UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFOMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.
Línea de Investigación:
Ciencias de la ingeniería aplicada a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Cauja Pilataxi Guillermo Patricio
Tutor/a:
Mg. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

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: Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.

Elaborado por: Guillermo Patricio Cauja Pilataxi, de C.I: 1720735933, estudiante de la Maestría: 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

_____

Renato Mauricio Toasa Guachi

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutora del proyecto de investigación titulado: Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.

Elaborado por: Guillermo Patricio Cauja Pilataxi, de C.I: 1720735933, estudiante de la Maestría: 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: 2025.03.12 11:36:27 -05'00'

_____

Maryory Urdaneta Herrera

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Cauja Pilataxi Guillermo Patricio con C.I: 1720735933, autor/a del proyecto de titulación denominado: Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A. 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., de marzo de 2025

_____

Cauja Pilataxi Guillermo Patricio

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El propósito de esta tesina propone la implementación herramientas de código libre para mitigar amenazas que puede surgir en el ámbito hotelero, se empleara normas ISO/IEC 27001 de acuerdo a la necesidad de la empresa Apartec S.A.

La seguridad de la información es un aspecto fundamental que las organizaciones en especial el sector hotelero deben priorizar para garantizar su sostenibilidad y éxito en la era digital.

La creciente dependencia de sistemas tecnológicos interconectados, la gestión de gran cantidad de datos sensibles y la sofisticación de las ciberamenazas han elevado la seguridad de la información a prioridad estratégica en la industria hotelera.

En el sector hotelero el resguardo de la información es un tema crucial, impactando los ámbitos administrativo, educativo y tecnológico.

- **Administrativamente**: Proteger la seguridad es esencial para el sector hotelero ya que afecta áreas cruciales como la mitigación de riesgos, dirección estratégica, la eficiencia operativa y el cumplimiento legal. Las brechas de seguridad pueden generar graves consecuencias legales, financieras y de imagen.

- **Educativamente**: Este tema es fundamental para la formación de profesionales del sector hotelero y de ciberseguridad. Es preciso incluir la seguridad de la información en planes de estudio y promover la investigación en este campo, considerando especialmente la aplicabilidad de herramientas libres.

  Se beneficiarán directamente empresas PYMES, ya que al no contar con un capital significativamente solido podrían optar por herramientas de código abierto.

- **Tecnológicamente**: La seguridad es el núcleo del problema. Los hoteles dependen de infraestructuras tecnológicas complejas que son vulnerables a diversas ciberamenazas. Las herramientas de código abierto ofrecen una alternativa económica y adaptable para fortalecer la seguridad, aunque requieren personal especializado para su correcta implementación y gestión.

Asegurar la información en el sector hotelero es un gran reto que necesita estrategias completas en gestión, formación y tecnología. Las herramientas de código abierto representan una valiosa oportunidad para mejorar la seguridad de manera accesible, pero requieren un

enfoque profesional y una inversión en capacitación para maximizar sus beneficios y proteger eficazmente el negocio hotelero en la era digital.

Problema de investigación

El sector hotelero enfrenta una problemática significativa en relación de gestión y protección de información, derivada en la creciente dependencia de sistemas tecnológicos interconectados, el manejo de datos de huéspedes y la necesidad de cumplir normas de protección de datos.

La era tecnológica ha llegado y ha facilitado procesos en la cadena hotelera ya que mediante aplicaciones Web o Móviles se pueden realizar reservas en línea y proporcionar información personal. Aunque estas tecnologías optimizar procesos y mejoran la experiencia del cliente, también introducen vulnerabilidades críticas en la seguridad de la información.

La creciente sofisticación de los ataques cibernéticos, como el ransomware o phishing, son los más comunes a la hora de robo de información, ya que los delincuentes cibernéticos usan plataformas clonadas para que usuario introduzca información personal y así lograr su cometido.

Las PYMES en empresas hoteleras suelen carecer de presupuesto por lo que contar con herramientas sofisticadas para ofrecer al cliente una seguridad extremadamente segura es complicado además de que no cuentan con personal especializado en ciberseguridad.

Existen herramientas d código abierto que pueden ser eficaces para ofrecer seguridad, pero deben ir a la par con personal especializado en ciberseguridad.

Apartec S.A es una empresa constituida hace más de 20 años en la ciudad de Quito. Su actividad económica es administrar el sector hotelero y para ello cuenta con sistemas de almacenamiento en servidores y equipos de cómputo que usa el personal administrativo y empleados.

Dado que es una empresa legar cuenta con un SGSI pero no cuenta con sistemas de código abierto para mitigar amenazas que puedan surgir en cada control que se realice con la norma ISO/IEC 27001.

Objetivo general

Proponer medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.

Objetivos específicos

- Contextualizar los fundamentos teóricos relacionados con análisis de riesgos, resguardo de información y uso de herramientas de código abierto en el contorno hotelero.
- Diagnosticar la situación actual de riesgos y seguridad de la información en Apartec S.A, identificando vulnerabilidades, amenazas.
- Elaborar medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001.
- Validar por medio del especialista en el área el impacto de la metodología propuesta.

Vinculación con la sociedad y beneficiarios directos:

Este proyecto de titulación propone un sistema integral en seguridad de la información para la empresa Apartec S.A. utilizando herramientas de código abierto y estándares ISO/IEC 27001, se vincula con la sociedad al buscar fortalecer la ciberseguridad en el sector hotelero, un área crítica para la economía y la confianza ciudadana.

Su relevancia se extiende a los ámbitos administrativo, educativo y tecnológico, generando un impacto social positivo y tangible.

El proyecto se vincula con la sociedad a través de la creación de un modelo de seguridad que puede ser adaptable a otros sistemas hoteleros, por lo tanto su impacto social se centra en:

- **Seguridad Ciudadana:** Protección de datos de huéspedes y reducción de delitos informáticos.
- **Sector Hotelero:** Fortalecimiento de PYMES hoteleras y la economía turística.
- **Promoción del Código Abierto:** Democratización del acceso a la ciberseguridad.
- **Cultura de Ciberseguridad:** Promover cultura en aspectos de educación en ciberseguridad.

Aportará capacitación, asesoría, un modelo de seguridad replicable, publicaciones y materiales de estudio. Los beneficiarios directos son:

- **Apartec S.A.:** Mejora de su seguridad informática.
- **Huéspedes de Hoteles:** Mayor protección de sus datos personales.
- **Personal Hotelero:** Capacitación y herramientas para la gestión de la seguridad.

- **Comunidad Académica y Profesional:** Nuevos conocimientos y recursos en ciberseguridad hotelera.

En resumen, el proyecto busca beneficiar a la sociedad en general al mejorar la seguridad del sector hotelero, utilizando soluciones accesibles y promoviendo una cultura de ciberseguridad.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Antecedentes Investigativos

Este trabajo consiste en diseñar un plan de seguridad informática para la empresa Apartec S.A. Nos basaremos en las normas proporcionadas por el hotel y la normativa ISO/IEC 27001.

“En la perspectiva empresarial actual, la transformación digital ha trascendido, convirtiéndose en un requisito fundamental tanto para las organizaciones como para las personas. Este cambio paradigmático se centra en la hiperconectividad de datos, permitiendo la integración de información diversa para alcanzar objetivos específicos, optimizar recursos y ahorrar tiempo. La era digital ha reconfigurado los modelos tradicionales de pensamiento y acción impulsando a las empresas a adoptar enfoques innovadores que mejoren la eficiencia y la productividad. Al priorizar la experiencia del cliente y ofrecer soluciones personalizadas, gracias a ello las organizaciones pueden fortalecer su posición en el mercado y fomentar la lealtad del cliente.” (Medina et al., 2023).

Con la expansión de las tecnologías modernas y el acceso a Internet, la información fluye hacia la sociedad a una velocidad inimaginable. Por tal motivo los ataques a organizaciones son más frecuentes ya que los piratas informáticos también se actualizan con nuevas herramientas y métodos de ataques sofisticados.

"La industria hotelera es un objetivo atractivo para los ciberdelincuentes debido a la gran cantidad de datos personales y financieros que maneja. Los ataques de ransomware, phishing y robo de datos son cada vez más frecuentes y sofisticados" (Roiback, s.f.). Este aumento se debe a la digitalización de procesos que los convierte más vulnerables.

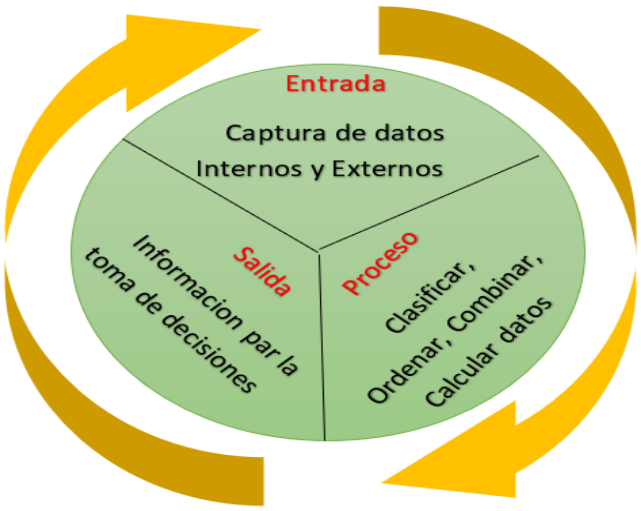
Sistemas de Información

Según Sisti (2019) “Los SGSI son herramientas que ayudan a las empresas a usar sus datos para una mejor toma de decisiones además de ser más competitivas. Su funcionamiento consiste en recolectar información, analizar y usar esos datos para mejorar”.

Un sistema es una herramienta que ayuda a organizar y procesar información para lograr objetivos. Su ciclo de vida asegura que la información se maneje de manera eficiente y segura, desde su entrada hasta su salida.

Figura 1.

Ciclo de la información.



Nota. Auditoria propia Basado en (Sisti, 2019).

Seguridad de la Información

"Las regulaciones de protección de datos, como GDPR, exigen a los hoteles implementar medidas de seguridad fuertes para protección de información de sus huéspedes. El incumplimiento de estas normativas puede acarrear sanciones económicas significativas y dañar la reputación del hotel" (Lean Hotel System, s.f.).

“La implementación de una defensa cibernética robusta requiere una combinación de soluciones de software y hardware, lo que implica costos significativos y una planificación cuidadosa. Componentes como firewalls, antivirus, sistemas de detección y prevención de intrusiones (IDS/IPS) y detección y respuesta de puntos finales (EDR) trabajan conjuntamente para salvaguardar los activos digitales de una organización. Dada la creciente sofisticación de las amenazas, es inevitable que las empresas deban destinar mayores recursos económicos a la ciberseguridad. Según un informe de Kaspersky, el presupuesto promedio global para ciberseguridad en pequeñas y medianas empresas alcanzó los 150.000 dólares en 2022, y se prevé un aumento del 14% para el año siguiente” (Kaspersky, 2022).

De acuerdo a (Bosch, 2010) “El Sistema de Gestión de Seguridad de la Información (SGSI) actúa como el núcleo de la norma ISO 27001, proporcionando un marco para evaluar y manejar los riesgos que amenazan la información de una organización. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de dichos datos”.

Normas de Seguridad ISO/IEC 27001

La ISO 27001 es un estándar internacional que proporciona pasos necesarios para instalar al mismo tiempo de mantener y con el transcurso del tiempo perfeccionar un Sistema Gestor de Seguridad de la Información.

La normativa ISO/IEC 27001 aporta importantes actualizaciones para una SGSI, con el objetivo de adaptarse a la evolución del panorama digital y reforzar las defensas contra las amenazas a la ciberseguridad (NQA, 2024).

1.2. Proceso investigativo metodológico

El desarrollo y la investigación de este proyecto de titulación se han estructurado de forma metódica y rigurosa, aplicando un marco metodológico mixto para abordar el problema de seguridad en la empresa.

A continuación, un detalle del proceso evidenciando las fases, métodos y técnicas empleados:

1.2.1. Enfoque de Investigación

Se opto por un método de investigación mixto, combinando métodos cualitativos y cuantitativos. Esta elección metodológica se fundamenta en la necesidad de:

- Comprender el contexto específico de la empresa, incluyendo las percepciones y experiencias del personal respecto a la seguridad (método cualitativo).
- Medir y evaluar objetivamente el impacto de las herramientas de código abierto en la seguridad, a través de indicadores concretos (método cuantitativo).
- Triangular la información obtenida de ambas fuentes para lograr una comprensión más completa y robusta del problema y la solución propuesta.

1.2.2. Tipos de Investigación

El proyecto se desarrolló a través de los siguientes tipos de investigación, cada uno con un propósito específico:

- **Investigación Exploratoria:** Fase inicial del proyecto para identificar y delimitar los principales riesgos de seguridad de la información que enfrenta la empresa y a explorar herramientas de código abierto relevantes para mitigarlos. Se basó en la revisión bibliográfica inicial y un acercamiento preliminar a la empresa.

- **Investigación Descriptiva:** Se centró en describir detalladamente el estado actual del resguardo de información y las medidas de seguridad existentes en la empresa. Esto incluyó la identificación de la infraestructura tecnológica, las políticas de seguridad implementadas y la percepción del personal sobre la seguridad actual.

