UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021.

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnologías De La Información Y Comunicación
Autor/a:
Ing. Oscar Gustavo Lema Parco
Tutor/a:
Mgs. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005.

Elaborado por: Oscar Gustavo Lema Parco, de C.I:1721967394, estudiante de la Maestría: Maestría en Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.03.12 11:28:42 -05'00'

_____

PhD. Maryory Urdaneta Herrera

APROBACIÓN DEL TUTOR

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005.

Elaborado por: Oscar Gustavo Lema Parco, de C.I: 1721967394, 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

_____

Mgs. Renato Mauricio Toasa Guachi

C.I: 1804724167

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Oscar Gustavo Lema Parco con C.I: 172196739-4, autor/a del proyecto de titulación denominado: Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005. Previo a la obtención del título de Magister en Magister en Seguridad Informática.

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

Quito D.M., marzo de 2025

Firmado electrónicamente por:
OSCAR GUSTAVO LEMA PARCO

Ing. Oscar Lema Parco

Tabla de contenidos

APROBACIÓN DEL TUTOR ii
APROBACIÓN DEL TUTOR iii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE iv
INFORMACIÓN GENERAL 1
Contextualización del tema 1
Problema de investigación 2
Objetivo general 4
Objetivos específicos 4
Vinculación con la sociedad y beneficiarios directos: 4
1.1. Contextualización general del estado del arte 6
1.1.1. Seguridad de la Información 6
1.1.2. ISO 27000 y su relación con la seguridad de la información 6
1.1.2.1. ISO/IEC 27001 7
1.1.2.2. Gestión de Riesgos 7
1.1.2.3. ISO/IEC 27005 8
1.2. Proceso investigativo metodológico 9
1.2.1. Enfoque de la Investigación 9
1.2.2. Tipo de Investigación Aplicado 9
1.2.3. Métodos Teóricos y Prácticos Aplicados 10
1.2.4. Técnicas de recolección de datos. 10
1.2.4.1. Encuestas 10
1.2.4.2. Análisis Documental 10
1.2.4.3. Análisis de casos de éxito 10
1.3. Análisis de resultados 11
CAPÍTULO II: PROPUESTA 17
2.1. Fundamentos teóricos aplicados 17

2.1.1. Gestión de riesgos de seguridad de la información 17
2.1.2. Metodologías para análisis de riesgos 17
2.1.2.1. OCTAVE 18
2.1.2.2. MEHARI 18
2.1.2.3. MAGERIT 18
2.1.2.4. ISO/IEC 27005 19
2.2. Descripción de la propuesta 21
2.3. Validación de la propuesta 26
2.4. Matriz de articulación de la propuesta 27
CONCLUSIONES 29
RECOMENDACIONES 30
BIBLIOGRAFÍA 31
ANEXOS 33

Índice de tablas

Tabla 1 Población y muestra 11
Tabla 2 Criterio 1 Conocimiento 12
Tabla 3 Cumplimiento de las Normas SI 13
Tabla 4 Cultura sobre SI 14
Tabla 5 Percepción de las Normas de SI 15
Tabla 6 Valoración de activos 23
Tabla 7 Identificación de amenazas 24
Tabla 8 Estimación de riesgo 24
Tabla 9 Matriz de articulación 27

Índice de figuras

Figura 1 Porcentajes Criterio 1 12
Figura 2 Criterio 2 Cumplimiento 13
Figura 3 Cultura 14
Figura 4 Percepción de las Normas 15
Figura 5 Proceso para la Gestión del Riesgo 20
Figura 6 Ciclo Planificar-hacer-verificar-hacer (PHVA) 21
Figura 7 Estructura general de la propuesta 22

INFORMACIÓN GENERAL

Contextualización del tema

De acuerdo a Morales (2020), en el panorama actual la protección de los datos ha pasado a ser un fenómeno mundial, en parte al gran significado y relevancia que ha ocupado la información para todas las empresas ya sea pequeñas, medianas o grandes al tiempo que se relaciona con el aumento de ataques y violaciones a la información que ha existido en los últimos años. Considerando que ya no es suficiente proteger los equipos informáticos mediante un antivirus, sino que a medida que aparecen nuevas tecnologías, los atacantes descubren nuevas formas para vulnerar los sistemas.

En consecuencia, en el contexto de una empresa de telecomunicaciones, el área de soporte técnico desempeña un papel importante debido a que garantiza la continuidad operativa y la eficiencia de las operaciones en la organización. Esta área es responsable de responder a incidentes técnicos y brindar soluciones a problemas que afectan tanto a usuarios internos como externos y de atender las solicitudes relacionadas con equipos, software, mantenimientos, etc. lo que implica un manejo constante de información confidencial y datos sensibles de los clientes.

Sin embargo, emplear información importante de muchos clientes, han convertido al área de soporte técnico en un objetivo atractivo, debido que, al estar en el centro de interacciones, se vuelve vulnerable a varias amenazas a su integridad que, si no son gestionadas adecuadamente, pueden comprometer su seguridad.

Entre los riesgos comunes que enfrenta el área se encuentran el ingreso no autorizado a sistemas, ingeniería social dirigidos al personal de soporte técnico por medio phishing y la ejecución de ejecución de programas maliciosos en dispositivos administrados, ejecución de software no autorizado, accesos a portales web no autorizados.

A nivel organizacional, estas vulnerabilidades pueden traducirse en severas consecuencias, como perder datos, interrupciones operativas y daños a la imagen además de exponer la información a serios daños a su integridad pudiendo ocasionar pérdidas económicas sino se toman las acciones necesarias.

Según Babilonia (2023) las normas ISO 27000 son un conjunto de estándares que abordan las buenas prácticas para la SI y brindan varias ventajas, como mayor confianza hacia los clientes al mejorar la seguridad, el cumplimiento normativo y ventaja competitiva sobre otras empresas. Siendo estas normas adaptables a distintos tipos de organizaciones, independiente del tamaño o actividad que realice. Su implementación es de vital importancia para la organización debido que garantiza que la información cumpla con sus tres pilares fundamentales (confidencialidad, integridad y disponibilidad).

Según lo expuesto por Guevara y Soriano (2022) la norma ISO 27005 permite gestionar los riesgos que amenacen la SI de una empresa siendo aplicable a distintos tipos de organizaciones cuyo enfoque radica en mostrar un sistema de gestión del riesgo de seguridad de la información, destacando la tecnología de la información y puede aplicarse de forma complementaria a la ISO 27001 o de forma independiente.

Al seguir esta norma se lograría una adecuada implementación de controles específicos, como políticas de acceso restringido, capacitación contra ingeniería social y procedimientos estandarizados para la gestión de incidentes.

En este contexto, se tiene como objetivo diseñar una Propuesta para la aplicación de la Norma ISO/IEC 27005 para el área de Soporte Tecnico de una Empresa de Telecomunicaciones, tomando como base las directrices de la norma ISO 27005. La propuesta busca reforzar la capacidad de esta área para gestionar riesgos, proteger activos de información, reducir la exposición a riesgos tecnológicos y garantizar la continuidad operativa frente a amenazas cibernéticas. Además, la propuesta podrá ser adaptable y replicable, contribuyendo al fortalecimiento de la seguridad de la información a otras empresas de telecomunicaciones que deseen adoptarla.

Problema de investigación

En una empresa de Telecomunicaciones el área de soporte técnico mantiene una relación directa con el cliente; debido a que es responsable de atender requerimientos y dar respuesta a diversos tipos de incidentes relacionados con servicios internet, datos, telefonía o cloud etc., siendo necesaria para esta labor el manejo de información sensible de los clientes.

“En Latinoamérica desde hace algunos años se viene dando un incremento en el alza de los ataques cibernéticos; y el Ecuador no se encuentra exento de esto, especialmente en el sector financiero, y según de la ITU (2022) se encuentra en el lugar 119 de 182 países en cuanto a su vulnerabilidad a ataques cibernético” (Ponce, 2023, p. 120).

“Actualmente las organizaciones del mundo usan masivamente sistemas de información, para la automatización, transformación y digitalización de procesos como: planificación, organización, producción, entre otros, mismos que se generan a diario en los departamentos de la organización. No obstante, la digitalización viene por añadidura con inconvenientes relacionados con seguridad de la información, por lo cual, las organizaciones deben implementar políticas, para protección de los datos que antes se almacenaban de manera física y hoy en dispositivos digitales (Velecela y Tapia ,2020, pp. 63-64).

De esa forma resguardar la información y evitar daños, robo o incluso destrucción de su activo, puesto que un sistema casi siempre es vulnerado con la finalidad de extraer datos valiosos para la organización, entre ellos: credenciales de acceso, infiltraciones en modo espía, instalación de scripts, entre otros. El empleo de políticas de seguridad ayuda a controlar muchos incidentes, de lo contrario, la organización será un blanco fácil para recibir ciberataques según medios digitales recopilados por el autor” (Velecela y Tapia,2020, pp. 63-64).

Para conocer la situación actual se ha consultado a varias personas del área de Soporte Tecnico de lo cual se obtuvo como resultado que dentro del marco de la seguridad de la información ha existido incidentes como, pérdida de datos, manipulación de información de clientes y accesos no autorizados a base de datos, falta de concientización y la escasa capacitación al personal.

Aunque en el escenario de la empresa materia de este estudio esta implementada la norma ISO/IEC 27001, no habido mayor compromiso por la organización, tampoco se ha definido su alcance, sumado a una falta de concientización y capacitación al personal sobre la importancia de un SGSI, además de que tampoco se ha hecho un análisis de riesgos adecuado y una escasa documentación clara y concisa acerca de las políticas y procesos.

Para lo cual existe la necesidad de proponer la implementación de la ISO27005 como herramienta para complementar y fortalecer la ISO 27001, especialmente enfocado en gestionar los riesgos y mantener una continuidad operativa de la organización.

¿Con la adopción del sistema de SI se lograra prevenir accesos no autorizados, alteraciones o pérdida de datos?

Objetivo general

Desarrollar una propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones Bajo la Norma ISO/IEC 27005, aplicado al área de Soporte Tecnico, con el objetivo de identificar, analizar y mitigar los riesgos asociados, garantizando la seguridad de la información.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre los riesgos de seguridad de la información presentes en el área de soporte técnico, considerando las actividades, herramientas y datos críticos manejados.
- Determinar el nivel de impacto y probabilidad de los riesgos identificados, utilizando los lineamientos de la norma ISO/IEC 27005.
- Diseñar una propuesta de sistema de seguridad de la información, basada en los principios de ISO/IEC 27005, adaptada a las necesidades específicas del área de soporte técnico, para fortalecer la gestión de riesgos y proteger los activos críticos.
- Validar la propuesta del sistema de seguridad de la información mediante el criterio de especialistas.

Vinculación con la sociedad y beneficiarios directos:

Según el reporte de las Naciones Unidas (s.f.) El desarrollo de la propuesta se alinea en forma directa con el Objetivo de Desarrollo Sostenible (ODS) 9: Industria, Innovación e Infraestructura**,** que busca construir infraestructuras resilientes, promover la industrialización inclusiva y fomentar la innovación.

En particular, esta iniciativa contribuye a:

“Meta 9.4 De aquí a 2030, modernizar la infraestructura y reconvertir las industrias para que sean sostenibles, utilizando los recursos con mayor eficacia y promoviendo la adopción de tecnologías y procesos industriales limpios y ambientalmente racionales, y logrando que todos los países tomen medidas de acuerdo con sus capacidades respectivas” (Naciones Unidas, s.f.)

Se eligió la norma ISO 27005 como base; debido que proporciona un enfoque estructurado para la gestión de riesgos, siendo compatible con otras normas, como la ISO/IEC 27001.

Se basa en su capacidad para ofrecer un método sistemático de supervisión de riesgos, alineando con otras referencias como ISO/IEC 27001

Beneficiarios Directos

La adopción de un sistema enfocado en gestionar los riesgos basado en la ISO 27005 fomenta prácticas sostenibles para gestionar la información; este enfoque brindará varios beneficios a la empresa de telecomunicaciones materia de este estudio, así también a trabajadores debido que se desarrollará una propuesta que pueda ser replicable y permita anticiparse a las amenazas. A continuación, se detalla los beneficios de esta propuesta

- Protección de datos sensibles. - Al aplicar este enfoque para la gestión se riesgos, se garantiza la seguridad de los datos.
- Cumplimiento normativo. - Al sujetarse a los estándares internacionales fortalecería el cumplimiento de regulaciones locales y globales, siendo adaptable a cualquier entorno.
- Fortalecimiento de la confianza. -Mejora la percepción del cliente.
- Contribución a la sostenibilidad. - Al impulsar el uso de tecnologías seguras, se reduciría costos asociados con incidentes de seguridad.

El desarrollo de esta propuesta contribuirá al conocimiento en materia de la seguridad de la información, permitiendo su implementación de manera eficiente y adaptada a las necesidades del área de soporte técnico. Simultáneamente tendrá un impacto significativo al establecer un modelo adaptable a otras empresas del sector, contribuyendo al avance en la gestión de riesgos y la mejora continua de la seguridad.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

1.1.1. Seguridad de la Información

La seguridad de la información es un estándar internacional que estableces los requisitos de un SGSI, actualmente se encuentra inmerso en varios aspectos de la cotidianidad, ya sea en ámbitos como teletrabajo, juegos y educación en línea, compra de productos en Internet entre otras.

También podría definirse como un conjunto de procesos y buenas prácticas que buscan garantizar la seguridad de la información, del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada.

