para su implementación. Incluso en organizaciones pequeñas, la designación de un responsable de seguridad de la información puede contribuir a mejorar la coordinación de las medidas de protección.

4.3.3 Documentación esencial del SGSI

La documentación constituye un componente fundamental dentro de cualquier sistema de gestión de seguridad de la información. Estos documentos permiten formalizar políticas, procedimientos y controles, garantizando que las prácticas de seguridad sean consistentes y puedan ser evaluadas periódicamente.

La norma ISO/IEC 27001 de la International Organization for Standardization establece que la organización debe mantener información documentada que respalde el funcionamiento del SGSI. Entre los documentos más importantes se encuentran la política de seguridad de la información, el inventario de activos, el análisis de riesgos y los procedimientos operativos relacionados con la protección de datos.

En el caso de las microempresas, la documentación puede ser más sencilla que en organizaciones grandes, pero sigue siendo necesaria para asegurar coherencia en la gestión de la seguridad. Documentar procesos permite que las prácticas de seguridad se mantengan incluso cuando cambian los responsables o cuando se incorporan nuevos miembros al equipo.

4.3.4 Indicadores clave de desempeño (KPIs)

Los indicadores clave de desempeño (Key Performance Indicators o KPIs) permiten evaluar la efectividad de las medidas de ciberseguridad implementadas dentro de una organización. Estos indicadores proporcionan información cuantitativa que facilita la toma de decisiones y la mejora continua del sistema de seguridad.

El National Institute of Standards and Technology (2018) señala que los indicadores de desempeño ayudan a medir el progreso de las iniciativas de ciberseguridad y a identificar áreas que requieren ajustes o mejoras. Entre los indicadores más utilizados se encuentran el número de incidentes de seguridad registrados, el tiempo de respuesta ante incidentes y el porcentaje de empleados capacitados en ciberseguridad.

En el contexto de microempresas, los KPIs deben ser simples y fáciles de monitorear para evitar sobrecargar los procesos administrativos. Por ejemplo, indicadores como la frecuencia de copias de seguridad, la actualización de sistemas o la participación del personal en programas de capacitación pueden proporcionar información valiosa sobre el nivel de madurez en seguridad.

4.4 Medición, auditoría y mejora continua

Una vez implementado un Sistema de Gestión de Seguridad de la Información (SGSI), es necesario establecer mecanismos que permitan evaluar su desempeño y garantizar su eficacia a lo largo del tiempo. La

seguridad de la información no es un proceso estático, ya que las amenazas digitales evolucionan constantemente y los entornos tecnológicos cambian de manera acelerada. Por esta razón, las organizaciones deben adoptar procesos sistemáticos de seguimiento, auditoría y mejora continua que permitan fortalecer su capacidad de respuesta frente a riesgos emergentes.

La norma ISO/IEC 27001, desarrollada por la International Organization for Standardization, establece que las organizaciones deben monitorear, medir, analizar y evaluar regularmente la efectividad de sus controles de seguridad (International Organization for Standarization, 2022). Este enfoque garantiza que las medidas implementadas continúen siendo adecuadas frente a cambios tecnológicos, organizacionales o regulatorios.

4.4.1 Seguimiento y evaluación del desempeño

El seguimiento del desempeño del SGSI permite determinar si las medidas de seguridad implementadas están cumpliendo con los objetivos establecidos por la organización. Este proceso implica recopilar información sobre el funcionamiento de los controles de seguridad, analizar los resultados obtenidos y evaluar si existen desviaciones respecto a los niveles de protección esperados.

La norma ISO/IEC 27001 de la International Organization for Standardization establece que las organizaciones deben definir métricas e indicadores que permitan evaluar el desempeño del sistema de gestión

de seguridad de la información. Estos indicadores pueden incluir el número de incidentes reportados, el tiempo promedio de respuesta ante incidentes o el nivel de cumplimiento de las políticas de seguridad.

4.4.2 Auditorías internas de seguridad

Las auditorías internas constituyen un mecanismo fundamental para evaluar de manera sistemática el cumplimiento de las políticas y controles establecidos dentro del SGSI. A través de estas evaluaciones, las organizaciones pueden verificar si los procedimientos de seguridad se están aplicando correctamente y si los controles implementados son efectivos para mitigar los riesgos identificados.

