# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución: RPC-SO-02-No.053-2021*

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER**

| |
|---|
| **Título del proyecto:** |
| Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022 |
| **Línea de Investigación:** |
| Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable |
| **Campo amplio de conocimiento:** |
| Tecnologías de la Información y la Comunicación (TIC) |
| **Autor/a:** |
| Jorge Luis Nepas |
| **Tutor/a:** |
| Renato Mauricio Toasa Guachi<br>Maryory Urdaneta Herrera |

**Quito – Ecuador**

**2025**

**APROBACIÓN DEL TUTOR**

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022.

Elaborado por: Jorge Luis Nepas Yanacallo, de C.I: 1719325118, estudiante de la Maestría: En Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

**Firma**

**APROBACIÓN DEL TUTOR**

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022.

Elaborado por: Jorge Luis Nepas Yanacallo, de C.I: 1719325118, estudiante de la Maestría: En Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.03.10 12:12:17 -05'00'

_____

**Firma**

**DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE**

Yo, Jorge Luis Nepas Yanacallo con C.I: 1719325118, autor/a del proyecto de titulación denominado: Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
JORGE LUIS NEPAS YANACALLO

_____

**Firma**

**Tabla de contenidos**

**Índice de Tablas**

**Índice de Figuras**

## INFORMACIÓN GENERAL

### Contextualización del tema

El ámbito de la ciberseguridad evoluciona infatigablemente y mantenerse a la vanguardia es esencial para proteger la información confidencial y prevenir los ciberataques. Con el surgimiento de nuevas tecnologías todo el tiempo, puede resultar difícil mantenerse actualizado con las últimas tendencias y desarrollos de los cibercriminales. Los cibercriminales son cada día más sofisticados en sus tácticas y, como resultado, las violaciones de datos son cada vez más comunes. Algunas de las últimas amenazas de ciberseguridad incluyen ataques que pueden causar pérdidas financieras significativas, daños a la reputación e incluso responsabilidad legal.

En consecuencia, la ciberseguridad abarca todas las tecnologías y prácticas, con su respectivo instrumental, que deben usarse para mantener seguros los sistemas informáticos y los datos electrónicos, debido a que, en mundo tan interconectado y abierto, en el que cada vez más actividades comerciales y sociales son realizados online, se trata de un campo y área de conocimiento enorme y en continuo crecimiento.

Actualmente en un mundo impulsado por la tecnología, la ciberseguridad es primordial y su importancia se extiende a todos los ámbitos profesionales, especialmente en el sector educativo, el administrativo y el tecnológico. Con todas las herramientas, dispositivos inteligentes conectados digitalmente y los recursos en línea convirtiéndose en parte integral del aprendizaje, la cantidad de amenazas cibernéticas ha aumentado significativamente. Por tanto, los ciberdelincuentes apuntan a las instituciones educativas debido a los datos valiosos y confidenciales que poseen. En este orden de ideas, el sector educativo es un objetivo cada vez mayor para los ciberdelincuentes no solo por los datos importantes, sino por los os presupuestos limitados y los sistemas de seguridad que en algunos casos están obsoletos. Las restricciones presupuestarias suelen dar lugar a medidas de ciberseguridad más débiles, lo que hace que las escuelas y universidades sean más vulnerables. El malware y el phishing son los tipos de ataque más frecuentes y afectan a una gran cantidad de instituciones. Los efectos de los ciberataques implican la pérdida de datos, los costos financieros y las amenazas a la seguridad de los menores, alterando todo el proceso lo que altera el proceso educativo. Por ello, es preciso que las medidas proactivas, la formación del personal administrativo, docente y el cuerpo directivo y las soluciones de seguridad integrales son vitales para mejorar la protección de los sistemas de información en el sector educativo (Novikava, 2024).

En el ámbito profesional administrativo, en la actualidad, se reconoce considerablemente que las computadoras y la tecnología de la información son una parte esencial de cada organización, incluidas las instalaciones administrativas. Efectivamente, su uso ha aumentado significativamente la eficiencia del mantenimiento de registros y la gestión de datos. También se reconoce que la información es un bien valioso y que el acceso, uso o destrucción no autorizados de la misma pueden tener efectos adversos para el propietario. A medida que se almacena y comparte cada vez más información electrónicamente, los riesgos de acceso no autorizado o uso indebido de los datos han incrementado considerablemente. Las instalaciones administrativas corren un riesgo particular de diversas formas de ciberataques. Esto se debe a que frecuentemente se almacenan grandes cantidades de información personal y financiera, y los datos son generalmente confidenciales. Las infraestructuras administrativas y sus sistemas de información contienen información sobre el uso de servicios del sector público, del sector financiero, de aspectos laborales, legales, tributarios y todo tipo de información gerencial de las organizaciones. Por tanto, cualquier violación de datos podría tener graves consecuencias para las personas afectadas y podría dar lugar a acciones legales contra la organización involucrada. Por ello es forzoso que las instalaciones administrativas adopten las medidas necesarias para garantizar la seguridad de los datos (Eid-Almanaseer y Matrouk-Aloun, 2023).

En el contexto profesional tecnológico, surge la ciberseguridad, como práctica que procura la protección de sistemas, redes y programas de ataques digitales. Estos ciberataques usualmente tienen como finalidad acceder, modificar o destruir información confidencial; extorsionar a los usuarios; o interrumpir procesos comerciales normales. Implementar medidas de ciberseguridad eficientes y sólidas es específicamente muy complejo y difícil actualmente debido a la existencia de más dispositivos que personas y los atacantes se están volviendo cada vez más innovadores. La ciberseguridad cubre muchos aspectos del panorama digital reciente, como las medidas de seguridad para suministrar protección a los datos, seguridad de la información, seguridad de aplicaciones, seguridad de redes, seguridad en la nube, seguridad de dispositivos de punto final y protección de personas: personal, clientes, consumidores y usuarios públicos de servicios de Tecnologías de la información. Los avances tecnológicos recientes abren nuevas posibilidades para la ciberseguridad, pero penosamente, los adversarios igualmente se han beneficiado de estos avances. Por ello, es preciso que profesionales de la tecnología cada día avancen y se formen en aspectos muy recientes de ciberseguridad (Michigan Technological University, 2025).

**Problema de investigación**

Los riesgos de ciberseguridad, actualmente, representan un peligro latente y se han convertido en una verdadera preocupación global y una amenaza económica progresiva. Con el incremento de la digitalización de las organizaciones y de los procedimientos operativos de estas a nivel mundial, las violaciones y conspiraciones cibernéticas son cada día más y más frecuentes y los costos potenciales para las organizaciones y las economías de los países continúan en aumento. Si bien las innovaciones tecnológicas constituyen nuevos retos, igualmente suministran novedosas soluciones. En tal sentido, la ciberseguridad es una inquietud corporativa cada vez más necesaria en la actualidad. Mientras que cada vez más empresas se digitalizan, estas son más vulnerables a los ciberataques que ponen en riesgo la información y la infraestructura que las respalda (Basu, 2024).

Penosamente, muchas organizaciones no son conscientes de las enormes consecuencias que enfrentarían sus sistemas ante un ataque informático exitoso y siguen con sus prácticas usuales como si nada ocurriese. Sin embargo, el desconocimiento no es garantía de protección: actualmente, más que nunca, es preciso ser consciente institucionalmente de los riesgos que representa la inseguridad cibernética, principalmente para sectores específicos representativos de una determinada economía. Por tanto, sea cual sea la organización, deben adoptarse inmediatamente medidas que ayuden a minimizar las posibilidades de ser susceptibles a delincuentes digitales (Basu, 2024).

En este orden de ideas, los estándares de ciberseguridad proponen un enfoque ordenado para la gestión y evaluación de gestionar de los riesgos de ciberseguridad. Constituyen el fin primordial de los requerimientos, controles e intervenciones de seguridad utilizadas por las organizaciones para disminuir la probabilidad y el efecto de los ataques en el marco de la ciberseguridad. Por tanto, es preciso señalar que la adopción de tecnologías emergentes ha derivado en nuevas competencias y capacidades, valores y conocimientos adicionales considerables. Sin embargo, las innovaciones tecnológicas son objeto continuo de múltiples actores que las amenazan, cada uno inducido por diversas motivaciones, razones y capacidades. En consecuencia, para el aprovechamiento óptimo de la ventaja competitiva generado por estas innovaciones tecnológicas, la ciberseguridad es hoy más que nunca, una máxima prioridad en todos los sectores productivos (Djebbar y Nordströ, 2023).

A efectos de poner en contexto el problema de los ataques cibernéticos a las organizaciones, es preciso resaltar que los cibercriminales cada día se diversifican y mejoran sus formas de

actuar, el costo del cibercrimen continua en ascenso y se enfoca a alcanzar la sorprendente cifra estimada de 15,63 billones de dólares parta el año 2029. El incremento de los ataques de ransomware en sectores productivos clave, los complicados y rebuscados esquemas de phishing y el reforzamiento de las normas para su prevención y mitigación, son fuertes advertencias y recordatorios de la necesidad de la alerta corporativa y especialmente la adopción de tecnologías avanzadas para estar a la vanguardia ante las amenazas emergentes (Fox, 2025).

Este alarmante problema tiene costos y efectos significativos a nivel global, para ejemplificarlo se presentan las siguientes estadísticas:

Las estimaciones de los costos globales de los delitos cibernéticos alcanzarán anualmente los 10,5 billones de dólares para el año 2025, poniendo de relieve la importancia de optimizar todas las medidas de ciberseguridad posible, a modo complementario, se estima que el índice global titulado Costo estimado del cibercrimen en el mercado de la ciberseguridad incremente consecutivamente entre 2024 y 2029 en un total de 6,4 billones de US$ equivalente a un incremento global del 69,41% (Statista, 2025).

Las pérdidas económicas derivadas de delitos cibernéticos denunciadas y reportadas ante el Centro de denuncias de delitos en Internet (IC3) del FBI (Federal Bureau of Investigation de los Estados Unidos) incrementaron en un 22% en el periodo 2022 - 2023 (Federal Bureau of Investigation, 2023).

Durante el año 2024, en promedio, el costo mundial de una infiltración de datos fue de 4,88 millones de U$D (IBM, 2025).

Como puede observarse los ciberataques representan una verdadera amenaza global para las organizaciones que cada vez son más abiertas e interconectadas, por ello ante esta realidad como lo es el incremento de la ciberdelincuencia y el surgimiento continuo de nuevos peligros y amenazas, pareciera un trabajo arduo o inclusive improbable de gestionar los riesgos planteados por el cibercrimen, pero para ello la ISO/IEC 27001 permite a las organizaciones a crear consciencia de estos riesgos permanente así como a la identificación y abordaje de las debilidades organizacionales proactivamente. La ISO/IEC 27001 impulsa una orientación completa de la seguridad de toda la información corporativa, que incluye a “personas, las políticas y la tecnología. Un sistema de gestión de la seguridad de la información implantado conforme a esta norma es una herramienta clave para la gestión de riesgos, la resiliencia cibernética y la excelencia operativa” (ISO/IEC, 2022).

**Objetivo general**

Establecer una guía para el desarrollo de políticas de ciberseguridad en la empresa IEPHE, alineado con la norma ISO/IEC 27001:2022 y las mejores prácticas de gestión de riesgos, con el fin de proteger la información crítica y garantizar la continuidad operativa.

**Objetivos específicos**

- Contextualizar los fundamentos teóricos relacionados a la ciberseguridad, las políticas clave de Ciberseguridad y la Norma ISO/IEC 27001:2022.
- Diagnosticar la situación inicial de ciberseguridad en IEPHE, evaluando la infraestructura actual, identificando activos críticos y analizando vulnerabilidades y amenazas específicas a las que está expuesta la organización.
- Desarrollar una estructura y guía para la implementación de las políticas y procedimientos claros que cumplan con los requisitos establecidos por la norma ISO/IEC 27001:2022, incluyendo aspectos como gestión de accesos, clasificación de información y respuesta ante incidentes.
- Validar la propuesta mediante el criterio de especialistas.

**Vinculación con la sociedad y beneficiarios directos:**

En materia de Vinculación con la sociedad y beneficiarios directos de una propuesta metodológica para el Desarrollo de Políticas clave de Ciberseguridad en el sector empresarial, precisa resaltar que, en la era digital contemporánea, Internet es una plataforma creada para que se lleven a cabo varios aspectos de las interacciones sociales y comerciales. Por ello, las organizaciones se valen de Internet para simplificar las tareas, el almacenaje de datos corporativos y obtener acceso directo a la información cuando sea necesario. Pero, hay que considerar que Internet fue concebido originalmente como una red abierta y tolerante a fallos, por lo tanto, las empresas son vulnerables a las ciberamenazas.