Según Morales (2020) en la actualidad vivimos en una era de transformación digital, donde los negocios y sobre todo la información se encuentra en medios digitales, lo cual hace que las empresas enfrenten desafíos al intentar salvaguardar los datos. Según las cifras presentadas de la empresa Fortinet, en cada minuto existen 545000 intentos de intrusión siendo neutralizadas unas 140000 que corresponden a malware por cada minuto a nivel global. Las empresas que deseen continuar en el mercado deben innovar a través de estrategias que se apoyen en la participación de la alta gerencia y en también basándose en la toma de decisiones que se enfoquen en proteger su activo más importante la información.

Según lo indicado por Secaira (2020), indica que en la adopción de un SGSI por lo general está determinado por la estructura de la organización considerando varios factores como, el tamaño, el servicio que ofrece, los procesos y requerimientos de seguridad para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001.

1.1.2. ISO 27000 y su relación con la seguridad de la información

La norma ISO 27000 es un conjunto de estándares internacionales enfocados en la seguridad de la información, estos estándares proporcionan un conjunto de buenas prácticas para establecer, implementar, mantener y ofrecer un marco de mejorar continua de un SGSI.

En la investigación realizada por Babilonia (2023) indican que su implementación ofrece muchos ventajas competitivas a las empresas entre las que destacan, garantizar la seguridad, debido que ofrecen un marco estructurado para gestionar la SI en la organización además de establecer los requisitos y ofrecer recomendaciones para implementar controles que sean

efectivos y eficiente en su adopción y que estos sean los más pertinentes y adecuados para garantizar la seguridad de los datos .

Además Babilonia (2023) en su investigación indica que la norma ISO 27000 ofrece un enfoque de mejora continua en un SGSI el cual brinda a las empresas mantenerse al día en las actualizaciones y amoldarse con los cambios de entorno, ya sean estos internos o externos ,ofreciendo ciertos beneficios como salvaguardar la información ya que estará debidamente protegida , además de ser de gran utilidad en la seguridad y gestión de procesos pudiendo adoptarse a diferentes clases de instituciones sin considerar la naturaleza de la misma o el tamaño de la organización.

1.1.2.1. ISO/IEC 27001

Según Rodríguez et al. (2023) la norma ISO 27001 establece los requisitos para la implementación de un SGSI además de ofrecer las pautas necesarias que permitan establecer, implementar, mantener y mejora continua del sistema dentro del contexto de la organización**.**

De acuerdo a Cazar et al. (2022) indica que la ISO 27001 ofrece una serie de controles que pueden servir como un check list para la evaluación de riesgos siendo necesario considerar los controles necesarios para su adecuada adopción. Además, menciona que un factor importante para un SGSI exitoso es una evaluación de riesgos, siempre y cuando se sepa a qué amenazas se enfrentaran se podrá implementar las medidas adecuadas para defenderse.

1.1.2.2. Gestión de Riesgos

En la investigación realizada por Guevara (2021), en su investigación informa que la gestión de riesgos, es el procedimiento que permite aprovechar las ventajas que brinda las falencias en seguridad ya sea provocada por el desconocimiento, además que se tiende a minimizar las amenazas y vulnerabilidades, o no dar la suficiente importancia a las pérdidas ocasionadas ya sea que tengan un impacto positivo o negativo y según esto el impacto que pueda tener en los objetivos de la organización.

Según Morales (2019) indica que la gestión del riesgo tienes cambios constantes y cada marco de gestión de riesgos posee distintas ventajas y desventajas, para lo cual es necesario considerar el más simple, y que cumpla con los requisitos organizacionales de forma que se asegure una adecuada implementación. Para lo cual es imprescindible realizar evaluaciones periódicas de forma que se evalué el cumplimiento de las necesidades**.**

En el estudio realizado por Contreras et al. (2020) informa que es un desafío para las instituciones financieras manejar de los ataques cibernéticos, ya que, debido a la innovación en la era digital, cada día los atacantes encuentran nuevas formas de vulnerar la información. Además, define al riesgo como la probabilidad de que ocurra un evento negativo y que este dificulte a la institución su desenvolvimiento normal en las operaciones adicional interrumpe el cumplimiento de los objetivos organizacionales; en consecuencia, sugiere que las entidades deben estar preparadas para responder inmediatamente ante la ocurrencia de algún evento y el ofrecer una adecuada gestión reducirá el impacto y sus efectos serán mínimos.

En lo informado por Toro (2023), informa que únicamente cumpliendo con una ejecución idónea de controles se aseguraría la seguridad de los datos siempre y cuando se incluya los procedimientos, políticas y los procesos. Para implementar estos controles se debe asegurar la adecuada ejecución de las características en la triada de seguridad y que esta vaya de la mano de los objetivos de la organización.

1.1.2.3. ISO/IEC 27005

Según Abad (2022) define a la norma como las mejores prácticas que sirven para definir un marco estructurado que se enfoque en la gestión de riesgos en la SI indispensables para identificar los requerimientos en la SI que necesitan las entidades con el objetivo de ofrecer un sistema seguro.

En la investigación realizada por Yarleque (2024), indica que una vez implementado la norma la norma ISO/IEC 27005 se obtuvo como resultado que dicha norma logró ofrecer a la alta direccion, soluciones para la identificación de riesgos, y evaluar el entorno centrándose en la identificación de activos, amenazas y vulnerabilidades, de esta manera reducir el consumo, optimizar las operaciones y un más eficiente tiempo de respuesta.

Según lo indicado por Lobo (2022) Indica que la ISO 27005, establece lineamientos enfocados en la gestión de los riesgos relacionados a la SI, esta norma proporciona las directrices necesarias tomando como base fundamental los requerimientos definidos en la ISO 27001.

De igual manera Lobo et al. (2022) informa que la norma es aplicable a las instituciones, que deseen mejorar su sistema gestión de riesgos sobre SI, a fin de obtener una lista completa de riesgos en función de los eventos y que poseen la capacidad de reducir, evitar, aumentar, crear, retrasar o aumentar el logro de los objetivos.

En su investigación Fajardo y Rojas (2022) describen que a raíz del incremento acelerado de la tecnología nos vemos abocados en gestionar herramientas, que nos permitan no ser presas fáciles para los delincuentes cibernéticos, es indispensable contar con medios económicos para el diseño de estrategias de seguridad así como que proveedores y clientes del mercado bancario y privado exigen a empresas prestadoras de servicios de SI, tener sus amenazas y vulnerabilidades identificados y gestionados, es estratégico contar con una evaluación del riesgo propuesto y tener en sus objetivos la implementación de la norma ISO 27005:2018.

"En términos del estándar ISO 27005:2018, un riesgo es la probabilidad de que se produzca in impacto determinado a un activo de información está asociado también en la materialización de una amenaza aprovechando la vulnerabilidad de un activo "(Fajardo y Rojas ,2022).

Según Montoya (2020) describen una de las actividades esenciales en la gestión de riesgos, siendo la identificación de riesgo un factor clave el cual establece los efectos y el impacto potencial acerca de cómo o cuando pueden suceder. Además, establece a esta fase como punto de partida comenzando con la identificación de los activos seccionándolos en diferentes criterios como son: activos de información, activos de software, activos físicos, activos de personas y /o servicio, los cuales son valorados en función de los pilares fundamentales de la seguridad de la información.

1.2. Proceso investigativo metodológico

1.2.1. Enfoque de la Investigación

El enfoque usado para la presente investigación será mixto que usará el enfoque cualitativo y cuantitativo. Mediante el enfoque cuantitativo se procederá a realizar encuestas a los empleados para conocer la situación real de la empresa. Con las respuestas obtenidas después se tabulará y mediante las cifras de resultado se conocerá el estado de la empresa. También se empleará el enfoque cualitativo para realizar entrevistas a ciertas personas en el área para que informen la percepción que tienen de las normas de SGSI aplicadas al momento y de ser el caso recibir posibles propuestas de mejoras.

1.2.2. Tipo de Investigación Aplicado

Se realizo una investigación diagnostica para el planteamiento del problema ya que permitirá identificar y determinar los problemas reales del área. También se utilizó la investigación bibliográfica para el desarrollo del estado del arte ya que por medio de uso de fuentes confiables

como revistas o artículos científicas se recopilo información acerca del tema y adquirir una mejor comprensión de la propuesta planteada. Adicional se utilizó la investigación descriptiva para identificar y analizar los riesgos de seguridad de la información y finalmente se empleó la investigación aplicada para proponer soluciones, prácticas al problema planteado.

1.2.3. Métodos Teóricos y Prácticos Aplicados

El método teórico utilizó fue el análisis documental, para revisar conceptos sobre las normas ISO/IEC 27005 y 27001 y realizar una comparación entre ellas para determinar la que mejor se ajuste a la propuesta planteadas. su relación con las necesidades del área de soporte técnico, y la revisión bibliográfica para revisar estudios sobre la aplicación de la norma en empresas de telecomunicaciones.

Como método práctico, se utilizó la observación directa para recopilar información preliminar según las opiniones del personal del área. también se complementó mediante encuestas para sustentar las consultas realizadas.

1.2.4. Técnicas de recolección de datos.

1.2.4.1. Encuestas

Se realizaron encuestas a personal del área técnica para recopilar información acerca de su conocimiento sobre SGSI y mediante las actividades diarias que realizan poder identificar vulnerabilidades en la entidad. Estas encuestas permitirán obtener una retroalimentación sobre las políticas existentes y analizar las falencias existentes.

1.2.4.2. Análisis Documental

Simultáneamente, se revisó manuales de seguridad y políticas internas, con a fin de complementar los resultados obtenidos en las entrevistas. Este análisis permitió una mejor comprensión del contexto actual y de las medidas ya implementadas.

1.2.4.3. Análisis de casos de éxito

Se reviso los casos de empresas que han implementado la ISO 27005 y analizar las estrategias que funcionaron y los obstáculos que se presentaron para su implementación.

Población Y Muestra

En la población se consideró únicamente a los empleados del área de soporte técnico lo cual se presenta en la Tabla 1, que suman un total de 30 personas y se realizó una muestra no probabilística intencional debido que se seleccionó a 17 personas por su accesibilidad, disponibilidad y por estar involucradas de forma directa con el área.

Tabla 1

Población y muestra

Población y Muestra	**Número Total**
Total, de empleados del área	30
Muestra seleccionada	17

Este enfoque asegura la participación de varios individuos con conocimiento y experiencia directa en los procesos estudiados. Con base en los resultados obtenidos, se realizará una propuesta diseñada **a** las características específicas de la organización, aplicando los lineamientos de la norma ISO 27005. Finalmente, el sistema propuesto se validará mediante una revisión por parte de expertos en seguridad de la información, lo que permitirá ajustar y afinar detalles de la propuesta realizada antes de su implementación.

1.3. Análisis de resultados

En siguiente análisis se realizó el procesamiento de los datos recolectados resultado de la encuesta efectuada al personal del área de soporte técnico. Entre ellas se tuvo participación de la mayoría de los involucrados ,la muestra seleccionada por su accesibilidad son 17 personas obteniendo una mejor comprensión y una percepción del escenario real de la empresa.

Para su tabulación se identificaron cuatro criterios distintos, como puntos de materia de análisis, siendo el Conocimiento, Cumplimiento, Cultura, Percepción con respecto a la Políticas de Seguridad de la Informacion aplicadas en la organización.

Criterio 1.- Conocimiento

Las encuestas evidenciaron que la empresa enfrenta desafíos en materia de seguridad, siendo el primero el conocimiento, se visualiza que existe un porcentaje considerable que tiene los conocimientos básicos pero que contrastan con el desconocimiento de su aplicación en la empresa y un porcentaje indico que requiere más capacitación.

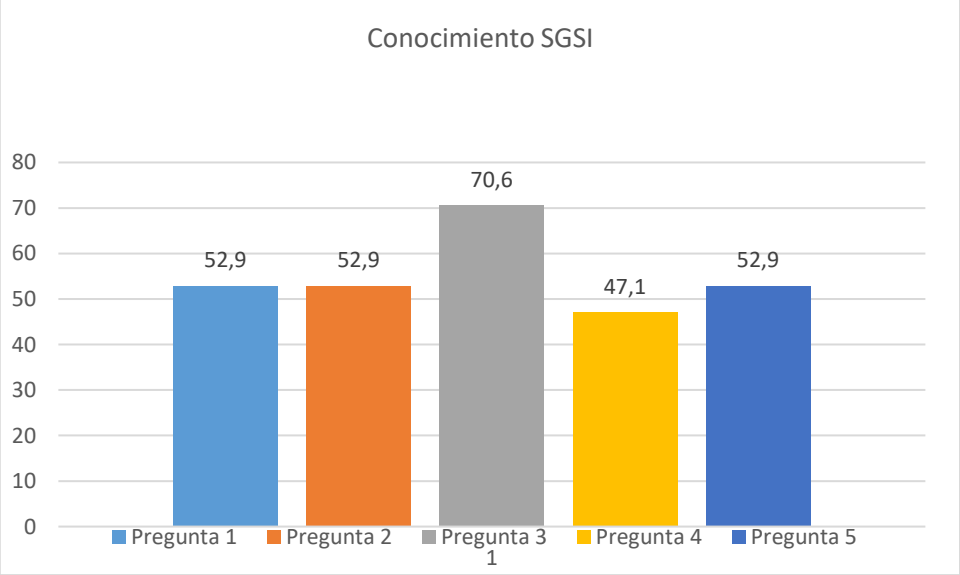
Las respuestas a las preguntas sobre el conocimiento general de las normas ISO se detallan en la tabla 2. Esta sección ilustra la proporción de conocimiento en relación con las normas implementadas en la organización.