Según la norma ISO/IEC 27001 de la International Organization for Standardization (2022), las auditorías internas deben realizarse a intervalos planificados para asegurar que el sistema de gestión de seguridad de la información cumple con los requisitos establecidos por la organización y por el estándar internacional. Estas auditorías pueden ser realizadas por personal interno capacitado o por auditores independientes dentro de la organización.

Durante una auditoría de seguridad se revisan diversos aspectos, como la implementación de políticas de seguridad, la gestión de accesos, la protección de datos sensibles y la documentación del sistema. También se evalúa el nivel de conocimiento del personal respecto a las políticas y procedimientos establecidos.

4.4.3 Gestión de no conformidades

La gestión de no conformidades es un proceso que permite identificar, registrar y corregir desviaciones respecto a los requisitos establecidos por el SGSI. Estas desviaciones pueden surgir durante auditorías internas, revisiones de desempeño o incidentes de seguridad que revelen fallas en los controles existentes.

La norma ISO/IEC 27001 de la International Organization for Standardization establece que las organizaciones deben tomar acciones correctivas cuando se detecten no conformidades dentro del sistema de gestión. Este proceso implica analizar las causas del problema, implementar medidas correctivas y verificar posteriormente que dichas acciones hayan sido efectivas (International Organization for Standarization, 2022).

La correcta gestión de no conformidades permite evitar que los mismos problemas se repitan en el futuro. En lugar de limitarse a solucionar incidentes puntuales, este enfoque busca identificar las causas raíz de los problemas para fortalecer los procesos organizacionales.

4.4.4 Mejora continua del sistema

La mejora continua constituye uno de los principios fundamentales de los sistemas de gestión basados en estándares internacionales. En el contexto de la ciberseguridad, este principio implica revisar y actualizar

constantemente las políticas, procedimientos y controles implementados para adaptarlos a nuevas amenazas y cambios organizacionales.

El modelo de mejora continua conocido como PDCA (Plan-Do-Check-Act), promovido por la International Organization for Standardization, proporciona una estructura que permite planificar mejoras, implementarlas, evaluar sus resultados y realizar ajustes cuando sea necesario. Este ciclo asegura que el sistema de gestión evolucione de manera constante y se mantenga alineado con los objetivos estratégicos de la organización.

Asimismo, el National Institute of Standards and Technology (2018) destaca que las organizaciones deben adaptar continuamente sus estrategias de ciberseguridad frente a la aparición de nuevas vulnerabilidades y métodos de ataque. La mejora continua permite fortalecer progresivamente la resiliencia digital de la empresa.

4.5 Construcción y sostenibilidad de la cultura de ciberseguridad

La implementación de medidas técnicas y organizacionales de seguridad no garantiza por sí sola la protección efectiva de los activos de información. Para que un sistema de seguridad sea realmente eficaz, es necesario que exista una cultura organizacional que promueva comportamientos responsables y prácticas seguras en el uso de tecnologías. En este sentido, la cultura de ciberseguridad se refiere al conjunto de valores, conocimientos y actitudes que orientan la forma en

que los miembros de una organización gestionan y protegen la información.

La familia de normas desarrollada por la International Organization for Standardization destaca que la participación activa del personal es un elemento fundamental para el funcionamiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Cuando los empleados comprenden la importancia de la seguridad y adoptan prácticas responsables en su trabajo cotidiano, los controles técnicos se vuelven significativamente más efectivos (International Organization for Standarization, 2022).

4.5.1 Liderazgo y compromiso directivo

El liderazgo organizacional desempeña un papel esencial en la construcción de una cultura sólida de ciberseguridad. La alta dirección es responsable de establecer prioridades estratégicas, asignar recursos y promover políticas que refuercen la importancia de la protección de la información dentro de la organización.

La norma ISO/IEC 27001 de la International Organization for Standardization establece que la dirección debe demostrar liderazgo y compromiso con el SGSI, asegurando que las políticas de seguridad estén alineadas con los objetivos organizacionales y que las responsabilidades estén claramente definidas (International Organization for Standarization, 2022). Este liderazgo es clave para garantizar que la

seguridad de la información se integre en la gestión empresarial y no se perciba únicamente como una función técnica.

