
**UNIVERSIDAD POLITECNICA SALESIANA**

**SEDE GUAYAQUIL**

**CARRERA DE COMPUTACION**

# Revisión de literatura de la norma ISO/IEC 27001 en el sector de las telecomunicaciones de la ciudad de Guayaquil: Evaluación de la seguridad de las redes y sistemas informáticos

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

**AUTORES:** Luis Andrés Gallegos Manrique y Cristhopher Daniel Lynch Escobar

**TUTOR:** Joe Frand Llerena Izquierdo

Guayaquil – Ecuador

2024

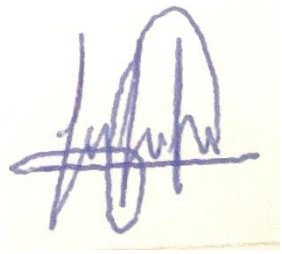
# CERTIFICADO DE RESPONSABILIDAD Y AUTORIA DEL TRABAJO DE TITULACION

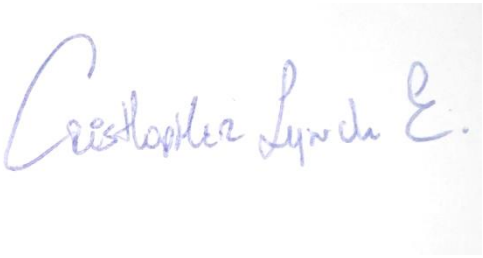
Nosotros, Luis Andrés Gallegos Manrique con documento de identificación N° 0950319459 y Cristhopher Daniel Lynch Escobar con documento de identificación N° 0958153082; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la universidad politécnica salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 4 de febrero del año 2024

Atentamente,





| | |
|---|---|
| Luis Andrés Gallegos Manrique | Cristhopher Daniel Lynch Escobar |
| 0950319459 | 0958153082 |

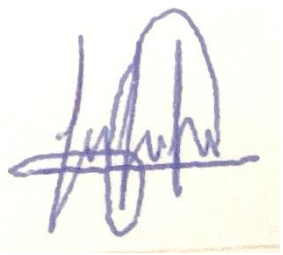
**CERTIFICADO DE CESION DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACION A LA UNIVERSIDAD POLITECNICA SALESIANA**

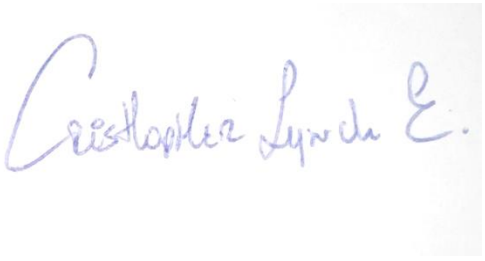
Nosotros, Luis Andrés Gallegos Manrique con documento de identificación N° 0950319459 y Cristhopher Daniel Lynch Escobar con documento de identificación N° 0958153082, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del articulo académico: "Revisión de literatura de la norma ISO/IEC 27001 en el sector de las telecomunicaciones de la ciudad de Guayaquil: Evaluación de la seguridad de las redes y sistemas informáticos.", el cual ha sido desarrollado para optar por el título de: Ingeniero en Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana

Guayaquil, 4 de febrero del año 2024

Atentamente,





Luis Andrés Gallegos Manrique
0950319459

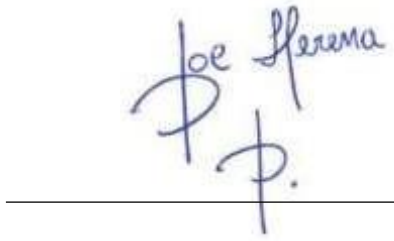
Cristhopher Daniel Lynch Escobar
0958153082

# CERTIFICADO DE DIRECCION DEL TRABAJO DE TITULACION

Yo, Joe Frand Llerena Izquierdo con documento de Identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Revisión de literatura de la norma ISO/IEC 27001 en el sector de las telecomunicaciones de la ciudad de Guayaquil: Evaluación de la seguridad de las redes y sistemas informáticos, realizado por Luis Andrés Gallegos Manrique con documento de identificación N° 0950319459 y Cristhopher Daniel Lynch Escobar con documento de identificación N° 0958153082, obteniendo como resultado final el trabajo de titulación bajo la opción Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 4 de febrero del año 2024

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

## DEDICATORIA

Dedico este trabajo en primer lugar a Dios Todopoderoso por bendecirme con el conocimiento, las habilidades y la inspiración para completar este artículo académico. Sin Su guía y apoyo, esto no habría sido posible.

También me gustaría expresar mi más sincero agradecimiento a mis padres, Luis Efrén Gallegos Recalde y Ana María Manrique Ruiz, por su amor, su aliento y su apoyo constante a lo largo de mi trayectoria académica. Siempre han sido una fuente de inspiración para mí y su fe en mí me ha impulsado a alcanzar cosas aún mayores. Sin ellos, no estaría donde estoy hoy.

Luis Andrés Gallegos Manrique

Dedico este trabajo a Dios Todopoderoso por Sus bendiciones al ayudarme a completar este artículo académico. Sin Su guía, nada de esto habría sido posible; También me gustaría extender mi más sincero agradecimiento a mi madre, Esther Marisol Escobar Coraizaca, por su constante amor, aliento y apoyo inquebrantable a lo largo de mi trayectoria académica. Sus sacrificios, dedicación y creencia constante en mí han sido una enorme fuente de inspiración y motivación que me ha mantenido en pie incluso en los momentos más difíciles.

Estaré siempre agradecido a mi madre y a Dios por darme la fuerza, la perseverancia y la determinación necesarias para completar este ciclo de mi vida.

Cristhopher Daniel Lynch Escobar

## AGRADECIMIENTO

Agradecer al Ing. Joe Frand Llerena Izquierdo el cual nos brindó su ayuda en mi proceso de elaboración del articulo académico con disposición de su tiempo y sugerencias.

A mi Padre, el cual creyó y confió en mi sin dudarlo y el cual me motivo, influyo y contribuyo al inicio de mi trayectoria estudiantil, hoy en día puedo decir que alcances sus expectativas y me siento orgulloso de este logro que alcance con mi esfuerzo y dedicación.

Luis Andrés Gallegos Manrique

Agradecer al Ing. Joe Frand Llerena Izquierdo el cual nos brindó su ayuda y paciencia a lo largo del proceso de la elaboración del articulo académico.

A Mis hermanos Sebastián David Rodríguez Escobar y Mathias Eduardo López Escobar que me brindaron su apoyo en proyectos importante, me levantaron la moral en momentos que me sentía agotado y la inspiración que recibí de parte de ellos.