1.2.3. Marco Metodológico Aplicado

El marco metodológico aplicado en este proyecto se caracteriza por ser mixto, combinando métodos cualitativos y cuantitativos en un proceso de investigación. Se basa en la revisión de fuentes bibliográficas, la investigación real en la empresa, el diseño centrado en el usuario, la validación por expertos y la propagación del conocimiento generado. Este enfoque metodológico busca asegurar la validez, confiabilidad y pertinencia de los resultados y la propuesta final contribuyendo de manera significativa a la seguridad de la información en el sector hotelero y al uso efectivo de herramientas de código abierto.

El ámbito de investigación incluyó al jefe del área de TI de la empresa, quien aceptó participar libre y voluntariamente en este proyecto, brindando su consentimiento para la realización de encuestas con el fin de respaldar la propuesta de estudio orientada a mejorar la seguridad informática. Además, participaron 4 colaboradores del área de TI y otro personal relacionado con el tema.

Para la realización de las encuestas emplee software en línea (Google Forms) que ayudo a una rápida recolección de datos y mediante ello se puede realizar un análisis gráfico para mejorar la comprensión de sus datos.

Las encuestas realizadas se encuentran en los Anexo1, Anexo2 y Anexo3.

1.3. Análisis de resultados

Habiendo aplicado las metodologías previamente mencionadas, la siguiente etapa consistió en recopilar información. Tal informacion será exhibidos a través de tablas e ilustraciones, que se detallan en la presente:

Para la obtención de datos se han realizado por grupos Personal de TI, Personal Administrativo y Atención al Cliente.

Personal de TI

Pregunta 1: ¿La empresa utiliza un firewall en el borde de su red?

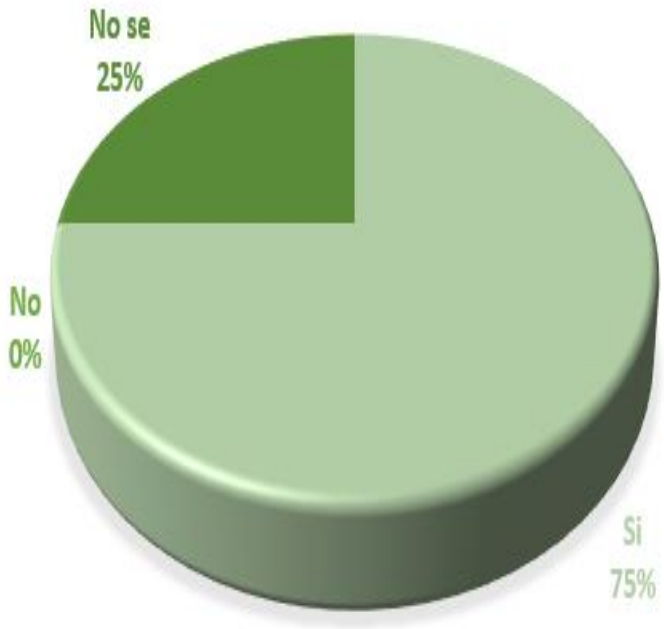
Tabla 1.
Utilización de Firewall en la Red.

Condición	Opinión	%
Si	3	0,75
No	0	0
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 2.

Utilización de Firewall en Red.



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿La empresa utiliza un firewall en el borde de su red? El 75% afirmo que la empresa usa firewall en la red y el 25% afirmo que no está seguro.

Pregunta 2: ¿Se realizan copias de seguridad de los datos críticos diariamente?

Tabla 2.

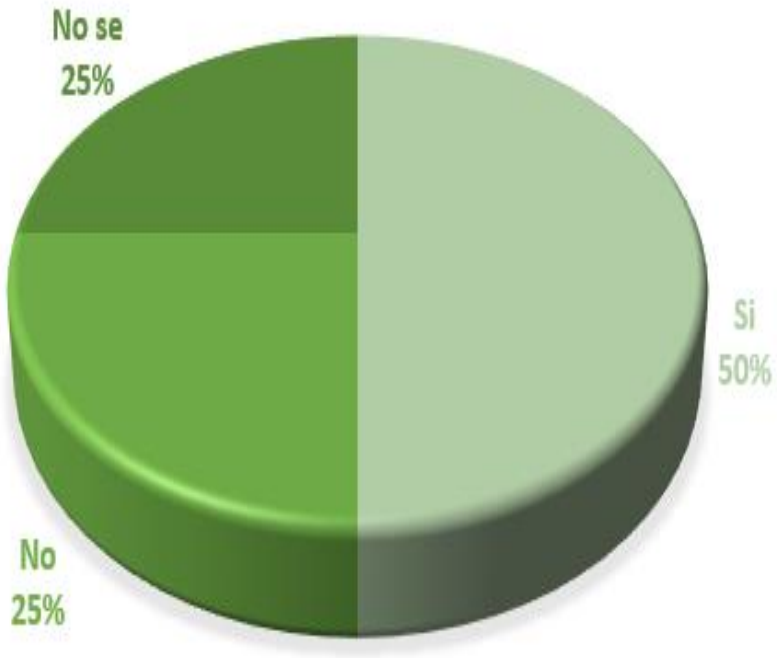
Copias de seguridad diariamente

Condición	Opinión	%
Si	2	0,5
No	1	0,25
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 3.

Copias de seguridad diariamente



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se realizan copias de seguridad de los datos críticos diariamente? El 50% afirmo que la empresa realiza copias de seguridad a diario y el 25% afirmo que no está seguro y el 25% afirma que no.

Pregunta 3: ¿Se utiliza cifrado en las comunicaciones de red?

Tabla 3.

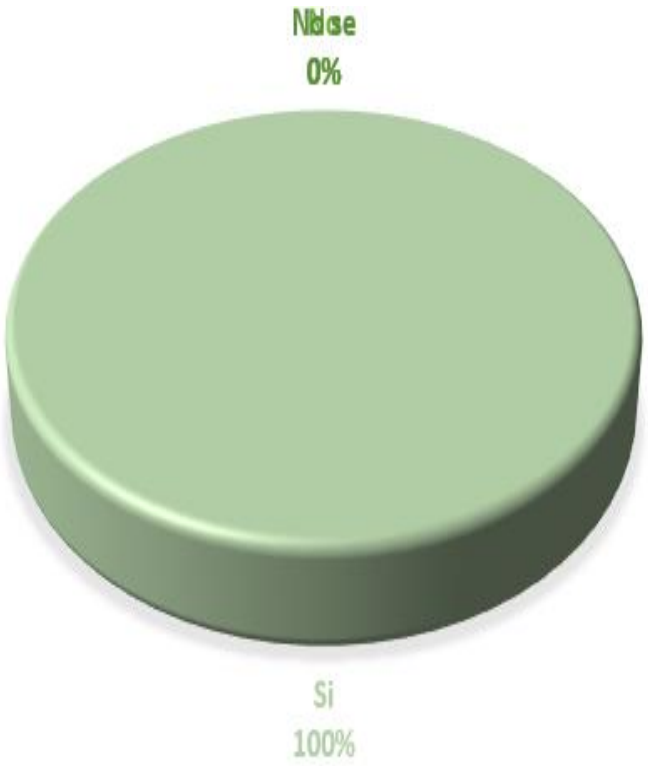
Cifrado en comunicaciones de red

Condición	Opinión	%
Si	4	1
No	0	0
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 4.

Cifrado en comunicaciones de red



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se utiliza cifrado en las comunicaciones de red? El 100% afirmo que la empresa cifra las comunicaciones en la red.

Pregunta 4: ¿Se realiza una auditoría de seguridad de la red al menos una vez al año?

Tabla 4.

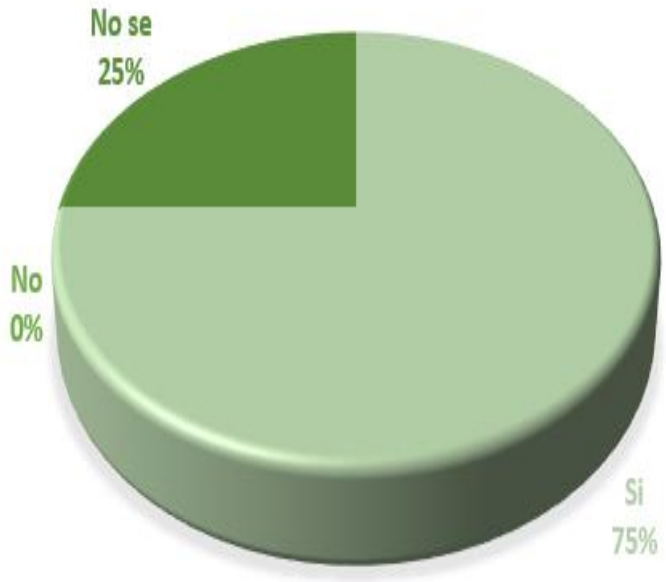
Auditoria seguridad de la red al año

Condición	Opinión	%
Si	4	1
No	0	0
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 5.

Auditoria seguridad de la red al año



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se realiza una auditoría de seguridad de la red al menos una vez al año? El 75% afirmo que la empresa realiza auditoria de la red una vez al año y el 25% no está seguro.

Pregunta 5: ¿Los sistemas operativos y las aplicaciones se mantienen actualizados con los parches de seguridad más recientes?

Tabla 5.

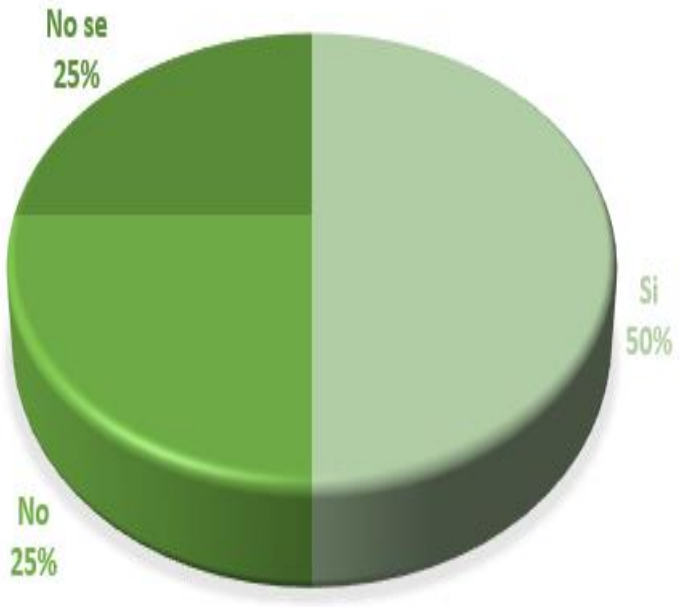
S.O y Aplicaciones con parches de seguridad actualizados

Condición	Opinión	%
Si	2	0,5
No	1	0,25
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 6.

S.O y Aplicaciones con parches de seguridad actualizados



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Los sistemas operativos y las aplicaciones se mantienen actualizados con los parches de seguridad más recientes? El 50% afirmo que la empresa posee S.O y Aplicaciones con parches de seguridad actualizados, el 25% no está seguro y el 25% afirma que no.

Pregunta 6: ¿Se emplea un sistema de detección de intrusiones (IDS) o un sistema de prevención de intrusiones (IPS)?

Tabla 6.

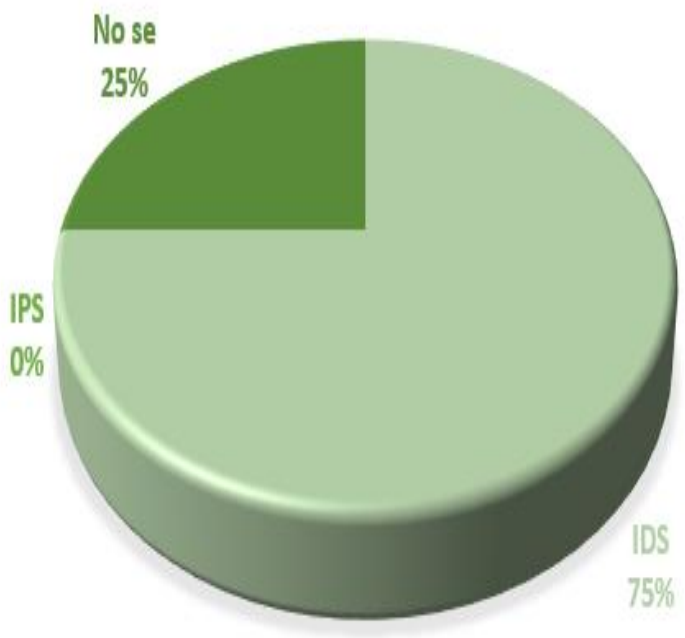
Sistemas IDS o Sistemas IPS

Condición	Opinión	%
IDS	3	0,75
IPS	0	0
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 7.

Sistemas IDS o Sistemas IPS



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se emplea un sistema de detección de intrusiones (IDS) o un sistema de prevención de intrusiones (IPS)? El 75% afirmo que la empresa posee sistemas de detección IDS y el 25% no sabe sobre este tipo de sistema.

Pregunta 7: ¿Se ha implementado la autenticación de dos factores (2FA) para el acceso remoto?

Tabla 7.