La ciberseguridad es decisiva y esencial en la era digital actual para la protección de la infraestructura y los datos críticos. Para minimizar los riesgos y proteger los activos, las organizaciones deben conceder ampliamente prioridad a la seguridad a pesar de sus retos. Los riesgos de seguridad cambian infatigablemente y mantenerse actualizado con los estándares de cumplimiento representa nuevos desafíos organizacionales. Para abordar ambos problemas, las organizaciones deben desarrollar políticas de ciberseguridad exhaustivas (Kour y Pierce, 2024)

En tal sentido, el presente proyecto de investigación, aspira generar conocimiento útil y practico, al entorno corporativo organizacional, especialmente a la empresa IEPHE, en el marco de la implementación de la Norma ISO/IEC 27001:2022, lo cual puede ser replicable a otras empresas similares, y se pretende constituir en un referente teórico, practico y metodológico, que puede ser usado para generar aspectos de ciberseguridad a las empresas y originar un marco de confianza en la protección de su información confidencial, lo cual garantiza un impacto efectivo en sus relaciones operativas, financieras y comerciales, beneficiando no solo a la empresa, sus actores, gestores y decisores, sino un amplio conglomerado de grupos de interés como los clientes, acreedores, organismos gremiales laborales y los empresariales, entes del Estado, el sector académico y de investigación universitario y a la sociedad en general.

# CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

## 1.1. Contextualización general del estado del arte

En una investigación que lleva como título, Implementación de la norma ISO/IEC 27001:2022 en una PYME: un estudio de caso con Cyberday, realizada por Nygård (2024), plantea que la actual era digital está amenazada cotidiana y progresivamente, donde las violaciones y filtraciones de datos y el ransomware, suponen un verdadero reto a las organizaciones que prestan consultoría gestionando datos para y de sus clientes. Por consiguiente, la norma ISO/IEC 27001:2022 proporciona un marco global ampliamente reconocido para la construcción de un Sistema de Gestión de Seguridad de la Información (SGSI) con la finalidad de optimizar la salvaguardia de datos, la observancia normativa y la confianza y seguridad de los clientes.

El objetivo de este estudio consistió en investigar la puesta en marcha temprana de la norma ISO/IEC 27001:2022 en una pyme finlandesa de consultoría de Tecnologías de la Información mediante un estudio de caso a través de un enfoque cualitativo. Metodológicamente, el investigador participó proactivamente en el equipo de implementación, enfocándose de manera muy centrada en la alineación operativa con las cláusulas 4 a 10 de la norma. Del mismo modo, el estudio evaluó el rol de la herramienta Cyberday en la mejora del cumplimiento de la norma ISO 27001 por medio de la sistematización de la gestión de riesgos y los procesos documentales, avalando el cumplimiento del RGPD (General Data Protection Regulation, en español Reglamento general de protección de datos)

Los hallazgos del estudio revelan la importancia de una hoja de ruta práctica para que las pymes acometan y empiecen la implementación de la norma ISO 27001 y refuercen la seguridad de la data informativa usando para ello herramientas efectivas. Utilizando Cyberday, la organización consiguió organizar el proceso de implementación, aprovechándose así de un marco debidamente ordenado y constituido para gestionar aspectos relativos a la ciberseguridad, amparar la documentación y monitorear el progreso, ayudando significativamente a la eficiencia y la organización, permitiendo a la corporación dar cumplimiento con los requerimientos de la norma ISO 27001, mientras que simultáneamente reforzaba sus prácticas operativa de seguridad de la información y gestión de riesgos. Como resultado, se obtuvo un desarrollo importante en la alineación de las prácticas institucionales con la norma ISO 27001, particularmente por medio de las funcionalidades de Cyberday, igualmente se evidenció que la organización estableció exitosamente las políticas,

procedimientos y los controles fundamentales, logró realizar auditorías internas, demostrando un compromiso con la mejora continua.

Otro referente estimado como importante para esta investigación, es el estudio titulado Marco de ciberseguridad para las universidades de Kenia de conformidad con la norma ISO/IEC 27001:2022, realizado por Gichubi, et al., (2024), señala que la vertiginosa adopción de la planificación de recursos empresariales (ERP), así como la necesidad de acceso remoto a los sistemas de información y el acelerado desarrollo de tecnologías digitales, tales como la IoT y la computación en la nube, incrementaron de manera exponencial los ciberataques a las organizaciones, incluidas entre estas las universidades. No obstante, aun cuando no son tan atacadas como industrias de mayor relevancia económica y productiva, las universidades se han hecho cada vez más vulnerables en virtud de los sistemas ERP abiertos, la poca inversión en ciberseguridad y la experiencia cibernética restringida y condicionada.

El objetivo general de este estudio fue mejorar la ciberseguridad en las universidades de Kenia a través de la identificación y reconocimiento de amenazas de ciberseguridad, la evaluación de los controles actuales y el ofrecimiento de un marco de ciberseguridad alineado con la norma ISO/IEC 27001:2022.

A nivel metodológico, fue aplicado un instrumento en forma de una encuesta descriptiva para la recolección de los datos cuantitativos, aprovechando las bondades de la Metodología de Investigación de Ciencias del Diseño (DSRM) para investigaciones en el área de sistemas de información. La población objetivo estaba integrada globalmente por 60 universidades kenianas autorizadas, tanto públicas como privadas. El muestreo fue no probabilístico intencional seleccionando a los consultados de cada universidad muestreada, igualmente se apeló al muestreo aleatorio simple eligiendo universidades públicas y privadas. De 48 cuestionarios distribuidos por medio de Google Forms, se recibieron solo 45, evidenciando una tasa de respuesta del 93,75%. Para analizar los datos fueron utilizados parámetros estadísticos como frecuencia, porcentajes, media y desviación estándar, y los hallazgos fueron graficados a través de tablas y figuras.

Los hallazgos evidenciaron que la mayoría de las universidades analizadas sufrieron ciberataques y enfrentaron amenazas significativas de ciberseguridad. Asimismo, muchas universidades no contaban con políticas y controles de ciberseguridad apropiados, así como medidas corporativas, humanas, físicas y tecnológicas. Fue evaluado el marco de ciberseguridad planteado y se consideró conveniente para atenuar los riesgos de ciberseguridad en las

universidades kenianas. El estudio recomienda adelantar más investigaciones comparativas entre universidades kenianas e instituciones de otros países para la identificación y adaptación de mejores prácticas al entorno keniano.

Esta investigación provee información tanto valiosa como significativa para quienes están responsabilizados de formular políticas públicas, los administradores y los profesionales de la ciberseguridad que procuran optimizar las prácticas de seguridad en el sector universitario. Un reto importante que afrontó el desarrollo del estudio fue garantizar el anonimato de los encuestados con miras a recabar opiniones fidedignas. El estudio concluye que, las crecientes amenazas cibernéticas destacan la imperiosa necesidad de construir y poner en marcha un marco de ciberseguridad consistente y concreto para cada universidad, ajustado a sus requerimientos específicos de las universidades de Kenia para proteger los activos digitales efectivamente.

Una investigación liderada por Mahfud, et al., (2024), titulada Diseño de la gestión de riesgos de seguridad de la información basado en las normas ISO/IEC 27005:2022, ISO/IEC 27001:2022 y NIST SP 800-53 Revisión 5 (Estudio de caso en la Agencia ABC), resalta que a medida que las ciudades inteligentes surgen globalmente, XYZ Regency avanza en su iniciativa Smart City mediante seis dimensiones, entre las cuales se incluye la gobernanza inteligente, a través del desarrollo de un sistema de gobierno electrónico (SPBE). Las prioridades clave en esta iniciativa comprenden la gestión de riesgos y de la seguridad de la información. La Agencia ABC, tiene la responsabilidad de la seguridad de la información, y hasta los momentos del desarrollo del estudio, enfrentó ciberataques como virus y piratería, y el dominio de gestión fue evaluado con el puntaje más bajo entre otros dominios en el año correspondiente a la evaluación SPBE 2023, lo cual evidencia forzosamente la necesidad de una apropiada y suficiente gestión de riesgos de seguridad de la información.

Metodológicamente, el estudio diseña una gestión de riesgos de seguridad de la información basada en ISO/IEC 27005:2022 seleccionado medidas de control de ISO/IEC 27001:2022 y NIST SP 800–53 en su Revisión 5. El análisis identificó 102 escenarios de riesgo con categorías en niveles alto, medio, bajo y muy bajo. Los riesgos altos y medios son clasificados como inaceptables, pero los riesgos bajos y muy bajos son aceptables. De los 102 riesgos, 27 fueron aceptados, pero 75 fueron inaceptables, y a estos se les implementó modificaciones a través de recomendaciones de control. El estudio concluye proponiendo 19 recomendaciones de control con la finalidad de optimizar la gestión de riesgos de seguridad en la Agencia ABC y se aspira que mejoren el índice SPBE y refuercen la seguridad de la data informativa general de la agencia.

Una investigación titulada Análisis de la implementación del sistema de gestión de seguridad de la información en BSN, llevada a cabo por Puspo-Arianty, (2025), relata que la norma SNI ISO/IEC 27001:2013, que fue adoptada por la Agencia Nacional de Normalización de Indonesia (BSN), es una norma nacional procedente de la norma internacional ISO/IEC 27001 divulgada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

El estudio tuvo como objetivo evaluar la eficacia de la puesta en marcha del sistema de gestión de seguridad de la información (SGSI) de BSN, enfocándose principalmente en la observancia de las normas internacionales, las estrategias de gestión de riesgos y el compromiso institucional para salvaguardar la información.

A nivel metodológico, el estudio se concibió como una investigación descriptiva cualitativa enfocada en un estudio de caso ejecutado en la Agencia Nacional de Normalización (BSN), permitiendo al investigador comprender a profundidad la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en BSN y su entorno subyacente. El método de investigación descriptiva cualitativa consiste en indagar un objeto, una situación, un grupo de personas u otros fenómenos en su ambiente natural o real (sin asumir un trasfondo experimental) para facilitar una descripción puntual, sistemática y minuciosa. Este estudio se llevó a cabo en BSN en un lapso de tiempo de tres meses, el cual inició en el mes de octubre de 2024 y concluyó en el mes de diciembre del mismo año. La elección de la ubicación es significativa en virtud del papel primordial de BSN en la estandarización y la ejecución de políticas de seguridad de la información en Indonesia. Los datos fueron recolectados a través de entrevistas, análisis de documentos y observaciones en sitio.

Los hallazgos más importantes revelan el papel primordial del compromiso del liderazgo, las evaluaciones integrales de riesgos y las evaluaciones periódicas del sistema para alcanzar los objetivos del SGSI. Sin embargo, a pesar de los logros significativos, implícita la obtención de la certificación del Sistema de Gestión Integrado en el año 2023, aun a la fecha del estudio persisten los retos para mejorar los recursos y ajustares a las amenazas de seguridad emergentes.

Las recomendaciones apuntan a las mejoras de las competencias digitales y de ciberseguridad del talento humano de la organización, realizar inversiones en tecnologías avanzadas y comenzar la transición hacia la norma SNI ISO/IEC 27001:2022 en su última versión. El estudio

fortalece la relevancia del SGSI para la protección de la información confidencial, promover la confianza y alinearse con las mejores prácticas globales en la materia de ciberseguridad.

Un estudio titulado Requisitos de ciberseguridad para sistemas de control de maquinaria industrial realizado por Kasprzyczak, et al., (2025), refiere que la ciberseguridad efectiva y eficiente de los sistemas industriales precisa de la contribución conjunta tanto de los fabricantes de las maquinarias como de sus usuarios. El acceso remoto digital, así como la supervisión de contraseñas no son ni deben constituir simplemente una casualidad, debido a que la omisión o descuido puede llegar a generar el surgimiento de ciberataques, que, a modo de ejemplo, pueden ser exempleados internos como de los mismos fabricantes, igualmente de fuentes externas perniciosas.

El estudio señala que los ciberataques están asociados especialmente a ataques a vía Internet; pero, igualmente pueden ser debido a una infección involuntaria del sistema a través de la conexión de un soporte de datos infectado por virus, o como como una memoria USB portátil, o quizás el sabotaje premeditado vinculado al acceso sin restricciones por parte de un colaborador de la organización a punto de conexión programables en las líneas productivas.