Además, el ISACA (2019) destaca que la gobernanza efectiva de las tecnologías de la información requiere la participación activa de la alta dirección en la supervisión de los riesgos digitales. Cuando los líderes organizacionales promueven activamente la ciberseguridad, es más probable que los empleados adopten comportamientos alineados con las políticas establecidas.

4.5.2 Comunicación interna efectiva

La comunicación interna constituye un elemento fundamental para fortalecer la cultura organizacional de ciberseguridad. Las políticas y procedimientos de seguridad solo pueden ser efectivos si son comprendidos por todos los miembros de la organización y si existe un flujo constante de información sobre riesgos, buenas prácticas y cambios en los protocolos de seguridad.

El National Institute of Standards and Technology (2018) señala que los programas de concienciación en ciberseguridad deben incluir estrategias de comunicación que permitan transmitir información relevante de manera clara y accesible para los empleados. Estas estrategias pueden incluir capacitaciones periódicas, campañas informativas y sesiones de sensibilización sobre amenazas digitales.

Además, la comunicación efectiva contribuye a fomentar un entorno en el que los empleados se sientan motivados a reportar incidentes o comportamientos sospechosos sin temor a represalias. Este aspecto es particularmente importante, ya que muchos incidentes de seguridad pueden detectarse tempranamente gracias a la observación y reporte oportuno del personal.

4.5.3 Cultura preventiva como proceso continuo

La cultura de ciberseguridad no debe entenderse como una iniciativa temporal, sino como un proceso continuo que evoluciona junto con los cambios tecnológicos y organizacionales. A medida que surgen nuevas amenazas digitales y se desarrollan nuevas herramientas tecnológicas, las organizaciones deben adaptar constantemente sus estrategias de protección.

Figura No. #15 Cultura de Ciberseguridad

Nota. Fuente. *Imagen creada con IA*.

Según Von Solms y Van Niekerk (2013), la evolución de la seguridad de la información hacia la ciberseguridad implica un enfoque más amplio que integra factores tecnológicos, organizacionales y humanos. Este enfoque reconoce que la protección de los activos digitales depende tanto de los sistemas técnicos como del comportamiento de las personas que interactúan con ellos.

Asimismo, el European Union Agency for Cybersecurity (2019) destaca que la concienciación y capacitación continua del personal constituye una de las medidas más efectivas para reducir el riesgo de incidentes de seguridad. Programas de formación periódicos permiten actualizar conocimientos y reforzar las buenas prácticas dentro de la organización.

4.5.4 Retos y tendencias futuras en ciberseguridad

El entorno digital continúa evolucionando rápidamente, lo que genera nuevos retos para las organizaciones en materia de seguridad de la información. Tecnologías emergentes como la computación en la nube, el Internet de las cosas (IoT) y la inteligencia artificial han ampliado las capacidades tecnológicas de las empresas, pero también han incrementado la complejidad de los riesgos asociados.

El World Economic Forum (2023) advierte que los ciberataques se han vuelto cada vez más sofisticados y que las organizaciones deben adoptar enfoques proactivos para anticipar estas amenazas. Esto implica invertir en tecnologías de seguridad avanzadas, fortalecer las capacidades del personal y promover la cooperación entre sectores públicos y privados.

Además, el International Telecommunication Union (2022) señala que el desarrollo de capacidades en ciberseguridad será uno de los principales desafíos para las economías digitales en los próximos años. La formación de profesionales especializados y la adopción de estándares internacionales serán factores clave para fortalecer la resiliencia digital.

En este contexto, las organizaciones que logren consolidar una cultura sólida de ciberseguridad estarán mejor preparadas para enfrentar los desafíos del futuro digital, proteger sus activos estratégicos y mantener la confianza de sus clientes y socios comerciales.

BIBLIOGRAFÍA

/IEC, I. (2017). Internacional Estandar. *Scribd*.

27001, N. I. (Marzo de 2022). *ISO 27001*. Obtenido de https://www.iso.org/es/norma/27001?page%25252525253D1%25252525252525252C1%252525252526topic%25252525253DCloud%2525252525252525252CData%252525252525252525520Center%252525252526zPage%25252525253DOverview-c58a53dc%252525252526zContent%25252525253DThe-State-of-the

Albánez.et.al. (2023). *Universidad de Navarra.* Obtenido de https://www.unav.edu/documents/4889803/44362196/47-+Vilavella+El+impacto+de+la+digitalizacio%CC%81n+en+el+a%CC%81mbito+educativo.pdf/4bc7df70-cfdc-04cd-54d2-5278639f21bc?t=1678717064447

Alenezi, M., & Akour, M. (2023). Digital Transformation Blueprint in Higher Education: A Case Study of PSU. *OUCI*.