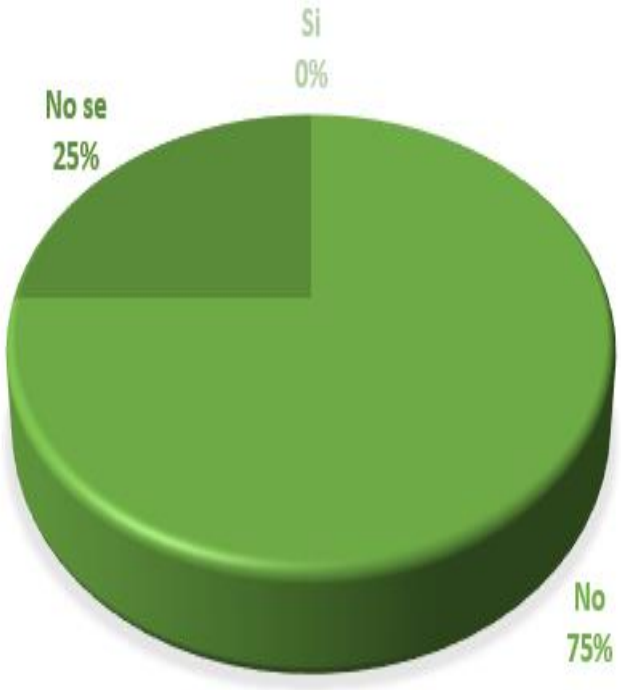
Autentificación 2 factores para el acceso remoto

Condición	Opinión	%
Si	0	0
No	3	0,75
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 8.

Autentificación 2 factores para el acceso remoto



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se ha implementado la autenticación de dos factores (2FA) para el acceso remoto? El 75% afirmo que la empresa no posee la autentificación 2FA y el 25% desconoce de lo que es.

Pregunta 8: ¿Se realiza un análisis de vulnerabilidades de las aplicaciones web periódicamente?

Tabla 8.

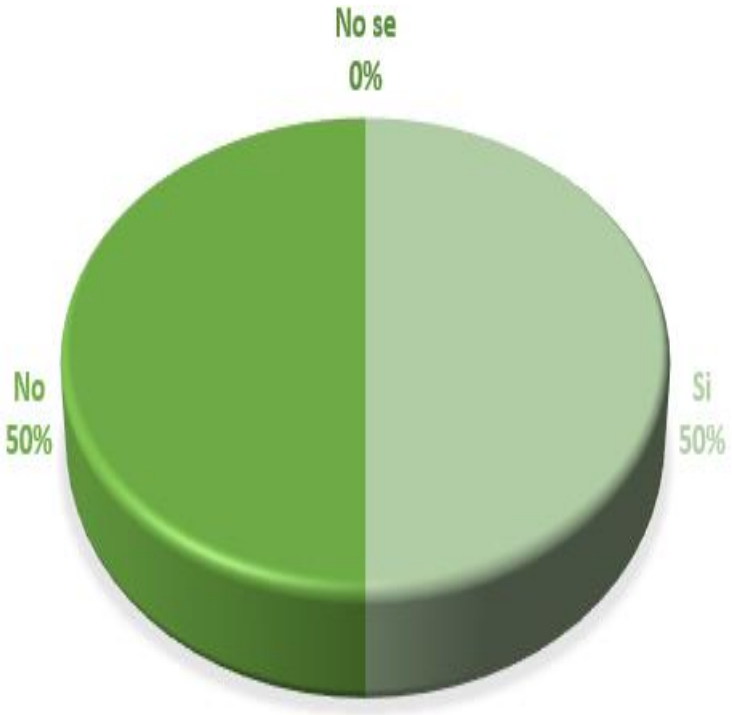
Análisis de vulnerabilidades de páginas web a diario

Condición	Opinión	%
Si	2	0,5
No	2	0,5
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 9.

Análisis de vulnerabilidades de páginas web a diario



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se realiza un análisis de vulnerabilidades de las aplicaciones web periódicamente? El 55% afirmo que la empresa realiza análisis de vulnerabilidades de páginas web a diario mientras el otro 50% afirma que no.

Pregunta 9: ¿Está familiarizado con la norma ISO/IEC 27001?

Tabla 9.

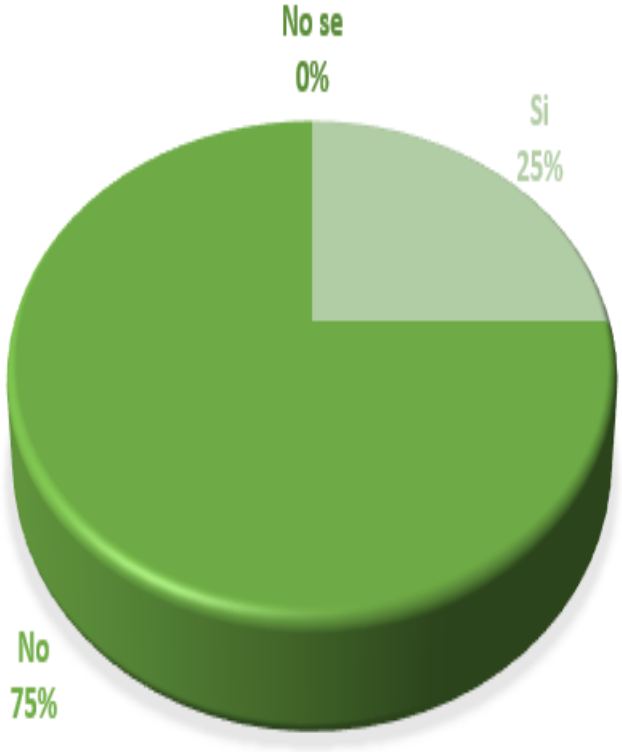
Familiaridad con la norma ISO 27001

Condición	Opinión	%
Si	1	0,25
No	3	0,75
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 10.

Familiaridad con la norma ISO 27001



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Está familiarizado con la norma ISO/IEC 27001? El 25% está familiarizado con la norma ISO 27001 y el 75% desconoce sobre la norma ISO 27001.

Pregunta 10: ¿Considera que la empresa cumple actualmente con los principales requisitos de la norma?

Tabla 10.

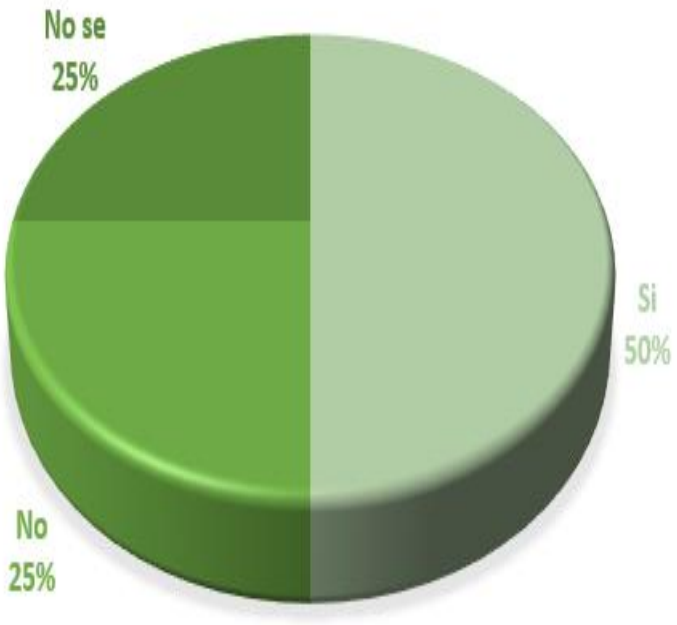
Empresa cumple con los principales requisitos de la norma

Condición	Opinión	%
Si	2	0,5
No	1	0,25
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 11.

Empresa cumple con los principales requisitos de la norma



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Considera que la empresa cumple actualmente con los principales requisitos de la norma? El 50% está seguro de que la empresa si cumple con los principales requisitos de la norma mientras que el 25% asegura que no y el otro 25% no está seguro.

Pregunta 11: ¿Se ha implementado alguna herramienta de seguridad de código abierto en la empresa?

Tabla 11.

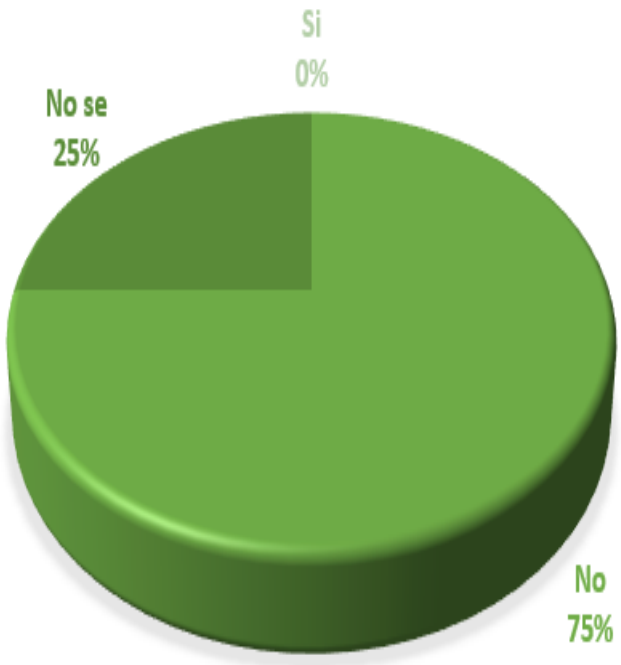
Empresa implementado herramientas de código abierto

Condición	Opinión	%
Si	0	0
No	3	0,75
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área TI de la empresa.

Figura 12.

Empresa implementado herramientas de código abierto



Nota. Datos recopilados de cuatro empleados área TI de la empresa.

En conformidad a la pregunta ¿Se ha implementado alguna herramienta de seguridad de código abierto en la empresa? El 75% afirma que la empresa no ha implementado herramientas de código abierto mientras el 25% afirma que no saben.

Personal Administrativo

Pregunta 12: ¿Existen políticas de seguridad de la información documentadas y accesibles?

Tabla 12.

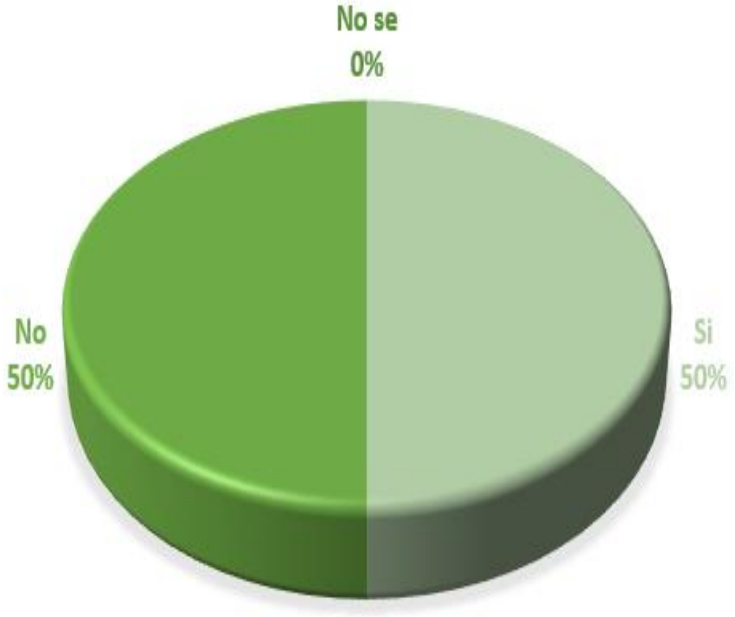
Políticas de seguridad accesibles

Condición	Opinión	%
Si	2	0,5
No	2	0,5
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

Figura 13.

Políticas de seguridad accesibles



Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

En conformidad a la pregunta ¿Existen políticas de seguridad de la información documentadas y accesibles? El 50% afirma que las políticas de la seguridad de la información son accesibles para todos los empleados mientras el otro 50% afirma que no.

Pregunta 13: ¿Se realiza capacitación en seguridad de la información para los empleados una vez al año?

Tabla 13.

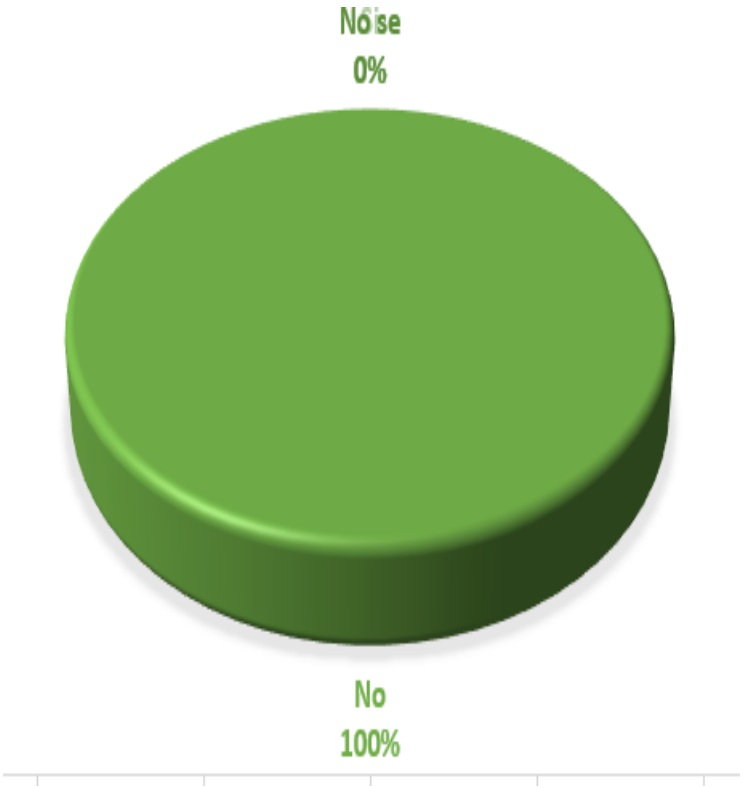
Capacitación en Seguridad de la Información

Condición	Opinión	%
Si	0	0
No	4	1
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

Figura 14.