El estudio plantea como objetivos de investigación analizar y profundizar en materia del desarrollo de la Industria 4.0 y la progresiva importancia del IoT, que conlleva novedosos desafíos en términos de ciberseguridad. Del mismo modo evalúa las ciberamenazas y la necesidad de incrementar cada vez más el nivel de protección en los sistemas de control de máquinas, que son esencialmente sensibles a los ataques en virtud de su conexión a Internet. De modo que el objetivo se centra en analizar los requerimientos de los niveles de seguridad (SL) y la puesta en marcha efectivamente de los estándares internacionales adecuados y oportunos.

El estudio presenta como resultados y a la vez conclusiones una especie de planteamiento que vincule los niveles de seguridad de las funciones de seguridad con los niveles de seguridad. Se suministraron siete ejemplos verdejamente representativos de diversas máquinas y funciones de seguridad puestas en marcha en sus sistemas de control. El análisis evidenció los niveles de ciberseguridad SL-T demandados para cada función específica de seguridad. Posteriormente, sugiere como conclusión, resultado y a la vez recomendación que deben implementarse a la brevedad posible, hardware, software y métodos convenientes para alcanzar los niveles SL-A adecuados de acuerdo al SL-T requerido. Igualmente aclara como resultado a la organización que, los objetivos de ciberseguridad nunca deben entrar en conflicto

ni en competencia con los sistemas de control asociados con la seguridad y la eficiencia de la producción. Se recomiendan auditorías periódicas concernientes con la eficacia de las medidas de seguridad implementadas. Las contramedidas contra los ciberataques deben ser auditadas según sea necesario y de acuerdo con las circunstancias, si fuese necesario, pueden realizarse ciberataques controlados para la detección de las vulnerabilidades de seguridad presentes en la organización.

Una vez analizados todos estos referentes considerados como parte del Estado del arte en el marco del estado actual del conocimiento en el tema objeto de estudio, es preciso acotar que estos estudios constituyen valiosos aportes tanto para la construcción de la perspectiva teórica del estudio, como metodológicos. En aspectos teóricos estos referentes estudian a profundidad el tema de la ciberseguridad y la importancia para las organizaciones actuales altamente abiertas e interconectadas, el riesgo y la vulnerabilidad ante los ciberatacantes que cada vez refinan sus estrategias para vulnerar sistemas y apropiarse de datos con fines manipulativos. Igualmente abordan las normativas para minimizar estos riesgos, especialmente la Norma ISO/IEC 27001:2022, Como referentes a nivel metodológico proponen rutas de acción para minimizar esta realidad y fortalecer las estrategias organizacionales para reforzar la seguridad interna de los sistemas de información.

### 1.2. Proceso investigativo metodológico

El enfoque, tipo y diseño de la investigación se concibe desde una perspectiva cuantitativa, de tipo descriptiva y explicativo, con un fuerte respaldo documental y estudio de campo. Los métodos cuantitativos de acuerdo a la opinión de autores como Hernández, et al., (2014), incorporan una serie de procesos metódicos, prácticos y críticos de investigación “e implican la recolección y el análisis de datos cuantitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio” (p. 534). En cuanto al enfoque cuantitativo**,** se usarían datos numéricos para evaluar el nivel de vulnerabilidades en los sistemas, el cumplimiento de normas de ciberseguridad, y los costos asociados con riesgos y amenazas. Por ejemplo, la cantidad de incidentes de seguridad previos o el porcentaje de cumplimiento con las normativas de ISO 27001:2022. Aquí, se podría explorar la cultura organizacional hacia la seguridad de la información y las percepciones sobre los riesgos cibernéticos.

En consecuencia, el presente estudio desde su concepción seria cuantitativa se caracterizará por obtener y contar con una perspectiva de mayor amplitud y profundidad, y de una mayor y

extensa teorización sobre el tema objeto de estudio, los datos recolectados a través de la visión conjunta cuantitativa serán más enriquecedores y diversamente variados, más creativos y derivados de búsquedas dinámicas, concediendo al estudio una rigurosidad científica sólida producto de una óptima exploración y aprovechamiento de los datos recabados.

La investigación, igualmente asume una visión descriptiva y explicativa**.** Conceptualmente una investigación descriptiva se define como aquella que "consiste en la caracterización de un hecho, fenómeno, individuo, grupo con el fin de conocer su estructura o comportamiento" (Arias, 2016, p. 24). A este respecto, el objetivo inicial de esta investigación sería describir el estado actual de la ciberseguridad en la empresa IEPHE, identificando y caracterizando los riesgos, las vulnerabilidades y los procesos de gestión existentes. También se describirían los aspectos relacionados con la normativa ISO 27001:2022, cómo se aplica o se está implementando, y su efectividad en la protección de la información. Como investigación explicativa, pretende:

Buscar el porqué de los hechos mediante el establecimiento de relaciones causa-efecto. En este sentido, los estudios explicativos pueden ocuparse tanto en la determinación de las causas (investigación post facto), como de los efectos (investigación experimental). Sus resultados y conclusiones constituyen el nivel más profundo de conocimientos (Arias, 2016, p. 26).

Por consiguiente, como estudió explicativo, se buscaría explicar las causas y los factores que influyen en la situación actual de la ciberseguridad de la empresa. Por ejemplo, ¿por qué no se han implementado de manera eficaz las políticas de seguridad? ¿Qué barreras existen? ¿Cómo afectan los procesos internos y la cultura organizacional a la implementación de la norma ISO 27001:2022?

### 1.3 Población y Muestra

La población global a considerar para alcanzar los objetivos del estudio estará conformada por todos los actores, gestores y decisores involucrados en los procesos de ciberseguridad dentro de la empresa IEPHE. Esto incluye al siguiente talento humano de la organización:

- Personal de Tecnología.
- Directivos y responsables de la gestión de riesgos.
- Empleados que interactúan con los sistemas y gestionan información sensible.

En cuanto a la muestra está se seleccionará utilizando el muestreo estadístico no probabilístico intencional y por conveniencia. Estos muestreos se definen de la siguiente manera

Intencional: Permite seleccionar casos característicos de una población limitando la muestra sólo a estos casos. Se utiliza en escenarios en las que la población es muy variable y consiguientemente la muestra es muy pequeña. Por conveniencia: Permite seleccionar aquellos casos accesibles que acepten ser incluidos. Esto, fundamentado en la conveniente accesibilidad y proximidad de los sujetos para el investigador (Otzen & Manterola, 2017, pg. 230).

La muestra se seleccionó de forma estratégica, asegurando que se incluya una representación adecuada de cada grupo relevante. Para ello se consideraron:

- 2 empleados clave del área de Tecnología.
- 2 directivos que toman decisiones sobre la ciberseguridad.
- 7 empleados de distintas áreas para obtener una visión diversa de la cultura organizacional en relación con la seguridad de la información.

**1.4 Métodos, Técnicas e Instrumentos de recolección de la información**

En virtud de la característica cuantitativa del estudio, se implementarán los siguientes métodos, técnicas e instrumentos para la recolección de la información

- **Métodos:**
    - **Método cuantitativo:** Análisis estadístico de datos, por ejemplo: se pueden utilizar cuestionarios para medir el nivel de conocimiento sobre la norma ISO 27001:2022 entre los empleados, directivos y evaluar la cantidad de incidentes de seguridad ocurridos a lo largo de un período determinado.
- **Técnicas:**
    - **Encuesta estructurada**: El diagnóstico acerca de los aspectos generales preliminares la normativa ISO 27001:2022 sobre las políticas de ciberseguridad de las empresas se realizarán mediante una encuesta estructurada, la cual se aplicará a los involucrados de la empresa IPEHE (Ver encuesta en anexo 1).
- **Instrumentos:**
    - **Cuestionarios de autoevaluación de la ISO 27001:2022.** Instrumentos que permitan a la empresa medir su nivel de cumplimiento con los requisitos de la nogrma ISO 27001:2022, identificando áreas que requieren mejoras.

- El cuestionario se lo realizara en línea mediante un link, con la herramienta Google From.

## 1.5 Análisis de resultados

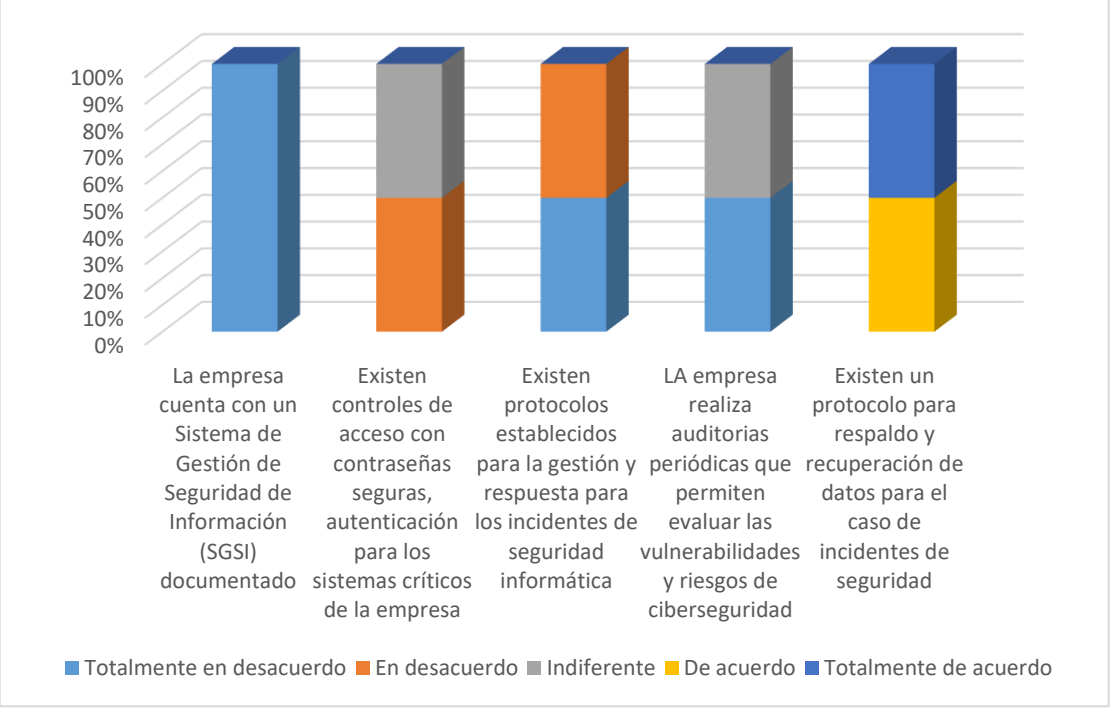
**Tabla 1**

*Resultados de las preguntas para el Personal de Tecnologías de la Información (TI)*

| | Totalmente en desacuerdo | En desacuerdo | Indiferente | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| La empresa cuenta con un Sistema de Gestión de Seguridad de Información (SGSI) documentado | 100% | 0% | 0% | 0% | 0% |
| Existen controles de acceso con contraseñas seguras, autenticación para los sistemas críticos de la empresa | 0% | 50% | 50% | 0% | 0% |
| Existen protocolos establecidos para la gestión y respuesta para los incidentes de seguridad informática | 50% | 50% | 0% | 0% | 0% |
| LA empresa realiza auditorias periódicas que permiten evaluar las vulnerabilidades y riesgos de ciberseguridad | 50% | 0% | 50% | 0% | 0% |
| Existen un protocolo para respaldo y recuperación de datos para el caso de incidentes de seguridad | 0% | 0% | 0% | 50% | 50% |

**Figura 1**

*Resultados de las preguntas para el Personal de Tecnologías de la Información (TI)*



En la tabla 1 y el gráfico 1 se puede observar que el personal de tecnologías de la información existente está completamente en desacuerdo en que la empresa cuenta con un Sistema de Gestión de Seguridad de Información (SGSI) documentado, es decir que se verifica la inexistencia de este sistema, con el respectivo riesgo que esto conlleva.

Por su parte al preguntar al personal especializado si existen controles de acceso con contraseñas seguras, autenticación para los sistemas críticos de la empresa existe duda, es decir un 50% considera estar en desacuerdo y un 50% es indiferente, es decir que mayormente no existe un control claro y un sistema establecido, pero existen ciertos controles que pueden no ser lo suficientes o lograr un adecuado control.

Al consultar sobre la existencia de protocolos establecidos para dar respuesta a los incidentes informáticos el personal está en desacuerdo o totalmente en desacuerdo en que existan estos protocolos. Al consultar si existen auditorías periódicas mencionan estar totalmente en desacuerdo o indiferentes, es decir que no conocen sobre su aplicación o control.