Almache,V;et.al. (2024). Transformación digital en los procesos de aprendizaje de la educación superior. *Magazine de las ciencias*.

American Psychological Association. (2020). *Publication Manual of the American Psychological Association.* APA.

Astudillo, K. (2025). *Como iniciarte en Ciberseguridd.* Independiente.

auraquantic. (2025). *auraquantic*. Obtenido de https://www.auraquantic.com/es/blog/top-tendencias-tecnologicas/

Ávila, F. (2023). Ransomware, una amenaza latente en Latinoamérica. *Scielo*.

Ayerdi, A. (31 de Enero de 2025). *Docuware*. Obtenido de https://start.docuware.com/es/blog/tendencias-tecnologicas

Babilonia, G. (05 de Junio de 2023). *Portal Universidad Catolica de Trujilla.* Obtenido de file:///C:/Users/DELL/Downloads/ID_2023004___June_2023-2-4.pdf

Barnes, T. (16 de Septiembre de 2025). *Digital Toolkit*. Obtenido de https://www.digitaltoolkit.co/your-digital-toolkit/cyber-

awareness-best-practices-for-employees/?utm_source=chatgpt.com

BBVA. (2026). *BBVA*. Obtenido de https://www.bbva.mx/educacion-financiera/banca-digital/ciberseguridad/que-es-el-fraude-digital.html

Bello, M., & Galindo, F. (2020). *Charting the digital transformation of science.* New York: OECD.

Boettiger, C. (2015). An introduction to Docker for reproducible research. *ACM SIGOPS Operating Systems Review, 49*(1), 71-79. doi:10.1145/2723872.2723882

Bonnie, E. (1 de Enero de 2026). *secureframe*. Obtenido de https://secureframe.com/blog/iso-27005

Bromwich, M., & Bromwich, R. (2016). Riesgos de privacidad al utilizar dispositivos móviles en la atención médica. *National Library Of Medicine*.

Brown, C. (12 de Septiembre de 2024). *VikingCloud*. Obtenido de https://www.vikingcloud.com/blog/iso-27000-family-standards

Castellano, L. (2015). *Seguridad en informatica.* Independiente.

Castillo, K., Aguilar, J., & Madrigal, A. (2024). Desafíos éticos de la inteligencia artificial generativa en las nuevas formas organizacionales. *RedTIS*.

Choque,J,et.al. (2025). Ciencia Abierta y Colaborativa en la Era de la Inteligencia Artificial. *Veritas*.

Comisión Europea. (2016). *H2020 Programme. Guidelines on FAIR Data Management in Horizon 2020.* Publications Office of the European Union.

Contreras, V. (12 de Enero de 2026). *dpl news*. Obtenido de https://dplnews.com/ia-agentica-autonomia-que-pondra-a-prueba-a-empresas/

Creative Commons. (2025). *About CC Licenses*. Obtenido de Creative Commons: https://creativecommons.org/licenses/

cyberhaven. (26 de Noviembre de 2025). Obtenido de https://www.cyberhaven.com/infosec-essentials/what-is-incident-response?utm_source=chatgpt.com

DataGuard. (23 de Enero de 2026). Obtenido de https://www.dataguard.com/blog/iso-27001-annex-a5-information-security-policies

Davenport, T., & Harris, J. (2007). *Competing on Analytics: The New Science of Winning.* Harvard Business School Press.

Day, R., & Gastel, B. (2012). *How to Write and Publish a Scientific Paper.* Cambridge University Press.

De Leon, D. (2023). Digitization, digitalización y transformación digital: conceptos clave para la práctica empresarial . *Serie Científica de la Universidad de las Ciencias Informáticas*.

Delacruz, R., & Rondon, R. (2024). xperiencias del Servicio Digital en Gestión Documentaria de las Instituciones Educativas Públicas del Perú. *Tecnologica -Educativa Docentes 2.0*.

Diaz,V.et.al. (2023). Managing Digital Transformation: A Case Study in a Higher Education Institution. *MDPI*.

Disterer, G. (2013). ISO/IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información. *Scientific Reserch*.