Tabla 2
Criterio 1 Conocimiento

Criterio 1 Conocimiento	**Porcentaje**
Desconocimiento acerca del área encargada a la SI.	52,9
Desconocen acerca de la aplicación de normas de SI.	52,9
Posee los conocimientos básicos	70,6
Desconocimiento acerca de la aplicación de normas 27001.	47,1
Informaron que requieren mayor capacitación	52,9

En la Figura 1 se aprecia de forma gráfica el resultado del primer criterio, se visualiza que existe un 70,6 % que posee los conocimientos básicos y a su vez un 52,9% informaron desconocimiento acerca de la aplicación de las normas y de la existencia de las normas en la organización adicional indicaron la necesidad de requerir más capacitación.

Figura 1
Porcentajes Criterio 1



Criterio 2.- Cumplimiento

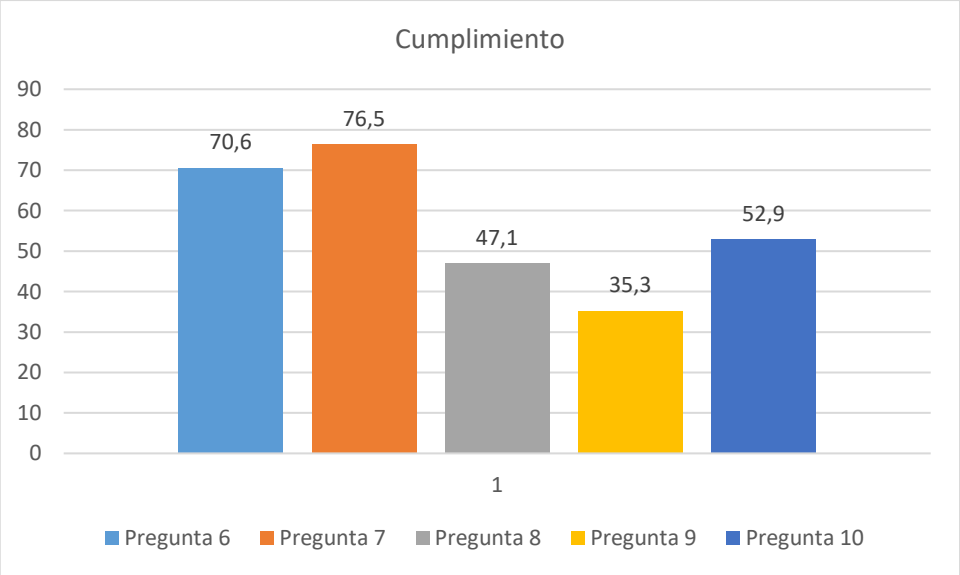
En la encuesta realiza se obtiene las siguientes respuestas sobre su cumplimiento estas se muestran en la Tabla 3. en donde se evidencia el porcentaje de aceptación según la percepción de los encuestados.

Tabla 3
Cumplimiento de las Normas SI

Criterio 3 Cumplimiento	**Porcentaje**
Recibieron capacitación esporádica	70,6
Desconocen si revisan y/o actualizan las políticas.	76,5
Desconocen si realizan simulacros ante incidentes.	47,1
Conocimiento acerca de canales de comunicación	35,3
Medidas correctivas en el incumplimiento de políticas	52,9

En la Figura 2 se aprecia de forma gráfica el resultado del segundo criterio donde se visualiza que un 70,6 % han recibido capacitación y un 76,5% desconocen si se revisan o actualizan las normas y un 52,9 desconoce si se toman medida en caso de su incumplimiento.

Figura 2
Criterio 2 Cumplimiento



Criterio 3.- Cultura

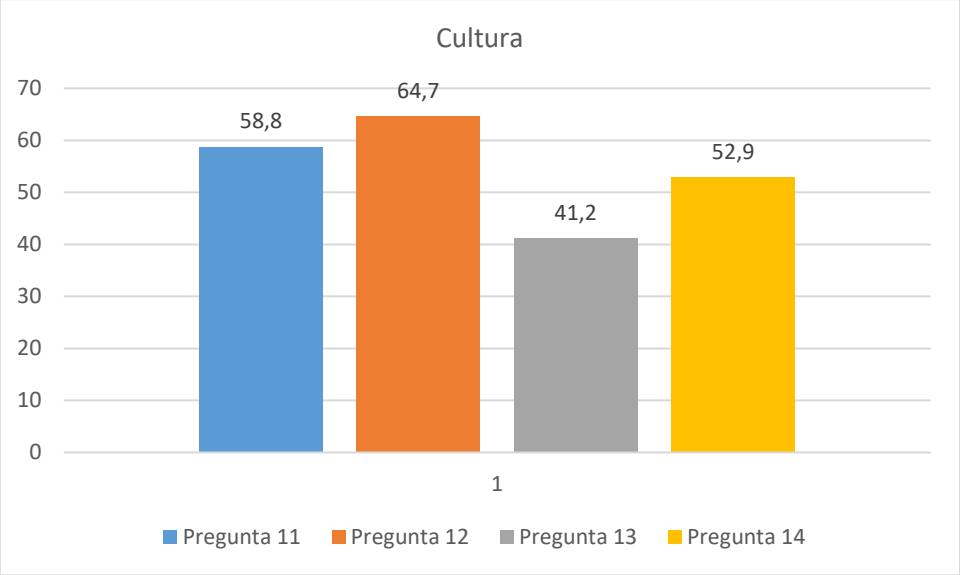
Las respuestas obtenidas sobre la cultura se muestran en la Tabla 4. en donde se evidencia el porcentaje de aceptación según la percepción de los encuestados.

Tabla 4
Cultura sobre SI

Criterio 3	**Porcentaje**
Compromiso regular en la aplicación de políticas.	58,8
Falta de apoyo a su cumplimiento.	64,7
Cumplimiento de políticas por parte del personal	41,2
Necesidad de mayor capacitación	52,9

En la Figura 3 puede visualizarse el resultado del criterio Cultura donde se observa que el 64,7 % de los encuestados menciona la falta de apoyo a su cumplimiento, con un 58,8 % mencionaron falta de compromiso y un 52,9 informaron que necesitan más capacitación.

Figura 3
Cultura



Criterio 4.- Percepción

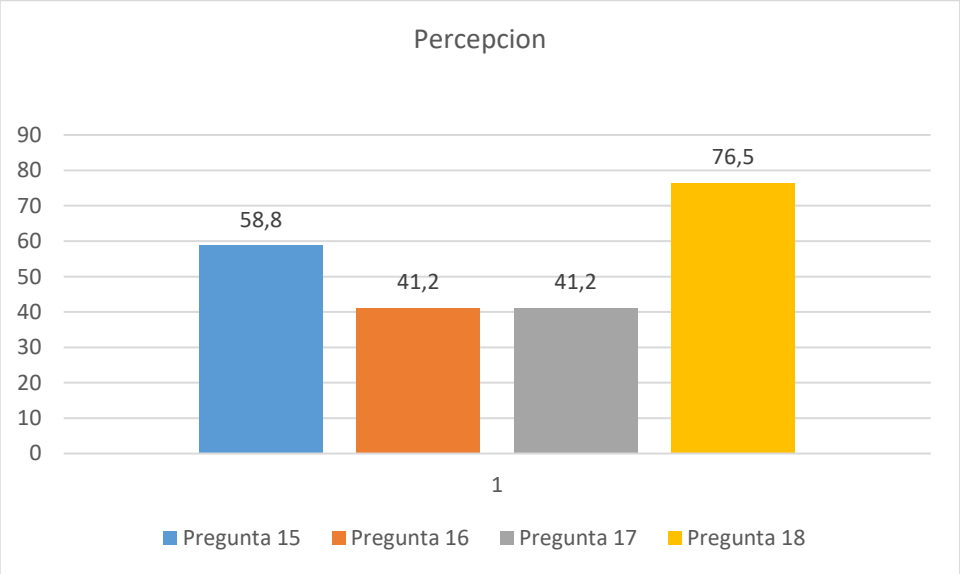
Las respuestas obtenidas sobre la cultura se muestran en la Tabla 5. en donde se evidencia el porcentaje de aceptación según la percepción de los encuestados.

Tabla 5
Percepción de las Normas de SI

Criterio 4 Percepción	Porcentaje
Moderadamente efectivas	58,8
Cumplimiento parcial	41,2
Conocimiento regular	41,2
Medianamente satisfecho con las políticas implementadas	76,5

Como se observa en la Figura 4 se aprecia el resultado obtenido del criterio percepción el cual muestra a un 76,5 % estar medianamente satisfechos con un 58,8 % de los encuestados recalcaron que las normas existente no son efectivas.

Figura 4
Percepción de las Normas



Resumen de la recolección de los datos

Por medio de la tabulación de las encuestas se encontró varios avances, donde enfatizaron que se posee el conocimiento básico de las normas de un SGSI, pero a su vez desconocían acerca de la aplicación de las normas ISO27001 en la organización otros informaban que recibían capacitación esporádica y recalcaban la ausencia de compromiso por parte de los mandos superiores para el cumplimiento además consideran su insatisfacción con las políticas implementadas. Estas particularidades encontradas destacan la necesidad de una solución que permita reforzar las falencias encontradas en la implementación de la ISO/IEC 27001, para lo cual con la propuesta basada en la ISO 27005 se puede mejorar su SGSI y tener mayor eficiencia en la seguridad de la información.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

2.1.1. Gestión de riesgos de seguridad de la información

Según Santos (2022), indica que la gestión de riesgos es una tarea fundamental debido que permite identificar, evaluar y reducir los riesgos de forma que ayude a reducir los peligros y enmarcarlos en un modelo de mejora continua. Los marcos normativos en el gobierno de la seguridad exhortan que las organizaciones implementen controles para prevenir los riesgos que puedan amenazar su integridad.

En su misma investigación Santos (2022), informa que es un limitante implementar muchos controles, por eso informa que es necesario establecer una gestión de riesgos de seguridad de la información como parte del gobierno y que estos procesos permitan identificar que riesgos son más relevantes y que medida o control puede establecerse para mitigar sus efectos o evitarlos en la medida posible, siendo una norma específica para esta finalidad es la ISO/IEC 27005**.**

De acuerdo a Marín y Medina (2024) indicaron que la gestión del riesgo es adaptable y flexible a adoptarse a una parte de la organización, a una sección o toda en conjunto, además pudiendo también aplicarse hacia algún sistema de información o a un aspecto de control planificado.

2.1.2. Metodologías para análisis de riesgos

"Las metodologías permiten realizar un análisis y evaluación de los peligros presentes en el resguardo de la información, realizando escaneos de vulnerabilidades, amenazas y riesgos mediante el seguimiento de diversas fases o procesos. Algunos de los objetivos de estas metodologías se enfocan en la planificación del control en los sistemas para reducir el nivel de los riesgos, prevenir pérdidas de información y detectar las debilidades existentes en los sistemas informáticos" (Miranda, 2021).

De acuerdo a (Miranda, 2021) indica que los objetivos de las metodologías se centran en la planificación del control en los sistemas con el fin de reducir los riesgos, y prevenir posibles pérdidas de información y identificar las vulnerabilidades en un sistema informático.

Existen metodologías que permiten hacer un uso adecuado del análisis de riesgos y así asegurar los sistemas de información de las organizaciones. Entre las principales tenemos:

2.1.2.1. OCTAVE

OCTAVE es un enfoque de gestión de riesgos de seguridad de la información que toma en consideración los riesgos operativos que puedan vulnerar a los usuarios de la organización o internos. Además, está diseñada para identificar, evaluar y gestionar los riesgos asociados a sus activos de información de manera estructurada para realizarlo consta de 3 fases:

- Fase 1 enfocada en la visión de la organización, en esta se identifica la información y los elementos como activos clave; análisis de amenazas, identificación de vulnerabilidades y requisitos de seguridad de los activos. Además, se encarga de organizar y arreglar el plan, antes de su ejecución previo al análisis de riesgos.
- Fase 2 centrada en la tecnología, aquí se evalúan todos los elementos de la infraestructura tecnológica en busca de vulnerabilidades, análisis de configuraciones inseguras, análisis de amenazas en busca de brechas de seguridad.
- Fase 3 enfatiza la reducción de riesgos y la planificación de medidas, aquí clasifica la evaluación y se pondera el riesgo según su impacto vs probabilidad, definen estrategias de mitigación y desarrollo de un plan de acción basado controles de seguridad.

2.1.2.2. MEHARI

En su estudio Miranda (2021) indica que el objetivo de esta metodología es proporcionar un instrumento que permita desarrollar el análisis de riesgos, ya sean cualitativos o cuantitativos, además está esquematizado de forma que unifique el proceso de análisis de riesgo considerando también el riesgo a futuro. Este análisis se realiza en base a los pilares fundamentales de seguridad y para realizar este análisis en virtud del uso de tecnología depende en gran medida del empleo de técnicas informáticas y base de datos informatizadas para efectuar el análisis de cada uno de los riesgos.

2.1.2.3. MAGERIT

En esta metodología Alemán (S.f.) informa que sobresalen dos objetivos, el primero encargado del estudio de los riesgos inherentes manejados por el sistema de información y su ambiente relacionado, definiendo también al riesgo como la probabilidad de existencia de un perjuicio o daño, y un segundo objetivo vinculado a recomendaciones que en conjunto con la toma de medidas adecuadas aportarían al impedimento, prevención, conocimiento y reducción del riesgo asociado. Los principales elementos para el análisis de riesgos, según Magerit son: activos, amenaza, vulnerabilidades, impacto, riesgo y salvaguardas.

El empleo de esta metodología permite planificar las medidas más pertinentes con el fin de que el riesgo sea controlable y servir de apoyo para preparar a la organización ante procesos de acreditación, auditoría, certificación o evaluación, de la misma manera ofrece ciertas ventajas debido que las decisiones que requieran efectuarse necesiten ser validadas previamente por la dirección siendo fácilmente defendibles y debidamente fundamentadas.