Cristhopher Daniel Lynch Escobar

# RESUMEN

La Norma ISO/IEC 27001 son Sistemas de seguridad de la información como medio eficaz para minimizar los riesgos de perdidas, robos, manipulación indebida de información privada. El objetivo general es desarrollar una revisión de literatura sobre el uso de la norma ISO/IEC 27001 enfocada en el sector de las empresas de telecomunicaciones en la cuidad de Guayaquil mediante el uso de bases indexadas de artículos relevantes de los últimos 5 años, se utiliza la investigación exploratoria y empírica-analítica, el uso del grafico sobre estatura lógica de SGSI (Sistema de Gestión de Seguridad de la Información) , se utiliza un enfoque cualitativo, se utiliza la técnica de encuesta a 20 profesionales de telecomunicaciones expertos en SGSI, usando el enfoque cuantitativo, los resultados están en la revisión sistemática que se obtuvo de los 40 artículos, elaborando una arquitectura lógica de 3 niveles: Táctico, estratégico, operativo y además una encuesta sobre la arquitectura a los expertos en SGSI. En forma general la encuesta habla sobre la arquitectura, conocer si los expertos están de acuerdo con las características del modelo propuesto.

**Palabras claves:** Certificación, Nomas ISO, Evaluación, Seguridad, vulnerabilidad, arquitectura

## ABSTRACT

The ISO/IEC 27001 standard is Information security systems as an effective means to minimize the risks of loss, theft, and improper manipulation of private information. The general objective is to develop a literature review on the use of the ISO/IEC 27001 standard focused on the sector of telecommunications companies in the city of Guayaquil through the use of indexed bases of relevant articles from the last 5 years. Exploratory and empirical-analytical research, the use of the graphic on logical stature of ISMS (Information Security Management System), a qualitative approach is used, the survey technique is used to 20 telecommunications professionals experts in ISMS, using The quantitative approach, the results are in the systematic review that was obtained from the 40 articles, developing a logical architecture of 3 levels: Tactical, strategic, operational and also a survey on the architecture to ISMS experts. In general, the survey talks about the architecture, knowing if the experts agree with the characteristics of the proposed model.


**Keywords:** Certification, ISO Standards, Evaluation, Security, vulnerability, architecture.

# INDICE

1. INTRODUCCION .....10
2. REVISION DE LITERATURA .....13
2.1 Estándares de Sistema de Gestión de seguridad de la Información (SGSI). .....13
2.2 Certificación técnica de la Norma ISO/IEC 27001 en el ámbito legal. .....14
2.3 Evaluaciones de sistemas de seguridad de la información con la Norma ISO/IEC 27001 ....15
3. METODOLOGIA .....16
4. RESULTADOS .....17
5. DISCUSION .....31
6. CONCLUSION .....32
REFERENCIAS .....33

# 1. INTRODUCCION

La economía de una sociedad se basa cada vez más en datos, y para garantizar la seguridad de la información dentro de las empresas, entidades u organizaciones que manejan todo tipo información relevante para ellos es recomendable establecer un sistema de gestión en la seguridad de la información o también conocida por sus siglas SGSI (Culot et al., 2021a; de la Nube Toral Sarmiento et al., 2018; Muñoz Campuzano, 2021)). La Seguridad de la information ya no es más un tema reservado para ingenieros o técnicos especializados en la materia, se ha convertido en unos de los desafíos principales gerenciales en la década actual (Ayala Carabajo et al., 2017; Miranda Jiménez, 2021; Yigit Ozkan & Spruit, 2023). Esto se ha visto en constante crecimiento y ha despertado el interés en el mundo académico con las prácticas de la norma de gestión de la seguridad de la información ISO/IEC 27001 (Ayala et al., 2016; Moncayo Ronquillo, 2021; Russo et al., 2024). Existen otras normas que También forman parte en la seguridad de la información, por ejemplo, ISO 14001, ISO 9001, OHSAS 18001, ISO 45001 son herramientas de gestión orientadas a procesos (Coello Ochoa, 2021; Escalante Quimis, 2021; Russo et al., 2024) . En la actualidad, la Norma ISO/IEC 27001 es ahora la cuarta norma ISO más adoptada en el mundo solo en año 2020 tuvo más de 45.000 empresas certificadas el cual se registra una tasa de incremento del 22%, ha sido destacada por proveedores de tecnología que acogieron la norma como: Apple Internet Services, Amazon Web Services, Microsoft, NVidia (Spencer, 2022).

La Implementación de SGSI incluye estrategias y políticas para mantener la seguridad, confidencialidad e integridad de los activos importantes de información empresarial, además el SGSI permite aumentar la efectividad en las gestiones de la información (AlBenJasim et al., 2023; Alcívar-Cruz & Llerena-Izquierdo, 2023; Carvajal Nagua & Solano Cedeño, 2021; Lindao Guevara, 2023; Vera Cuesta, 2023). Teniendo en cuenta el estándar se establecen criterios específicos, requisitos y medidas de seguridad que pueden integrarse con SGSI, que proporcionan a las empresas u organizaciones de las plataformas necesarias que sirvan para administrar información y estándares para brindar apoyo para la implementación, innovación, gestión y mejora en la empresa con el fin de que estas permiten adaptarse (Falconi Tamayo, 2021; Kheir et al., 2022; Montalvo & Morán, 2012; Reinoso Ordóñez, 2021; Robles Balaz, 2021; Salazar Guzmán, 2021; Soto Eras, 2021). Las necesidades de una empresa u organización son específicas, si bien ISO/IEC 27001 proporciona evaluaciones sobre medidas de seguridad, también proporciona recomendaciones

detalladas centrándose en medidas de seguridad técnicas y oficiales. La falta de un sistema de gestión en la seguridad de la información adecuado para sistemas de tecnologías de la información puede amenazar la capacidad de garantizar la continuidad de las empresas o entidades (Koulierakis, 2023).

La creciente popularidad de esta práctica de seguridad informática en la última década, las personas saben muy poco sobre las consecuencias de los indicadores financieros de las normas ISO/IEC 27001 para empresas que se encuentran certificadas (Lenning & Gremyr, 2022). La introducción de las Tecnologías de la información y la comunicación (TI-TT) en las empresas y entidades de telecomunicaciones crean más oportunidades de desarrollo y nuevas estrategias para la competitividad del mercado, pero el desarrollo de suministros indispensables, otorgados por las tecnologías también aumenta la vulnerabilidad en la información (Al-Karaki et al., 2022). Rutas que se transfieren, archivan, restauran, esto se refiere a los medios tecnológicos que las empresas deben implementar proyectos de gestión en seguridad donde se aprendan, analizar y reducir el riesgo de información para determinar las medidas de protección apropiadas (Olkiewicz et al., 2023). Según informes de cisco (cisco, 2016), las pymes usan poco mecanismo de protección que las grandes empresas que son el 39%, en comparación con el 52% que está conformado por las compañías más grandes, donde se refleja el control de sus debilidades en los mecanismos de seguridad en la información (Sánchez-García et al., 2023).

Este enfoque es particularmente adecuado a los desafíos que presenta esta era digital. En un entorno que cambia rápidamente, (Abdullayeva, 2023). Al implementar la serie de norma ISO/IEC en este caso 27001 garantiza que una empresa de telecomunicaciones tenga un SGSI apropiado, las empresas deben utilizar estándares de seguridad de la información con el objetivo de tener los controles de seguridad adecuados (Bounagui et al., 2019).