Capacitación en Seguridad de la Información



Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

En conformidad a la pregunta ¿Se realiza capacitación en seguridad de la información para los empleados una vez al año? El 100% afirma que no se ha realizado capacitaciones acerca de la seguridad de la información.

Pregunta 14: ¿Se exige el uso de contraseñas complejas y se cambia periódicamente?

Tabla 14.

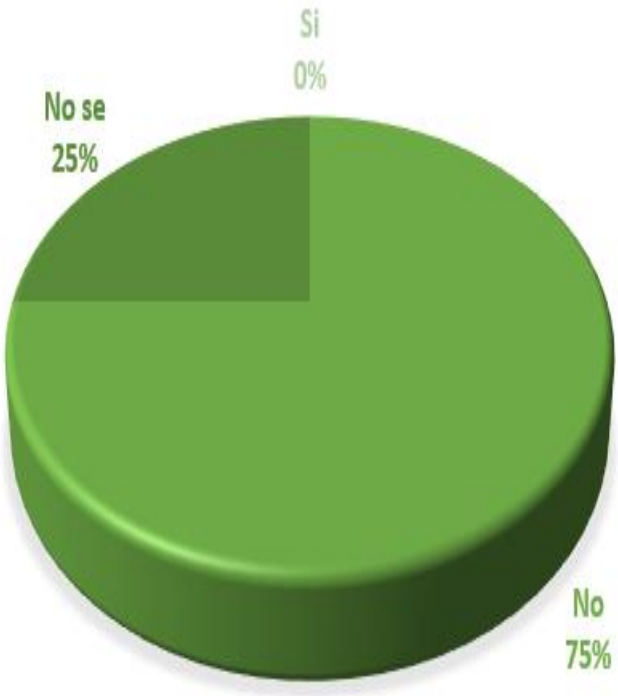
Contraseñas complejas

Condición	Opinión	%
Si	0	0
No	3	0,75
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

Figura 15.

Contraseñas complejas



Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

En conformidad a la pregunta ¿Se exige el uso de contraseñas complejas y se cambia periódicamente? El 75% afirma que no se les solicita contraseñas complejas mientras el 25% no sabe si las contraseñas que poseen son complejas o cumplen los requisitos.

Pregunta 15: ¿Ha habido acontecimientos de seguridad de la información en su departamento el último año?

Tabla 15.

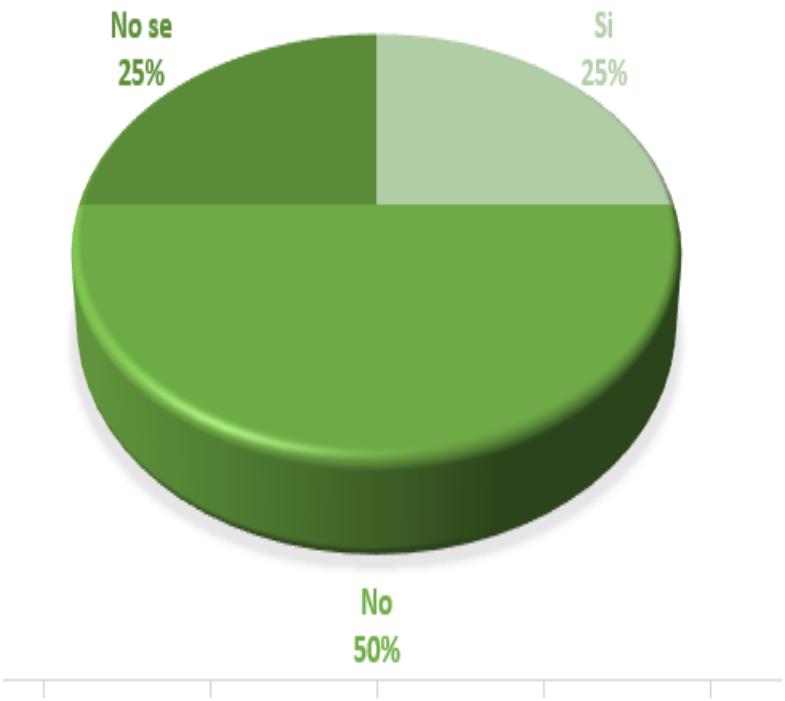
Incidentes seguridad de la información

Condición	Opinión	%
Si	1	0,25
No	2	0,5
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

Figura 16.

Incidentes seguridad de la información



Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

En conformidad a la pregunta ¿Ha habido acontecimientos de seguridad de la información en su departamento el último año? El 50% afirma que no han sufrido incidentes con la seguridad de la información el otro 25% afirma que si mientras el otro 25% afirma que desconoce si ha sufrido incidentes.

Pregunta 16: ¿Conoce el procedimiento para reportar un incidente de seguridad?

Tabla 16.

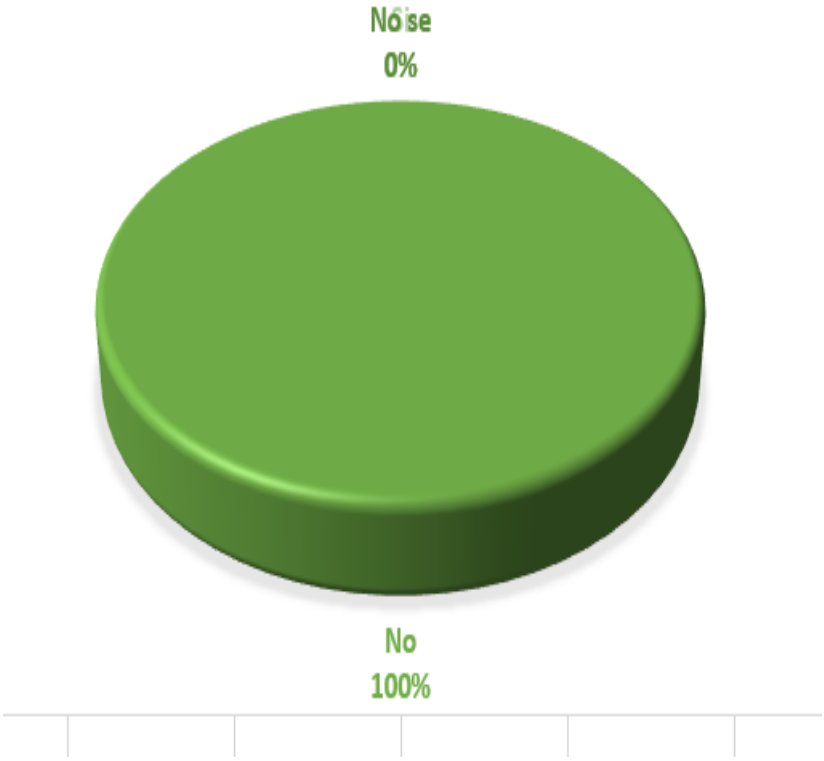
Reportar incidentes de seguridad

Condición	Opinión	%
Si	0	0
No	4	1
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

Figura 17.

Reportar incidentes de seguridad



Nota. Datos recopilados de cuatro empleados área Administración de la empresa.

En conformidad a la pregunta ¿Conoce el procedimiento para reportar un incidente de seguridad? El 100% afirma que desconoce como reportar un incidente de seguridad.

Atención al Cliente

Pregunta 17: ¿Se destruyen los documentos con información de los huéspedes de forma segura?

Tabla 17.

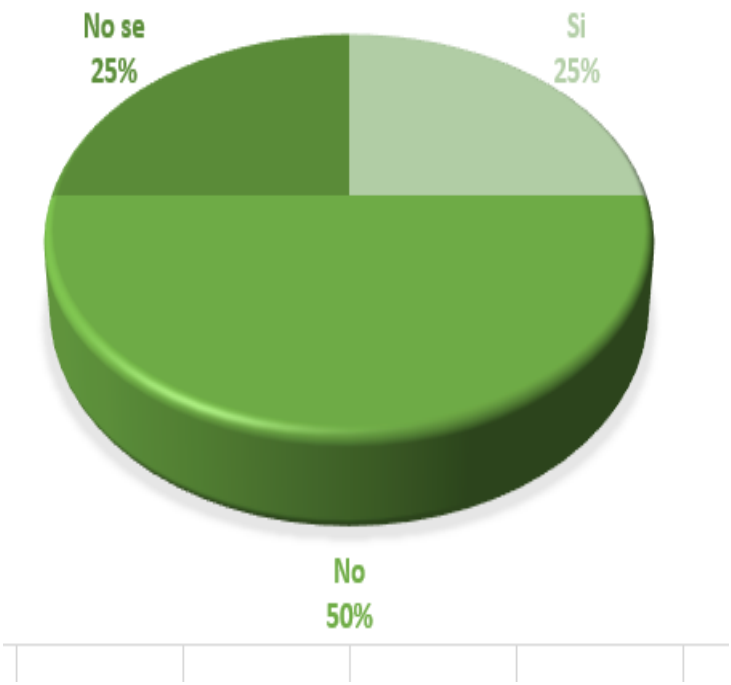
Destrucción de información de huespedes

Condición	Opinión	%
Si	1	0,25
No	2	0,5
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

Figura 18.

Destrucción de información de huespedes



Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

En conformidad a la pregunta ¿Se destruyen los documentos con información de los huéspedes de forma segura? El 50% afirma que no se destruye la información de forma segura mientras que el otro 25% afirma que sí y el otro 25% afirma que no sabe.

Pregunta 18: ¿Se verifica la identidad de los huéspedes antes de proporcionar información personal?

Tabla 18.

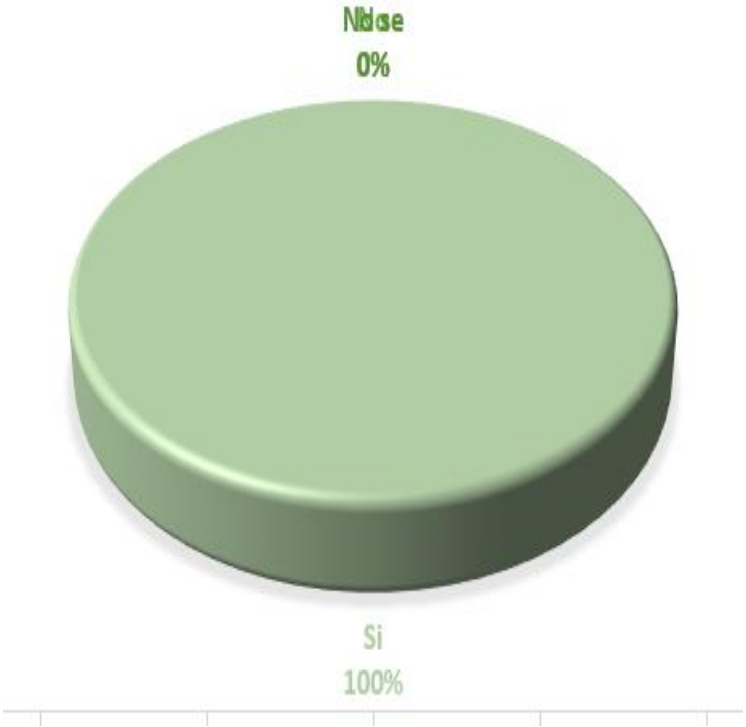
Verificación de huespedes

Condición	Opinión	%
Si	4	1
No	0	0
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

Figura 19.

Verificación de huespedes



Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

En conformidad a la pregunta ¿Se verifica la identidad de los huéspedes antes de proporcionar información personal? El 100% afirma que si solicitan documentación para proporcionar información.

Pregunta 19: ¿Se guarda información de tarjetas de crédito de los clientes en algún medio físico?

Tabla 19.

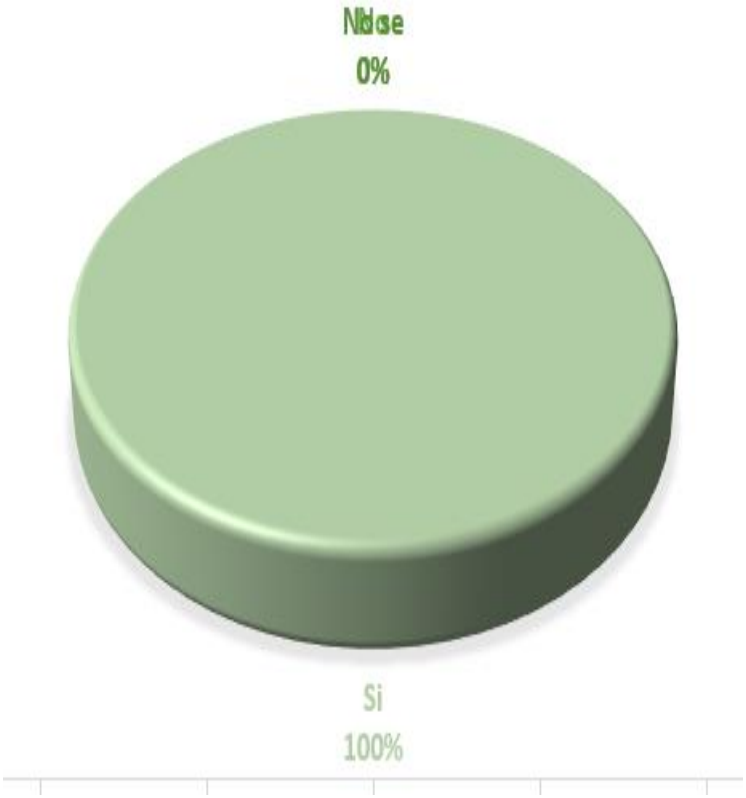
Guardar información en medios físicos

Condición	Opinión	%
Si	4	1
No	0	0
Desconozco	0	0
Total	4	1

Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

Figura 20.