Domingo, J. (26 de Enero de 2024). *GESDATA CONSULTING*. Obtenido de https://gesdataconsulting.es/iso-27003

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* Official Journal of the European Union.

European Union Agency for Cybersecurity . (2021). *Cybersecurity for SMEs: Challenges and Recommendations.* . Publications Office of the European Union.

European Union Agency for Cybersecurity. (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.* Publications Office of the European Union.

European Union Agency for Cybersecurity. (2025). *Threat Landscape for SMEs.* Publications Office of the European Union.

Feher, K., & Demeter, M. (2025). Generative Knowledge Production Pipeline Driven by Academic Influencers. *Cornell University*.

Flinders, M., & Smalley, I. (4 de Abril de 2024). *IBM*. Obtenido de https://www.ibm.com/es-es/think/topics/business-continuity-disaster-recovery

Floridi, L. (2013). *The Ethics of Information.* Oxford University Press.

Fortinet. (2025). *Fortinet*. Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/internet-fraud

Fraser,N.et.al. (6 de Abril de 2021). *PHYS ORG*. Obtenido de https://phys.org/news/2021-04-preprints-science-pandemic.html?utm_source=chatgpt.com

Fuentealba, S. (5 de Mayo de 2025). *Tiempos Sustentables*. Obtenido de https://tiempossustentables.cl/2025/05/05/sostenibilidad-digital-guia-basica-para-un-futuro-digital-responsable/

Fuks, L. (17 de Enero de 2024). *aqua*. Obtenido de https://www.aquasec.com/cloud-native-academy/cspm/top-7-risks-of-cloud-computing/

Galindo, O. (2020). Transformación digital: una agenda de oportunidades para la investigación y la práctica. *Redalyc*.

García, J., Rojas, W., & Sanabria, M. (2025). The role of artificial intelligence in detecting emerging trends in scientific publications. *Revista Ciencitifica Gneral JoséMaria Cordoba*.

Gomez,S.et.al. (2018). A Digital Ecosystems Model of Assessment Feedback on Student Learning . *Canadian Center of Science and Education*.

González,G.etl.al. (2025). Inteligencia Artificial y su impacto sobre la gerencia estratégica y la cultura investigativa. *Revista de Ciencias Sociales*.

Greitzer, F. F. (2010). Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. *Insider Threats in Cyber Security*, 85-113. doi:10.1007/978-1-4419-7133-3_5

Grossman,R.et.al. (2024). A Framework for the Interoperability of Cloud Platforms: Towards FAIR Data in SAFE Environments. *scientific data*.

Guarin, E. (15 de Marzo de 2025). Obtenido de https://www.piranirisk.com/es/blog/como-gestionar-riesgos-con-la-metodologia-iso-27005

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking (2nd ed.).* Wiley.

Hermida,K.etl.al. (2025). La ética en la investigación científica: desafíos y prácticas responsables en la era digital. *Sinergia*.

hichex. (Octubre de 2024). Obtenido de https://www.hichex.com/implementacion-iso-27001-evitar-riesgos-y-pasos-a-seguir/?utm_source=chatgpt.com

Hicks, D., & Wouters, P. (2015). Bibliometrics: The Leiden Manifesto for research metrics. *Nature, 520*, 429-431. doi:10.1038/520429a

Holdsworth, J., & Kosinski, M. (2025). ¿Qué es la gestión de accesos? *IBM*.

Holloway, D. (15 de Septiembre de 2025). *isms.online*. Obtenido de https://es.isms.online/iso-27001/requirements-2013/5-1-leadership-commitment-2013/

Imbaquingo, D., Pusdá, M., & Jácome, J. (2016). *Fundamentos de auditoria Informatica basada en riesgos.* Ibarra: UTN.

India, T. t. (2 de Septiembre de 2025). Vincula todas las publicaciones academicas al identificador de objetos digitales. *The times of the India*.

International Committee of Medical Journal Editors. (2025). *Recommendations for the Conduct, Reporting, Editing, and Publication of Scholarly Work in Medical Journals.* ICMJE.

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience.* ISO.

International Organization for Standarization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems.* ISO.

International Telecommunication Union. (2022). *Global Cybersecurity Index 2020.* ITU Publications.

ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives.* . ISACA.