Las empresas deben evidenciar su compromiso para garantizar las operaciones comerciales aplicando los principios de confiabilidad, esto es importante teniendo en cuenta que la información que se protege es de clientes empresariales y natural pueden exigir pruebas de que sus datos y bases de información están protegidos, por ende, se debe evidenciar las medidas de protección adecuadas (Meriah & Rabai, 2019). La aplicación de estándares de seguridad de la información principalmente con fines de gestión

empresarial y de mercado. Hoy en día, estos estándares se consideran herramientas esenciales e influyen en medio del incremento de amenazas de delitos cibernéticos, piratería informática, ataques de recursos de los gobiernos y recursos valiosos de entidades privadas (Gaitero et al., 2021). Proteger activos de información de entidades es fundamental, espacialmente orientada a empresas privadas, para minimizar el impacto de los incidentes de seguridad y garantizar la vigencia en los negocios (Azinheira et al., 2023).

La literatura sobre ISO/IEC 27001 enfatiza el contraste que ha tenido con relación a la mejora de los sistemas de información y si tiene una mayor eficiencia en los procesos, las políticas de seguridad informáticas son medidas donde se ocupan empresas para proteger sus datos. Por lo tanto, cuando la empresa requiere certificación, requiere obtener la documentación con el propósito de controlar lo que sucede en la Gestión de seguridad de la información, por esa razón debe tener en cuentas a detalle las cláusulas de las normas ISO/IEC 27001 (Shojaeshafiei et al., 2020)

El presente proyecto puede brindar fundamentos en los procesos planteados en la norma ISO 27001, que ayudará a la identificación del nivel de seguridad en las empresas de telecomunicaciones de la cuidad de Guayaquil y contribuir a la toma de decisiones relacionadas a inversiones de seguridad informática que permita asumir cambios regulatorios todo esto siendo necesario que las empresas regularicen, estandaricen los controles de seguridad para minimizar los riegos.

El objetivo general es evaluar la implementación de la norma ISO/IEC 27001 en el sector de las Telecomunicaciones de la cuidad de Guayaquil, centrándose en la seguridad de las redes y sistemas informáticos

Los objetivos específicos son:

- Categorizar los sistemas de gestión de la seguridad en el sector de las Telecomunicaciones de la ciudad de Guayaquil, mediante la revisión de la literatura científica relevante.
- Clasificar las técnicas y buenas prácticas más eficaces utilizadas en el sector de las telecomunicaciones de Guayaquil que implementen la norma ISO/IEC 27001 mediante el uso de una table de control.
- Identificar los requisitos que las empresas de telecomunicaciones deben cumplir para obtener la certificación ISO/IEC 27001 en la gestión de seguridad y

protección a la información, contrastando los resultados de la revisión bibliográfica.

El documento está estructurado de la siguiente forma, el primer capítulo describe la introducción y objetivos de la investigación, el segundo capítulo describe los conceptos de la evaluación en sistemas de seguridad de la información basado en la norma ISO/IEC 27001, el capítulo tercer describe la metodología utilizada para obtener los resultados, el capítulo cuatro describe los resultados que tienen relación con el objetivo de la investigación, el capítulo cinco se describe las discusiones y finalmente las conclusiones.

## 2. REVISION DE LITERATURA

### 2.1 Estándares de Sistema de Gestión de seguridad de la Información (SGSI).

Se pueden considerar que las normas son un repositorio de mejores prácticas basadas en conocimientos expertos en un campo particular que incluyen un conjunto de requisitos de un producto o sistema que debe brindar una solución a problemas que se presentan de manera recurrente (Antunes et al., 2022). En el campo de la seguridad de la información, existen algunos estándares recomendados que las organizaciones pueden adoptar para garantizar la seguridad de sus activos de información (Razikin & Soewito, 2022). Esto representa una base para lograr CIP (Confidencialidad, Integridad y Disponibilidad) de la información que tienen las empresas u organizaciones, el cual es el objetivo fundamental de la seguridad de la información (Syreyshchikova et al., 2019).

En la última versión internacional de la norma se publicó en el 2013 tuvo sus cambios significativos como la adaptación de una estructura a otras normas como ISO/IEC 9001, 14001, los requisitos y procedimientos deben ser registrados y documentados los cuales pueden ser reemplazados por información que se encuentre documentada y cumpla con los requisitos que ya han sido revisados o eliminados (Tout et al., 2023). En la familia de la Norma ISO/IEC 27000 se centra en la gestión de riesgos que tiene un aproximado de 114 medidas de seguridad. La Norma ISO/IEC 27001 específica los requisitos que debe cumplir un SGSI para poder ser certificado que se clasifica con 7 elementos claves: configuración, implementación, análisis, operación, mantenimiento en los sistemas y mejoras del mismo. Este estándar está diseñado para poder usarse junto con la Norma ISO/IEC 27002, aunque este estándar ofrece una serie de medidas de seguridad en la información, donde las empresas son libre de implementar otras medidas eficientes

siempre que cumplan con ISO/IEC 27001 (Angelo Edu et al., 2023), (Dax & Kunnemann, 2021).

La legitimidad en los procesos del sistema de protección de datos se basa en el concepto de eficiencia en los resultados esperados por parte de la empresa, teniendo en cuenta que este valor sea el resultado se encuentre relacionado en las partes interesadas (Putra et al., 2021).

2.2 Certificación técnica de la Norma ISO/IEC 27001 en el ámbito legal.

Para (Culot et al., 2021b), la certificación tiene un alcance enorme ya que no es solo un concepto técnico o legal, esto los lleva a explorar la naturaleza de mecanismos que los lleva comprender de mejor manera las oportunidades potenciales que ofrecen.

El tener un predominio de las normas de una manera técnicas se comenzará a pasar concepto netamente técnico a una regulación normativa, puede tener un impacto significativo tanto en su nombre como en su efecto legal posteriormente, tanto que ahora esos mecanismos se vinculan a las normas jurídicas y técnicas reales (Monev, 2020). Dado que muchas organizaciones operan con grandes cantidades de datos personales, a menudo sin que los clientes, usuarios tengan en cuenta como utilizan posteriormente estos datos, se recomienda que dichos certificados proporcionen una mayor transparencia en los datos internos que manejan las empresas (Lopez-Leyva et al., 2020).Este tipo de certificación comenzó a impulsarse para optar mayor transferencia al funcionamiento en las empresas, ya que muchas de estas entidades procesas grandes cantidades de datos de los clientes, como los estándares que forman parte de la serie ISO/IEC 27001 busca aumentar la confianza de los usuarios en el comercio digital o electrónico (Santos & Amon, 2023).Al ser una norma certificada describe requisitos técnicos, necesarios para reducir riegos de incumplimiento del RGPD, las organizaciones al tener una certificación les permite orientar y determinar cómo realizar las respectivas evaluaciones y protección de datos (DPIA) dentro de su entidad (Barraza de la Paz et al., 2023). En la práctica dentro de las organizaciones realizan un informe detallado de las medidas tomadas para abordar los riesgos, un ejemplo general seria las actividades y novedades que presentan cuando hacen uso del sistema para gestionar la seguridad de la información en la empresa (Mayayise, 2021).