Finalmente, al consultar sobre la existencia de un respaldo para la recuperación de datos para el caso de incidentes de seguridad, están de acuerdo o completamente de acuerdo, es decir que este aspecto sí está cubierto por la empresa para evitar la pérdida de información.

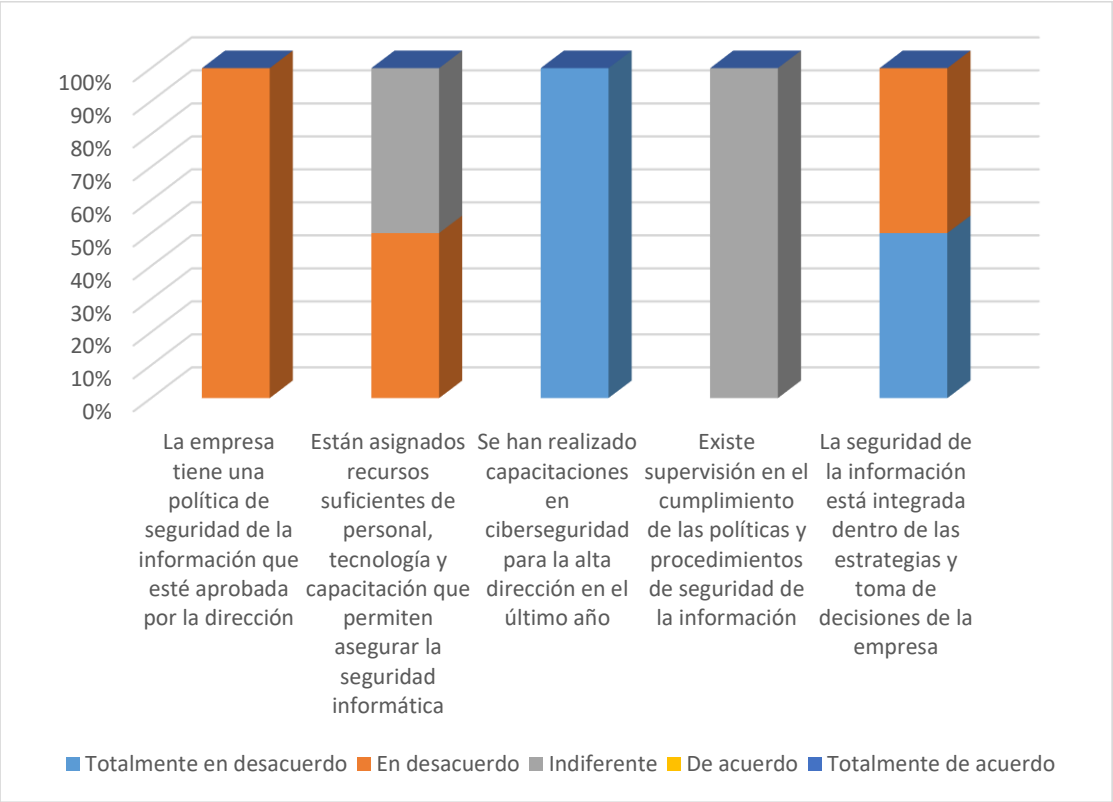
**Tabla 2**

*Resultados de las Preguntas para Directivos*

| | **Totalmente en desacuerdo** | **En desacuerdo** | **Indiferente** | **De acuerdo** | **Totalmente de acuerdo** |
|---|---|---|---|---|---|
| La empresa tiene una política de seguridad de la información que esté aprobada por la dirección | 0% | 100% | 0% | 0% | 0% |
| Están asignados recursos suficientes de personal, tecnología y capacitación que permiten asegurar la seguridad informática | 0% | 50% | 50% | 0% | 0% |
| Se han realizado capacitaciones en ciberseguridad para la alta dirección en el último año | 100% | 0% | 0% | 0% | 0% |
| Existe supervisión en el cumplimiento de las políticas y procedimientos de seguridad de la información | 0% | 0% | 100% | 0% | 0% |
| La seguridad de la información está integrada dentro de las estrategias y toma de decisiones de la empresa | 50% | 50% | 0% | 0% | 0% |

**Figura 2**

*Resultados de las Preguntas para Directivos*




Como se muestra en la tabla 2 y el gráfico 2, los directivos indican estar en desacuerdo en que la empresa tiene definida una política de seguridad de la información que esté aprobada por la dirección. Por otra parte, al consultar si Están asignados recursos suficientes de personal, tecnología y capacitación que permiten asegurar la seguridad informática existen dudas, uno de los ejecutivos menciona estar en desacuerdo y el otro indiferente, es decir que si bien se asignan recursos no son lo suficientes para lograr un control adecuado.

Al consultar si se han realizado capacitaciones en ciberseguridad para la alta dirección en el último año están completamente en desacuerdo el 100% de los encuestados. Por otra parte, al consultar a los directivos si existe supervisión en el cumplimiento de las políticas y procedimientos de seguridad de la información la respuesta es indiferente para el 100% de estos indicando que puede existir algún tipo de control, pero no suficiente o estructurado.

Finalmente están en desacuerdo en que la seguridad de la información está integrada dentro de las estrategias y toma de decisiones de la empresa, siendo un tema que no se lo ha considerado de prioridad estratégica hasta el momento.

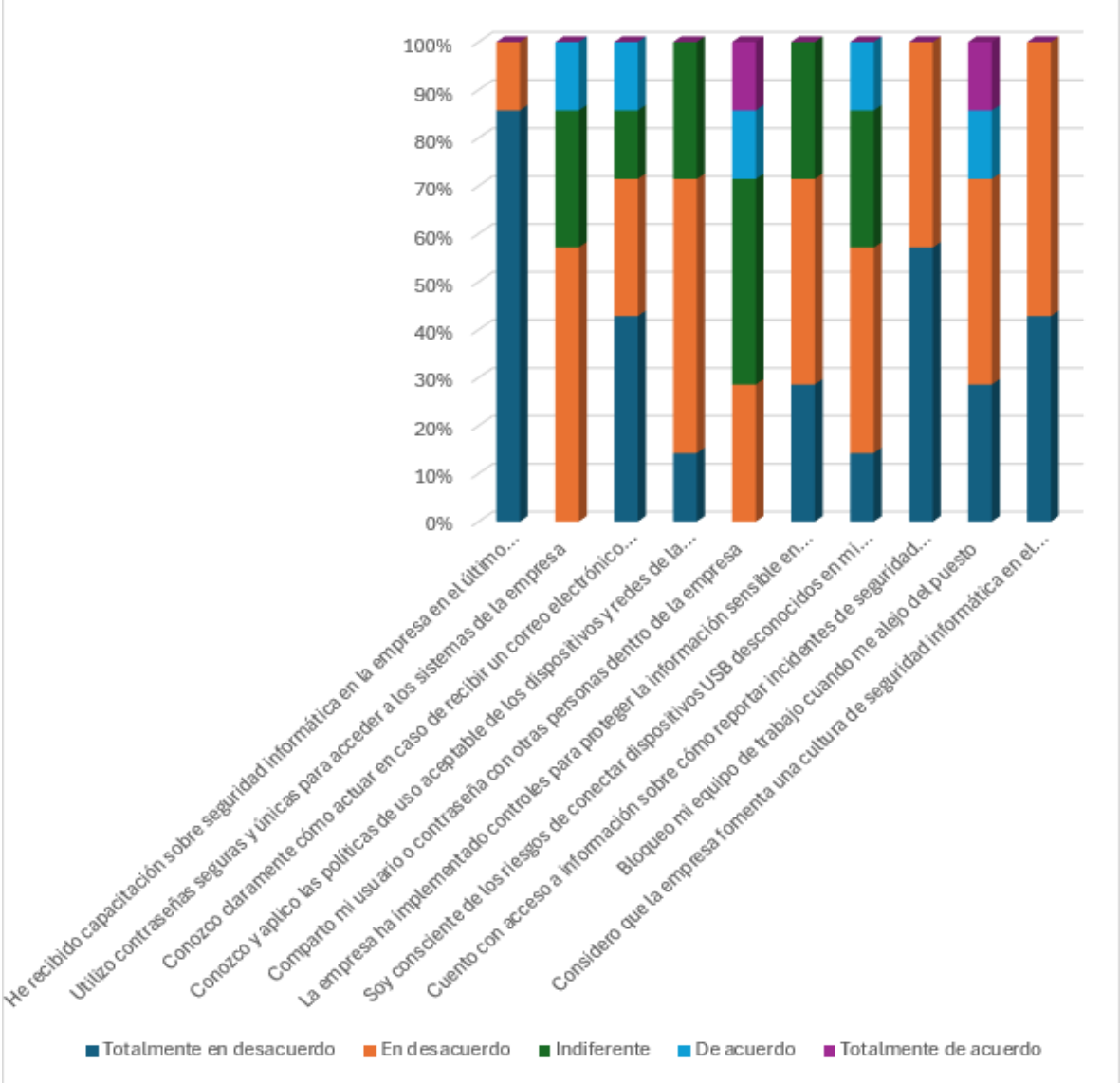
**Tabla 3**

*Resultados de las Preguntas para el Personal General (Diferentes Áreas)*

| | Totalmente en desacuerdo | En desacuerdo | Indiferente | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| He recibido capacitación sobre seguridad informática en la empresa en el último año | 86% | 14% | 0% | 0% | 0% |
| Utilizo contraseñas seguras y únicas para acceder a los sistemas de la empresa | 0% | 57% | 29% | 14% | 0% |
| Conozco claramente cómo actuar en caso de recibir un correo electrónico sospechoso (phishing) | 43% | 29% | 14% | 14% | 0% |
| Conozco y aplico las políticas de uso aceptable de los dispositivos y redes de la empresa | 14% | 57% | 29% | 0% | 0% |
| Comparto mi usuario o contraseña con otras personas dentro de la empresa | 0% | 29% | 43% | 14% | 14% |
| La empresa ha implementado controles para proteger la información sensible en los sistemas que uso | 29% | 43% | 29% | 0% | 0% |
| Soy consciente de los riesgos de conectar dispositivos USB desconocidos en mi equipo de trabajo | 14% | 43% | 29% | 14% | 0% |
| Cuento con acceso a información sobre cómo reportar incidentes de seguridad informática en la empresa | 57% | 43% | 0% | 0% | 0% |
| Bloqueo mi equipo de trabajo cuando me alejo del puesto | 29% | 43% | 0% | 14% | 14% |
| Considero que la empresa fomenta una cultura de seguridad informática en el personal | 43% | 57% | 0% | 0% | 0% |

**Figura 3**

*Resultados de las Preguntas para el Personal General (Diferentes Áreas)*




Al consultar al personal en general de diferentes áreas sobre su punto de vista en la ciberseguridad, se puede observar en la tabla 3 y el gráfico 3 que mayoritariamente el personal está en Total desacuerdo y en desacuerdo con los ítems que les fueron consultados con respecto a la capacitación en materia de ciberseguridad recientemente, tampoco utilizan suficientemente contraseñas seguras y únicas para acceder a los sistemas de la empresa, desconocen con claridad cómo proceder en caso de recibir un correo electrónico sospechoso (phishing), de una manera riesgosa comparten sui usuario o contraseña con otras personas dentro de la empresa, tampoco la empresa ha implementado controles para proteger la información sensible en los

sistemas que usan. Hay una fuerte debilidad en cuanto a la consciencia de los riesgos de conectar dispositivos USB desconocidos en su equipo de trabajo, no cuentan con información sobre cómo reportar incidentes de seguridad informática en la empresa, no boquean su equipo de trabajo al alejarse de su puesto de trabajo, y finalmente no consideran que la empresa promueve una cultura de seguridad informática a nivel del personal en general. en el personal

## CAPÍTULO II: PROPUESTA

### 2.1 Fundamentos teóricos aplicados

La ciberseguridad tiene como finalidad la protección corporativa de los sistemas digitales, las redes y los datos de las organizaciones contra el acceso de personas no autorizadas para ello, su robo con fines inconfesables y fraudulentos o su daño parcial o total. Comprende la puesta en marcha de todas las medidas suficientes y competentes, así como aquellas innovaciones tecnológicas que aseguren tanto la confidencialidad, como la integridad y disponibilidad de toda la información almacenada y procesada en los sistemas de informática de las empresas. Sus aspectos claves más importantes son:

Prevenir: Implementar todas las disposiciones y medidas de seguridad para impedir y en lo posible minimizar en la medida de lo posible, el acceso no consentido o las infracciones por parte de cibercriminales o personas que, aun perteneciendo a la organización, no están autorizado para este fin.