Guardar información en medios físicos



Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

En conformidad a la pregunta ¿Se guarda información de tarjetas de crédito de los clientes en algún medio físico? El 100% afirma la información si se almacena en medios físicos.

Pregunta 20: ¿Ha recibido capacitación sobre protección de datos personales?

Tabla 20.

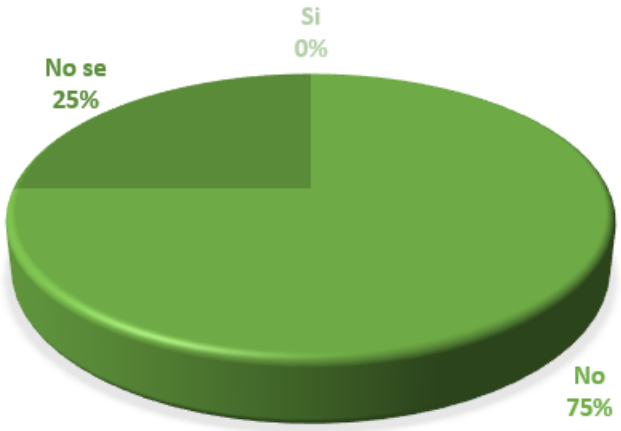
Capacitación protección de datos personales

Condición	Opinión	%
Si	0	0
No	3	0,75
Desconozco	1	0,25
Total	4	1

Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

Figura 21.

Capacitación protección de datos personales



Nota. Datos recopilados de cuatro empleados área Atención al Cliente de la empresa.

En conformidad a la pregunta ¿Ha recibido capacitación sobre protección de datos personales? El 75% afirma que no han recibido capacitación para la protección de datos personales y otro 25% desconocen si recibieron capacitación.

Análisis general de la encuesta aplicada.

Tras la realización de las encuestas, se ha identificado que la empresa presenta deficiencias en los controles, procesos y procedimientos estratégicos en todas las áreas administrativas. Es crucial establecer controles que contribuyan a mitigar estas falencias, y la normativa ISO 27001 es la más adecuada, ya que ofrece controles específicos para abordar y corregir estas deficiencias.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

2.1.1. Seguridad de la Información

"La seguridad de la información implica proteger los datos sensibles de una organización contra accesos no permitidos, usos indebidos, modificaciones o interrupciones. Su objetivo es garantizar que la información esté disponible solo para usuarios autorizados además que se mantenga privada y conserve su exactitud." (Holdsonsworh y Kosinski, 2024).

Los tres pilares de la seguridad de la información:

Confidencialidad: Las organizaciones deben adoptar medidas que garanticen que únicamente los usuarios autorizados tengan acceso a la información. Para proteger la confidencialidad de los datos, es dable emplear herramientas como el cifrado, la autenticación de múltiples factores y los sistemas de prevención de fugas de información.

Integridad: Las empresas deben preservar la integridad de los datos durante todo su proceso, asegurando su fidelidad y fiabilidad. Para ello evitan que usuarios no autorizados accedan, modifiquen o interfieran en la información. Herramientas como los permisos de archivos, administración de identidades y autentificación de accesos contribuyen a garantizar esta integridad.

Disponibilidad: El mantenimiento constante del hardware y la actualización del sistema aseguran que usuarios autorizados tengan accesos seguros y consistente a la información requerida.

2.1.2. ISO/IEC 27001

Norma más utilizada a nivel mundial para sistemas de gestión de la seguridad de la información. Este estándar define requisitos esenciales que un SGSI debe cumplir y proporciona a las organizaciones sin importar su tamaño o sector de trabajo, propone directrices claras para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información.

Además promueve buenas prácticas y un enfoque estructurado para proteger los datos y garantizar la confidencialidad, integridad y disponibilidad de la información.

Implica que una organización o empresa ha implantado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja, y que este sistema

respeta todas las buenas prácticas y principios contemplados en esta Norma Internacional (ISO, 2022).

2.1.3. Herramientas de Código Abierto

Software con código fuente accesible y modificable que ofrece flexibilidad, transparencia y en muchos casos, una alternativa económica a soluciones propietarias. En seguridad abarcan desde sistemas cortafuegos, sistemas de detección de intrusos hasta herramientas de análisis de vulnerabilidades y gestión de seguridad.

2.1.4. Sector Hotelero y PYMES

Las PYMES hoteleras en particular enfrentan desafíos únicos en seguridad de la información debido al manejo de datos sensibles, la dependencia de sistemas tecnológicos y las limitaciones presupuestarias.

2.1.5. Medidas de Seguridad

Según Arcos (2023) Se trata de crear un documento que establezca las acciones y medidas necesarias para proteger la información empresarial. Su propósito principal es definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) y del documento en sí estableciendo las normas y responsabilidades para asegurar la seguridad de los datos y los sistemas.

2.1.6. Sistema Gestión de Seguridad de la Información

Se trata de un conjunto de herramientas, controles y procedimientos diseñados para administrar y salvaguardar todos los activos de información que una empresa utiliza. (Tigse Moposita, 2020).

2.2. Descripción de la propuesta

Hoy en día la seguridad de la información es crucial para organizaciones de todo tipo y tamaño en especial para las entidades hoteleras donde el manejo de datos sensibles es una prioridad.

Ante el aumento de ciberataques además de fugas de información y normativas más rigurosas sobre privacidad asegurar la protección de datos sensibles se ha vuelto esencial para el buen funcionamiento y la continuidad de las empresas. En este escenario, la norma ISO 27001 se posiciona como un estándar global ampliamente reconocido y apreciado para la administración efectiva de la seguridad informática.

El planteamiento investigación parte por desarrollar políticas de seguridad que gestionen los errores humanos, siguiendo los estándares ISO/IEC 27001. Estas políticas establecerán criterios e indicadores para evaluar, controlar y monitorear para posterior ser compartidas con los trabajadores y altos mandos de la empresa.

La creación de estas políticas se enfoca en los requisitos y controles establecidos por la norma ISO/IEC 27001, con el objetivo de aplicar buenas prácticas en seguridad informática.

Uno de los principales beneficios de adoptar la norma ISO/IEC 27001 como base para este plan de seguridad es su enfoque orientado a la gestión de riesgos. A diferencia de las soluciones genéricas, la norma ISO 27001 fomenta que las empresas evalúen sus propios riesgos de seguridad de la información y desarrollen controles a medida para mitigarlos. Esta estrategia preventiva no solo evita incidentes, sino que también permite una respuesta ágil a los cambios en el entorno de amenazas.

En consecuencia, desarrollar un plan de seguridad alineado con las regulaciones de seguridad informática para el sector hotelero y la norma ISO/IEC 27001 requiere la incorporación de las mejores prácticas para garantizar la protección de los activos de información en el ámbito hotelero. A continuación, se presentan los elementos clave que constituirán la base de este plan de seguridad y el enfoque principal de esta propuesta.:

- **Evaluación de riesgos y análisis de impacto:** Proceso para identificar, evaluar y priorizar los riesgos que impacten en la seguridad de la información. Este proceso incluye la identificación de activos, amenazas y vulnerabilidades, así como la estimación de los impactos críticos. El propósito es concentrar los esfuerzos en los riesgos más relevantes.
- **Desarrollo de políticas:** Creación de documentos formales que establezcan reglas y procedimientos para proteger la información. Incluye políticas de uso aceptable, contraseñas, acceso a la información y respuesta a incidentes, alineadas con normas como ISO/IEC 27001.
- **Implementación de controles de seguridad:** Medidas técnicas, físicas y administrativas para mitigar riesgos. Incluye firewalls, cifrado de datos, control de acceso físico y políticas de seguridad. Se pueden usar herramientas de código abierto
- **Gestión de accesos privilegiados:** Control y supervisión a usuarios con permisos especiales para permitir el acceso a sistemas críticos. Se fundamenta en el principio de acceso mínimo, la autenticación de dos factores (2FA) y el monitoreo continuo de actividades.

- **Protección de datos personales y confidenciales:** Asegurar que la información confidencial no sea accesible y mucho menos alterada ni eliminada por usuarios no autorizados. Esto incluye el cifrado y la clasificación de la información además de la eliminación segura.
- **Preparación para respuesta de incidentes:** Plan estructurado para detectar, contener y recuperarse de incidentes de seguridad. Incluye detección temprana con un plan de respuesta, plan de recuperación de desastres y simulacros.
- **Formación y concienciación:** Capacitación regular del personal para que comprendan los riesgos y sepan cómo actuar. Incluye simulaciones de phishing, materiales de apoyo y sesiones de formación.

Asegurar que todas las medidas implementadas estén alineadas con los controles de la norma ISO/IEC 27001, especialmente en áreas como gestión de vulnerabilidades, accesos privilegiados, gestión de incidentes y formación del personal.

a. Estructura general

La presente Figura 22. Enfoca el proceso en el cual se va a estructurar la presente investigación para llevar un orden en la aplicación de normas ISO/IEC 27001 y la propuesta a implementar.

Figura 22.

Mapa conceptual estructura general

b. Explicación del aporte

Esta propuesta radica en desarrollar una guía de seguridad que sea adaptable a las necesidades de Apartec S.A, integrando normas ISO/IEC 27001 y utilizando herramientas de código abierto.

Esta tesina tiene como objetivo no solo salvaguardar la información de la empresa, sino también optimizar tiempos de proceso y fomentar la confianza de los clientes.

Para la explicación lo desarrollare en los siguientes puntos para lo posterior mostrar las estrategias implementadas.

- **Evaluación de riesgos y análisis de impacto:** Permite identificar vulnerabilidades específicas de Apartec S.A y priorizar riesgos según su gravedad.
- **Desarrollo de políticas de seguridad:** Establece un modelo normativo conciso para la protección de la información, alineado con estándares internacionales.
- **Implementación de controles de seguridad:** Propone medidas técnicas, físicas y administrativas concretas para minimizar los riesgos expuestos.
- **Gestión de accesos privilegiados:** Controla y supervisa los accesos ante sistemas comprometidos, reduciendo los incidentes internos.
- **Protección de datos personales y confidenciales:** Garantiza el desempeño de la normativa vigente y protege la información sensible de la empresa y sus clientes.
- **Preparación para respuestas a incidentes:** Define un plan de acción claro para minimizar impactos de posibles incidentes de seguridad.
- **Formación y concienciación:** Capacitar al personal de Apartec S.A en temas de seguridad de la información y desarrollando su interés en estos temas.

Beneficios Específicos para Apartec S.A

- **Reducción del riesgo de incidentes de seguridad:** Minimiza la probabilidad de pérdidas económicas, daños a la reputación y sanciones legales.
- **Mejora de la eficiencia operativa:** Optimiza procesos de seguridad y reduce el tiempo de respuesta por incidentes.
- **Fortalecimiento de la confianza de los clientes:** Demuestra el compromiso de Apartec S.A con la protección de la información.
- **Cumplimiento de la norma vigente**: Evita sanciones y mejora la imagen de la empresa.

- **Acceso a herramientas de seguridad de alta calidad a bajo costo:** El uso de sistemas de código abierto o licencia gratuita reduce la dependencia de herramientas comerciales costosas.

c. Estrategias y/o técnicas

Los métodos y estrategias utilizados en la elaboración de la propuesta de seguridad para Apartec S.A. se pueden resumir en los siguientes puntos.:

1. Evaluación de riesgos y análisis de impacto

La evaluación de riesgos Tabla 21. Es un proceso sistemático para identificar, analizar y priorizar los riesgos que pueden afectar la seguridad de la información en una empresa. El análisis de impacto ayuda a determinar las consecuencias potenciales de estos riesgos.

Tabla 21.

Evaluación de riesgos

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Identificación de activos	Listar los activos de información críticos (información de huéspedes, sistemas de reservas, bases de datos, etc.).	A.8.1.1 (Inventario de activos), A.8.2.1 (Clasificación de la información).	OWASP Risk Assessment Framework
Identificación de amenazas	Reconocer posibles amenazas (ciberataques, errores humanos, desastres naturales).	Cláusula 6.1.2 (Identificación de riesgos), A.5.7 (Amenazas a la seguridad de la información).	
Evaluación de vulnerabilidades	Determinar las debilidades en los sistemas y procesos que podrían ser explotadas.	Cláusula 6.1.2 (Evaluación de riesgos), A.12.6.1 (Gestión de vulnerabilidades técnicas).	
Calculo y riesgo	Estimar la probabilidad de que ocurra incidentes y su impacto potencial.	Cláusula 6.1.2 (Análisis y evaluación de riesgos), A.5.1 (Políticas para la gestión de riesgos).	
Priorización	Clasificar los riesgos según su gravedad	Cláusula 6.1.3 (Tratamiento de riesgos),	

	para enfocar los esfuerzos en los más críticos.	A.5.1.2 (Aceptación de riesgos).