## 2.3 Evaluaciones de sistemas de seguridad de la información con la Norma ISO/IEC 27001

La información se considera datos muy importantes de una organización, por ende, se debe resguardar esa gran cantidad de información que poseen las empresas contra las vulnerabilidades y amenazas que ocurren en las empresas (Diamantopoulou et al., 2020). La información que tienen las empresas sobre sus clientes no es solamente un producto también es un recurso que debe organizarse y gestionarse, teniendo en cuenta este detalle la información se divide en 2 categorías: activos de información primaria y activos como información de soporte (Mirtsch, Kinne, et al., 2021). Estos activos de información primaria son relacionados en procesos centrales (Suorsa & Helo, 2023). Y los activos de información de soporte son relacionados a toda la información que es propiedad de la empresa (Suorsa & Helo, 2023).

También cabe mencionar que la NORMA ISO/IEC 29134, Brinda una orientación relevante sobre como iniciar una evaluación basada en la protección de datos y la estructura en la elaboración de un informe asociado a las operaciones y procesos cumplan efectivamente con los requisitos de la evaluación desde este estándar (Kamil et al., 2023).

La adopción de estándares requiere la participación de muchas partes interesadas en los diferentes procesos, comenzando desde la alta dirección hasta los empleados. También dar a conocer los altos resultados como medida de eficacia y capacidad de resolver o solucionar un problema de la norma (Wu et al., 1 C.E.). es decir que la difusión de estándares de seguridad la vuelve necesaria para crear un sistema sostenible de estandarización porque ayuda a contribuir y garantizar la legitimidad de los resultados (Culot et al., 2021c).

Dado la validez y de los resultados obtenidos, en este contexto las evaluaciones son relevantes al contenido descrito en documentos donde se realizan las observaciones como los cambios realizados y la influencia en el comportamiento de los participantes relacionados con la Norma ISO/IEC 27001 (Sengupta et al., 2019), (Podrecca et al., 2022).

## 3. METODOLOGIA

Para “Revisar artículos científicos sobre las Normas ISO/IEC 27001 en el sector de las telecomunicaciones” se utiliza el método PRISMA que permite seleccionar y filtrar artículos científicos de las bibliotecas virtuales de Scopus, Web of Science, IEEE Xplore. Donde se utilizaron filtros con criterio inclusión y exclusión. Criterios de inclusión: artículos desde al año 2019 hasta el presente, con relación a la Norma ISO/IEC 27001 en el sector de las telecomunicaciones artículos en el idioma del inglés. Criterios de exclusión: artículos de resumen o libros y con idioma diferente al inglés y que son de pago. Se usa la investigación exploratoria para evaluar la seguridad de los sistemas informáticos en el sector de telecomunicaciones, además de la revisión de la literatura se ejecutan 3 etapas principales: planificación, análisis de los datos obtenidos, elaboración del informe.

### Fase 1: Planificación

A. Identificación de necesidad de investigación

Identificar las amenazas y riesgos, conocer si las empresas de telecomunicaciones están preparadas frente a un posible ataque ocurra en cualquier momento, conocer cuáles son sus políticas de seguridad donde se garantice la integridad confiabilidad y disponibilidad de la información y con sus recursos

B. Identificar preguntas de investigación

P1. ¿Qué categorías se utilizan para conseguir la certificación de la Norma ISO/IEC 27001?

P2. ¿Cuáles son los protocolos más comunas aplicadas en las telecomunicaciones con la Norma ISO/IEC 27001?

P3. ¿Cuáles son las características comunes de seguridad que requieren según ISO/IEC 27001 para la gestión de riesgos de seguridad de la información?

P4. ¿Como puede asegurarse la continuidad del negocio en el caso de las telecomunicaciones ocurra una violación a la seguridad de la información?

P5. ¿Cuáles son las tecnologías emergentes que plantean nuevos desafíos de seguridad en la información a las entidades de telecomunicaciones?

Para evaluar la estructura que miden la norma se seguridad informática, se utiliza la encuesta en al menos 20 TI en empresas de telecomunicaciones, se realiza una encuesta de 11 preguntas relacionadas a la estructura de la seguridad informática en el sector de las telecomunicaciones en Guayaquil. Las preguntas son cerradas, y se procede con el enfoque cualitativo y realizar un diseño a detalle.

## 4. RESULTADOS

**Fase 2: Análisis de los datos**

### 4.1 Revisión de literatura

La selección de los artículos relevantes y la cantidad de artículos seleccionados inicialmente con los criterios de inclusión - exclusión que se encuentran en la tabla 1 se aplica en los artículos.

*Tabla 1. Criterios de inclusión y exclusión*

| Inclusión | Exclusión |
|---|---|
| Idioma inglés | No escritos en idioma ingles |
| Artículo principales | Artículos secundarios y resumidos |
| Artículos entre 2019 y 2023 | Artículos antes del 2019 |
| Tema sobre ISO 27001 en telecomunicaciones | No incluye las telecomunicaciones |

Fuente: Realizado por autores.

La revisión de la literatura de los artículos se inició con una cantidad de 100 y en la primera exclusión se sacaron los duplicados por otras razones se eliminan 20 artículos, se excluyeron 15 artículos por los temas y la rápida lectura de resumen. No se pudieron bajar 15 artículos por tener derechos exclusivos hacia otras universidades, se descartaron 10 artículos por ser artículos secundarios, de paga, resúmenes y que están fuera de alcance sobre el tema.

Finalmente se obtuvieron los 40 artículos para su lectura y análisis, ver figura 2.

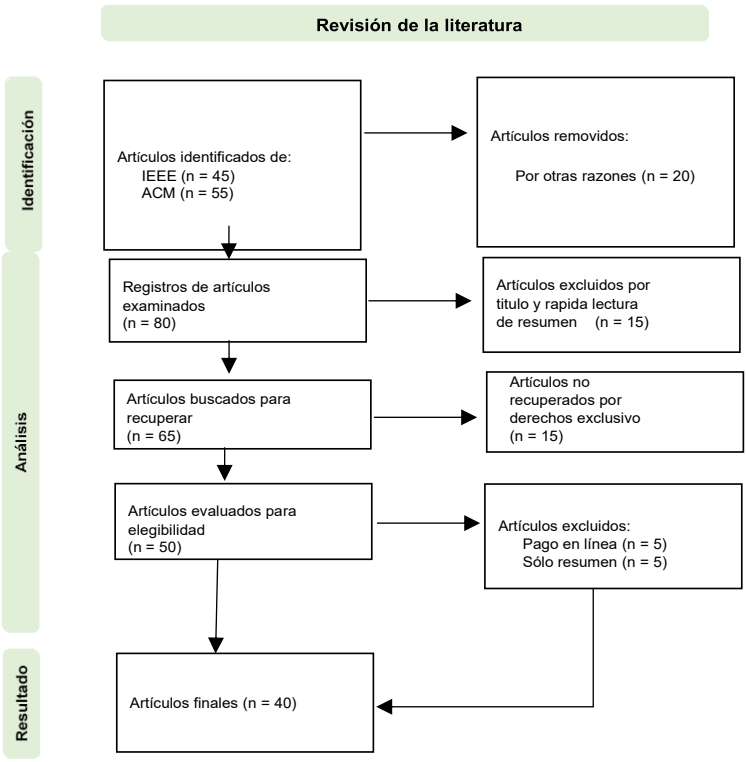



*Figura 2. Selección de artículos modelo de PRISMA.*

## Fase 3: Elaboración del informe

La tabla 2 muestra los 40 artículos agrupados en varias aristas con sus características que contestan las preguntas de investigación que son: la implementación de las normas, certificación de la norma, protocolos de seguridad, tecnologías a utilizar, para especificar la dimensión del método: Se presentan los artículos seleccionados de acuerdo con la metodología utilizada en esta investigación.