Detectar: Permite la identificación de posibles amenazas y vulnerabilidades en un sistema informático…

Responder oportunamente: Asumir de manera oportuna de todas las medidas y disposiciones requeridas para mitigar el impacto de un incidente o delito informático que amenace la seguridad de la información corporativa almacenada en los sistemas de información de una organización (National University, 2025).

En este orden de ideas, se pretende a través de un marco metodológico de puesta en marcha de ciberseguridad corporativa la creación de estrategias consistentes y sólidas para que las organizaciones logren la protección adecuada y oportuna de sus activos digitales, el mantenimiento de la confianza de los clientes y de todos los grupos de interés y el cumplimiento de las regulaciones. Los elementos claves fundamentales y esenciales que se pretende con una estrategia de ciberseguridad exitosa son los siguientes que de acuerdo a la National Universito (2025) son los siguientes:

Evaluar los riesgos: Permite la comprensión de los riesgos corporativos, como el fundamento una estrategia de ciberseguridad sólida. Desde esta perspectiva, se identifican las posibles amenazas, vulnerabilidades y el potencial impacto del cibercrimen en la organización, permitiendo priorizar la energía, esfuerzos y asignación de recursos eficazmente.

Políticas y procedimientos de seguridad: Permite el desarrollo de políticas y procedimientos de seguridad precisos, claros e integrales que puntualicen las funciones y responsabilidades de los colaboradores, el uso aceptable y razonable de la tecnología y de las gestiones a seguir en caso de presentarse un incidente de seguridad. Por ello, las revisiones de estas medidas deben ser actualizadas continuamente para incorporar los cambios en la tecnología y el panorama de nuevas amenazas.

Seguridad de red y de puntos finales: Favorece la aplicación de medidas de seguridad sólidas de red y de puntos finales, donde se incluyan firewalls, sistemas de detección y prevención de intrusiones, software antimalware y acceso seguro a Wi-Fi. Igualmente deben ser actualizadas continuamente para abordar y afrontar las vulnerabilidades conocidas.

Controles de acceso: El establecimiento de controles de acceso rigurosos para restringir el acceso a datos y sistemas confidenciales. Por ello es forzoso y necesario la implementación de controles de acceso establecidos en roles, autenticación multi factor y auditorías constantes de los privilegios de los usuarios para disminuir el riesgo de acceso no autorizado.

Cifrado de datos confidenciales en reposo y en tránsito para que sean protegidos del acceso no autorizado y posibles violaciones, agregando así otra capa de seguridad, dificultando que los cibercriminales accedan a la información corporativa confidencial.

Desarrollo de un plan de respuesta a incidentes bien definido que describa los pasos a seguir por la organización en caso de una violación de seguridad, el cual debe contemplar de manera suficiente todos los protocolos de comunicación claros, roles y compromisos, y normas para la reparación y recuperación.

Gestión de riesgos de terceros que favorezca la evaluación de la postura de ciberseguridad de sus proveedores y socios externos, en virtud de que estos pueden introducir vulnerabilidades a la seguridad corporativa, donde se contemplen todos los requisitos de seguridad estrictos para terceros y la revisión periódica de su cumplimiento.

Incorporando estos elementos clave en la estrategia corporativa de ciberseguridad, cualquier organización estará debidamente equipada para una exitosa protección de los activos digitales, salvaguardar la confianza de los clientes y disminuir el riesgo de incidentes de seguridad costosos. En este sentido, la norma ISO/IEC 27001:2022 para sistemas de gestión de la seguridad de la información (SGSI), establece los requerimientos a cumplir por un SGSI. Suministra a las organizaciones no importando sus dimensiones y de cualquier sector todos los lineamientos

para el establecimiento, implantación, mantenimiento y mejora continua de un SGSI. La conformidad con la ISO/IEC 27001 significa que una organización ha establecido un sistema para gestionar los riesgos vinculados con la seguridad de los datos con los que cuenta o gestiona, y que dicho sistema acata todas las buenas prácticas y principios establecidos en la Norma Internacional ISO/IEC 27001:2022 (International Organization for Standardization, 2022)

## 2.2 Descripción de la propuesta

La propuesta contempla una guía para la implementación de políticas y protocolos sólidos de ciberseguridad basados en la Norma ISO/IEC27001:2022 para la Empresa IEPHE con la finalidad de proveer y suministrar un enfoque completo de la seguridad de toda la información almacenada en su sistema informático, abarcando a todos y cada uno los grupos de interés corporativos, las políticas, procedimientos y la tecnología necesaria para ello. Por tanto, la propuesta derivará en un SGSI, puesto en marcha acorde a la norma *in comento* como un instrumento clave para gestionar riesgos, la resiliencia cibernética y la calidad operativa (International Organization for Standardization, 2022).

Las ventajas y beneficios de la propuesta para la Empresa IEPHE son potencialmente los siguientes

Resistencia y severidad contra los ciberataques

Preparación y previsión corporativa ante nuevas amenazas de los cibercriminales

Integridad, confidencialidad, seguridad y disponibilidad de la información sobre los activos digitales almacenada corporativamente en los sistemas informáticos

Seguridad sostenida en la totalidad de los soportes de la organización

Protección total para la organización

Ahorro de costos ante posibles ataques a la información corporativa (International Organization for Standardization, 2022)

Esta propuesta está fundamentada en una orientación sistemática que abarca el diagnóstico del estado actual de la seguridad de la información corporativa, la determinación de políticas y controles de seguridad, la puesta en marcha del Sistema de Gestión de Seguridad de la Información (SGSI) y la evaluación permanente a través de indicadores de desempeño y auditorías internas, contemplados en una guía que permitirá a la Empresa IEPHE la gestión eficiente y eficaz de sus riesgos de ciberseguridad, salvaguardando la información confidencial

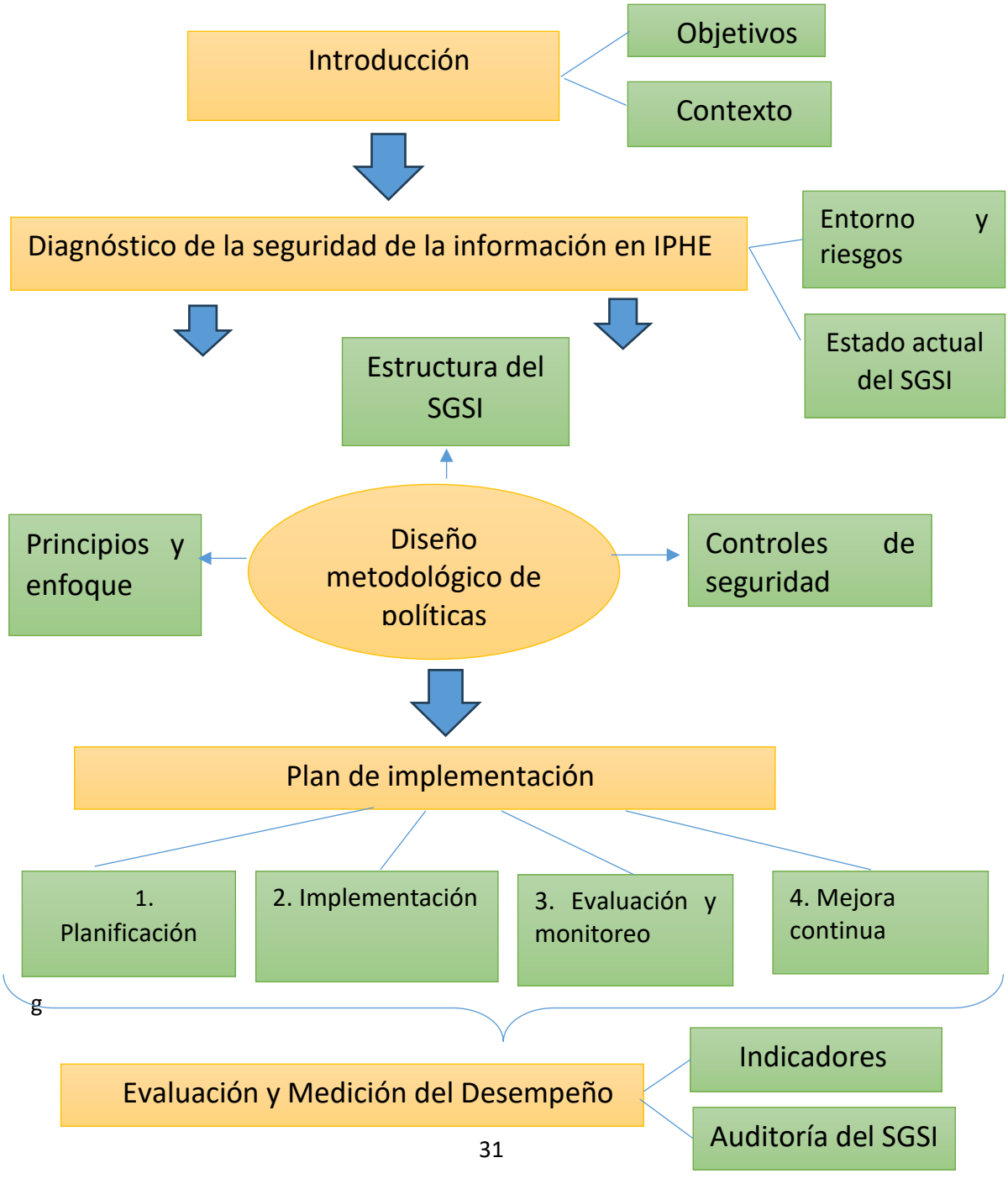
importante y prometiendo la continuidad operativa. El enfoque asumido se fundamenta en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar), garantizando la mejora continua del SGSI y la adaptabilidad de las políticas a los requerimientos concretos de la Empresa IEPHE.

**a. Estructura general**

La estructura de la aplicación de la norma para la empresa deberá seguir el esquema:

**Figura 4**

*Estructura de la aplicación de la norma para IEPHE*



La estructura para la aplicación de la norma se inicia con el desarrollo del contexto y objetivos de ciberseguridad para la empresa. Con esta introducción para una aplicación exitosa se realiza un diagnóstico de la seguridad de la información en la empresa, considerando el entorno y los riesgos que se han detectado en función de un análisis profundo de los potenciales riesgos de seguridad informática que se podrían presentar. Adicionalmente se realizará una evaluación en base al SGSI en el que se determine qué aspectos se han considerado previamente o ya estén avanzados en relación con el sistema de gestión. Con este diagnóstico se estructura la metodología de aplicación y políticas de ciberseguridad en la empresa, dentro de este sistema se estructuran los principios y enfoque al que se quiere llegar, se sigue la estructura del SGSI y se establecen los protocolos de seguridad con sus respectivos controles permanentes.

Una vez estructurado el modelo, estructura y documentación del sistema se debe implementar el mismo, donde estarán integrados la planificación, implementación misma y una evaluación y monitoreo continuo para garantizar la aplicación y los ajustes que se requiere. Finalmente, aunque ya implementado el sistema es necesario un seguimiento de mejora continua que permite eliminar problemas e ir logrando un mejoramiento permanente. Todo el proceso debe evaluarse mediante indicadores de desempeño y una auditoría para garantizar el cumplimiento.

La guía para el desarrollo de políticas de ciberseguridad en la empresa IEPHE, alineado con la norma ISO/IEC 27001:2022 se presenta en el Anexo 2 y la descripción de la misma en el Anexo 3.

**a) Explicación del aporte**

Los aportes corporativos de la implementación de la norma ISO/IEC 27001:2022 genera a la Empresa IEPHE beneficios y ventajas para la empresa. Entre estos beneficios se cuentan los siguientes:

Provee una guía tecnológica que brinda seguridad y protección a la información clave, disminuyendo y gestionando aquellas circunstancias vulnerables de la entidad ante violaciones de los mismos por personas autorizada o no, así como de ciberataques. Del mismo modo, permite la observancia de normas legales vinculadas con la seguridad de la información contenida en los sistemas corporativos, generando ahorros por multas y sanciones, y de minimizando problemas legales derivadas de la violación de los datos corporativos. Igualmente, optimiza la gestión de riesgos identificando, evaluando y moderando los riesgos que afronta la

información de la empresa. Todos estos beneficios permiten acrecentar no solo la confianza y seguridad de los clientes sino del resto de todos los grupos de interés

La implementación de la norma ISO/IEC 27001:2022, favorece la eficacia y eficiencia operativa, acelerando los procedimientos y procesos de protección y seguridad de los datos, lo cual termina generando una significativa Ventaja competitiva que diferenciará a la Empresa IEPHE del resto de las empresas del sector en el mercado. Favorece la permanencia y subsistencia del negocio, la concienciación de la fuerza laboral, favorece el reconocimiento mundial del negocio a través del estándar de la norma, proveyendo la confianza y reconocimiento de la Empresa a nivel mundial. Conjuntamente, permite dinámicamente la mejora continua del sistema de seguridad de la información ante un mundo cambiante que amenaza cada vez más a los negocios.