2. Desarrollo de políticas

Las políticas de seguridad Tabla 22. Son documentos oficiales que definen normas y procedimientos para salvaguardar la información y los sistemas de una empresa.

Tabla 22.

Desarrollo de políticas

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Política de uso aceptable	Define cómo los empleados deben utilizar los recursos tecnológicos.	A.8.1.3 (Aceptación del uso de activos), A.6.2 (Uso de dispositivos móviles y teletrabajo).	**Políticas de Seguridad:** OWASP Security Policy Templates, Snipe-IT. **Respuesta a incidentes:** TheHive, MISP.
Política de contraseñas	Establece requisitos para la creación y gestión de contraseñas seguras.	A.9.4.3 (Gestión de información de autenticación), A.9.2.4 (Gestión de credenciales).	
Política de acceso a la información	Define quien puede acceder a que información y bajo qué condiciones.	A.9.1 (Controles de acceso), A.9.2.3 (Derechos de acceso privilegiados), A.9.4.1 (Restricción de acceso).	
Política de respuesta a incidentes	Establece los pasos a seguir en caso de un incidente de seguridad.	A.5.24 (Gestión de incidentes), A.5.25 (Aprendizaje de incidentes), A.5.26 (Recopilación de evidencia)	

3. Implementación de controles de seguridad

Los controles de seguridad Tabla 23. Son medidas técnicas, físicas y administrativas que se adoptan para reducir los riesgos identificados.

Tabla 23.

Controles de seguridad

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Controles técnicos:	Firewalls, sistemas de detección de intrusiones (IDS), cifrado de datos y actualizaciones de software.	A.8.1 (Gestión de activos), A.9 (Control de acceso), A.12 (Seguridad de las operaciones).	**OSSEC** (detección de intrusiones). **Snort** (sistema de prevención de intrusiones). **OpenVAS** (análisis de vulnerabilidades).
Controles físicos	Acceso restringido a áreas críticas, sistemas de vigilancia, protección contra incendios.	A.7.1 (Seguridad física y del entorno), A.11.1 (Áreas seguras), A.11.2 (Equipos).	
Controles administrativos	Políticas de seguridad, capacitación del personal, auditorías periódicas.	A.5 (Políticas de seguridad de la información), A.6 (Organización de la seguridad de la información), A.7 (Gestión de recursos humanos), A.12 (Seguridad de las operaciones).	

4. Gestión de accesos privilegiados

La gestión de accesos privilegiados Tabla 24. Se refiere al control y supervisión de los usuarios que tienen permisos especiales para acceder a sistemas críticos.

Tabla 24.

Gestión acceso privilegiados

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Principio de mínimo privilegio	Otorgar solo los permisos necesarios para realizar una tarea específica.	A.9.1.2 (Control de acceso a redes y servicios), A.9.2.3 (Gestión de derechos de acceso privilegiados), A.9.4.1 (Restricción de acceso a la información).	**Wazuh** para la monitorización de accesos.
Autenticación de dos factores(2FA)	Requerir una segunda forma de autenticación para acceder a sistemas críticos.	A.9.4.2 (Autenticación de usuarios), A.9.4.3 (Gestión de información de autenticación).	
Monitoreo y registro	Registrar todas las actividades realizadas por usuarios privilegiados para detectar comportamientos sospechosos.	A.12.4.1 (Registro de eventos), A.12.4.3 (Protección de la información de registro), A.12.4.4 (Monitoreo y análisis de registros).	

5. Protección de datos personales y confidenciales

La protección de datos personales y confidenciales Tabla 25. Consiste en asegurar que la información confidencial de los huéspedes y de la empresa no pueda ser accedida, alterada ni eliminada por personas no autorizadas.

Tabla 25.

Protección de datos personales

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Cifrado de datos	Garantizar que los datos sensibles estén cifrados tanto en reposo como en tránsito. Esto ayuda a mitigar el riesgo de accesos no autorizados en caso de robo o pérdida de dispositivos.	A.10.1.1 (Política de uso de controles criptográficos), A.8.2.3 (Protección de la información en medios), A.12.3.1 (Copia de seguridad de la información).	**GnuPG (GNU Privacy Guard):** Herramienta gratuita de código abierto del estándar OpenPGP para procesos de cifrado y firma digital.
Clasificación de datos	Identificar y etiquetar los datos según su nivel de confidencialidad.	A.8.2.1 (Clasificación de la información), A.8.2.2 (Etiquetado de la información), A.8.2.3 (Protección de la información en medios).	**Metaclassifier:** Herramienta de código abierto para clasificar y etiquetar datos según su sensibilidad.
Eliminación segura	Asegurar que los datos obsoletos se eliminen de manera segura (por ejemplo, mediante la destrucción física de discos duros y sobreescritura).	A.8.3.2 (Eliminación de medios), A.8.3.3 (Recolección segura de activos), A.12.3.1 (Copia de seguridad de la información).	**DBAN (Darik's Boot and Nuke):** Herramienta de eliminación segura de discos duros mediante arranque desde USB o CD.

6. Preparación para respuesta a incidentes

La preparación para respuesta a incidentes Tabla 26. Consiste en una guía estructurada para detectar, contener y recuperarse de incidentes de seguridad.

Tabla 26.

Respuesta a incidentes

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Detección temprana:	Uso de sistemas de monitoreo y alertas tempranas.	A.12.4.1 (Registro de eventos), A.12.6.1 (Gestión de vulnerabilidades técnicas).	**OSSEC** (HIDS), **Snort** (NIDS), **Wazuh** (SIEM).
Plan de respuesta:	Establecer roles y responsabilidades, además de pasos a seguir en caso de un incidente.	A.5.24 (Gestión de incidentes de seguridad de la información), A.5.25 (Aprendizaje de incidentes de seguridad de la información).	**TheHive** (gestión de incidentes). **MISP** (inteligencia de amenazas).
Pruebas y simulacros:	Realizar ejercicios periódicos para asegurar que el personal esté preparado.	A.5.26 (Recopilación de evidencia), A.17.1 (Continuidad del negocio).	**Metasploit** (simulación de ataques)
Recuperación:	Tener un plan de recuperación de desastres que incluya copias de seguridad y instrucciones para restituir sistemas.	A.12.3.1 (Copia de seguridad de la información), A.17.1 (Continuidad del negocio).	**Bacula:** Es un software gestión de copias de seguridad, recuperación y verificación de datos en una red.

7. Formación y concienciación

La formación y concienciación en seguridad de la información Tabla 27. Es crucial para asegurar que todos los empleados comprendan los riesgos y tengan un criterio para positivo para proteger los activos de la organización.

Tabla 27.

Formación y concienciación

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Capacitación regular:	Sesiones de formación sobre políticas de seguridad, phishing, y buenas prácticas.	A.7.2.2 (Concienciación, educación y formación en seguridad de la información), A.7.3.1 (Términos y condiciones de empleo).	**Moodle** (plataforma de aprendizaje en línea).
Simulaciones de phishing:	Realizar pruebas para evaluar la concienciación de los empleados.	A.7.2.2 (Concienciación, educación y formación), A.12.6.1 (Gestión de vulnerabilidades técnicas).	**GoPhish** (Herramienta de código abierto para crear y enviar campañas de phishing simuladas)
Materiales de apoyo:	Crear guías, carteles y recursos digitales para reforzar los mensajes de seguridad.	A.7.2.2 (Concienciación, educación y formación), A.6.1.1 (Responsabilidades de seguridad de la información).	**OWASP Security Knowledge Framework** (guías de seguridad). **Canva** (creación de materiales visuales)

Estos aspectos son esenciales para crear un sistema de gestión de seguridad de la información (SGSI) sólido y en conformidad con las mejores prácticas internacionales.

La implementación de estas medidas no solo protegerá a Apartec S.A de ciberamenazas, sino que también mejorará la confianza de los huéspedes y cumplirá con las normativas vigentes.

2.3. Validación de la propuesta

Se ha elegido a un conjunto de especialistas idóneos para evaluar la propuesta presentada, los cuales cuentan con formación académica y experiencia laboral o académica en seguridad informática, y han mostrado su disposición a participar en la evaluación. La información detallada se encuentra en el **Anexo 4** y **Anexo 5**.

Tabla 28.

Resultado validación

Indicador	Experto 1	Experto 2	Total	Porcentaje
Impacto	5	4	9	12.86%
Aplicabilidad	4	5	9	12.86%
Conceptualización	4	5	9	12.86%
Actualidad	5	5	10	14,29%
Calidad Técnica	5	5	10	14,29%
Factibilidad	5	5	10	14,29%
Pertinencia	5	5	10	14,29%
Total	33	34	67	95.74

2.4. Matriz de articulación de la propuesta

En la TABLA 30. Se presenta una matriz que sintetiza la integración del producto desarrollado con los fundamentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos utilizados.

Tabla 29.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Estudio de la ISO 27001	Norma establecida para realizar un SGSI para la protección de la información (ISO, 2022).	Metodología Bibliográfica.	Análisis de la norma.	Proporciona una visión integral y establece definiciones clave en el ámbito de la seguridad informática.	Investigación Bibliográfica.
Determinar los límites y los objetivos de la política	Definir, considerando el entorno empresarial, significa establecer el alcance y los objetivos	Metodología de investigación mixta.	Análisis de bibliografía y encuestas.	Determina el alcance y objetivos en función de la empresa.	Encuestas.

Selección de controles de Seguridad de Información.	Análisis de controles (NQA, 2024).	Metodología Bibliográfica.	Elaboración de matriz con controles a usar.	Implementación de controles factibles.	Investigación, Observación.
Selección de Herramientas de Software Libre o Código Abierto.	Análisis de controles ISO/IEC 27001 (NQA, 2024).	Experimental	Elaboración de matriz y aplicabilidad	Analiza cada control y propone un sistema para gestionarla.	Investigación, Observación.

CONCLUSIONES

Con la elaboración de esta tesina se logró identificar que la seguridad de la información es fundamental para el sector hotelero en especial para la empresa Apartec S.A, dado que la protección de datos de los huéspedes es crítica. La propuesta de herramienta de código abierto es una opción viable para las PYMES hoteleras, ya que ofrecen soluciones económicas y adaptables al medio, pero para gestionarlas se necesita personal capacitado en protección de la información y en normas ISO/IEC 27001.

A través de encuestas realizados a ciertos sectores de la empresa se identificaron varias vulnerabilidades, como falta de capación en seguridad informática, ausencia de políticas de seguridad y falta de herramientas de código abierto. Por otro lado, se detectó que la empresa cuenta con controles básicos de la norma ISO/IEC 27001 pero no son suficientes para garantizar un correcto manejo de informacion sensible.

Se propuso un plan de seguridad integral que incluye la evaluación de riesgos, implementación de controles técnicos y administrativos y gestión de accesos. El plan fue elaborado en base de norma ISO/IEC 27001 para proponer en base de controles analizados, herramientas que gestionen su seguridad de manera eficiente y económica.

Este proyecto fue validado por especialistas en el tema de seguridad informática y especialistas en el manejo del negocio hotelero. Los especialistas destacaron la importancia de formación y concienciación del personal en temas de seguridad, además de la realización de auditorías periódicas para garantizar la efectividad de los controles aplicados. Además, resaltaron que este plan puede ser replicado en otras empresas del sector hotelero.

En conclusión, este proyecto destaco la necesidad de un sistema integral de seguridad de la informacion que se acople con herramientas de código libre y estándares de la norma ISI/IEC27001, demostrando que el uso de herramientas de código abierto es una solución viable para PYMES hoteleras, reduciendo costos sin comprometer la calidad de la seguridad.

RECOMENDACIONES

Es recomendable realizar estudios detallados de la efectividad de herramientas de software libre o código abierto en sectores hoteleros para garantizar mejores prácticas.

Dado que se identificó que el personal de la empresa no está debidamente capacitado en temas de seguridad de información, es factible realizar capacitaciones donde el personal experimente en primera persona, simulaciones de ataques de phishing, ingeniería social, prácticas de protección de datos y sobre todo talleres de políticas de seguridad.

Se recomienda que la empresa Apartec S.A realice un cronograma para auditorías internas y externas para evaluar el cumplimiento de políticas de seguridad, además de verificar si los controles aplicados dan efecto en la seguridad de la empresa.

Socializar los resultados de este proyecto en publicaciones académicas relacionadas con la seguridad informática en PYMES hoteleros para compartir experiencias con profesionales en la misma área.

Dado que el modelo propuesto es adaptable a otros PYMES hoteleros se recomienda compartir esta información con empresas hoteleras que enfrenten los mismos problemas en términos de seguridad de la información.

BIBLIOGRAFÍA

Arcos, M. (2023). *Análisis de brechas para la protección de datos personales en base a LOPD: Caso Mobilvendor.* https://repositorio.uisrael.edu.ec/bitstream/47000/3544/1/UISRAEL-EC-MASTER-SEGINF%

Bosch. (2010). On the impact of software product lines global development and ecosystems. *83*, 67-76.