*Tabla 2. Artículos seleccionados.*

| Año | Artículos |
|---|---|
| 2019 | (Bounagui et al., 2019); (Meriah & Rabai, 2019); (Sengupta et al., 2019); (Syreyshchikova et al., 2019) |
| 2020 | (Diamantopoulou et al., 2020); (Lopez-Leyva et al., 2020); (Monev, 2020); (Shojaeshafiei et al., 2020) |
| 2021 | (Culot et al., 2021ª), (2021b), (2021c); (Dax & Kunnemann, 2021); (Gaitero et al., 2021); (Mayayise, 2021; (Mirtsch, Blind, et al., 2021); (Mirtsch, Kinne, et al., 2021); (Putra et al., 2021) |
| 2022 | (Al-Karaki et al., 2022); (Antunes et al., 2022); (Kheir et al., 2022); (Lenning & Gremyr, 2022); (Podrecca et al., 2022); (Razikin & Soewito, 2022); (Spencer, 2022; Wu et al., 1 C.E.) |
| 2023 | (Abdullayeva, 2023); (AlBenJasim et al., 2023); (Angelo Edu et al., 2023); (Azinheira et al., 2023); (Barraza de la Paz et al., 2023); (Kamil et al., 2023); (Koulierakis, 2023); (Olkiewicz et al., 2023); (Sánchez-García et al., 2023); (Santos & Amon, 2023); (Suorsa & Helo, 2023); (Tout et al., 2023); (Yigit Ozkan & Spruit, 2023) |

| | |
|---|---|
| 2024 | (Russo et al., 2024) |

De acuerdo a esta tabulación se responden a las siguientes preguntas de investigación:
P1. ¿Qué categorías se utilizan para conseguir la certificación de la Norma ISO/IEC 27001?

Entre los 40 artículos seleccionados, el 60% del total utiliza procesos de evaluación de riegos, el 40% utiliza los procesos de tratamiento de riesgos. Esto significa que las empresas de telecomunicaciones tienden a utilizar los procesos de evaluación de riesgos para obtener la certificación, ver figura 3.

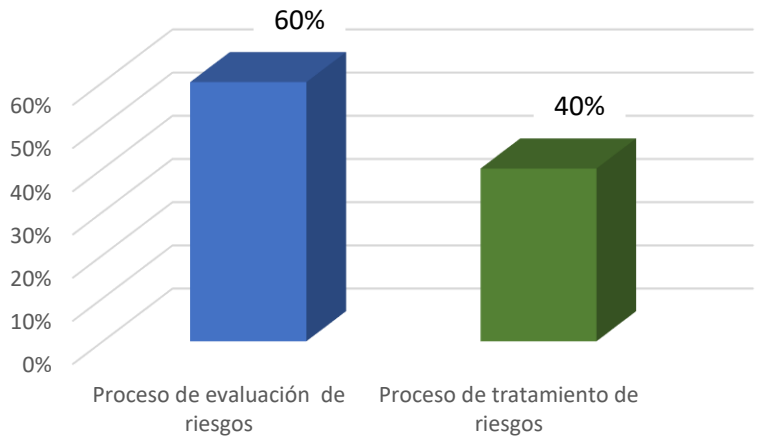



*Figura 3. Tipos de categoría para obtener la certificación*

P2. ¿Cuáles son los protocolos más comunas aplicadas en las telecomunicaciones con la Norma ISO/IEC 27001?

Los protocolos encontrados en los 40 artículos están distribuidos de la siguiente manera: 60% en controles de la entidad, 25% controles enfocados a los clientes, 10% controles físicos, 5% controles tecnológicos. Esto significa que los estándares de los artículos tienen una buena definición para su entendimiento, ver figura 4.

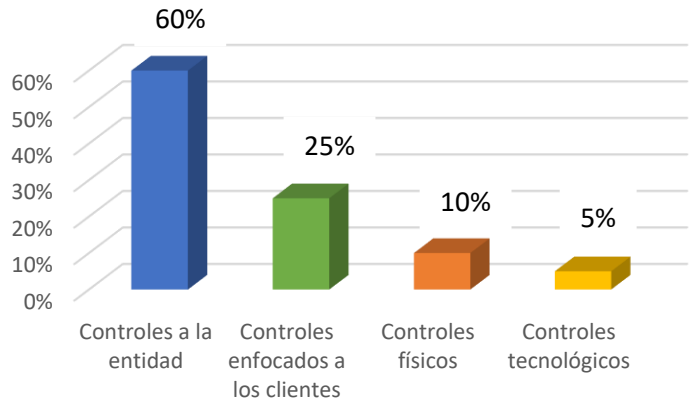



*Figura 4. Protocolos utilizados en telecomunicaciones*

P3. ¿Cuáles son las características comunes de seguridad que requieren según la Norma ISO/IEC 27001 para la gestión de riesgos de seguridad de la información?

Las características encontradas en los 40 artículos, 26% a la gestión de políticas de seguridad, 18% en el personal responsable del sistema, 26% a una planificación operativa, y el 30% en la elaboración de la documentación al realizar una gestión de riesgo de seguridad. Esto significa que la estructura de los artículos está bien definida, ver figura 5.

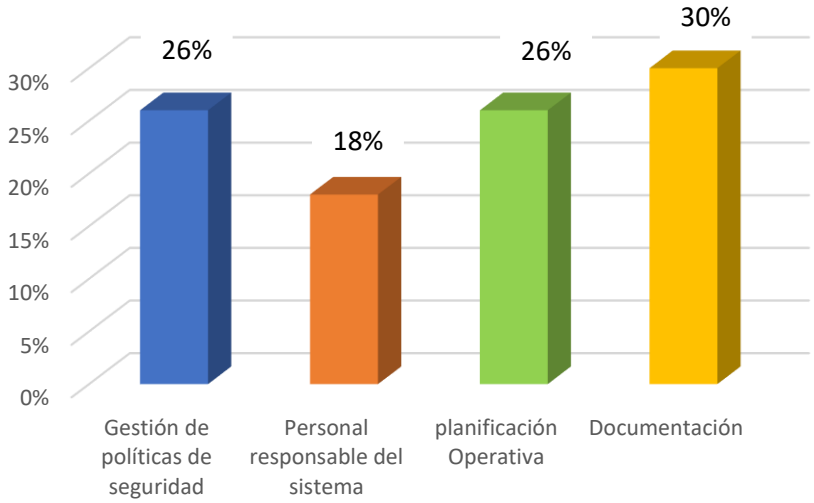



*Figura 5. Características comunes de seguridad encontradas.*

P4. ¿Como puede asegurarse la continuidad del negocio en el caso de las telecomunicaciones ocurra una violación a la seguridad de la información?