Otra característica es que establece un enfoque en los resultados los mismos deben expresarse en términos económicos que, a la vez es una desventaja debida que, al realizar la traducción de sus valoraciones a términos financieros, la hacen muy costosa al momento de su implementación.

2.1.2.4. ISO/IEC 27005

La ISO/IEC 27005 es una norma internacional que proporciona directrices específicas para la gestión de riesgos en la seguridad de la información y es parte de la serie ISO/IEC 27000; se centra en ayudar a las organizaciones a implementar un enfoque sistemático para identificar, evaluar y gestionar los riesgos de seguridad de la información.

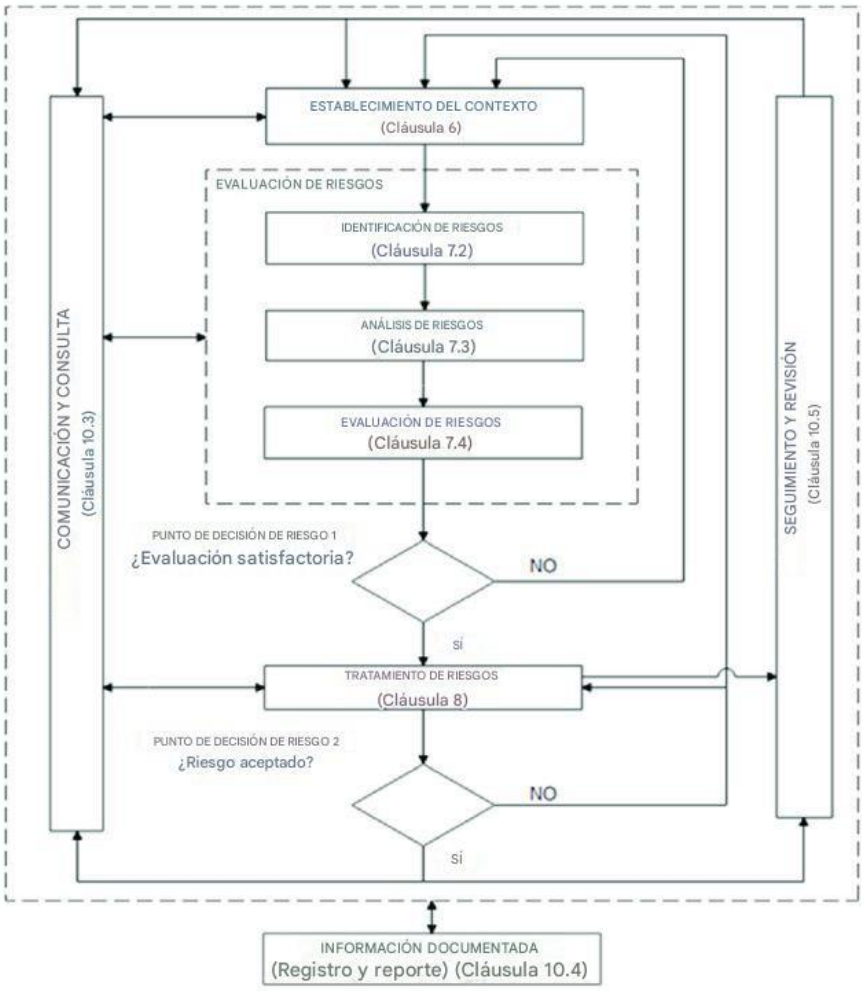
Para comprender la ISO 27005 Marín y Medina (2024) mencionan que es necesario conocer los componentes de esta normativa como son los, modelos, términos, procesos y los conceptos. Además, está diseñada de forma que brinde una fácil aplicación efectiva del SI cuyo eje es la gestión de riesgos, haciéndola importante para una variedad de instituciones, incluyendo a las entidades gubernamentales, empresas comerciales, y entidades sin fines de lucro. Además, la ISO 27005 no menciona si es existe una metodología en específico, debido que depende algunas variables siendo uno de ellos su alcance, sector, proceso o tamaño de las organizaciones.

Para una empresa de telecomunicaciones, metodologías como ISO/IEC 27005, MAGERIT, OCTAVE y MEHARI pueden ser útiles debido a su enfoque en riesgos en SI y TICS. Es importante adaptar la metodología seleccionada a las necesidades específicas de la organización, dado que las telecomunicaciones dependen en gran medida de infraestructuras digitales y de la protección de datos, estas metodologías son altamente aplicables.

Estructura de la ISO/IEC 27005

A continuación, en la figura 5 se muestra el proceso de gestión de riesgos:

Figura 5
Proceso para la Gestión del Riesgo



Nota. *Traducción al español de ISO/IEC 27005:2022(E)*

El ciclo PHVA (Planificar, Hacer, Verificar y Actuar es ideal para estructurar su implementación como se observa en la Figura 6, ya que se alinea con el enfoque de la ISO27001 y complementa la gestión de riesgos de la ISO27005.

Figura *6*
Ciclo Planificar-hacer-verificar-hacer (PHVA)

Nota. *Tomado de Diseño de un plan director de seguridad para una empresa privada que brinda servicios de auditoría para reducir riesgos expuestos en un entorno seguro (p. 43), por Marín y Medina, 2024, ESPOL, FIEC.*

2.2. Descripción de la propuesta

Para el desarrollo de la Propuesta del sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo el lineamiento de la ISO27005 se toma como referencia la figura 7 mostrada a continuación:

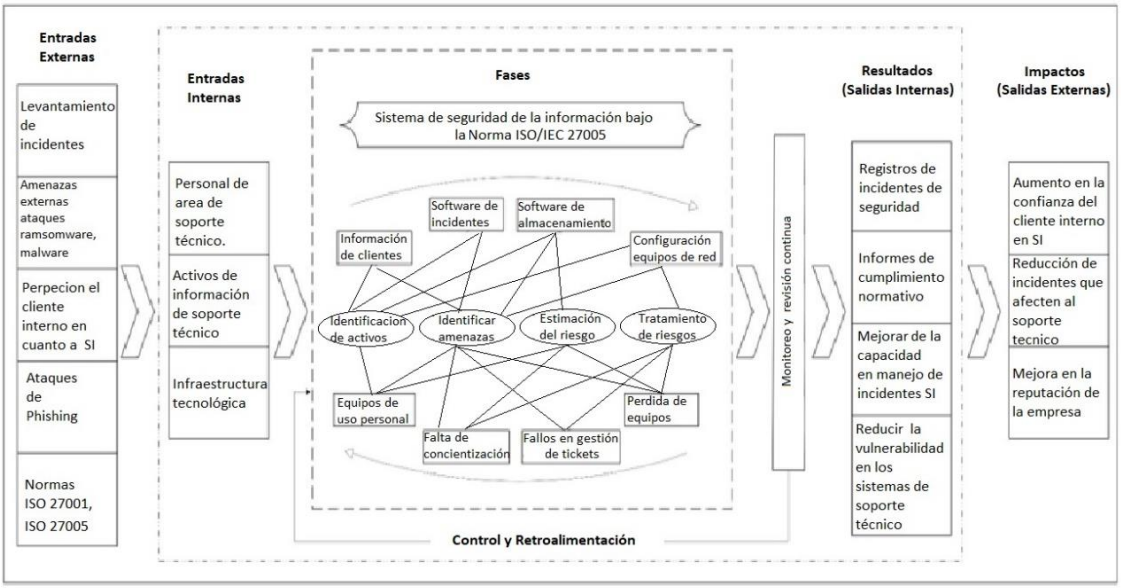
a. Estructura general

La presente propuesta tiene como objetivo fortalecer la gestión de seguridad de la información para una empresa de Telecomunicaciones, por medio de lineamientos basados en la norma ISO27005, específicamente orientada al área de soporte técnico.

La propuesta busca abordar las debilidades identificadas y reforzarlas, mediante el proceso de identificación de activos y análisis de vulnerabilidades se logrará brindar sistema de mejora continua, a continuación, en la Figura 7, se detalla la estructura general.

Figura *7*

Estructura general de la propuesta



b. Explicación del aporte

Estudio de la organización

En la empresa materia de la investigación esta implementada la norma ISO/IEC 27001, pero no ha existido el compromiso por la organización por su difusión, tampoco se ha definido su alcance, sumado a la falta de concientización; por lo que la propuesta basada en la ISO/IEC 27005 busca reforzar las falencias identificadas y confirmadas como resultado de la encuesta realizada al personal del área de soporte técnico.

Determinar el área y alcance

Se ha determinado aplicar a la gestión del soporte técnico de una empresa de Telecomunicaciones y como alcance se enfocará en identificar y evaluar de riesgos siguiendo los lineamientos de la ISO/IEC 27005.

Identificación de activos

Una vez determinada el área de estudio se procedió a identificar los activos más importantes que se utilizan para la gestión del soporte técnico, los cuales se clasifican en activos de:

- Información (nombres, ingeniería de clientes, registro de incidentes)
- Software (Programas para levantamiento de incidentes, almacenamiento de información)

- Hardware (Pc ’s, Sw, Routers, teléfonos).

Valoración de activos

Una vez identificado los activos de la organización se continua con su valoración considerando la confidencialidad, integridad y disponibilidad**.** Para lo cual se clasifico según su impacto e importancia para la gestión, en escalas de bajo (1), medio (2) y alto (3).

Tabla *6*
Valoración de activos

Activo	Confidencialidad	Integridad	Disponibilidad	Valoración
Información de clientes	3 (Alto)	3 (Alto)	2 (Medio)	8 (Crítico)
Software para levantamiento de incidentes	2 (Medio)	2 (Medio)	3 (Alto)	7 (Alto)
Software para almacenamiento de información	2 (Medio)	3 (Alto)	3 (Alto)	8 (Crítico)
Configuración equipos de red	3 (Alto)	3 (Alto)	3 (Alto)	9 (Crítico)
Equipos de uso personal	2 (Medio)	2 (Medio)	2 (Medio)	6 (Medio)

Interpretación:

- Valores iguales o menores a 6, se considera impacto moderado y puede gestionarse con medidas estándar.
- Valores de 6 y 7 se considera alto impacto y necesitan protección adecuada.
- Valores de 8 y 9 se considera impacto crítico y requieren medidas de seguridad más estrictas.

Identificar Amenazas

Una amenaza es cualquier evento o suceso que puede comprometer la seguridad de la información, para lo cual después de identificar y valorar los activos importantes, se procede a identificarlas tomando como referencia lo indicado en la ISO 27005:2002 y evaluando dependiendo de las categorías que esta normativa detalla.

Tabla 7
Identificación de amenazas

Amenazas Técnicas	Amenazas Humanas	Amenazas Físicas y Ambientales
Ataques de malware, ransomware, phishing, DDos	Ingeniería social	Desastres naturales
Accesos no autorizados a base de datos o programas de soporte.	Falta de concientización (contraseñas inseguras, accesos a sitios inseguros)	Fallos eléctricos
Errores en la configuración de equipos de red.	Fallos operativos en la gestión de tickets.	Pérdida o robo de equipos de la empresa.

Estimación de riesgo

La estimación de riesgo es un factor clave dentro del proceso ya que permitirá analizar y evaluar las amenazas y posibles impactos en los activos importantes y según eso diagnosticar el nivel del riesgo.

De acuerdo a ISO27005 para la estimación de riesgo se calcula multiplicando la probabilidad de que ocurra de un incidente por su impacto (consecuencias) sobre el activo afectado. Para lo cual se usó un enfoque cualitativo clasificándolo en escalas de muy bajo (1), bajo (2), medio (3) y alto (4).

Tabla 8
Estimación de riesgo

Amenazas	Activo Afectado	Probabilidad (1-4)	Impacto (1-4)	Riesgo	Prioridad de Atención
Ataque de malware, ransomware	Software para almacenamiento de información	3(Media)	4 (Crítico)	12 (Crítico)	Alta
Phishing	Información de clientes	4 (Alta)	3 (Alto)	12 (Crítico)	Alta
Ataque DDoS	Software para almacenamiento de información	3 (Media)	3 (Alto)	9 (Alto)	Alta
Errores en la configuración de equipos de red.	Configuración equipos de red	2 (Baja)	4 (Crítico)	8 (Medio)	Media

Acceso no autorizado a servidores	Configuración equipos de red	Alto (4)	Alto (4)	Crítico (16)	Alta
Falta de concientización	Equipos de uso personal	4 (Alta)	3 (Alto)	12 (Crítico)	Alta
Fallos operativos en la gestión de tickets.	Software para levantamiento de incidentes	3 (Media)	3 (Alto)	9 (Alto)	Alta
Perdida de equipos de la empresa	Equipos de uso personal	2 (Baja)	3 (Alto)	6 (Medio)	Media

Interpretación:

- Valoración baja 1 - 4: Monitoreo, no requiere acciones inmediatas.
- Valoración media 5 - 8: requiere aplicar controles básicos
- Valoración alta 9 - 12: requiere aplicar medidas correctivas urgentes.
- Valoración critica 13 – 16: requiere acciones inmediatas para evitar impactos severos.

Tratamiento de Riesgos

El tratamiento de los riesgos implica tomar decisiones frente a los diferentes riesgos existentes para lo cual se seleccionan controles para reducir, aceptar, evitar o transferir los riesgos y definir un plan para el tratamiento del riesgo.

Existen cuatro opciones disponibles para el tratamiento del riesgo:

- Mitigar: Implementar controles para reducir la probabilidad o el impacto del riesgo.
- Transferir: Transferir el riesgo a un tercero.
- Evitar: Eliminar la actividad o condición que genera el riesgo.
- Aceptar: Aceptar el riesgo si el costo de mitigación es mayor que el impacto potencial.