Holdsonsworh, J., y Kosinski, M. (26 de 07 de 2024). *IBM*. https://www.ibm.com/mx-es/topics/information-security

ISO. (10 de 2022). *https://www.iso.org/es/norma/27001.*

Kaspersky. (2022). ITSecurity Economics 2022 Executive Summary. https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf

Medina, P., Chango, M., Corella , M., y Guizado, D. (2023). Transformación digital en las empresas: una revisión conceptual. *14*.

NQA. (2024). Cuenta atrás para el final de la transición a ISO 27001:2022.

Sisti, M. A. (2019). SEGURIDAD INFORMÁTICA: LA PROTECCION DE LA INFORMACION EN UNA EMPRESA VITIVINÍCULA DE MENDOZA.

Tigse Moposita, J. L. (2020). *PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGIA DE LA INFORMACÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.* https://repositorio.uta.edu.ec/server/api/core/bitstreams/856f7eb5-6416-41e0-895d-fafebc6aff27/content

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

Datos

Nombre:

Cargo: **Personal de TI**

Infraestructura:

Pregunta 1: ¿La empresa utiliza un firewall en el borde de su red?

Pregunta 2: ¿Se realizan copias de seguridad de los datos críticos diariamente?

Pregunta 3: ¿Se utiliza cifrado en las comunicaciones de red?

Pregunta 4: ¿Se realiza una auditoría de seguridad de la red al menos una vez al año?

Software y sistemas:

Pregunta 5: ¿Todos los sistemas operativos y aplicaciones están actualizados con los últimos parches de seguridad?

Pregunta 6: ¿Se utiliza un sistema de detección de intrusiones (IDS) o un sistema de prevención de intrusiones (IPS)?

Pregunta 7: ¿Se ha implementado la autenticación de dos factores (2FA) para el acceso remoto?

Pregunta 8: ¿Se realiza un análisis de vulnerabilidades de las aplicaciones web periódicamente?

Conocimiento de la norma:

Pregunta 9: ¿Está familiarizado con la norma ISO/IEC 27001:2022?

Pregunta 10: ¿Considera que la empresa cumple actualmente con los principales requisitos de la norma?

Código abierto:

Pregunta 11: ¿Se han considerado herramientas de seguridad de código abierto en la empresa?

Pregunta 12: ¿Se ha implementado alguna herramienta de seguridad de código abierto en la empresa?

ANEXO 2

FORMATO DE ENCUESTA

Datos

Nombre: _____

Cargo: **Personal Administrativo**

Gestión de la información:

Pregunta 13: ¿Existen políticas de seguridad de la información documentadas y accesibles para todos los empleados?

Pregunta 14: ¿Se realiza capacitación en seguridad de la información para los empleados al menos una vez al año?

Pregunta 15: ¿Se exige el uso de contraseñas complejas y se cambia periódicamente?

Incidentes:

Pregunta 16: ¿Ha habido incidentes de seguridad de la información en su departamento en el último año?

Pregunta 13: ¿Conoce el procedimiento para reportar un incidente de seguridad?

ANEXO 3

FORMATO DE ENCUESTA

Datos

Nombre: _____

Cargo: **Atención Al Cliente**

Manejo de datos:

Pregunta 14: ¿Se destruyen los documentos con información de los huéspedes de forma segura?

Pregunta 15: ¿Se verifica la identidad de los huéspedes antes de proporcionar información personal?

Pregunta 16: ¿Se guarda información de tarjetas de crédito de los clientes en algún medio físico?

Capacitación:

Pregunta 17: ¿Ha recibido capacitación sobre protección de datos personales?

ANEXO 4

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: BRYAN RENAN SOTALIN QUIJIA

Titulo obtenido
Ingeniero en sistemas informáticos
Cédula de Identidad
1721297313
E- mail
z0tabrs@gmail.com
Institución de Trabajo
Puntonet S.A.
Cargo
Analista de la Dirección de Infraestructura, Seguridad y Soporte de T.I.
Años de experiencia en el área
9 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- 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: Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		X			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		X			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		25	8			

Observaciones: Es esencial contar con un plan de respuesta a incidentes que detalle claramente los protocolos a seguir en caso de ciberataques. Además, mantenernos informados sobre las amenazas cibernéticas y las tácticas de ingeniería social permitirá mitigar los riesgos de posibles ataques de manera efectiva.

Recomendaciones

Para asegurar un servicio de calidad, es esencial mantener los sistemas actualizados con los últimos parches de seguridad e implementar herramientas que ayuden a prevenir y gestionar posibles ataques de manera eficaz.

Lugar, fecha de validación: Quito D.M. 07 de marzo de 2025

Firma del especialista

ANEXO 5

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: OBANDO CHANTRE DARWIN ALEXANDER

Título obtenido
INGENIERO EN SISTEMAS DE INFORMACIÓN
Cédula de Identidad
1719706994
E- mail
Darex_47@hotmail.com
Institución de Trabajo
Hospital Ingles CIA.LTDA
Cargo
Coordinador del área de sistemas
Años de experiencia en el área
5

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- 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: Medidas de seguridad mediante Código Abierto bajo Normas ISO/IEC 27001 para la protección de Información en Apartec S.A.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		X			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	X				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*		X			
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	X				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		25	8			

Observaciones: La capacitación del personal administrativo en temas de seguridad de la información es crucial para proteger los datos sensibles. Además, la implementación de un sistema de autenticación y controles de doble factor (2FA) fortalecerá la seguridad de los sistemas, reduciendo el riesgo de accesos no autorizados.

Recomendaciones

Es esencial cifrar los datos sensibles de la empresa y de los clientes para que, en caso de una filtración, los ciberdelincuentes no puedan aprovechar esa información. Además, es crucial realizar copias de seguridad regularmente para prevenir posibles ataques de denegación de servicio, ya que un incidente de este tipo podría reducir la confianza de los clientes.

Lugar, fecha de validación: Quito D.M. 07 de marzo de 2025

Firma del especialista

ANEXO 6

Versión 1.0 Año: 2025

Universidad Israel

Guía

Medidas de Seguridad aplicando Normas ISO/IEC 27001 mediante uso de herramientas de Código Abierto.

Autor: Guillermo Cauja

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Contextualización del Problema de Seguridad Informática.

La seguridad de la información es un aspecto fundamental que las organizaciones en especial el sector hotelero deben priorizar para garantizar su sostenibilidad y éxito en la era digital.

Sin embargo, este escenario también atrae amenazas cibernéticas cada vez más sofisticadas, como ransomware, phishing y brechas de datos, que ponen en riesgo no solo la operatividad de las empresas, sino también su reputación y cumplimiento legal.

Objetivo del Modelo

La presente guía se encamina en una proposición del uso de herramientas de código libre para mitigar amenazas que puede surgir en el ámbito hotelero, se empleara normas ISO/IEC 27001 de acuerdo a la necesidad de la empresa Apartec S.A.

Público Objetivo

La seguridad de la información es un aspecto fundamental que las organizaciones en especial el sector hotelero deben priorizar para garantizar su sostenibilidad y éxito en la era digital.

La creciente dependencia de sistemas tecnológicos interconectados, la gestión de gran cantidad de datos sensibles y la sofisticación de las ciberamenazas han elevado la seguridad de la información a prioridad estratégica en la industria hotelera.

Metodología utilizada para su desarrollo

Para el desarrollo de este modelo de investigación se uso la metodóloga cuantitativa y cualitativa ya que con encuestas planteadas a diferentes áreas de trabajo como TI, Administrativas y Atención al Cliente. Además de representar tal información en tablas y gráficos para un mejor entendimiento de los problemas que presenta la empresa.

Como utilizar el modelo

El presente modelo se debe implementar en fases estructuradas que incluyen la evaluación de riegos, aplicación de controles de seguridad y aplicación de herramientas de código abierto o software libre.

2. FUNDAMENTOS TEÓRICOS Y CONCEPTUALES

2.1 ISO/IEC 27001

Norma más utilizada a nivel mundial para sistemas de gestión de la seguridad de la información. Este estándar define requisitos esenciales que un SGSI debe cumplir y proporciona a las organizaciones sin importar su tamaño o sector de trabajo, propone directrices claras para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información.

Además, promueve buenas prácticas y un enfoque estructurado para proteger los datos y garantizar la confidencialidad, integridad y disponibilidad de la información.

Implica que una organización o empresa ha implantado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja, y que este sistema respeta todas las buenas prácticas y principios contemplados en esta Norma Internacional. (ISO, 2022).

2.3 Herramientas de Código Abierto

Software con código fuente accesible y modificable que ofrece flexibilidad, transparencia y en muchos casos, una alternativa económica a soluciones propietarias. En seguridad abarcan desde sistemas cortafuegos, sistemas de detección de intrusos hasta herramientas de análisis de vulnerabilidades y gestión de seguridad.

2.4 Sector Hotelero y PYMES

Las PYMES hoteleras en particular enfrentan desafíos únicos en seguridad de la información debido al manejo de datos sensibles, la dependencia de sistemas tecnológicos y las limitaciones presupuestarias.

2.5 Medidas de Seguridad

Según Arcos (2023) Consiste en elaborar un documento que encuadre en un conjunto de acciones y medidas adecuadas para proteger la información de las empresas, su objetivo principal es establecer el propósito del Sistema de Gestión de

Seguridad Informática (SGSI) y del propio documento, definiendo las normas y responsabilidades necesarias para garantizar la seguridad de los datos y los sistemas.

2.6 Sistema Gestión de Seguridad de la Información

Abarca un conjunto de manuales, controles y técnicas diseñados para gestionar y proteger todos los activos de información que se manejan dentro de una empresa. (Tigse Moposita, 2020).

3. DESCRIPCIÓN DEL MODELO DE SEGURIDAD INFORMÁTICA

3.1. Elementos del Modelo

El modelo de seguridad informática basada en la norma ISO/IEC 27001 par la empresa Apartec S.A, está compuesto por varios elementos clave que garantizan la protección de la informacion y mitigación de riesgos.

Estos elementos se demuestran en un enfoque estructurado:

3.1.1. Principales componentes de seguridad.

Gestión de riesgos y políticas de seguridad: Conste en la evaluación y clasificación de activos para identificar amenazas y vulnerabilidades para posterior implementar controles de seguridad alineados con la norma IO/IEC 27001.

Protección de la información: La empresa debe contar con controles que salvaguarde los datos de la empresa como de sus huéspedes. Se debe implementar un control de acceso según roles administrativos, crear políticas de seguridad de contraseñas seguras, autentificación multifactorial (2FA) y sobre todo cifrar datos.

Detección de amenazas: Implementar sistemas que detecten amenazas en el contorno de la red LAN y red WAN, es viable la implementación de sistemas de detección de instrucciones y prevención.

Respuesta de Incidentes y Recuperación: Realizar copias de seguridad periódicas de información es viable ya que por si ocurre algún desastre o filtración de datos la empresa pueda recuperar esa información para su correcto funcionamiento.

Capacitación y Concienciación: Capacitar al personal periódicamente en temas de seguridad de la información ayudara a que el personal detecte cuando este ante un posible ataque de phishing o ingeniería social. Por ende, el personal de TI a

cargo de la seguridad de la información debe realizar simulacros de estos posibles ataques.

3.1.2. Representación visual o diagramas del modelo.

Figura 1.

Diagrama Estructura General

3.2. Implementación del Modelo aplicando Normas ISO/IEC 27001.

Para la realización de este modelo enfocado en la Figura1. Procederemos a realizar tablas en la cuales se definen:

- Evaluación de riesgos
- Desarrollo de políticas
- Implementación de controles de seguridad
- Gestión de accesos
- Protección de datos
- Respuesta a incidentes
- Formación y concienciación

Todos estos puntos muestran la aplicabilidad, normas ISO/IEC 27001 a utilizar y herramientas se software libre a usar para mitigar cada punto.

A continuación de definirá un modelo de tabla a aplicar para procesar los puntos propuestos donde su estructura se define por pasos clave, aplicabilidad, normas ISO/27001 y herramientas. Ver Tabla 1 para comprender esta propuesta.

Tabla 1.

Diseño de las tablas a aplicar

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramientas
Puntos a integrar controles	Se describe la forma de aplicabilidad.	Se identifica controles de la Norma ISO/IEC 27001.	Se propone una herramienta de Código Abierto o Software libre

3.2.1 Evaluación de riesgos

La evaluación de riesgos es un proceso sistemático para identificar, analizar y priorizar los riesgos que pueden afectar la seguridad de la información en una empresa. El análisis de impacto ayuda a determinar las consecuencias potenciales de estos riesgos.

Tabla 2.

Evaluación de riesgos

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramientas
Identificación de activos	Listar los activos de información críticos (información de huéspedes, sistemas de reservas, bases de datos, etc.).	✓ A.8.1.1 (Inventario de activos) ✓ A.8.2.1 (Clasificación de la información)	OWASP Risk Assessment Framework
Identificación de amenazas	Reconocer posibles amenazas (ciberataques, errores humanos, desastres naturales).	✓ Cláusula 6.1.2 (Identificación de riesgos) ✓ A.5.7 (Amenazas a la seguridad de la información)	OWASP Risk Assessment Framework
Evaluación de vulnerabilidades	Determinar las debilidades en los sistemas y procesos que podrían ser explotadas.	✓ Cláusula 6.1.2 (Evaluación de riesgos) ✓ A.12.6.1 (Gestión de vulnerabilidades técnicas)	OWASP Risk Assessment Framework
Calculo y riesgo	Estimar la probabilidad de que ocurra incidentes y su impacto potencial.	✓ Cláusula 6.1.2 (Análisis y evaluación de riesgos) ✓ A.5.1 (Políticas para la gestión de riesgos).	OWASP Risk Assessment Framework
Priorización	Clasificar los riesgos según su gravedad para enfocar los esfuerzos en los más críticos.	✓ Cláusula 6.1.3 (Tratamiento de riesgos) ✓ A.5.1.2 (Aceptación de riesgos)	OWASP Risk Assessment Framework

3.2.2. Desarrollo de políticas

Las políticas de seguridad son documentos oficiales que definen normas y procedimientos para salvaguardar la información y los sistemas de una empresa.