Entre los 40 artículos seleccionados, el 24% implementa copias de seguridad, el 18% cuenta con un plan de repuestas a incidentes, el 28% realiza evaluaciones regulares, el 30% establece políticas de seguridad, esto significa que para las empresas de

telecomunicaciones actúan mayormente utilizando todos estos protocolos como plan de contingencia frente a un ataque a la entidad, ver figura 6.

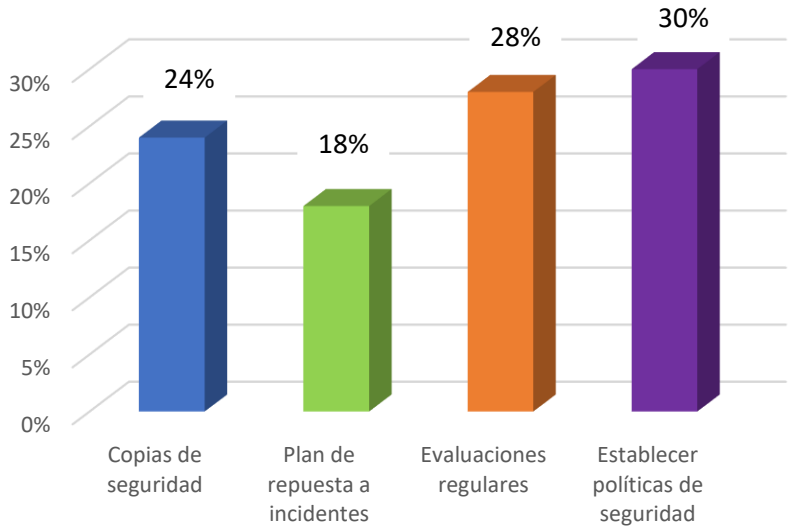



*Figura 6. plan de seguridad frente a un ataque de seguridad*

P5. ¿Cuáles son las tecnologías emergentes que plantean nuevos desafíos de seguridad en la información a las entidades de telecomunicaciones?

En los 40 artículos seleccionado, 15% presenta un bajo desafío con la tecnología 5G, el 25% un desafío medianamente bajo con las tecnologías IoT, y con un 60% computación en la nube con un desafío alto, debido a que tiende a sufrir ataques de hacking con más frecuencia, ver figura 7.

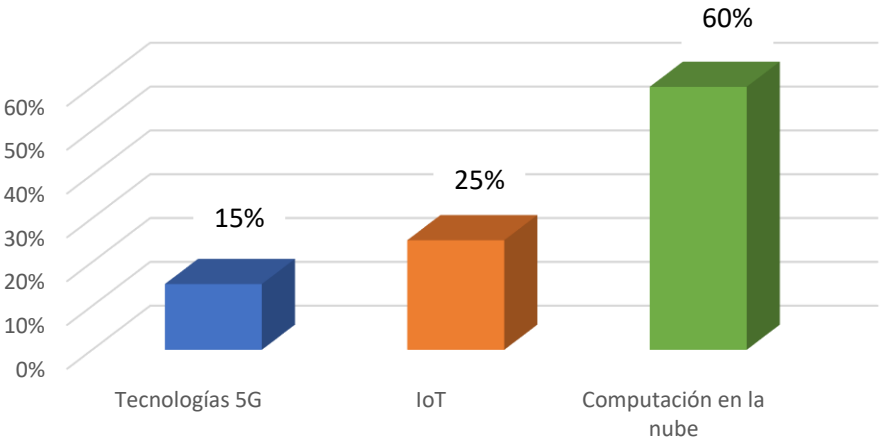



*Figura 7. Tecnologías emergentes que presentan un riesgo de seguridad.*

4.2 Diseño de Estructura Lógica del Sistema de Gestión de seguridad de la información.

La información es considerada un activo importante en las empresas por esta razón de debe proteger de las innumerables amenazas, presentando este modelo piramidal donde se describe los niveles y componentes de seguridad en las empresas. Donde la política de seguridad tiene aspectos operativos y técnicos. La imagen tiene un diagrama piramidal divido en tres niveles. En primer nivel llamado "Táctico", se encuentran: políticas de seguridad, aspectos organizativos para la seguridad. En el segundo nivel llamado" Estratégico", incluye: clasificación y control de activos, control de accesos, conformidad, seguridad física orientada al entorno, seguridad del personal. En el tercer y último nivel llamado "Operativo" se encuentran: Desarrollo y mantenimientos de sistemas, gestión de continuidad del negocio, gestión de comunicaciones, en cada bloque contiene elementos específicos que están relacionada a su categoría donde se proporciona una estructura detallada sobre como implementar la gestión de seguridad en las empresas de telecomunicaciones.