ISO. (2015). Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es

Iso Tools. (10 de Septiembre de 2024). Obtenido de https://isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools. (2026). Obtenido de https://cl.isotools.org/isoiec-27004/

Jain, N. (8 de Septiembre de 2023). *Ideascale*. Obtenido de https://ideascale.com/es/blogs/que-es-el-diseno-de-la-investigacion/?utm_source=chatgpt.com

Jimenez, E., & Rivera, S. (2025). Transformaci n digital en el sector educativo: retos, innovaciones y experiencias exitosas. *Polo del conocimiento*.

Juca, F. (18 de Marzo de 2025). *Fernando Juca Maldonado*. Obtenido de https://fernandojuca.com/controles-de-seguridad-ciberseguridad/?utm_source=chatgpt.com

Kiser, Q. (2020). *CIBER Seguridad.* Independiente.

Klein, A. (2022). Ethical Issues of Digital Transformation. *Scielo*.

Larraga, I., Lema, D., & Campoverde, G. (2026). Transformación digital en la gestión académica universitaria: un caso de estudio en el Distrito Metropolitano de Quito. *Qualitas*.

Linkedin. (20 de Mayo de 2024). Obtenido de https://es.linkedin.com/pulse/la-importancia-de-formaci%C3%B3n-continua-en-ciberseguridad-kbj7e

López,A; et.al. (2025). La transformación digital en la administración pública: evolución y tendencias de investigación. *Perspectivas sociales y administrativas*.

Lozada, F. (2024). La revolución digital: impacto de la tecnología en la evolución de la investigación científica. *Revista del Instituto de Investigaciones Científicas de la UniversidadArturo Michelena*.

Mabotha, P., & Ngcamu, B. (2025). Digital Transformation in the Higher Education Sector: A Systematic Literature Review. *MDPI*.

Mantilla, W. (2012). LA GESTIÓN DE LA INVESTIGACIÓN: DIFERENCIACIONES Y RELACIONES. *Universidad Santo Tomas*.

Martinescu, L. (23 de Octubre de 2023). *Oxford Insights*. Obtenido de https://oxfordinsights.com/insights/exploring-the-concepts-of-digital-twin-digital-shadow-and-digital-model/?utm_source=chatgpt.com

McBride, N. (Junio de 2025). *Strategy*. Obtenido de https://www.o8.agency/blog/digital-transformation/breaking-

down-barriers-digital-transformation-overcome-challenges-and-accelerate-growth?utm_source=chatgpt.com

Medina, M. (2025). *Metodología Integral de la Investigación Científica: Fundamentos, Estrategias y Aplicaciones Digitales:.* Madrid: SciELa.

Méndez, E., Méndez, H., & Partida, O. (17 de Abril de 2023). *CEITAM Jalisco.* Obtenido de https://ceidtamjalisco.gob.mx/diseno-e-implementacion-de-una-plataforma-digital-para-coadyuvar-al-desarrollo-del-programa-de-investigacion-educativa-en-instituciones-de-la-dgetaycm?utm_source=chatgpt.com

Mishra, A. (17 de Marzo de 2025). *Edureka*. Obtenido de https://www.edureka.co/blog/password-management-in-cybersecurity/

Monteza, C. (2018). Modelo de gestión de la investigación y nivel d. *Redalyc*.

Morales, E. (16 de Diciembre de 2025). *TecnetOne*. Obtenido de https://blog.tecnetone.com/evaluacion-de-ciberseguridad-que-es-y-por-que-la-necesitas?utm_source=chatgpt.com

Muñoz,H. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Redalyc*.

Nassi, C. (19 de Agosto de 2022). *SciELO en perspectiva*. Obtenido de https://blog.scielo.org/es/2022/08/19/la-evaluacion-de-la-investigacion-debe-ir-mas-alla-de-comparar-metricas-de-impacto/?utm_source=chatgpt.com

National Academies of Sciences, Engineering and Medicine. (2019). *Reproducibility and Replicability in Science.* The National Academies Press. doi:10.17226/25303

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* US. Department of Health, Education and Welfare.

National Cybersecurity Alliance. (26 de Julio de 2024). Obtenido de https://www.staysafeonline.org/es/art%C3%ADculos/copias-de-seguridad

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* US. Department of Commerce.