**b) Estrategias y/o técnicas**

En la creación de un producto contentivo con estrategias y/o técnicas empleadas en una guía completa de políticas clave de ciberseguridad basada en la norma ISO/IEC 27001:2022 se utilizan diversos procedimientos que se describen a continuación, para ello se consultó y se fundamentó en las siguientes fuentes:

- Implementation Guide ISO/IEC 27001:2022 - DISC InfoSec blog, (ISACA Germany Chapter, 2022)
- ISO 27001:2022: Your Comprehensive Implementation Guide, (ISMS Policiy Generator , 2024)
- ISO/IEC 27001:2022 Information Security Your implementation guide – BSI, (BSI Group, 2025)

Pasos, procedimientos y estrategias usados

1. Comprensión de la norma ISO/IEC 27001:2022, considerando para ello la descripción de la norma ISO/IEC 27001:2022 como una herramienta global para sistemas de gestión de seguridad de la información (SGSI). Lo cual suministró una cosmovisión sistemática e integral para la gestión de la información privada de la empresa, con miras a garantizar su seguridad.
2. Análisis y evaluación del ecosistema organizacional, con lo cual se pretendió vislumbrar los factores tanto internos como externos con potencial de afectar la seguridad de la

información confidencial corporativa, considerando, para ello, identificar plenamente los diferentes grupos de interés, sus requerimientos, así como los objetivos estratégicos organizacionales

3. Valoración rigurosa de los diferentes riesgos representados por potenciales amenazas y debilidades, priorizando así las medidas suficientes y competentes en materia de seguridad de la información.

4. Formulación del proyecto con su respectivo alcance, cronograma de actividades y recursos humanos y financieros a ser utilizados. Parta ello debe definirse claramente el alcance del SGSI (límites y viabilidad de la aplicación de las políticas, asegurando la cobertura de cada área importante e involucrada.

5. Creación del marco conceptual y documentación del SGSI donde se contemplen políticas, procesos, procedimientos y controles, (alineados directamente con los objetivos estratégicos mercantiles de la empresa) y la estrategia para gestionar los riesgos.

6. Desarrollo de políticas claves de ciberseguridad corporativa que contemplen los riesgos identificados y que cumplan con los requisitos establecidos en la norma ISO/IEC 27001:2022, con miras a dar cobertura al control de acceso, la salvaguardia de los datos, y la respuesta a acontecimientos y al negocio en marcha.

7. Selección e implementación de controles de seguridad apropiados y acordes al Anexo A de la norma ISO/IEC 27001:2022, por tanto, deben tomar en cuenta los riesgos reconocidos e identificados y proteger los objetivos de seguridad corporativos. Lo cual puede incluir disposiciones medidas técnicas, como por ejemplo el cifrado de datos y programas de capacitación y concienciación organizacional.

8. Establecer una organización o estructura para gestionar la seguridad de la información, incluyendo los roles, compromisos, contemplar y determinar las métricas de desempeño y llevar a cabo monitoreos continuos.

9. Desarrollar procesos para gestionar el abordaje de incidentes, que permitan la detección, y la respuesta necesaria para recobrarse de los incidentes que afecten la seguridad, incluyendo reportes oportunos de incidentes, indagación y acciones correctivas.

10. Implicar a todo el liderazgo estratégico corporativo para apoyar el SGSI, asignado los recursos requeridos y promover la cultura de seguridad corporativa

11. Garantizar la asignación de recursos humanos, financieros y tecnológicos apropiados que estén a la disponibilidad para la implementación y mantenimiento del SGSI.
12. Realizar auditorías internas periódicas con la finalidad de la evaluación de la eficiencia del SGSI, ubicando las áreas a mejorar
13. Trabajar conjuntamente con un ente de certificación para obtener la certificación ISO/IEC 27001:2022.
14. Revisión y actualización permanente de políticas que garanticen su continua efectividad y relevancia.

### 2.3 Validación de la propuesta

La validación de la guía para el desarrollo de políticas de ciberseguridad en la empresa IEPHE se ha realizado mediante expertos, para ello se utilizó el formato de validación en el que se integran:

- Introducción a la validación
- Datos del validador especialista
- Instructivo de validación
- Indicadores de evaluación de la guía con valoración mediante escala de Likert
- Observaciones y recomendaciones abiertas para el validador.

En el anexo 4 se presenta los resultados de la validación realizada a los especialistas.

### 2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

***Tabla 4***

*Matriz de articulación*

| EJES O PARTES PRINCIPALES | SUSTENTO TEÓRICO | SUSTENTO METODOLÓGICO | ESTRATEGIAS / TÉCNICAS | DESCRIPCIÓN DE RESULTADOS | INSTRUMENTOS APLICADOS |
|---|---|---|---|---|---|
| **Contexto y Justificación** | - Importancia de la ciberseguridad (Novikava, 2024; Eid-Almanaseer & Matrouk-Aloun, 2023). | - Revisión documental ciberseguridad normativa ISO/IEC 27001:2022. | - Identificación de amenazas y vulnerabilidades | - La ciberseguridad es muy importante para la protección de la información crítica | - Revisión de literatura<br>Y normativa internacional. |
| **Análisis del Entorno y Riesgos** | - Evaluación de riesgos y vulnerabilidades en la empresa IEPHE (National University, 2025). | - análisis de datos cuantitativos<br>Análisis de campo (encuestas) | - Identificación de amenazas y vulnerabilidades en el entorno de la empresa. | - Diagnóstico establecido de los riesgos de ciberseguridad en IEPHE. | - Encuestas en línea mediante Google Forms. |

| | | | | | |
|---|---|---|---|---|---|
| **Evaluación del Estado Actual del SGSI** | - Norma ISO/IEC 27001:2022 (ISO/IEC, 2022). | - Análisis comparativo (estado actual de IEPHE y requisitos de la norma ISO 27001. | - Evaluación de controles de seguridad existentes<br>Identificación de brechas con el SGSI. | - La empresa IEPHE no cuenta con un SGSI documentado<br>Existen importantes debilidades en la gestión de la seguridad de los datos. | - Cuestionarios de autoevaluación ISO 27001:2022. |
| **Principios y Enfoque del Marco Metodológico** | - Ciclo PHVA (International Organization for Standardization, 2022). | - Enfoque sistemático basado (ciclo PHVA) | - Aplicación del ciclo PHVA para garantizar la mejora continua del SGSI. | - Determinación del marco metodológico que facilite la implementación de políticas y procedimientos de ciberseguridad. | - Guía de implementación de políticas de ciberseguridad basada en la norma ISO/IEC 27001:2022. |
| **Estructura del Sistema de Gestión de Seguridad de la Información (SGSI)** | - Norma ISO/IEC 27001:2022 (ISO/IEC, 2022). | - Desarrollo de políticas, procedimientos y controles de seguridad (norma ISO/IEC 27001:2022). | - Definición de roles y responsabilidades- Desarrollo de políticas de seguridad - Procedimientos para la gestión de riesgos. | - Desarrollo de la estructura del el SGSI aplicado a la empresa (políticas, procedimientos, controles) | - Documentación del SGSI<br>– políticas<br>-procedimientos. |
| **Controles de Seguridad Basados en la ISO/IEC 27001:2022** | - Controles de seguridad del Anexo de la norma (International Organization for Standardization, 2022). | - Propositivo (controles de seguridad) | - Aplicación de controles organizativos, físicos y humanos. | - Implementación de los controles de seguridad para disminuir los riesgos de la información de IEPHE. | - Documentación del SGSI. |
| **Contexto y Justificación** | - Importancia de la ciberseguridad (Novikava, 2024; Eid-Almanaseer & Matrouk-Aloun, 2023). | - Revisión documental ciberseguridad normativa ISO/IEC 27001:2022. | - Identificación de amenazas y vulnerabilidades | - La ciberseguridad es muy importante para la protección de la información crítica | - Revisión de literatura<br>Y normativa internacional. |
| **Objetivos** | - Norma ISO 2700 (ISO/IEC, 2022). | - Enfoque cuantitativo, explicativo. | - Definición de objetivos en base a la meta a conseguir | - Establecimiento del objetivo que permita la implementación de políticas de ciberseguridad para IEPHE. | - Cuestionarios de autoevaluación ISO 27001:2022. |

## CONCLUSIONES

Analizados los hallazgos de la investigación de campo se evidencia que para el personal de tecnologías de la información existente en la empresa no cuenta con un Sistema de Gestión de Seguridad de Información (SGSI) documentado, incrementando los riesgos de ataques en virtud de esta circunstancia vulnerable. Igualmente, su postura es muy débil con respecto a la existencia de controles de acceso con contraseñas seguras, autenticación para los sistemas críticos de la empresa existe duda, lo mismo sucede con respecto a la existencia de protocolos establecidos para dar respuesta a los incidentes informáticos, a la vez que afirman la inexistencia de auditorías periódicas. Sin embargo, se concluye que existe un respaldo para la recuperación de datos para el caso de incidentes de seguridad, evitando así la pérdida de información.

En cuanto a la opinión del personal directivo consultado, los hallazgos son coherentes con los manifestados por el personal de informático de la empresa, en tal sentido sus opiniones permiten inferir que la empresa no cuenta con una política de seguridad de la información aprobada por la dirección, tampoco consideran que estén asignados recursos suficientes de personal, tecnología y capacitación para garantizar la seguridad informática. Del mismo modo, no se han realizado capacitaciones en ciberseguridad, y por tanto existe una débil supervisión en el cumplimiento de las políticas y procedimientos de seguridad de la información.

La evaluación al personal en general de la empresa permite concluir mayoritariamente que no han recibido capacitación en materia de ciberseguridad recientemente, tampoco utilizan suficientemente contraseñas seguras y únicas para acceder a los sistemas de la empresa, desconocen con claridad cómo proceder en caso de recibir un correo electrónico sospechoso (phishing), de una manera riesgosa comparten su usuario o contraseña con otras personas dentro de la empresa, tampoco la empresa ha implementado controles para proteger la información sensible en los sistemas que usan.

A nivel general, es evidente el riesgo y la vulnerabilidad de la empresa ante ataques y violaciones a la seguridad de la información confidencial por la presencia de debilidades muy significativas en cuanto a las políticas de ciberseguridad corporativa. Igualmente se concluye que las deficiencias en la protección y seguridad corporativa de la información confidencial pueden tener consecuencias importantes para la Empresa objeto de estudio. Por cuanto pueden presentarse fallas de datos por medidas pobres en materia de seguridad dando pie a filtraciones de datos, exponiendo información confidencial referente a clientes, proveedores, registros financieros y propiedad intelectual, resultando en pérdidas financieras y problemas legales.

## RECOMENDACIONES

Es fundamental el desarrollo de la presente propuesta en su totalidad siguiendo la guía propuesta, puesto que de esta manera se podrá asegurar los diferentes procedimientos y se establecerán las políticas para el cumplimiento.

Es muy importante que la empresa fortalezca el cumplimiento de los procedimientos para el buen desempeño de cualquier sistema, en este caso el sistema de gestión de la seguridad informática de la empresa.

Se recomienda a la empresa hacer uso de auditores externos calificados que no solamente cumplan con el requisito, sino que analicen de manera crítica la implementación y con ello puedan aportar al fortalecimiento de la ciberseguridad en IEPHE.

Es muy importante que la ciberseguridad en la empresa sea parte de la cultura organizacional de la misma, siendo este un futuro tema de investigación sobre la cultura existente de la ciberseguridad de la información en la empresa.

**BIBLIOGRAFÍA**


Arias, F. (2016). *El Proyecto de Investigación: Introducción a la metodología científica. 7a Edición.* Caracas: Editorial Episteme.