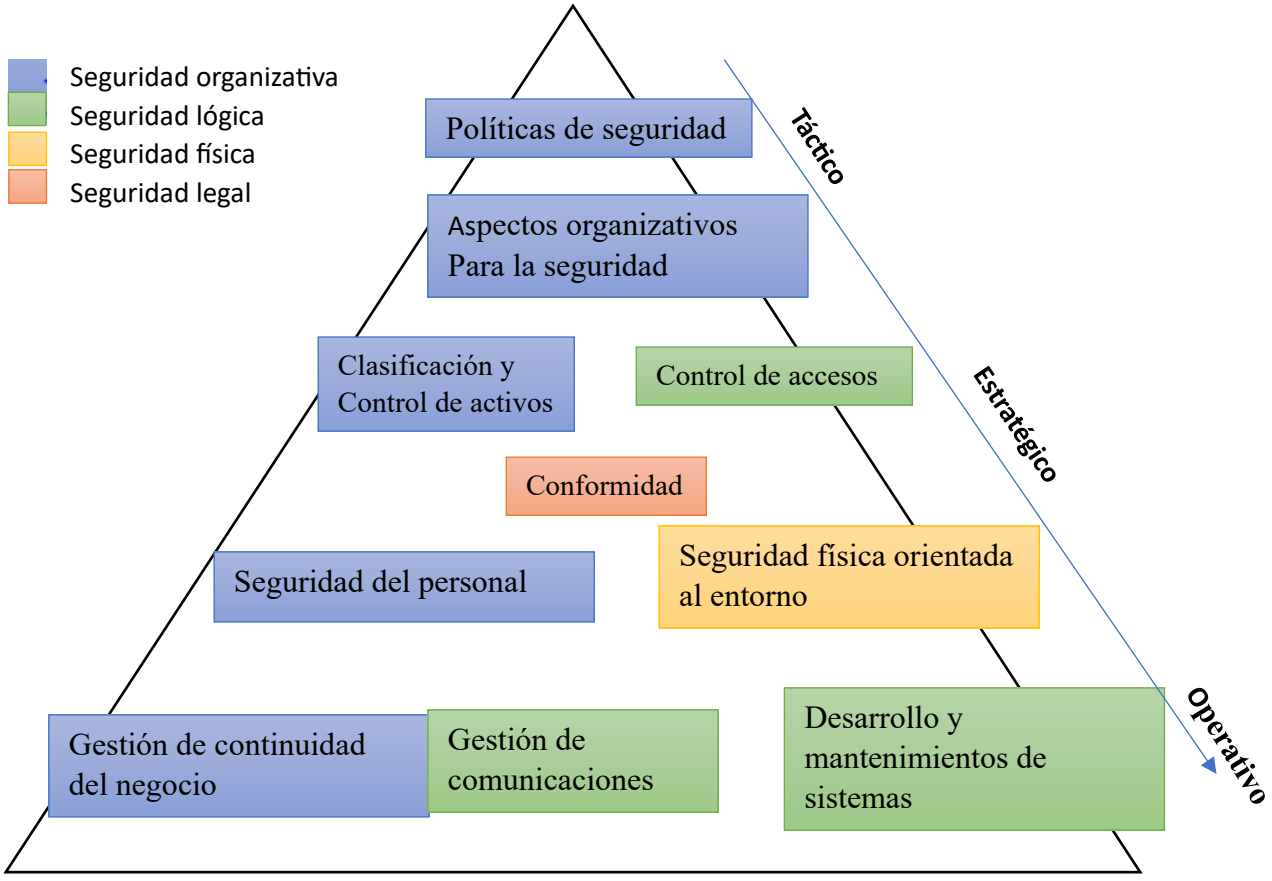



*Figura 8. Estructura de Gestión de seguridad de la información.*

Cada nivel que se propone en la arquitectura está basado en los 40 artículos científicos seleccionados en la revisión de la literatura, se adoptaron elementos que se ajustan a la estructura que se proponen en este documento

**Nivel Táctico:** Se enfoca en la política de seguridad de la empresa y en gestión de los riesgos de seguridad. La sección de política de seguridad: se basa en establecer requisitos de seguridad de la empresa para asegurar la confidencialidad, integridad y disponibilidad de los activos de información, tener el control de seguridad para resguardar los activos y garantizar que las estrategias del negocio se cumplan. La sección Aspectos organizativos para la seguridad: se basa en definir, priorizar, evaluar los proyectos que tengan que ver con los riegos o iniciativas de seguridad en sectores definidos, en este contexto lo que se busca es mantener una estructura de políticas, estándares, normas y certificaciones en la empresa.

**Nivel estratégico:** Está enfocado en planificación y definición de los objetivos de seguridad en la información. La sección clasificación y control de activos: identifica los activos de información crítica y establece un marco de clasificación y control de acceso para protegerlos, donde se establecen los requisitos de seguridad para la información y definir los controles para protegerlos. La sección control de accesos. Establece controles para garantizar que los usuarios tengan accesos a los recursos e información solo si tienen los permisos necesarios, es decir, se establecen los requisitos de autenticación y autorización para los usuarios. La sección conformidad: garantiza que la empresa cumpla con las leyes y regulaciones aplicables a la seguridad, es decir se definen los controles necesarios para que la organización cumpla con las leyes y regulaciones aplicables. La sección seguridad del personal: se enfoca que el personal encargado de esta área este capacitado y consciente de los riesgos de seguridad que pueden llegar a presentarse. La sección seguridad física orientada al entorno: establece los controles necesarios para proteger los recursos físicos de la empresa.

**Nivel Operativo:** Se basada en la ejecución de los planes y estrategias de seguridad en la empresa. La sección gestión de continuidad del negocio: garantiza que la organización pueda continuar operando en caso de interrupciones o desastres, es decir que establecen procedimientos necesarios para que empresa pueda recuperarse de cualquier interrupción. La sección gestión de comunicaciones: garantiza que la empresa tenga una comunicación

efectiva y segura. La sección de desarrollo y mantenimiento de sistemas: garantiza que los sistemas de la empresa sean seguros y estén actualizados.

4.3 Evaluación de la Estructura lógica del Sistema de Gestión de Seguridad de la Información.

En esta fase se realiza una encuesta a profesionales de SGSI que trabajan en empresas de telecomunicaciones en la cuidad de Guayaquil, la encuesta contiene once preguntas acerca de la estructura lógica que se propone en esta investigación, se realiza de forma remota y se realiza en Google form para sea llenada por los entrevistados.

La encuesta fue contestada por 20 profesionales de Sistema de Gestión de Seguridad de la Información, donde todos son ingenieros en el área de sistemas y afines, con experiencias en sistemas de seguridad o ciberseguridad, de este grupo el 85% son hombres y el 15% son mujeres, las preguntas tienen un enfoque de que el encuestado considera que:

1. La política de seguridad se comunica a todos los empleados.
2. Poseen programa de capacitación y concientización en seguridad.
3. Poseen programa de monitoreo y auditoria de los activos de información críticos.
4. Poseen marco autentificación y autorización para los usuarios.
5. Cumplimiento de leyes y regulaciones aplicables a la seguridad.
6. Cumplimiento de leyes y regulaciones de la Norma ISO/IEC27001.
7. Capacitación en seguridad orientado al personal.
8. Marco de políticas, normas y estándares de seguridad física de los equipos.
9. Pruebas de plan de continuidad del negocio.
10. Programa de capacitación en las comunicaciones seguras.
11. Capacitación en seguridad para el desarrollo y mantenimiento de sistemas

A continuación, se presenta los gráficos estadísticos del tipo de barras para expresar la respuesta de cada pregunta.

4.3.1 La política de seguridad se comunica a todos los empleados.

El 45% considera que siempre se comunican las políticas de seguridad a los empleados, el 40% considera que se comunica con frecuencia y el 15% a veces a esta propuesta, es

decir que las empresas de telecomunicaciones en Guayaquil si cumplen con esta propuesta, ver figura 9.

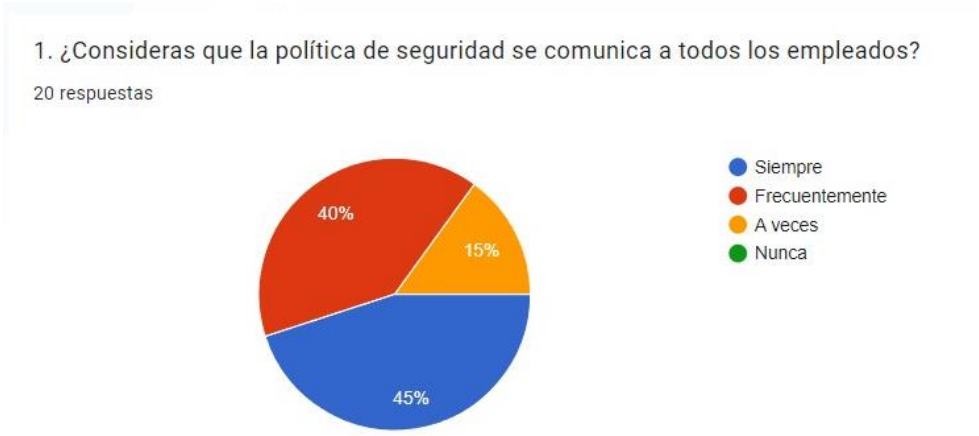



*Figura 9. Política de seguridad*

4.3.2 Poseen programa de capacitación y concientización en seguridad.

El 80% afirman que, si tienen programa de capacitación y concientización en seguridad, no obstante, el 20% niega que tienen o reciben un programa de capacitación, es decir que la mayoría de las empresas de telecomunicaciones en Guayaquil tiene un programa de capacitación, mientras que una pequeña parte de encuestado no están seguros, figura 10.