Se ha definido un plan de tratamiento de riesgos el cual se encuentra en los ANEXOS.

Monitoreo y revisión continua

Se presenta el plan de mejora continúa basado en la norma ISO/IEC 27005. Este plan usa el ciclo PHVA (planificar, hacer, verificar, actuar) el cual se enfoca en los riesgos identificados. Cada fase del ciclo se detalla con acciones específicas, responsables y plazos.

- Planificar: identifican los problemas y planificar acciones.
- Hacer: llevar a cabo las acciones planificadas en la fase anterior.

- Verificar: consiste en monitorear y evaluar los resultados.
- Actuar: Evaluar si las acciones emprendidas han dado el resultado esperado

Se ha definido un plan de monitoreo y mejora continua el cual se encuentra en los ANEXOS.

Matriz de valoración de ISO 27005:2022

Mediante la matriz de valoración mostrada en la Tabla 7 y 8 se detalla todo el proceso desde la identificación de activos, valoración de activos, y estimación de riesgos en función de su impacto y probabilidad.

c. Estrategias y/o técnicas

Para el desarrollo de la presente propuesta se siguieron las siguientes fases:

Identificación de activos. -se identificó cuáles son considerados importantes.

Valoración de activos. - se consideró la confidencialidad, integridad disponibilidad para su valoración.

Identificación de amenazas. - se analiza las amenazas que puede comprometer la seguridad de la información

Estimación de riesgos. - se multiplica la probabilidad de ocurrencia por el impacto sobre el activo afectado que tendrá en la organización.

Matriz de Valoración de riesgos. - se realizó una valoración de riesgos mostrada en la Tabla 8 para abordar los riesgos identificados según los lineamientos de la ISO27005

2.3. Validación de la propuesta

Para la validación de la propuesta será realizada por medio del juicio de expertos como: La

- Sra. Ing. Silvia Adriano quien desempeña el cargo de Analista de Soporte Técnico Corporativo en la Corporación Nacional de Telecomunicaciones, (Anexos)
- El Sr. Ing. Victor Vilaña quien desempeña el cargo de Analista de seguridad de la información 3 en el .Consejo Nacional para la Igualdad, (Anexos)

La propuesta se valida a través del criterio de especialista considerando que el proyecto es viable en cuanto a aplicabilidad, factibilidad y es apropiado para cualquier empresa de telecomunicaciones que desee implementar y/o complementar su sistema de seguridad para la protección de la información. (Anexos)

2.4. Matriz de articulación de la propuesta

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

Tabla 9
Matriz de articulación

Ejes o Partes Principales	Sustento Teórico	Sustento Metodológico	Estrategias / Técnicas	Descripción de Resultados	Instrumentos Aplicados
Norma ISO/IEC 27005:2022	La norma ISO / IEC 27005:2022 brinda un enfoque para la gestión de riesgos en seguridad de la información, al definir los principios requeridos; para reconocerlos y abordarlos dentro de la organización.	Investigación bibliográfica	Análisis comparativo de normas ISO 27005 e ISO 27001 para identificar sus falencias en la empresa.	Mejor comprensión de la norma y como aplicarlos al desarrollo de la propuesta.	Revisión documental, análisis de casos de éxito y artículos científicos.
Diagnóstico de la situación de la empresa en materia de seguridad de la información	Principios de gestión de seguridad según la ISO 27001 e ISO 27005.	Enfoque cualitativo y cuantitativo. Investigación diagnóstica	Aplicación de encuestas al personal del área de soporte técnico.	Identificación de brechas en la implementación de la norma ISO 27001 y falta de concientización del personal sobre seguridad de la información.	Encuestas al personal del soporte técnico.
Determinación del área y alcance del sistema de seguridad	Aplicación de la norma ISO/IEC 27005 para definir un sistema enfocado en el área de soporte técnico.	Metodología de análisis de riesgos siguiendo las directrices de la ISO 27005.	Identificación y delimitación del alcance del sistema, priorizando los activos críticos del área de soporte técnico.	Definición clara del alcance de la propuesta y delimitación del entorno de aplicación.	Matriz de riesgos, y encuestas con responsables de seguridad.

Identificación y valoración de activos	Clasificación de activos según los criterios de confidencialidad, integridad y disponibilidad, basados en la ISO 27005.	Enfoque cualitativo. Investigación de campo	Aplicación de metodología de valoración de activos mediante el modelo CID y priorizar según su criticidad.	Lista priorizada de activos críticos y su valoración en función de su impacto en la seguridad de la información.	Observación directa, encuesta con administradores de TI, matrices de valoración de activos.
Identificación de amenazas y vulnerabilidades	Definición de amenazas en función del análisis de riesgos. Se las clasifica en categorías como errores humanos, ataques cibernéticos, fallas técnicas y desastres naturales.	Enfoque cuantitativo y cualitativo. Investigación descriptiva	Identificación de amenazas mediante revisión documental y análisis de casos de estudio.	Lista de las amenazas potenciales para los activos identificados y priorizar según su impacto	Matriz de amenazas y vulnerabilidades, encuestas con personal de seguridad de la información.
Evaluación y tratamiento de riesgos	Métodos de evaluación de riesgos considerando impacto y probabilidad, según ISO 27005.	Metodología basada en matrices de impacto y probabilidad. Y evaluación cuantitativa de riesgos.	Creación de una matriz de evaluación de riesgos y priorizar riesgos según su criticidad.	Obtener un plan de tratamiento de riesgos permitiendo una adecuada toma de decisiones.	Matriz de riesgos, análisis de impacto en la organización.
Monitoreo y mejora continua del sistema de seguridad	Aplicación del ciclo PHVA en la gestión de riesgos	Mejora continua mediante análisis de causa raíz y planes de acción correctiva.	Definición de controles de seguridad en conjunto con una evaluación periódica de incidentes.	Mejora continua en la seguridad de la información mediante la implementación de controles efectivos y acciones correctivas.	Reportes y revisión de incidentes.

CONCLUSIONES

La aplicación de los lineamientos de la norma ISO/IEC 27005 permitió clasificar los riesgos según su impacto y probabilidad. Se observó que los incidentes más críticos están relacionados con accesos no autorizados, pérdida de información y ataques de malware, los cuales pueden afectar tanto la operatividad del soporte técnico como la seguridad de los activos organizacionales.

El uso de las directrices ISO/IEC 27005 facilitó la categorización de los riesgos basados en su impacto y probabilidad, logrando como resultado que los incidentes más relevantes que implican entradas no autorizada, pérdida de datos y ataques de malware, afectando tanto la funcionalidad de soporte técnico como la seguridad de los activos de información.

La propuesta de un sistema de seguridad basado en la ISO/IEC 27005 demostró brindar grandes ventajas debido que permitió fortalecer la gestión de riesgos. Siendo necesario establecer controles adecuados y medidas de mitigación específicas para el área de soporte técnico, priorizando la protección de datos, la implementación de protocolos seguros.

La validación de la propuesta por parte de especialistas permitió determinar su viabilidad, efectividad y factibilidad. De acuerdo a la opinión de los expertos recalcaron la importancia de la integración de políticas de seguridad con las operaciones diarias del soporte técnico, asegurando su aplicabilidad en el entorno real y su alineación con los estándares internacionales.

RECOMENDACIONES

Es fundamental capacitar continuamente al personal de soporte técnico en buenas prácticas de seguridad de la información, ya que de esta manera se promoverá el cumplimiento de normativas y la concientización sobre los riesgos asociados a su actividad.

Se recomienda usar mecanismos de autenticación multifactorial, controles de acceso basados en roles y/o monitoreo continuo de las actividades de los usuarios para minimizar la posibilidad de accesos no autorizados.

Es esencial establecer un proceso de revisión y mejora continua del sistema de seguridad, adaptándolo a las nuevas amenazas y necesidades del área de soporte técnico para garantizar su eficacia a largo plazo.

Se recomienda desarrollar y documentar un plan de respuesta ante incidentes de seguridad que permita actuar de manera rápida y eficiente en caso de una brecha de seguridad, minimizando su impacto en la organización.

BIBLIOGRAFÍA

Abad García, I. A. (2022). Aplicación de la Norma internacional ISO 27005 para la gestión de riesgos operacionales en la empresa Canvia, Lima 2022.

Babilonia, G. S. (2023). Beneficios de las normas ISO 27000. *HIGH TECH-ENGINEERING JOURNAL, 3*(2), 31-39. https://revista.uct.edu.pe/index.php/hightech/article/view/514/550

Contreras, F. I. O., Narváez, V. P. M., & Palacios, M. M. T. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *Cienciometría*, *6*(2), 192-219.

Fajardo-Rojas, R. L. (2022). Evaluación de riesgos de seguridad de la información para la empresa Makoto SAS basado en la Norma ISO 27005: 2018.

Guevara Arias, V. I., & Soriano, S. D. (2022). *La nube en Pymes mediante las normas ISO 27005*. *Ingeniería y sus Alcances: Revista de Investigación*, 6(15), 169–182. https://doi.org/10.33996/revistaingenieria.v6i15.98

Guevara Chambergo, J. D. (2021). Implementación de una metodología de gestión de riesgos ad hoc basada en estándares internacionales y buenas prácticas para una empresa manufacturera peruana.

Lobo, M. M. (2022). Software para la gestión de riesgos en las prácticas forenses de derecho basado en los principios de la norma ISO 31000 e ISO 27005. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, (1), 243-257.

Montoya Ortecho, M. E. (2020). Evaluación de riesgo de seguridad de información según ISO 27005, OGITT–Instituto Nacional de Salud.

Morales, M. N. Z. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista peruana de computación y sistemas*, *2*(2), 43-60.

Morales, F., Toapanta, S., y Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Iberica de sistemas e tecnologías de informacao*, (E27), 553-565.

Naciones Unidas. (s.f.). *Objetivos de Desarrollo Sostenible: Industria, innovación e infraestructura*. https://www.un.org/sustainabledevelopment/es/infrastructure/

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119-123. http://dx.doi.org/10.36097/rsan.v1i58.2667

Secaira, J. I. M., Ocampo, R. D., Mera, E. R. Z., y Kovalenko, E. D. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). (Original). *Roca: Revista Científico-Educaciones de la provincia de Granma*, *16*(1), 546-559.

Toro Cabrera, O. E. (2023). *Evaluación de la seguridad física del centro de datos de la prefectura de Esmeraldas basado en la norma ISO 27005* (Doctoral dissertation, PUCESE-Escuela de Sistemas y Computación).

Velecela, C. L., y Tapia, J. P. C. (2020). Plan de gestión de seguridad de la información: caso de estudio: Gobierno Provincial del Cañar. *Journal of Science and Research: Revista Ciencia e Investigación*, *5*(4), 62-75.

Yarleque Aldana, L. M. (2024). Gestión de seguridad de la información usando Normas ISO 27005 en el Poder Judicial Período 2024.

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

Encuesta de Medición Impacto Seguridad de la Información

* Indica que la pregunta es obligatoria

Sección 1

1.- ¿Su organización cuenta con un área específica para seguridad de la información? *

- o Sí
- o No
- o No lo se

2.-En su organización, ¿se aplican normas de seguridad de la información? *

- o Sí, se siguen estándares oficiales.
- o Sí, pero sin un estándar formal
- o No se aplican normas específicas
- o No estoy seguro/a

3.-Conoces los principios básicos de la seguridad de la información? *

- o Si
- o No
- o No estoy seguro/a

4.-¿Conoces si la norma ISO/IEC 27001 se aplica en tu organización ?*

- o Mucho
- o Algo
- o Poco
- o No lo se

5.-Qué recursos o herramientas adicionales cree que necesitaría para cumplir mejor con las políticas de seguridad? *

- o Más capacitación.
- o Herramientas tecnológicas (por ejemplo, software de seguridad).
- o Mayor apoyo del equipo de TI.
- o No lo se

6.-La empresa ofrece capacitación en seguridad de la información a sus empleados? *

- o Sí, de manera regular.
- o Sí, pero de manera esporádica.
- o No
- o No lo sé.

7.-Con qué frecuencia se revisan y actualizan las políticas de seguridad de la información? *

- o Anualmente.
- o Cada dos años.
- o Cada 6 meses
- o No lo sé.

8.-Se realizan simulacros o pruebas para evaluar la respuesta ante incidentes de seguridad? *

- o Sí, regularmente.
- o Sí, ocasionalmente.
- o No.
- o No lo sé.

9.-Conoce los canales de comunicación para reportar problemas o sugerencias relacionadas con la seguridad? *

- o Sí.
- o No.
- o No lo sé.

10.-Conoce si se aplican sanciones o medidas correctivas en caso de incumplimiento de las políticas? *

- o Sí, siempre.
- o A veces.
- o No lo sé.
- o No.

11.-Considera que la alta dirección demuestra compromiso con las políticas de seguridad de la información? *

- o Sí, siempre.
- o A veces.

- o No.
- o No estoy seguro/a.

12.-Se siente apoyado/a por la empresa para cumplir con las políticas de seguridad de la información? *

- o Sí, siempre.
- o A veces.
- o No.
- o No estoy seguro/a.

13.-Sus compañeros y superiores cumplen con las políticas de seguridad de la información? *

- o Sí, siempre.
- o A veces.
- o No.
- o No estoy seguro/a.