Basu, S. (18 de January de 2024). *The Financial Impact of Cyber Insecurity on the World Economy*. Recuperado el 6 de Enero de 2025, de https://www.spiceworks.com/it-security/security-general/guest-article/the-financial-impact-of-cyber-insecurity-on-the-world-economy/

BSI Group. (2025). *ISO/IEC 27001:2022 Information Security Your implementation guide*. Recuperado el 7 de Marzo de 2025, de https://www.bsigroup.com/globalassets/localfiles/en-gb/iso-27001/pdf/v2.0_27001_implementation_guide.pdf

Cyber Consultancy Services. (2025). *Top 10 Reasons to Transition Now to ISO 27001:2022 for Enhanced Business Security*. Recuperado el 24 de Febrero de 2025, de https://www.ccsrisk.com/top10-iso27001#:~:text=ISO%2027001%3A2022%20introduces%20new,maintain%20a%20robust%20security%20posture.

Djebbar, F., & Nordströ, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access , 11*, 85315-85332. doi:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10210561

Eid-Almanaseer, S., & Matrouk-Aloun, D. (2023). *Cybersecurity for administrative facilities.* Zarqa University, . DOI:10.13140/RG.2.2.16439.74408.

Federal Bureau of Investigation. (2023). *2023 INTERNET CRIME REPORT.* FBI. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf.

Fox, J. (2025). *Top Cybersecurity Statistics for 2025*. Recuperado el 6 de Enero de 2025, de Cobalt: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025

Gichubi, P., Maake, B., & Chweya, R. (2024). Cybersecurity Framework for Kenyan Universities in Conformity with ISO/IEC 27001:2022 Standard. . *Open Access Library Journal,, 11,* , 1-16. . doi:doi: 10.4236/oalib.1110810.

Hernández, R., Fernández, C., & Baptista, M. d. (2014). *Metodología de la Investigación Sexta Edición.* México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

IBM. (2025). *Cost of a Data Breach Report 2024.* IBM. https://www.ibm.com/reports/data-breach.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022*. Recuperado el 24 de Febrero de 2025, de Information security, cybersecurity and privacy protection — Information security management systems — Requirements: https://www.iso.org/es/norma/27001

ISACA Germany Chapter. (2022). *Implementation Guide ISO/IEC 27001:2022*. Recuperado el 7 de Marzo de 2025, de Practical guide for the implementation of an information security

management system (ISMS) according to ISO/IEC 27001:2022: https://blog.deurainfosec.com/implementation-guide-iso-iec-270012022/

ISMS Policiy Generator . (19 de April de 2024). *ISO 27001:2022: Your Comprehensive Implementation Guide*. Recuperado el 7 de Marzo de 2025, de https://ismspolicygenerator.com/docs/iso-27001-2022-implementation-guide/

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Recuperado el 6 de Enero de 2025, de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en

Kasprzyczak, L., Manowska, A., & D´zwiarek, M. (2025). Cybersecurity Requirements for Industrial Machine Control Systems. *Appl. Sci., 15*(1267), 1-19. doi:https://doi.org/10.3390/app15031267

Kour, M., & Pierce, J. (2024). *Cybersecurity Policies Implementation: A Theoretical Model Based on Process Thinking Perspective. n book: Strengthening Industrial Cybersecurity to Protect Business Intelligence (pp.149-179).* DOI:10.4018/979-8-3693-0839-4.ch007.

Mahfud, A., Hikmah, I., Sunaringtyas, S., & Yulita, T. (2024). Information Security Risk Management Design Based on ISO/IEC 27005:2022, ISO/IEC 27001:2022, and NIST SP 800-53 Revision 5 (A Case Study at ABC Agency). *4th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), Yogyakarta, Indonesia,*, 81-186. doi:doi: 10.1109/ICE3IS62977.2024.10775428.

Michigan Technological University. (2025). *What is Cybersecurity?* Recuperado el 12 de Febrero de 2025, de College of Computing: https://www.mtu.edu/computing/cybersecurity/

National University. (24 de Febrero de 2025). *What is Cybersecurity and Its Importance to Business*. Recuperado el Febrero de 2025, de https://www.nu.edu/blog/what-is-cybersecurity/#:~:text=The%20Growing%20Importance%20of%20Cybersecurity%20for%20Businesses&text=One%20of%20the%20primary%20reasons,records%2C%20and%20proprietary%20intellectual%20property.

Novikava, A. (6 de August de 2024). *Cybersecurity in education: back to school, back to risks*. Recuperado el 12 de Febrero de 2025, de https://nordlayer.com/blog/cybersecurity-challenges-in-education/

Nygård, M. (2024). *Implementing ISO/IEC 27001:2022 in a SME Bachelor's thesis.* Turku University of Applied Sciences. doi:https://www.theseus.fi/bitstream/handle/10024/876470/Nygard_Magdalena.pdf?sequence=2

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *Int. J. Morphol. 35(1)*, 227-232,.

Puspo-Arianty, K. (2025). Analysis of Information Security Management System. *Jurnal Informatika: Jurnal pengembangan IT, 10*(1), 119-129. doi:DOI:10.30591/jpit.v10i1.8211

Sharron, M. (21 de May de 2024). *How to Track ISO 27001 Milestones and Measure Success*. Recuperado el 24 de Febrero de 2025, de ISMS Online: https://www.isms.online/iso-

27001/how-to-track-iso-27001-milestones-and-measure-success/#:~:text=Book%20a%20demo-,Understanding%20the%20Role%20of%20KPIs%20in%20ISO%2027001%20Compliance,meets%20the%20ISO%2027001%20standards.

Statista. (2025). *Estimated cost of cybercrime worldwide 2018-2029 (in trillion U.S. dollars)*. Recuperado el 6 de Enero de 2025, de https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

**ANEXO 1**

**Formato de encuestas**

Preguntas para el **Personal de Tecnologías de la Información (TI)**

| | Totalmente en desacuerdo | En desacuerdo | Indiferente | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| La empresa cuenta con un Sistema de Gestión de Seguridad de Información (SGSI) documentado | | | | | |
| Existen controles de acceso con contraseñas seguras, autenticación para los sistemas críticos de la empresa | | | | | |
| Existen protocolos establecidos para la gestión y respuesta para los incidentes de seguridad informática | | | | | |
| LA empresa realiza auditorias periódicas que permiten evaluar las vulnerabilidades y riesgos de ciberseguridad | | | | | |
| Existen un protocolo para respaldo y recuperación de datos para el caso de incidentes de seguridad | | | | | |

**Preguntas para Directivos**

| | Totalmente en desacuerdo | En desacuerdo | Indiferente | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| La empresa tiene una política de seguridad de la información que esté aprobada por la dirección | | | | | |
| Están asignados recursos suficientes de personal, tecnología y capacitación que permiten asegurar la seguridad informática | | | | | |
| Se han realizado capacitaciones en ciberseguridad para la alta dirección en el último año | | | | | |
| Existe supervisión en el cumplimiento de las políticas y | | | | | |

| | |
|---|---|
| procedimientos de seguridad de la información | |
| La seguridad de la información está integrada dentro de las estrategias y toma de decisiones de la empresa | |

**Preguntas para el Personal General (Diferentes Áreas)**

| | Totalmente en desacuerdo | En desacuerdo | Indiferente | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| He recibido capacitación sobre seguridad informática en la empresa en el último año | | | | | |
| Utilizo contraseñas seguras y únicas para acceder a los sistemas de la empresa | | | | | |
| Conozco claramente cómo actuar en caso de recibir un correo electrónico sospechoso (phishing) | | | | | |
| Conozco y aplico las políticas de uso aceptable de los dispositivos y redes de la empresa | | | | | |
| Comparto mi usuario o contraseña con otras personas dentro de la empresa | | | | | |
| La empresa ha implementado controles para proteger la información sensible en los sistemas que uso | | | | | |
| Soy consciente de los riesgos de conectar dispositivos USB desconocidos en mi equipo de trabajo | | | | | |
| Cuento con acceso a información sobre cómo reportar incidentes de seguridad informática en la empresa | | | | | |
| Bloqueo mi equipo de trabajo cuando me alejo del puesto | | | | | |
| Considero que la empresa fomenta una cultura de seguridad informática en el personal | | | | | |

## ANEXO 2

### Estructura de la propuesta de Guía de Políticas de ciberseguridad

**1. Introducción**

1.1. Contexto y Justificación

1.2. Objetivo General

1.3. Objetivos Específicos

**2. Diagnóstico de la Seguridad de la Información en IEPHE**

2.1. Análisis del Entorno y Riesgos

2.2. Evaluación del Estado Actual del SGSI

**3. Marco Metodológico para la implementación de Políticas y protocolos de Ciberseguridad**

3.1. Principios y Enfoque del Marco Metodológico

3.2. Estructura del Sistema de Gestión de Seguridad de la Información (SGSI)

- Roles y responsabilidades.
- Desarrollo de políticas de seguridad
- Procedimientos para la gestión de riesgos.

3.3. Controles de Seguridad Basados en ISO/IEC 27001:2022

**4. Plan de Implementación de Políticas y Protocolos de Ciberseguridad**

4.1. Etapas de Implementación

1. **Fase 1: Planificación**

Aprobación de la alta dirección.

Definición del alcance y estructura del SGSI.

Priorización de riesgos y recursos.

2. **Fase 2: Implementación**

Aplicación de controles y políticas de seguridad.

Capacitación del personal.

Integración con procesos empresariales.

3. **Fase 3: Evaluación y Monitoreo**

Auditorías internas de seguridad.

Pruebas de respuesta a incidentes.

Evaluación de indicadores clave de desempeño (KPIs).

4. **Fase 4: Mejora Continua**

Ajustes en las políticas y procedimientos.

Actualización de estrategias de seguridad.

## Anexo 3

## Descripción de la Guía de Políticas de ciberseguridad

### 1. Introducción

#### 1.1. Contexto y Justificación

El contexto debe considerar la importancia de la ciberseguridad en la empresa, donde se pueden incluir aspectos como la prevención de ciberataques, además la importancia de favorecer a los diferentes grupos de interés y el cuidado de los datos de la empresa. Aspectos adicionales que se pueden considerar:

- Evitar las violaciones de datos
- Evitar pérdidas financieras
- Cuidar la reputación de la empresa e imagen corporativa.

Adicionalmente se debe justificar la aplicación de la norma ISO/IEC 27001:2022, considerando la claridad y especificidad de la Organización Internacional de Normalización (ISO) la cual entiende y fundamenta este problema mediante sus estándares para alinearse con el escenario cambiante de la seguridad de la información.

Finalmente se puede establecer acerca del impacto de la implementación de políticas de ciberseguridad en la continuidad del negocio, mitigando los riesgos además de considerar potenciales amenazas y vulnerabilidades emergentes, reduciendo el impacto potencial de las violaciones de seguridad **(Cyber Consultancy Services, 2025)**.

#### 1.2. Objetivo General

Se debe establecer los objetivos de la Guía.

#### 1.3. Objetivos Específicos

Establecer indicadores de monitoreo y mejora continua.

En base a los objetivos se establecerán los indicadores que permitirán la evaluación, monitoreo y mejoramiento permanente. La propia norma en sus anexos establece indicadores como:

- Tiempo de respuesta a incidentes
- Índices de finalización de la formación de los empleados

- Número de no conformidades detectadas durante las auditorías
- Entre otros que se deberán establecer.

## 2. Diagnóstico de la Seguridad de la Información en IEPHE

### 2.1. Análisis del Entorno y Riesgos

Para determinar un diagnóstico de la seguridad de la información, se inicia estableciendo el análisis del entorno actual y los potenciales riesgos, donde se debe considerar. La evaluación del contexto de la empresa, relacionado principalmente a la ciberseguridad. Se deben identificar amenazas y vulnerabilidades y se debe evaluar el impacto potencial que estas amenazas tienen para la empresa.

### 2.2. Evaluación del Estado Actual del SGSI

Parte fundamental del diagnóstico es realizar un comparativo o análisis del estado actual de la empresa en relación a los requerimientos del SGSI, para ello es necesario establecer cuáles son los controles de seguridad actuales; identificar las diferencias o brechas que tiene el sistema actual en relación a la ISO/IEC 27001:2022 y, las responsabilidades actuales del personal y capacitación que tienen. Estas diferencias permitirán entender desde donde se parte y visualizar los avances.

## 3. Marco Metodológico para la implementación de las Políticas y protocolos de Ciberseguridad

### 3.1. Principios y Enfoque del Marco Metodológico

El enfoque metodológico es necesario establecer y documentar como parte del sustento de la implementación, mismo que debe estar basado en la gestión de riesgos. Se puede mencionar y determinar la aplicación del ciclo PHVA (Planificar, Hacer, Verificar, Actuar) y cómo se adapta la metodología a las necesidades y estructura de la empresa IEPHE.