Obando, J. (11 de Marzo de 2025). *Linktik*. Obtenido de https://linktic.com/blog/5-tendencias-tecnologicas-que-estan-transformando-el-futuro/

Ochoa, M. (17 de Septiembre de 2025). *Network360*. Obtenido de https://www.itmastersmag.com/analytics-big-data/plan-de-contingencia-ante-una-filtracion-de-datos/

OECD. (2015). Making Open Science a Reality. *OECD Science, Technology and Industry Policy Papers*. doi:10.1787/5jrs2f963zs1-en.

OECD. (2015). *Manual de Frascati 2015: Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental.* OECD Publishing.

ORCID. (2026). *About ORCID*. Obtenido de ORCID: https://info.orcid.org/what-is-orcid/

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO.

Orozco, P. (13 de Marzo de 2018). *integra*. Obtenido de https://blog.consultoresdesistemasdegestion.es/a-que-empresas-se-recomienda-la-iso-27000/

Özkan, E., & Kök, I. (2025). System Development Life-Cycle Assisted Digital Twin Development Model for Smart Micro-grids. *Science Direct*.

Page, M., & al, e. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*. doi:10.1136/bmj.n71

Paletta, F., & Moreiro, J. (2018). La transformación digital en los métodos y temas de la investigación brasileña de Información y Documentación 2010-2019. *Revista Española de Documentación Científica* .

Paloaltonetwork. (21 de Diciembre de 2025). Obtenido de https://www.paloaltonetworks.lat/cyberpedia/what-is-incident-response

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 165-176. doi:10.1016/j.cose.2013.12.003

Patiño, O., & Valencia, J. (2024). Impacto de la transformación digital en la cultura de las organizaciones modernas . *Ciencia, Tecnología e Innovación*.

Pérez, M. (18 de Enero de 2023). *smowl Tech*. Obtenido de https://smowl.net/es/blog/ecosistema-digital/

Pérez, M., & Sánchez, V. (2024). Redes de colaboración científica potenciadas por TIC: avances en la investigación universitaria. *Ciencia&tecnologia*.

Pescadilla, J. (25 de Julio de 2025). *isms.online*. Obtenido de https://es.isms.online/iso-27001/statement-of-applicability/annex-a-controls/?utm_source=chatgpt.com

Project Management Institute. (2021). *Guía de los fundamentos para la dirección de proyectos.* PMI.

Puente, O. (22 de Noviembre de 2023). *IEBS Bussines School*. Obtenido de https://www.iebschool.com/hub/que-es-transformacion-digital-business/

Quijije, Y., Vélez, C., & Ponce, J. (2025). Ecosistemas Tecnológicos En La Transformación De La Educación Universitaria: Innovación Y Estrategias Claves. *REFCALE*.

Quilia,J;et.al. (2025). Herramientas digitales en la elaboración de investigación científica en educación superior. *Scielo*.

Ramirez, R. (18 de Noviembre de 2025). *Repositorio Universidad Espititu Santo.* Obtenido de https://repositorio.uees.edu.ec/items/3d56b777-e8ce-4e5b-b56a-5a409425923d/full?utm_source=chatgpt.com

Ravinderjeet, D. (2025). The Role of Technology in Advancing Academic Research in STEM in the U.S. *International Journal*

of Scientific Research in Computer Science, Engineering and Information Technology.

Rivera, H., & Castillo, M. (2025). Transformación Tecnológica e Innovación Educativa desde la Perspectiva de la Educación 4.0 a Nivel de Postgrado. *Ciencia Latina*.

Rojas, M., & Chiappe, A. (2024). Artificial Intelligence and Digital Ecosystems in Education:. *Technology, Knowledge and Learning*.

Romo, D., & Valarezo, J. (Agosto 14 de 2015). *Repositorio de la Universidad Politecnica Salesiana Ecuador.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

Royakkers,L.et.al. (2018). Societal and ethical issues of digitization. *Springer Nature* .

Rueda, J. (5 de Febrero de 2026). *factorial*. Obtenido de https://factorial.es/blog/iso-27002/?utm_source=chatgpt.com#importanciaiso27002

Saltos,J.et.al. (2024). Ecosistema de medios digitales: un análisis dimensional según el criterio de especialistas. *Scielo*.