14.-Qué cambios recomendaría para fortalecer la cultura de seguridad en la empresa? *

- o Mejor comunicación de las políticas.
- o Más capacitación práctica.
- o Mayor involucramiento de la alta dirección.
- o

15.-En una escala del 1 al 5, ¿Qué tan efectivas considera que son las políticas de seguridad de la información en la empresa? *

- o 1 (Nada efectivas)
- o 2
- o 3
- o 4
- o 5(Muy efectivas)

16.-Cree que las políticas de seguridad de la información protegen adecuadamente los datos de la empresa? *

- o Sí, completamente.
- o Parcialmente.
- o No del todo

- o No estoy seguro/a.

17.-¿En una escala del 1 al 5, Como calificarías tu conocimiento en seguridad de la información en la empresa? *

- o 1Muy deficiente
- o 2
- o 3
- o 4
- o 5 Muy Buena

18.-En una escala del 1 al 5, ¿qué tan satisfecho está con las políticas de seguridad de la información en la empresa? *

- o 1Nada Satisfecho
- o 2
- o 3
- o 4
- o 5 Muy Satisfecho

19.-Tiene sugerencias para mejorar las políticas de seguridad de la información en la empresa?

ANEXO 2

Validación de Especialistas

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Víctor Vilaña
Título obtenido: Ingeniero de Sistemas
C.I.: 1714075759
E-mail: victorvilana@igualdad.gob.ec
Institución de Trabajo: Consejo Nacional para la Igualdad
Cargo: Analista de seguridad de la información 3
Años de experiencia en el área:8 Años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

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

Tema: "Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad		x			
Factibilidad	x				
Novedad	x				
Fundamentación pedagógica	x				
Fundamentación tecnológica		x			
Indicaciones para su uso	x				
TOTAL	33				

Observaciones: Las empresas de telecomunicaciones lidian con grandes cantidades de información delicada de clientes. Sumado a la falta de concientización de los empleados y el uso de tecnología aumentan estos riesgos, para hacerlos frente es crucial implementar un sistema basado en la norma ISO / IEC 27005, que permita gestionar los riesgos de manera ordenada.

Recomendaciones: Se recomienda proteger los activos con controles como firewalls y cifrado, capacitar a los empleados para reconocer amenazas de phishing, actualización con herramientas modernas de seguridad. También es esencial realizar evaluaciones de riesgos periódicas, monitorear y responder a incidentes y fomentar una cultura de seguridad en todos los niveles.

Lugar, fecha de validación: Quito, 07 de marzo de 2025

VICTOR HUGO VILAÑA ECAZA

Firma del especialista
Ing. Víctor Vilaña

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Silvia Adriano
Título obtenido: Ing. Electrónica y Computacion
C.I.:0603346834
E-mail: silvia.adriano@cnt.gob.ec
Institución de Trabajo: Corporación Nacional de Telecomunicaciones
Cargo: Analista de Soporte Tecnico Corporativo Nivel 1
Años de experiencia en el área:10 Años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

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

Tema: " **"**

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica		x			
Indicaciones para su uso	X				
TOTAL	30	4			

Observaciones: Muchas empresas no cuentan con un plan sólido para recuperarse ante incidentes graves, como ciberataques o desastres naturales. Esto puede resultar en interrupciones prolongadas de los servicios, afectando a los clientes y generando pérdidas económicas.

Recomendaciones: Se recomienda desarrollar un plan detallado que identifique los servicios críticos, establecer tiempos de recuperación, definiendo roles y responsabilidades del equipo. Además, debe realizarse simulacros para asegurarse que el plan funcione y considerar tener copias de seguridad en ubicaciones seguras para proteger los datos ante ataques .

Lugar, fecha de validación: Quito, 07 de marzo de 2025

SILVIA DOLORES ADRIANO AMAGUAYA

Firmado digitalmente por SILVIA DOLORES ADRIANO AMAGUAYA
Fecha: 2025.03.07 15:26:39 -05'00'

Firma del especialista
ING. Silvia Adriano

ANEXO 3

Guía de Buenas Practicas

Guía de Buenas Prácticas para un Sistema de Seguridad de la Información en una Empresa de Telecomunicaciones (ISO/IEC 27005)

Elaborado por: Ing. Oscar Lema Parco

Universidad Tecnológica Israel

2025

Contenido

Introducción 45

Objetivo de la guía 46

Público objetivo 46

Metodología utilizada para su elaboración 46

Cómo utilizar la guía 46

1. Fundamentos teóricos y conceptuales 47

2. Importancia de la seguridad en telecomunicaciones 48

3. Relación con la norma ISO/IEC 27005 49

4. Gestión de riesgos según ISO/IEC 27005 50

5. Buenas Prácticas para la Implementación 51

5.1. Alcance 51

5.2. Identificación y Clasificación de Activos 51

5.3. Valoración de Activos 51

5.4. Identificación de Amenazas 52

5.5. Estimación de riesgo 52

5.6. Tratamiento de riesgos. 54

5.7. Monitoreo y revisión continua 56

6. Herramientas Complementarias 58

6.1. Plantillas para Análisis de Riesgos 58

6.2. Plantilla de evaluación de riesgos ISO/IEC 27005 59

7. Buenas Prácticas y Consideraciones Finales 61

7.1. Errores Comunes a Evitar 61

7.2. Sugerencias para una mejor implementación 62

7.3. Factores de Éxito 62

8. Conclusiones y Recomendaciones 63

Índice de Tablas

Tabla 1 Valoración de activos 51
Tabla 2 Identificación de amenazas..... 52
Tabla 3 Identificación de amenazas..... 53
Tabla 4 Tratamiento de riesgos 54
Tabla 5 Ciclo PHVA..... 57
Tabla 6 Plantilla de evaluación de riesgos ISO/IEC 27005 60

Índice de Figuras

Figura 1 Principales normas basado en los estándares de la familia ISO/IEC 27000..... 49
Figura 2 Proceso para la Gestión del Riesgo..... 50

Introducción

La seguridad de la información es la protección de la información importante contra el acceso, la divulgación, el uso, la alteración o la interrupción no autorizados. Además, ayuda a garantizar que los datos confidenciales de la organización estén disponibles para los usuarios autorizados, permanezcan confidenciales y mantengan su integridad

Actualmente se encuentra inmersa en varios aspectos de la cotidianidad, ya sea en ámbitos como teletrabajo, juegos, educación en línea, compra de productos en Internet entre otras. En una era de transformación digital, donde los negocios y sobre todo la información se encuentra en medios digitales, implica un mayor reto para las organizaciones el proteger sus datos. Una organización que quiera competir actualmente, deberá manejar una estrategia apoyada en la alta dirigencia y tomar decisiones orientadas a proteger su activo más valioso, la información.

Sin embargo, la implementación de un Sistema de Gestion de Seguridad de la Informacion se encuentra determinada por la estructura organizacional de las instituciones, lo cual abarca características como: tipo, tamaño, objetivos, servicios, procesos, personal y requerimientos de seguridad que establece la misma, para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001.

Objetivo de la guía

Esta guía tiene como objetivo proporcionar un conjunto de buenas prácticas para la implementación de un sistema de seguridad de la información en empresas de telecomunicaciones, basado en la norma **ISO/IEC 27005**. Con el fin de reducir los riesgos y protegerse ante amenazas que puedan vulnerar la confiabilidad, disponibilidad e integridad de la información que a diario es manejada por el área de soporte técnico.

Público objetivo

Esta guía está dirigida a:

- Responsables de seguridad de la información en empresas de telecomunicaciones.
- Administradores de Tic's
- Directivos y tomadores de decisiones en el ámbito de la seguridad.
- Personal del área de soporte técnico.
- Equipos de auditoría y cumplimiento normativo.

Metodología utilizada para su elaboración

La guía se ha desarrollado a partir de:

- Revisión de la norma ISO/IEC 27005
- Análisis de estudios de caso de empresas en el sector de telecomunicaciones.
- Validación de expertos en seguridad de la información.
- Análisis de criterios sugeridos por personal del área se soporte técnico.

Cómo utilizar la guía

Esta guía se estructura en secciones que facilitan la lectura como la consulta puntual, para obtener un panorama general de las buenas prácticas para un Sistema de Seguridad de la Información en una Empresa de Telecomunicaciones el cual es adaptable a las necesidades del usuario.

1. Fundamentos teóricos y conceptuales

Seguridad de la información

La seguridad de la información es la práctica de proteger los datos y los sistemas de información de amenazas como el acceso no autorizado o la fuga de datos que provoquen la divulgación, alteración o destrucción de información sensible.

Activos

Son cualquier tipo de recurso que contenga información valiosa para una organización. Estos incluyen datos, documentos, correos electrónicos, software, sistemas, redes, dispositivos, bases de datos etc.

Amenazas

Es todo elemento o acción capaz de atentar contra su confidencialidad, integridad y disponibilidad. Pudiendo ser amenazas relacionadas con fallas humanas, ataques malintencionados o catástrofes naturales.

Vulnerabilidad

Es una debilidad en los sistemas de tecnología de la información que pone en peligro la seguridad y privacidad de tu empresa

Riesgo

Un riesgo es la probabilidad de que se produzca in impacto determinado a un activo de información está asociado también en la materialización de una amenaza aprovechando la vulnerabilidad de un activo.

Gestión De Riesgos

Según Morales (2019) indica que la gestión del riesgo tienes cambios constantes y cada marco de gestión de riesgos posee distintas ventajas y desventajas, para lo cual es necesario considerar el más simple y que cumpla con los requisitos organizacionales de forma que se asegure una adecuada implementación. Para lo cual es imprescindible realizar evaluaciones periódicas de forma que se evalué el cumplimiento de las necesidades**.**

ISO/IEC 27005

Según Abad (2022) define a la norma como el conjunto de directrices que sirven para establecer un marco sistemático que se enfoque en la administración de riesgos en la seguridad informática necesarios para la identificación de los requisitos seguros de información que exige la entidad a fin de proponer un sistema de administración seguro.

2. Importancia de la seguridad en telecomunicaciones

La seguridad en telecomunicaciones es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información ya sea de clientes externos o internos que se transmite a través de redes de comunicación.

Además, es importante como protección contra las amenazas cibernéticas debido que al ofrecer una solución de seguridad bien estructurada reduce los gastos generales y protege a las organizaciones de costosas pérdidas que se producen por una violación de datos u otro incidente de seguridad. Garantizar el acceso legítimo a los sistemas, aplicaciones y datos permite las operaciones comerciales y la entrega de servicios y productos a los clientes.

Su importancia radica en varios aspectos clave:

Protección de datos: La protección de datos se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes.

Prevención de ciberataques: es el conjunto de medidas, tecnologías y prácticas que tienen como objetivo proteger los sistemas informáticos, las redes y los datos frente a accesos no autorizados, ataques maliciosos y fallos.

Confidencialidad de la comunicación: es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Disponibilidad del servicio: se mide en términos de cortes, que son los tiempos durante los que el sistema no está disponible para los usuarios

Confianza del usuario: se refiere a la integridad y precisión de los datos como una medida de qué tanto puede contarse con que son constantes y no presentan errores en los distintos tiempos y fuentes.

3. Relación con la norma ISO/IEC 27005

Según lo indicado por Lobo (2022) Indica que la ISO 27005, es una norma que se ocupa de la gestión de los riesgos relativos a la seguridad de información, esta norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001.

Figura 8
Principales normas basado en los estándares de la familia ISO/IEC 27000

Según Montoya (2020) describen una actividad esencial como la identificación de Riesgo cuyo propósito es establecer que podría suceder para producir una potencial perdida, y saber cómo, cuándo y por qué la sustracción podría suceder. La Identificación de Riesgos que se da por inicio con la identificación de los activos de información que son clasificados en cinco tipos: Información, software, Físico, Personas y Servicio, el cual debe ser definido los aspectos de seguridad de la información (confidencialidad, integridad y disponibilidad - CID) para determinar el valor de cada activo de información.

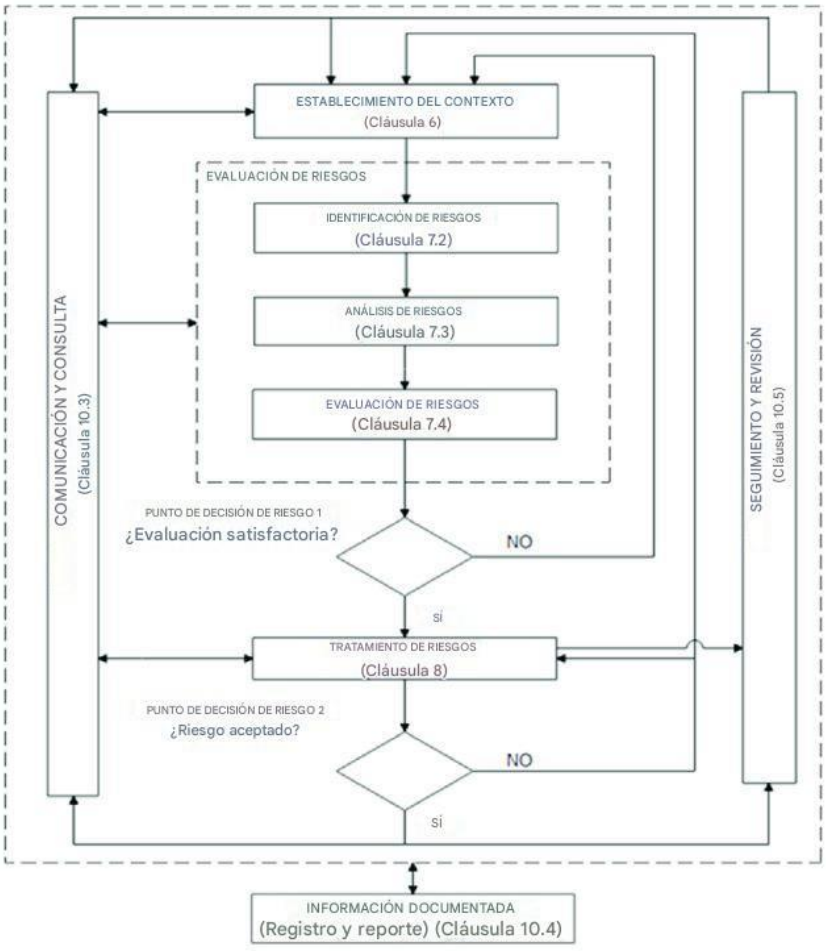
De igual manera Lobo et al. (2022) informa que la norma es aplicable a toda la organización, que tenga la intención de mejorar su gestión de riesgos sobre seguridad de la información, con el objeto de generar una lista completa de los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos.