### 3.2. Estructura del Sistema de Gestión de Seguridad de la Información (SGSI)

Para dar estructura al sistema de gestión de seguridad de la información se debe considerar:

- La definición de roles y responsabilidades para la aplicación del sistema.
- El establecimiento mismo de las políticas de seguridad, donde se debe considerar el acceso, el uso de dispositivos, la protección de datos, la gestión de incidentes, entre otros.
- Finalmente se debe establecer los procedimientos de cada parte o fase de gestión de riesgos.

### 3.3. Controles de Seguridad Basados en ISO/IEC 27001:2022

Establecer controles de seguridad fundamentado en la ISO/IEC 27001:2022 implica considerar los siguientes:

- Controles Organizativos, donde se integre la gobernanza de la seguridad de la información.
- Controles Técnicos, se incluirá la gestión de accesos, el cifrado de datos, el monitoreo de las redes.
- Controles Físicos, en los que se incluyen la protección de infraestructuras que puedan ser críticas.
- Controles Humanos, lo que implica la capacitación, así como la concienciación del personal en relación a la ciberseguridad en la empresa.

## 4. Plan de Implementación de Políticas y Protocolos de Ciberseguridad

Finalmente, la implementación de las políticas y protocolos de ciberseguridad incluyen las siguientes etapas:

**Fase 1: Planificación**

En la planificación, una vez establecida debe existir la aprobación por parte de la alta dirección. Además, establecer el alcance y la estructura del SGSI.

Debe existir un apartado en el que se establece la prioridad de los riesgos y recursos. Este aspecto debe considerar cualquier empresa, pero especialmente en el caso de IEPHE, en el cual los recursos son limitados y debe priorizarse los potenciales riesgos con mayor impacto.

**Fase 2: Implementación**

La implementación de las políticas y protocolos debe estar soportada por la aplicación de controles y las políticas de seguridad, en las cuales el personal esté capacitado para su accionar, entienda los procedimientos y la importancia de su aplicación.

**Fase 3: Evaluación y Monitoreo**

Además del entendimiento, manejo, importancia y capacitación previamente aplicados, será obligatoria su aplicación y se establecerá un procedimiento de mejor mediante las auditorías internas de seguridad. Se deben considerar además pruebas de potenciales riesgos y cómo la empresa da respuesta a los incidentes. Y finalmente para el monitoreo existirán responsables del levantamiento de datos y presentación de los indicadores clave de desempeño (KPIs), previamente establecidos y presentarlos en junta para la evaluación del sistema.

**Fase 4: Mejora Continua**

La mejor continua es clave en el proceso, puesto que siempre será necesario realizar mejoras y ajustes en las políticas y procedimientos con el fin de que el sistema vaya mejorando y corrigiéndose con las mismas experiencia, carencias y avances de los sistemas, por tanto, es necesario la creación de un plan de actualización y mejora continua con estrategias para mejorar en cada período de evaluación.

| Etapas de Implementación | | | | | |
|---|---|---|---|---|---|
| **EJES O PARTES PRINCIPALES** | SUSTENTO TEÓRICO | SUSTENTO METODOLÓGICO | ESTRATEGIAS / TÉCNICAS | DESCRIPCIÓN DE RESULTADOS | INSTRUMENTOS APLICADOS |
| **Fase 1: Planificación** | - Norma ISO/IEC 27001:2022 (ISO/IEC, 2022). | - Definición del alcance y estructura del SGSI, priorización de riesgos y recursos. | - Aprobación de la alta dirección, definición del alcance del SGSI y priorización de riesgos. | - Determinación del plan de implementación que incluye la aprobación de la alta dirección y definición del alcance del SGSI. | - Documentación del plan de implementación. |
| **Fase 2: Implementación** | - Controles de seguridad (Anexo A de la norma ISO/IEC 27001:2022 )(International Organization for Standardization, 2022). | - Aplicación de controles y políticas de seguridad, capacitación del personal e integración con procesos empresariales. | - Implementación de controles de seguridad, capacitación del personal y alineación de las políticas con los procesos empresariales. | - Implementación exitosa de controles de seguridad y políticas de ciberseguridad en IEPHE. | - Controles de seguridad implementados y documentación de capacitación. |
| **Fase 3: Evaluación y Monitoreo** | - Ciclo PHVA (International Organization for Standardization, 2022). | - Auditorías internas pruebas de respuesta indicadores clave de desempeño (KPIs). | - Realización de auditorías internas, pruebas de respuesta a incidentes y evaluación de KPIs | - Evaluación del desempeño del SGSI mediante auditorías y KPIs. | - Auditorías internas y evaluación de KPIs. |
| **Fase 4: Mejora Continua** | - Ciclo PHVA<br>- mejora continua del SGSI<br>(International Organization for Standardization, 2022). | - Ajustes en las políticas y procedimientos<br>- Actualización de estrategias de seguridad. | - Implementación de ajustes en las políticas y procedimientos basados en los resultados de las auditorías y KPIs. | - Establecimiento de un sistema de mejora continua que garantice la adaptabilidad del SGSI a las nuevas amenazas y vulnerabilidades. | - Documentación de ajustes y actualizaciones en las políticas de seguridad. |

**ANEXO 4**

**Validación de especialistas**

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN SEGURIDAD INFOMÁTICA**

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| |
|---|
| **Validado por: Mgs. Diego Iván Yanchapaxi Andrango** |
| **Título obtenido: Magíster en Seguridad Informática** |
| **C.I.: 1717644908** |
| **E-mail: sistemas@duquematriz.com.ec** |
| **Institución de Trabajo: Storage System DUQUEMATRIZ** |
| **Cargo: Analista de Tecnologías y Ciberseguridad** |
| **Años de experiencia en el área: 12** |

Universidad Israel

ESPOG | Escuela de Posgrados

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** "Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022".

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| Pertinencia | x | | | | |
| Aplicabilidad | x | | | | |
| Factibilidad | x | | | | |
| Novedad | x | | | | |
| Fundamentación pedagógica | x | | | | |
| Fundamentación tecnológica | x | | | | |
| Indicaciones para su uso | x | | | | |
| TOTAL | 35 | | | | |

**Observaciones:**

- La propuesta de guía generada en la investigación es viable, para la empresa IEPHE, en la cual se verifica la falta de seguridad de la información y es necesario aplicar la norma "ISO/IEC 27001:2022", para fortalecer su integridad en sus datos informáticos.

**Recomendaciones:**

- Con la propuesta de políticas de seguridad basada en la "ISO/IEC 27001:2022", generadas en la investigación, sería importante que la empresa continúe con el proceso de implementación, para salvaguardar la información.
- Se recomienda al personal de TI de la empresa, la revisión de la norma "ISO 27001:2022", para una mejor visión y análisis de diferentes enfoques de implementación de la norma.

Universidad Israel

ESPOG | Escuela de Posgrados

**Lugar, fecha de validación: Quito 7 de marzo 2025**

**Firma del especialista**
Mgs. Diego Iván Yanchapaxi Andrango

# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFOMÁTICA

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| |
|---|
| **Validado por: Mgtr. Stalin Marcelo Maldonado** |
| **Título obtenido: Magister en Seguridad Informática** |
| **C.I.: 1718528563** |
| **E-mail: stalin.maldonado@solucionesservife.com** |
| **Institución de Trabajo: Banco Pichincha** |
| **Cargo: Experto en Ciberseguridad** |
| **Años de experiencia en el área: 2** |

Universidad Israel

ESPOG | Escuela de Posgrados

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** "Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, basada en la Norma ISO/IEC 27001:2022"

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| Pertinencia | x | | | | |
| Aplicabilidad | x | | | | |
| Factibilidad | x | | | | |
| Novedad | | x | | | |
| Fundamentación pedagógica | x | | | | |
| Fundamentación tecnológica | x | | | | |
| Indicaciones para su uso | | x | | | |
| TOTAL | 25 | 8 | | | |

**Observaciones:**

- El documento de investigación presenta un análisis de la situación de la ciberseguridad en la empresa IEPHE, identificando las deficiencias y vulnerabilidades existentes.
- La propuesta de una guía para la implementación de políticas y protocolos de ciberseguridad basados en la norma ISO 27001:2022 es sólida y está bien fundamentada, demuestra un adecuado rigor científico en el trabajo.
- La inclusión de un diagnóstico detallado, un marco metodológico claro y un plan de implementación estructurado son aspectos que fortalecen la calidad del documento y su utilidad práctica.
- El documento presenta una visión amplia de los desafíos que enfrenta la empresa sujeta de investigación en materia de ciberseguridad y ofrece soluciones viables.

**Recomendaciones**

- Como paso previo a la implementación de la norma ISO 27001:2022, se recomienda incluir la elaboración de la Declaración de Aplicabilidad (SOA), documento fundamental para identificar los controles de seguridad aplicables a la organización y justificar aquellos que no lo son.
- Se recomienda ampliar la revisión de la literatura sobre la norma ISO 27001:2022 incluyendo estudios de casos y análisis comparativos de diferentes enfoques de implementación.
- Se sugiere describir con mayor detalle los métodos de recolección y análisis de datos utilizados en la investigación, así como los criterios de selección de la muestra y los instrumentos de medición aplicados.
- Se recomienda profundizar en el análisis de los resultados obtenidos, identificando indicadores, tendencias y relaciones significativas entre las variables estudiadas.
- Se sugiere incluir anexos con información complementaria, como el cronograma de actividades.
- Se recomienda incluir en el análisis la perspectiva de los diferentes grupos de interés de la empresa, stakeholders, con el fin de obtener una visión amplia de la situación de la organización.

**Lugar, fecha de validación: Quito 7 de marzo de 2025**

**Firma del especialista**
Mgtr. Stalin Marcelo Maldonado

# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFOMÁTICA

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| |
|---|
| **Validado por: Mgs. Patricio Jiménez** |
| **Título obtenido: Magister en Ciberseguridad** |
| **C.I.: 1716991342** |
| **E-mail: pjimenez@danec.com** |
| **Institución de Trabajo: Grupo Danec S.A.** |
| **Cargo: Jefe de Infraestructura Tecnológica y Seguridad de Información** |
| **Años de experiencia en el área: 20** |

Universidad Israel

ESPOG | Escuela de Posgrados

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** "Propuesta de Políticas claves de Ciberseguridad en la Empresa IEPHE, Basada en la Norma ISO/IEC 27001:2022" "

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| **Pertinencia** | X | | | | |
| **Aplicabilidad** | X | | | | |
| **Factibilidad** | X | | | | |
| **Novedad** | X | | | | |
| **Fundamentación pedagógica** | X | | | | |
| **Fundamentación tecnológica** | X | | | | |
| **Indicaciones para su uso** | X | | | | |
| **TOTAL** | 35 | | | | |

**Observaciones:**

Se identifica que IEPHE no cuenta con una metodología estructurada para identificar, analizar y tratar los riesgos de seguridad de la información. Esto implica que no hay claridad sobre las amenazas más críticas para la empresa, ni sobre las vulnerabilidades que podrían ser explotadas, lo que incrementa la posibilidad de incidentes de seguridad con impacto financiero, operativo y reputacional.

La empresa no tiene documentados, procesos claros para la detección, notificación y respuesta ante incidentes de seguridad de la información. Esto puede generar retrasos en la mitigación **de** eventos como accesos no autorizados, fuga de datos o ataques de malware, lo que puede afectar a los procesos críticos y la continuidad operativa y la confianza en la organización.

**Recomendaciones:**

IEPHE debe adoptar un enfoque sistemático para la identificación, análisis y tratamiento de los riesgos en seguridad y se recomienda la creación de una Matriz de Riesgos, en la que se evalúen probabilidad e impacto de los incidentes, así como la implementación de controles preventivos y correctivos basados en el Anexo A de la ISO/IEC 27001:2022. Además, este proceso debe actualizarse de forma periódica para garantizar su efectividad.

Se debe establecer proceso para la gestión de incidentes, que incluya roles y responsabilidades, tiempos de respuesta, procedimientos de escalamiento y comunicación interna. Se recomienda realizar simulaciones periódicas de incidentes (como ataques de phishing o pérdida de datos) para capacitar al personal en la ejecución del plan. La documentación de estos procesos debe ser accesible para los colaboradores, asegurando una rápida respuesta ante cualquier evento de seguridad.

Lugar, fecha de validación: Quito 7 de marzo 2025

**Firma del especialista**
MCS. Patricio Jiménez