San Francisco Declaration on Research Assessment. (2012). *Declaration on Research Assessment (DORA)*. Obtenido de https://sfdora.org/read/

Sandve, G., & al., e. (2013). Ten Simple Rules for Reproducible Computational Research. *PLoS Computational Biology*. doi:10.1371/journal.pcbi.1003285

Schein, E. (2010). *Organizational Culture and Leadership (4th ed.).* Jossey-Bass.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W. W. Norton & Company.

Security Everywhere. (3 de Noviembre de 2025). Obtenido de https://www.security-everywhere.com/the-critical-role-of-data-backup-in-cybersecurity/

Segovia, M., & Garcia, J. (2022). Design, Modeling and Implementation of Digital Twins. *MDPI*.

Seguridad 360. (18 de Septiembre de 2024). Obtenido de https://revistaseguridad360.com/noticias/control-de-

accesos/control-de-acceso-y-ciberseguridad-en-entornos-empresariales-estrategias-efectivas-para-proteger-tu-negocio/?utm_source=chatgpt.com

Sentineloen. (16 de Julio de 2025). Obtenido de https://www.sentinelone.com/es/cybersecurity-101/cybersecurity/what-is-security-policy/

Shapira, P. (2024). Rise of Generative Artificial Intelligence in Science. *Cornell University*.

Singun, A. (2025). Unveiling the barriers to digital transformation in higher education institutions: a systematic literature review. *Discovery Educations*, 37.

Storey, V., & Baskerville, R. (2025). Digitalization of the natural sciences: Design science research and computational science. *Science Direct*.

Suits, G. (03 de Diciembre de 2025). *Solutions,G*. Obtenido de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27002-y-para-que-sirve/

TN University Business School. (22 de Octubre de 2025). Obtenido de https://www.tnuniversity.edu.mx/editorial/articulo/amenazas-digitales-actuales-y-su-impacto-en-la-seguridad-corporativa/?utm_source=chatgpt.com/

Torres, H., & Lopez, M. (20 de Marzo de 2025). *Desafío de la Legislación Ecuatoriana frente a la regulación de la Inteligencia Artificial en la protección de datos personales.* Obtenido de https://repositorio.utn.edu.ec/handle/123456789/17033?utm_source=chatgpt.com

UCUENCA. (Junio de 2025). Obtenido de https://www.ucuenca.edu.ec/transformacion-digital/?utm_source=chatgpt.com#

UNAM. (19 de Agosto de 2019). *Direccion General de Repositorios Universitarios UNAM*. Obtenido de https://dgru.unam.mx/index.php/repositorio-institucional-unam-2/?utm_source=chatgpt.com

UNESCO. (2021). *UNESCO Recommendation on Open Science.* UNESCO. Obtenido de UNESCO Digital .

Unión Europea. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Official Journal of the European Union.

Universidad Europea. (28 de Febrero de 2023). Obtenido de https://universidadeuropea.com/blog/ecosistema-digital/

US. Department of Homeland Security. (2012). *The Menlo Report. Ethical Principles Guiding Information and Communication Technology Research.* US. Department of Homeland Security.

Vega, E. (2021). *Seguridad de la informacion.* Alicante: 3Ciencias.

Veracruzana, U. (2025). Obtenido de https://www.uv.mx/infosegura/files/2021/04/08_documento_formativo_consejo-1.pdf&embedded=true

Verhoef,P.et.al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Science Direct*.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004

Walker, B. (s.f.). *Hacking Ético: Guía completa para principiantes para aprender y entender los reinos del hacking ético.* Autonomo.

Wang, Y., Yu, Y., & Khan, A. (2025). Sostenibilidad digital: exploración de dimensiones y desarrollo de escala. *ScienceDirect*.

Whiting, J. (25 de Julio de 2025). *isms.online*. Obtenido de https://www.isms.online/iso-27005/

Wilkinson, M., Dumontier, M., & al., e. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*. doi:10.1038/sdata.2016.18

Wilson, G. (24 de Abril de 2025). *Symbolic Data*. Obtenido de https://www.symbolicdata.org/research-software-tools/?utm_source=chatgpt.com

Wilson, G., J, B., & Cranston, K. (2017). Good enough practices in scientific computing. *PLoS Computational Biology*. doi:10.1371/journal.pcbi.1005510

World Economic Forum. (2023). *Global Risks Report 2023.* WEF.

ANEXO 1

Revisión de pares ciegos.

ANEXO 2: Revisión anti-plagio.