4. Gestión de riesgos según ISO/IEC 27005

La norma ISO/IEC 27005 proporciona directrices para la gestión de riesgos en seguridad de la información, alineada con los requisitos de la norma ISO/IEC 27001. El proceso incluye:

- **Identificación de activos y riesgos:** Determinar qué información es crítica y qué amenazas podrían afectarla.
- **Evaluación de riesgos:** Analizar la probabilidad e impacto de cada riesgo.
- **Tratamiento de riesgos:** Implementar controles para mitigar, transferir, evitar o aceptar los riesgos.
- **Monitoreo y revisión:** Evaluar continuamente la efectividad de los controles.
- **Ciclo de vida de la gestión de riesgos**. - incluye las fases de planificación, implementación, evaluación y mejora continua, asegurando que el SGSI se adapte a los cambios en el entorno y las amenazas.

Figura 9
Proceso para la Gestión del Riesgo



5. Buenas Prácticas para la Implementación

5.1. Alcance

Se ha determinado aplicar a la gestión del soporte técnico de una empresa de Telecomunicaciones y como alcance se enfocará en la identificación y la evaluación de riesgos siguiendo los lineamientos de la ISO/IEC 27005

5.2. Identificación y Clasificación de Activos

Se procedió a identificar los activos más importantes que se utilizan para la gestión del soporte técnico, los cuales se clasifican en activos de:

- Información (nombres, ingeniería de clientes, registro de incidentes)
- Software (Programas para levantamiento de incidentes, almacenamiento de información)
- Hardware (Pc ’s, Sw, Routers, teléfonos).

5.3. Valoración de Activos

Para su valoración se considera los parámetros de confidencialidad, integridad y disponibilidad**.** Para lo cual se clasifico según su impacto e importancia para la gestión, en escalas de bajo (1), medio (2) y alto (3).

Tabla 10
Valoración de activos

Activo	Confidencialidad	Integridad	Disponibilidad	Valoración
Información de clientes	3 (Alto)	3 (Alto)	2 (Medio)	8 (Crítico)
Software para levantamiento de incidentes	2 (Medio)	2 (Medio)	3 (Alto)	7 (Alto)
Software para almacenamiento de información	2 (Medio)	3 (Alto)	3 (Alto)	8 (Crítico)
Configuración equipos de red	3 (Alto)	3 (Alto)	3 (Alto)	9 (Crítico)

Equipos de uso personal	2 (Medio)	2 (Medio)	2 (Medio)	6 (Medio)

Interpretación:

- Valores iguales o menores a 6, se considera impacto moderado y puede gestionarse con medidas estándar.
- Valores de 6 y 7 se considera alto impacto y necesitan protección adecuada.
- Valores de 8 y 9 se considera impacto crítico y requieren medidas de seguridad más estrictas.

5.4. Identificación de Amenazas

Una amenaza es un evento que puede comprometer la seguridad de la información, se procede a identificarlas tomando como referencia lo indicado en la ISO 27005:2002, las cuales pueden clasificarse según la Tabla 1.

Tabla 11
Identificación de amenazas

Amenazas Técnicas	Amenazas Humanas	Amenazas Físicas y Ambientales
Ataques de malware, ransomware, phishing, DDos	Ingeniería social	Desastres naturales
Accesos no autorizados a base de datos o programas de soporte.	Falta de concientización (contraseñas inseguras, accesos a sitios inseguros)	Fallos eléctricos
Errores en la configuración de equipos de red.	Fallos operativos en la gestión de tickets.	Pérdida o robo de equipos de la empresa.

5.5. Estimación de riesgo

Es un factor clave dentro del proceso ya que consiste en analizar y evaluar las amenazas, y posibles impactos en los activos de información y según eso determinar el nivel del riesgo.

De acuerdo a la ISO27005 para la estimación de riesgo se calcula multiplicando la probabilidad de ocurrencia de un incidente por el impacto (consecuencias) sobre el activo afectado. Para lo cual se usó un enfoque cualitativo clasificándolo en escalas de muy bajo (1), bajo (2), medio (3) y alto (4).

Tabla 12

Identificación de amenazas

Amenazas	Activo Afectado	Probabilidad (1-4)	Impacto (1-4)	Riesgo	Prioridad de Atención
Ataque de malware, ransomware	Software para almacenamiento de información	3(Media)	4 (Crítico)	12 (Crítico)	Alta
Phishing	Información de clientes	4 (Alta)	3 (Alto)	12 (Crítico)	Alta
Ataque DDoS	Software para almacenamiento de información	3 (Media)	3 (Alto)	9 (Alto)	Alta
Errores en la configuración de equipos de red.	Configuración equipos de red	2 (Baja)	4 (Crítico)	8 (Medio)	Media
Acceso no autorizado a servidores	Configuración equipos de red	Alto (4)	Alto (4)	Crítico (16)	Alta
Falta de concientización	Equipos de uso personal	4 (Alta)	3 (Alto)	12 (Crítico)	Alta
Fallos operativos en la gestión de tickets.	Software para levantamiento de incidentes	3 (Media)	3 (Alto)	9 (Alto)	Alta
Robo de equipos de la empresa	Equipos de uso personal	2 (Baja)	3 (Alto)	6 (Medio)	Media

Interpretación:

- Valoración baja 1 - 4: Monitoreo, no requiere acciones inmediatas.
- Valoración media 5 - 8: requiere aplicar controles básicos
- Valoración alta 9 - 12: requiere aplicar medidas correctivas urgentes.
- Valoración critica 13 – 16: requiere acciones inmediatas para evitar impactos severos

5.6. Tratamiento de riesgos.

El tratamiento de los riesgos implica tomar decisiones frente a los diferentes riesgos existentes Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo. Existen cuatro opciones disponibles para el tratamiento del riesgo:

- Mitigar: Implementar controles para reducir la probabilidad o el impacto del riesgo
- Transferir: Transferir el riesgo a un tercero.
- Evitar: Eliminar la actividad o condición que genera el riesgo.
- Aceptar: Aceptar el riesgo si el costo de mitigación es mayor que el impacto potencial.

Tabla 13

Tratamiento de riesgos

Amenaza	Activo Afectado	Probabilidad (1-4)	Impacto (1-4)	Nivel de Riesgo	Prioridad de Atención	Tratamiento	Controles Recomendados
Ataque de malware, ransomware	Software para almacenamiento de información	3 (Media)	4 (Crítico)	12 (Crítico)	Alta	Mitigar	Instalar y actualizar software antivirus/ antimalware.
							Realizar copias de seguridad y Restringir ejecución de archivos no autorizados.
Phishing	Información de clientes	4 (Alta)	3 (Alto)	12 (Crítico)	Alta	Mitigar	Capacitar al personal en identificación de phishing.
							Implementar filtros anti-phishing en el correo electrónico.
							Usar autenticación de dos factores
Ataque DDoS	Software para almacena	3 (Media)	3 (Alto)	9 (Alto)	Alta	Mitigar	Implementar firewalls y sistemas de

	miento de información						detección/prevención de intrusos (IDS/IPS).
							Contratar servicios de protección DDoS.
							Monitorear el tráfico de red.
Errores en la configuración de equipos de red	Configuración equipos de red	2 (Baja)	4 (Crítico)	8 (Medio)	Media	Mitigar	Establecer revisiones periódicas de configuración.
							Automatizar configuraciones mediante herramientas de gestión de red.
							Capacitar al personal en buenas prácticas de configuración.
Acceso no autorizado a servidores	Configuración equipos de red	4 (Alta)	4 (Crítico)	16 (Crítico)	Alta	Mitigar	Implementar autenticación de dos factores (2FA).
							Restringir accesos mediante el principio de mínimo privilegio.
							Monitorear logs de acceso.
Falta de concientización (contraseñas inseguras, accesos a sitios inseguros)	Equipos de uso personal	4 (Alta)	3 (Alto)	12 (Crítico)	Alta	Mitigar	Realizar capacitaciones periódicas en seguridad.
							Implementar políticas de contraseñas seguras.
							Bloquear el acceso a sitios web no seguros.

Fallos operativos en la gestión de tickets	Software para levantamiento de incidencias	3 (Media)	3 (Alto)	9 (Alto)	Alta	Mitigar	Establecer procedimientos claros para la gestión de tickets.
							Capacitar al personal en el uso del software.
							Monitorear el rendimiento del sistema.
Robo de equipos de la empresa	Equipos de uso personal	2 (Baja)	3 (Alto)	6 (Medio)	Media	Mitigar	Implementar medidas de seguridad física (cámaras, control de acceso).
							Cifrar discos duros de equipos portátiles.
							Establecer políticas de uso seguro de dispositivos.

5.7. Monitoreo y revisión continua

Se presenta el plan de mejora continúa basado en la norma ISO/IEC 27005, el cual utiliza el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) y se enfoca en los riesgos identificados en la tabla de tratamiento de riesgos proporcionada en la Tabla 4. Cada fase del ciclo se detalla con acciones específicas, responsables y plazos.

El ciclo PHVA consta de cuatro fases: Planificar: identifican los problemas y planificar acciones.

- Hacer: llevar a cabo las acciones planificadas en la fase anterior.
- Verificar: consiste en monitorear y evaluar los resultados.
- Actuar: Evaluar si las acciones emprendidas han dado el resultado esperado.

Tabla 14
Ciclo PHVA

Riesgo	Planificar	Hacer	Verificar	Actuar
Ataques de malware y/o ransomware	Instalación de antivirus, realizar copias de seguridad y restringir acceso o ejecución de archivos no autorizados.	Instalación de antivirus en todos las PC y configurar copias de seguridad automáticas.	Verificar que el antivirus esté activo y las copias de seguridad se ejecuten correctamente.	Si el número de incidentes se reduce, mantener los controles.
	Designar equipo de TI para antivirus y soporte técnico para copias de seguridad.	Realizar lo planificado.	Verificar el nro. de incidentes de malware reportados	Si los incidentes continúan, considerar la implementación de soluciones en equipos finales.
Phishing	Planificar simulacros	Realizar los simulacros de phishing.	Manejar reportes sobre de correos phishing detectados.	Realizar actualización de los filtros de correo.
	Implementación de filtros anti-phishing	Filtros anti-phishing implementados.	Verificar los resultados de simulacros de phishing.	Aumentar la frecuencia de simulacros.
Ataque DDoS	Planificar contratar servicios de protección DDoS.	Cumplir con lo planificado.	Verificar la cantidad de ataques DDoS bloqueados.	Revisar y realizar ajustes en las configuraciones de firewalls.
	Configurar firewalls y sistemas de IDS e IPS	Llevar a cabo lo planificado.	Tiempo de respuesta a ataques.	Revisar contratos de protección DDoS.
Errores en la configuración de equipos de red	Determinar revisiones periódicas en la configuración.	Realizar lo planificado.	Verificar los errores de configuración detectados.	Automatizar más procesos de configuración.
	Planificar que las configuraciones sean automáticas.	Cumplir lo planificado.	Monitorear el tiempo en su resolución.	Realizar capacitaciones al personal en nuevas herramientas.
Acceso no autorizado a servidores	Implementar autenticación multifactorial.	Autenticación de dos factores (2FA) implementada.	Número de accesos no autorizados detectados.	Revisar y ajustar políticas de acceso.

	Comprobar políticas de acceso.	Revisar las políticas de acceso.	Verificar el tiempo de respuesta a incidentes.	Implementar monitoreo continuo.
Falta de concientización	Realizar capacitaciones mensuales.	Cumplir con las capacitaciones mensuales realizadas.	Manejar reportes del porcentaje de empleados capacitados.	Brindar material actualizado para capacitación.
	Implementar políticas de contraseñas seguras.	Cumplir lo planificado.	Verificar la cantidad de incidentes relacionados a contraseñas.	Incrementar la frecuencia de entrenamientos.
Fallos operativos en la gestión de tickets	Capacitar al personal en el uso del software de gestión de tickets	Personal capacitado	Tiempo promedio de resolución de tickets.	Optimizar uso del software de gestión de tickets.
	Monitorear el rendimiento del sistema de tickets.	Monitoreado realizado	Manejar reportes del Número de fallos reportados.	Capacitar al personal en nuevas funcionalidades.
Robo de equipos de la empresa	Implementar medidas de seguridad física	Llevar a cabo lo planificado.	Investigar los incidentes de robo reportados	Reforzar medidas de seguridad física en las instalaciones.
	Cifrados discos duros.	Discos duros cifrados.	Comprobar la efectividad de las medidas de seguridad física.	Actualización de políticas de uso de equipos.

6. Herramientas Complementarias

6.1. Plantillas para Análisis de Riesgos

Las plantillas para análisis de riesgos son instrumentos estructurados que facilitan la identificación, evaluación y gestión de riesgos en el ámbito de la seguridad de la información.

La plantilla sirve como guía estandarizada, que garantiza que se revisen sistemáticamente áreas críticas como las vulnerabilidades del sistema, las amenazas potenciales y los impactos en las operaciones comerciales. Al seguir esta plantilla, las empresas pueden gestionar mejor su postura de seguridad, desarrollar estrategias de mitigación adecuadas y cumplir con las regulaciones de la industria.