Tabla 3.

Desarrollo de políticas

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramientas
Política de uso aceptable	Define cómo los empleados deben utilizar los recursos tecnológicos.	✓ A.8.1.3 (Aceptación del uso de activos) ✓ A.6.2 (Uso de dispositivos móviles y teletrabajo).	✓ OWASP Security Policy Templates, Snipe-IT.
Política de contraseñas	Establece requisitos para la creación y gestión de contraseñas seguras.	✓ A.9.4.3 (Gestión de información de autenticación) ✓ A.9.2.4 (Gestión de credenciales).	
Política de acceso a la información	Define quien puede acceder a que información y bajo qué condiciones.	✓ A.9.1 (Controles de acceso) ✓ A.9.2.3 (Derechos de acceso privilegiados) ✓ A.9.4.1 (Restricción de acceso).	
Política de respuesta a incidentes	Establece los pasos a seguir en caso de un incidente de seguridad.	✓ A.5.24 (Gestión de incidentes) ✓ A.5.25 (Aprendizaje de incidentes) ✓ A.5.26 (Recopilación de evidencia)	✓ TheHive, MISP.

3.2.3 Implementación de controles de seguridad

Los controles de seguridad son medidas técnicas, físicas y administrativas que se adoptan para reducir los riesgos identificados.

Tabla 4.

Controles de seguridad

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Controles técnicos:	Firewalls, sistemas de detección de intrusiones (IDS), cifrado de datos, actualizaciones de software.	✓ A.8.1 (Gestión de activos) ✓ A.9 (Control de acceso) ✓ A.12 (Seguridad de las operaciones).	✓ **OSSEC** (detección de intrusiones).
Controles físicos	Acceso restringido a áreas críticas, sistemas de vigilancia, protección contra incendios.	✓ A.7.1 (Seguridad física y del entorno) ✓ A.11.1 (Áreas seguras), A.11.2 (Equipos).	✓ **Snort** (sistema de prevención de intrusiones).
Controles administrativos	Políticas de seguridad, capacitación del personal, auditorías periódicas.	✓ A.5 (Políticas de seguridad de la información) ✓ A.6 (Organización de la seguridad de la información) ✓ A.7 (Gestión de recursos humanos) ✓ A.12 (Seguridad de las operaciones).	✓ **OpenVAS** (análisis de vulnerabilidades).

3.2.4 Gestión de accesos privilegiados

La gestión de accesos privilegiados se refiere al control y supervisión de los usuarios que tienen permisos especiales para acceder a sistemas críticos.

Tabla 5.

Gestión acceso privilegiados

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Principio de mínimo privilegio	Otorgar solo los permisos necesarios para realizar una tarea específica.	✓ A.9.1.2 (Control de acceso a redes y servicios) ✓ A.9.2.3 (Gestión de derechos de acceso privilegiados) ✓ A.9.4.1 (Restricción de acceso a la información).	✓ **Wazuh** para la monitorización de accesos.
Autenticación de dos factores(2FA)	Requerir una segunda forma de autenticación para acceder a sistemas críticos.	✓ A.9.4.2 (Autenticación de usuarios) ✓ A.9.4.3 (Gestión de información de autenticación).	
Monitoreo y registro	Registrar todas las actividades realizadas por usuarios privilegiados para detectar comportamientos sospechosos.	✓ A.12.4.1 (Registro de eventos) ✓ A.12.4.3 (Protección de la información de registro) ✓ A.12.4.4 (Monitoreo y análisis de registros).	

3.2.5 Protección de datos personales y confidenciales

La protección de datos personales y confidenciales consiste en asegurar que la información confidencial de los huéspedes y de la empresa no pueda ser accedida, alterada ni eliminada por personas no autorizadas.

Tabla 6.

Protección de datos personales

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Cifrado de datos	Garantizar que los datos sensibles estén cifrados tanto en reposo como en tránsito. Esto ayuda a mitigar el riesgo de accesos no autorizados en caso de robo o pérdida de dispositivos.	✓ A.10.1.1 (Política de uso de controles criptográficos) ✓ A.8.2.3 (Protección de la información en medios) ✓ A.12.3.1 (Copia de seguridad de la información).	✓ **GnuPG (GNU Privacy Guard):** Herramienta gratuita de código abierto del estándar OpenPGP para procesos de cifrado y firma digital.
Clasificación de datos	Identificar y etiquetar los datos según su nivel de confidencialidad.	✓ A.8.2.1 (Clasificación de la información) ✓ A.8.2.2 (Etiquetado de la información) ✓ A.8.2.3 (Protección de la información en medios).	✓ **Metaclassifier:** Herramienta de código abierto para clasificar y etiquetar datos según su sensibilidad.
Eliminación segura	Asegurar que los datos obsoletos se eliminen de manera segura (por ejemplo, mediante la destrucción física de discos duros y sobreescritura).	✓ A.8.3.2 (Eliminación de medios) ✓ A.8.3.3 (Recolección segura de activos) ✓ A.12.3.1 (Copia de seguridad de la información).	✓ **DBAN (Darik's Boot and Nuke):** Herramienta de eliminación segura de discos duros mediante arranque desde USB o CD.

3.2.6 Preparación para respuesta a incidentes

La preparación para respuesta a incidentes consiste en una guía estructurada para detectar, contener y recuperarse de incidentes de seguridad.

Tabla 7.

Respuesta a incidentes

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Detección temprana:	Uso de sistemas de monitoreo y alertas tempranas.	✓ A.12.4.1 (Registro de eventos) ✓ A.12.6.1 (Gestión de vulnerabilidades técnicas).	✓ **OSSEC** (HIDS), ✓ **Snort** (NIDS), ✓ **Wazuh** (SIEM).
Plan de respuesta:	Establecer roles y responsabilidades, además de pasos a seguir en caso de un incidente.	✓ A.5.24 (Gestión de incidentes de seguridad de la información) ✓ A.5.25 (Aprendizaje de incidentes de seguridad de la información).	✓ **TheHive** (gestión de incidentes). ✓ **MISP** (inteligencia de amenazas).
Pruebas y simulacros:	Realizar ejercicios periódicos para asegurar que el personal esté preparado.	✓ A.5.26 (Recopilación de evidencia) ✓ A.17.1 (Continuidad del negocio)	✓ **Metasploit** (simulación de ataques)
Recuperación:	Tener un plan de recuperación de desastres que incluya copias de seguridad e instrucciones para restituir sistemas.	✓ A.12.3.1 (Copia de seguridad de la información) ✓ A.17.1 (Continuidad del negocio).	✓ **Bacula:** Es un software gestión de copias de seguridad, recuperación y verificación de datos en una red.

3.2.7 Formación y concienciación

La formación y concienciación en seguridad de la información es crucial para asegurar que todos los empleados comprendan los riesgos y tengan un criterio positivo en proteger los activos de la organización.

Tabla 8.

Respuesta a incidentes

Pasos Clave	Aplicabilidad	Norma ISO 27001	Herramienta
Capacitación regular:	Sesiones de formación sobre políticas de seguridad, phishing, y buenas prácticas.	✓ A.7.2.2 (Concienciación, educación y formación en seguridad de la información) ✓ A.7.3.1 (Términos y condiciones de empleo).	✓ **Moodle** (plataforma de aprendizaje en línea).
Simulaciones de phishing:	Realizar pruebas para evaluar la concienciación de los empleados.	✓ A.7.2.2 (Concienciación, educación y formación) ✓ A.12.6.1 (Gestión de vulnerabilidades técnicas).	✓ **GoPhish** (Herramienta de código abierto para crear y enviar campañas de phishing simuladas)
Materiales de apoyo:	Crear guías, carteles y recursos digitales para reforzar los mensajes de seguridad.	✓ A.7.2.2 (Concienciación, educación y formación) ✓ A.6.1.1 (Responsabilidades de seguridad de la información).	✓ **OWASP Security Knowledge Framework** (guías de seguridad). ✓ **Canva** (creación de materiales visuales)

4. EVALUACIÓN Y VALIDACIÓN DEL MODELO

Para la validación del modelo y evaluar se recomienda hacerlo por los siguientes puntos:

4.3.1 Indicadores de Efectividad

- Números de incidentes de seguridad reportados antes y después de la implementación.
- Tiempo de respuesta ante incidentes de ciberseguridad
- Nivel de cumplimiento de seguridad.
- Tasa de éxito en simulaciones de ataques

4.3.2 Resultados Esperados y Métricas de Desempeño

- Reducción del 50% en vulnerabilidades críticas identificadas.
- Mejora del tiempo de respuesta ante incidentes en un 30%.
- Incremento del nivel de concienciación en seguridad del personal en un 70%.
- Cumplimiento del 100% de los controles de seguridad evaluados en auditorías.

5. APLICACIONES Y BENEFICIOS DE LA GUÍA

5.1 Áreas en la que se puede Aplicar

El modelo se seguridad basado en norma ISO/IEC27001 y herramientas de código abierto se puede aplicar en diferentes sectores:

- **Sector Hotelero:** Protección de datos de huéspedes y transacciones electrónicas.
- **Sector Financiero:** Seguridad en operaciones bancarias y cumplimiento normativo.
- **Sector Educativo:** Protección de información académica y datos personales.
- **Empresas de Comercio Electrónico:** Seguridad en plataformas de pago y prevención de fraudes.

5.2 Beneficios esperados en términos de seguridad

- **Reducción de Riesgos:** Disminución de ataques cibernéticos y filtraciones de datos.
- **Cumplimiento de Normativas:** Alineación con estándares internacionales como ISO/IEC 27001.

- **Ahorro de Costos**: Uso de herramientas de código abierto en lugar de soluciones comerciales costosas.
- **Mejora de la Confianza del Cliente**: Aseguramiento de la privacidad y protección de información personal.
- **Optimización de la Infraestructura de Seguridad**: Implementación de controles eficaces sin afectar la operatividad.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Con la elaboración de esta guía se logró identificar que la seguridad de la información es fundamental para el sector hotelero en especial para la empresa Apartec S.A, dado que la protección de datos de los huéspedes es crítica. La propuesta de herramienta de código abierto es una opción viable para las PYMES hoteleras, ya que ofrecen soluciones económicas y adaptables al medio, pero para gestionarlas se necesita personal capacitado en protección de la información y en normas ISO/IEC 27001.

Este proyecto fue validado por especialistas en el tema de seguridad informática y especialistas en el manejo del negocio hotelero. Los especialistas destacaron la importancia de formación y concienciación del personal en temas de seguridad, además de la realización de auditorías periódicas para garantizar la efectividad de los controles aplicados. Además, resaltaron que este plan puede ser replicado en otras empresas del sector hotelero.

6.2 Recomendaciones

Es recomendable realizar estudios detallados de la efectividad de herramientas de software libre o código abierto en sectores hoteleros para garantizar mejores prácticas.

Dado que se identificó que el personal de la empresa no está debidamente capacitado en temas de seguridad de información, es factible realizar capacitaciones donde el personal experimente en primera persona, simulaciones de ataques de phishing, ingeniería social, prácticas de protección de datos y sobre todo talleres de políticas de seguridad.

Se recomienda que la empresa Apartec S.A realice un cronograma para auditorías internas y externas para evaluar el cumplimiento de políticas de seguridad, además de verificar si los controles aplicados dan efecto en la seguridad de la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Arcos, M. (2023). *Análisis de brechas para la protección de datos personales en base a LOPD: Caso Mobilvendor*. https://repositorio.uisrael.edu.ec/bitstream/47000/3544/1/UISRAEL-EC-MASTER-SEGINF%

Bosch. (2010). On the impact of software product lines global development and ecosystems. *83*, 67-76.

Holdsonsworh, J., y Kosinski, M. (26 de 07 de 2024). *IBM*. https://www.ibm.com/mx-es/topics/information-security

ISO. (10 de 2022). *https://www.iso.org/es/norma/27001*.

Kaspersky. (2022). ITSecurity Economics 2022 Executive Summary. https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf

Medina, P., Chango, M., Corella , M., y Guizado, D. (2023). Transformación digital en las empresas: una revisión conceptual. *14*.

NQA. (2024). Cuenta atrás para el final de la transición a ISO 27001:2022.

Sisti, M. A. (2019). SEGURIDAD INFORMÁTICA: LA PROTECCION DE LA INFORMACION EN UNA EMPRESA VITIVINÍCULA DE MENDOZA.

Tigse Moposita, J. L. (2020). *PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGIA DE LA INFORMACÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.* https://repositorio.uta.edu.ec/server/api/core/bitstreams/856f7eb5-6416-41e0-895d-fafebc6aff27/content