6.2. Plantilla de evaluación de riesgos ISO/IEC 27005

Esta plantilla se ajusta a la norma ISO/IEC 27005, que se centra en la gestión de riesgos de seguridad de la información. Proporciona un enfoque sistemático para identificar y evaluar los riesgos y planificar las opciones de tratamiento de los mismos. Entre sus características principales se incluyen:

- Identificación y análisis de riesgos
- Evaluación de riesgos basada en el impacto en el negocio
- Planificación y documentación del tratamiento de riesgos
- Seguimiento y revisión continua

Explicación de la Plantilla

- ID: Identificador para cada riesgo evaluado.
- Activo: El recurso o información que está en riesgo.
- Amenaza: es un evento o acción que puede causar daño al activo.
- Vulnerabilidad: Debilidad o fallo que puede ser explotado por la amenaza
- Probabilidad (1-5): Probabilidad de que la amenaza ocurra
- Impacto (1-5): Consecuencia o daño que causaría la materialización de la amenaza
- Nivel de Riesgo (P x I): Resultado de multiplicar la probabilidad por el impacto.
- Controles Existentes: son medidas de seguridad ya implementadas para mitigar el riesgo.
- Nivel de riesgo después de aplicar los controles existentes.
- Tratamiento: Estrategia para gestionar el riesgo:
    - Mitigar: Reducir la probabilidad o el impacto.
    - Transferir: Compartir el riesgo con un tercero (ej: seguro).
    - Evitar: Eliminar la actividad que genera el riesgo.
    - Aceptar: Aceptar el riesgo si el costo de mitigación es mayor que el impacto.
- Controles Propuestos: Medidas adicionales recomendadas para reducir el riesgo residual.

Tabla 15

Plantilla de evaluación de riesgos ISO/IEC 27005

D	Activo	Amenaza	Vulnerabilidad	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo	Controles Existentes	Nivel de Riesgo Residual	Tratamiento	Controles Propuestos
1	Software de almacenamiento	Ataque de malware /ransomware	Falta de actualizaciones de software	4	5	20 (Crítico)	Antivirus básico	12 (Alto)	Mitigar	Implementar soluciones a equipos finales y realizar copias de seguridad diarias.
2	Información de clientes	Phishing	Falta de capacitación del personal	5	4	20 (Crítico)	Filtros anti-phishing	10 (Alto)	Mitigar	Capacitar al personal en identificación de phishing e implementar autenticación
3	Equipos de red	Ataque DDoS	Configuración insegura de firewalls	3	4	12 (Alto)	Firewall básico	8 (Medio)	Mitigar	Configurar reglas avanzadas en el firewall y contratar servicios de protección DDoS.
4	Equipos de uso personal	Robo de dispositivos	Falta de cifrado en discos duros	2	3	6 (Medio)	Ninguno	6 (Medio)	Mitigar	Implementar cifrado de discos y establecer políticas de uso seguro de dispositivos.
5	Software de gestión de incidencias	Fallos operativos en la gestión	Falta de procedimientos claros	3	3	9 (Alto)	Documentación básica	6 (Medio)	Mitigar	Establecer procedimientos detallados y capacitar al personal en el uso del software

7. Buenas Prácticas y Consideraciones Finales

En esta sección, se presentan recomendaciones clave para una implementación exitosa de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27005**.** Se incluyen errores comunes a evitar, sugerencias para una mejor implementación y factores de éxito.

7.1. Errores Comunes a Evitar

- Falta de compromiso de la alta dirección. - Sin el apoyo y compromiso de la dirección, el SGSI no tendrá los recursos ni la prioridad necesarios para ser efectivo.
- Subestimar la importancia de la capacitación. - No capacitar al personal en seguridad de la información puede llevar a errores humanos, como hacer clic en enlaces de phishing o usar contraseñas débiles.
- Identificación incompleta de activos**. -** Uno de los errores más comunes es no considerar todos los activos críticos durante la fase de identificación pudiendo dejar brechas de seguridad en el sistema.
- Evaluación subjetiva de riesgos. - Basar la evaluación de riesgos en percepciones personales en lugar de datos objetivos puede conducir a una gestión ineficaz.
- Falta de priorización en el tratamiento de riesgos. - Intentar abordar todos los riesgos simultáneamente puede diluir los esfuerzos y recursos.
- Solución: Establecer un sistema de clasificación que priorice los riesgos más críticos, enfocando los recursos en aquellos que representan una mayor amenaza para la organización
- Implementar controles sin evaluar su efectividad. -Aplicar controles sin medir su impacto real puede generar una falsa sensación de seguridad.
- No documentar procesos y políticas. - La falta de documentación dificulta la auditoría, el monitoreo y la mejora continua del SGSI.
- Ignorar la mejora continua. - La seguridad de la información es un campo dinámico; las amenazas evolucionan constantemente y el no revisar y actualizar el SGSI de forma periódica puede hacer que se vuelva obsoleto frente a nuevas amenazas.
- Subestimación de la formación y concienciación. -Considerar que la tecnología por sí sola es suficiente para garantizar la seguridad es un error debido que el factor humano juega un papel crucial.
- No Integrar la gestión de riesgos con los objetivos organizacionales. - Tratar la gestión de riesgos como un proceso aislado puede limitar su efectividad.

7.2. Sugerencias para una mejor implementación

- Involucrar a todas las áreas de la organización: Asegurar que todos los departamentos participen en la identificación de riesgos y la implementación de controles.
- Realizar un análisis de riesgos detallado: Identificar todos los activos críticos, amenazas y vulnerabilidades, y priorizar los riesgos según su impacto y probabilidad.
- Establecer políticas y procedimientos claros: Documentar políticas de seguridad, como la gestión de contraseñas, el acceso a sistemas y la respuesta a incidentes.
- Capacitar y concienciar al personal: Realizar capacitaciones periódicas en seguridad de la información y promover una cultura de seguridad en la organización.
- Implementar controles proporcionales al riesgo: asegurar que los controles sean adecuados para el nivel de riesgo y no generen costos innecesarios.
- Monitorear y revisar continuamente: Establecer métricas para evaluar la efectividad de los controles y realizar auditorías internas y externas.
- Utilizar herramientas y tecnologías adecuadas: Implementar soluciones como firewalls, sistemas de detección de intrusos (IDS), y software de gestión de vulnerabilidades.
- Mantener actualizado el SGSI: Revisar y ajustar el SGSI periódicamente para adaptarse a cambios en el entorno, las amenazas y los requisitos legales.

7.3. Factores de Éxito

- Compromiso de la alta dirección: El apoyo de la dirección es crucial para asignar recursos, establecer prioridades y promover una cultura de seguridad.
- Enfoque basado en riesgos: Centrarse en los riesgos más críticos permite optimizar recursos y maximizar la efectividad del SGSI.
- Participación de todos los niveles de la organización: Involucrar a empleados, gerentes y equipos técnicos asegura que el SGSI sea integral y aplicable en toda la organización.
- Capacitación y concienciación continua: Un personal bien capacitado es la primera línea de defensa contra amenazas como el phishing y los errores humanos.
- Documentación y trazabilidad: Mantener registros detallados de políticas, procedimientos y controles facilita la auditoría y la mejora continua.
- Adaptabilidad y mejora continua: Un SGSI flexible y actualizado puede responder rápidamente a cambios en el entorno y las amenazas.
- Cumplimiento normativo: Asegurar que el SGSI cumpla con normativas y estándares relevantes, como ISO/IEC 27001, GDPR, o leyes locales de protección de datos

8. Conclusiones y Recomendaciones

Conclusiones

La seguridad de la información es una parte fundamental en las empresas de telecomunicaciones, debido a la gran cantidad de datos sensibles que manejan. La implementación de un sistema de seguridad basado en la norma ISO/IEC 27005 permite gestionar los riesgos de manera eficiente, protegiendo la integridad, confidencialidad y disponibilidad de la información.

La elaboración de una guía de buenas prácticas proporciona un marco estructurado para la identificación, evaluación y mitigación de riesgos en la empresa. Esto facilita la adopción de estrategias de seguridad y fortalece la cultura organizacional en torno a la protección de la información.

La norma ISO/IEC 27005 ofrece un método sistemático para gestionar los riesgos de seguridad, permitiendo a la empresa evaluar el impacto y la probabilidad de incidentes y aplicar controles adecuados. La adaptación de este estándar garantiza un enfoque alineado con sus necesidades y objetivos estratégicos.

La guía de buenas prácticas no solo es un documento técnico, sino una herramienta estratégica para la empresa. Su correcta implementación y actualización continua garantizarán una gestión eficiente de la seguridad de la información, minimizando riesgos y optimizando su respuesta ante posibles incidentes

Recomendaciones

Es fundamental capacitar a todos los colaboradores en seguridad de la información, asegurando que comprendan los riesgos y adopten las buenas prácticas recomendadas en la guía.

Es necesario realizar auditorías periódicas para identificar nuevas vulnerabilidades y actualizar la guía con base en los cambios tecnológicos y regulatorios.

Se recomienda definir y documentar un plan de respuesta ante incidentes de seguridad, asegurando que la empresa pueda reaccionar de manera rápida y efectiva ante cualquier brecha o ataque.

Se sugiere alinear la guía con otras normativas como ISO/IEC 27001, ISO/IEC 27002 y regulaciones específicas del sector telecomunicaciones para fortalecer la protección de la información.

Posibles Mejoras Futuras

Considerar la implementación de herramientas de análisis de comportamiento para detectar anomalías y amenazas en tiempo real.

Fortalecer la seguridad en entornos de trabajo remoto por medio de políticas de seguridad para la protección de la información en modelos de teletrabajo.

Realizar pruebas de penetración y simulacros de ataques para evaluar la efectividad del sistema de seguridad y determinar posibles mejoras.

Referencias Bibliográficas

Abad García, I. A. (2022). Aplicación de la Norma internacional ISO 27005 para la gestión de riesgos operacionales en la empresa Canvia, Lima 2022.

Babilonia, G. S. (2023). Beneficios de las normas ISO 27000. *HIGH TECH-ENGINEERING JOURNAL, 3*(2), 31-39. https://revista.uct.edu.pe/index.php/hightech/article/view/514/550

Bitsight. (s.f.). *5 plantillas de evaluación de riesgos de ciberseguridad para VRM*. Recuperado el [fecha de acceso], de https://www-bitsight-com.translate.goog/blog/cybersecurity-risk-assessment-templates?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Ciberseguridad: qué es, cómo funciona y su importancia. (s.f.). Pirani. Recuperado de https://www.piranirisk.com/es/academia/especiales/ciberseguridad-que-es-como-funciona-y-su-importancia

Comisión Económica para América Latina y el Caribe (CEPAL). (s.f.). *Gestión de datos de investigación*. Recuperado de https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Contreras, F. I. O., Narváez, V. P. M., & Palacios, M. M. T. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *Cienciometría*, *6*(2), 192-219.

Confidencialidad de la información. (s.f.). Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán. Recuperado de https: //www.incmnsz.mx/ opencms/contenido /investigacion/ comiteEtica/ confidencialidadInformacion.html

Guevara Arias, V. I., & Soriano, S. D. (2022). *La nube en Pymes mediante las normas ISO 27005*. *Ingeniería y sus Alcances: Revista de Investigación*, 6(15), 169–182. https://doi.org/10.33996/revistaingenieria.v6i15.98

Guevara Chambergo, J. D. (2021). Implementación de una metodología de gestión de riesgos ad hoc basada en estándares internacionales y buenas prácticas para una empresa manufacturera peruana.

Fajardo-Rojas, R. L. (2022). Evaluación de riesgos de seguridad de la información para la empresa Makoto SAS basado en la Norma ISO 27005: 2018.

IBM. (s.f.). *¿Qué es la confiabilidad de los datos?* Recuperado de https://www.ibm.com/mx-es/topics/data-reliability.

Lobo, M. M. (2022). Software para la gestión de riesgos en las prácticas forenses de derecho basado en los principios de la norma ISO 31000 e ISO 27005. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, (1), 243-257.

Montoya Ortecho, M. E. (2020). Evaluación de riesgo de seguridad de información según ISO 27005, OGITT–Instituto Nacional de Salud.

Morales, M. N. Z. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista peruana de computación y sistemas*, *2*(2), 43-60.

Morales, F., Toapanta, S., y Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Iberica de sistemas e tecnologías de informacao*, (E27), 553-565.

Naciones Unidas. (s.f.). *Objetivos de Desarrollo Sostenible: Industria, innovación e infraestructura*. https://www.un.org/sustainabledevelopment/es/infrastructure/

Ponce, M. (2024). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119-123. http://dx.doi.org/10.36097/rsan.v1i58.2667

Secaira, J. I. M., Ocampo, R. D., Mera, E. R. Z., y Kovalenko, E. D. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). (Original). *Roca: Revista Científico-Educaciones de la provincia de Granma*, *16*(1), 546-559.

Toro Cabrera, O. E. (2023). *Evaluación de la seguridad física del centro de datos de la prefectura de Esmeraldas basado en la norma ISO 27005* (Doctoral dissertation, PUCESE-Escuela de Sistemas y Computación).

Velecela, C. L., y Tapia, J. P. C. (2020). Plan de gestión de seguridad de la información: caso de estudio: Gobierno Provincial del Cañar. *Journal of Science and Research: Revista Ciencia e Investigación*, *5*(4), 62-75.

Yarleque Aldana, L. M. (2024). Gestión de seguridad de la información usando Normas ISO 27005 en el Poder Judicial Período 2024.