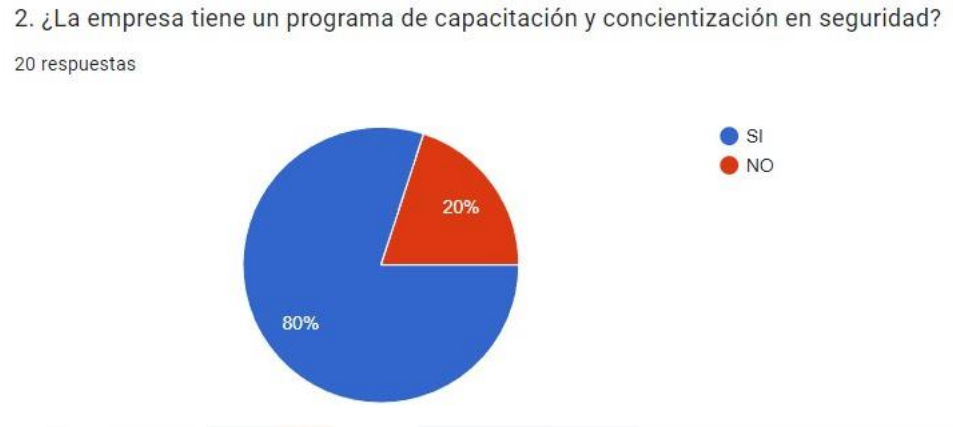



*Figura 10. Programa de capacitación en seguridad*

4.3.3 Poseen programa de monitoreo y auditoria de los activos de información críticos.

El 90% afirman que, si tienen programa de monitoreo y auditoria de los activos de información crítica que, no obstante, el 10% niegan que tienen un programa de monitoreo y auditoria sobre los activos de información, ver figura 11.


*Figura 11. Programa de monitoreo y auditoria*

4.3.4 Poseen marco autentificación y autorización para los usuarios.

El 95% afirman que las empresas si posee un marco de autentificación y autorización a los usuarios, no obstante, un 5% niega que existe un marco de autentificación, ver figura 12.


*Figura 12. Marco de autentificación y autorización.*

4.3.5 Cumplimiento de leyes y regulaciones aplicables a la seguridad.

El 45% considera que siempre cumplen con las leyes y regulaciones aplicada a la seguridad, el 35% que, si cumplen con frecuencia, y un 20% a veces lo hacen, es decir que todos los entrevistados consideran que, las empresas si están cumpliendo con las leyes, ver figura 13.

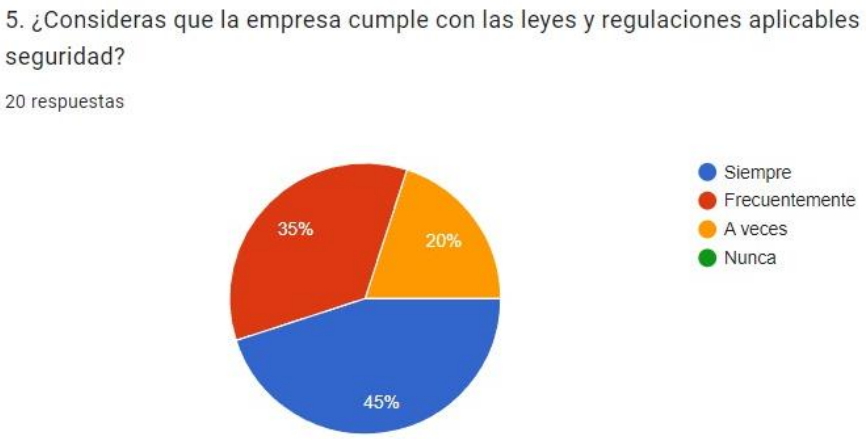



*Figura 13. Leyes y regulaciones aplicadas a la seguridad.*

4.3.6 Cumplimiento de leyes y regulaciones de la Norma ISO/IEC27001.

El 60% considera que, si cumplen con la leyes y regulaciones de las normas ISO/IEC 27001, el 25% considera que lo hacen con frecuencia debido a que deben cumplir con otras normas ISO y no solamente esta, el 15% también está de acuerdo que muchas veces les dan prioridad a otras normas ISO, es decir que los entrevistados están de acuerdo que las empresas si cumplen la Norma ISO/IEC 27001, ver figura 14.


*Figura 14. Leyes y regulaciones de la norma ISO/IEC 27001*

4.3.7 Capacitación en seguridad orientado al personal.

El 50% considera que frecuentemente reciben capacitación y concientización de seguridad orientado al personal, el 30% considera siempre en todo momento los capacitan, mientras el 20% no recibe con frecuencia capacitación sobre este tema presentado, es decir que las empresas de telecomunicaciones en Guayaquil poseen una reputación positiva en cuanto a esta capacitación, ver figura 15.


*Figura 15. Capacitación de seguridad orientado al personal*

4.3.8 Marco de políticas, normas y estándares de seguridad física de los equipos.

El 55% considera que la empresa tiene un buen manejo en el marco de la seguridad física de los equipos, el 35% considera que tienen un muy buen manejo de este marco, mientras que un 10% considera que la empresa carece de un buen marco de seguridad a los equipos de la empresa, es decir en que Guayaquil las empresas de telecomunicación manejan un buen marco de políticas, normas y estándares de seguridad física de los equipos, ver figura 16.

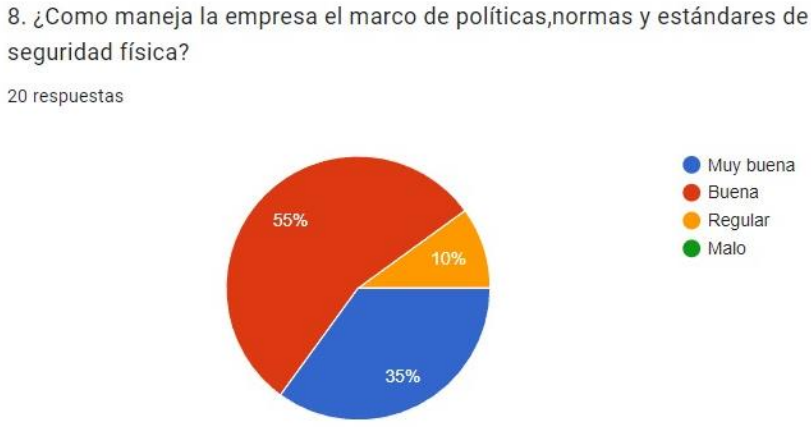



*Figura 16. Marco de políticas, normas y estándares de seguridad física*

4.3.9 Pruebas de plan de continuidad del negocio.

El 40% afirman que, si realizan pruebas del plan de continuidad del negocio con frecuencia, el 35% afirman que en todo momento siempre realizan dichas pruebas, el 25% afirman que solo pocas veces lo realizan solo cuando es necesario, esto quiere decir que en Guayaquil las empresas de telecomunicaciones una gran parte de ellas consideran necesario realizar estas pruebas y que están preparada ante una situación grave, ver figura 17.

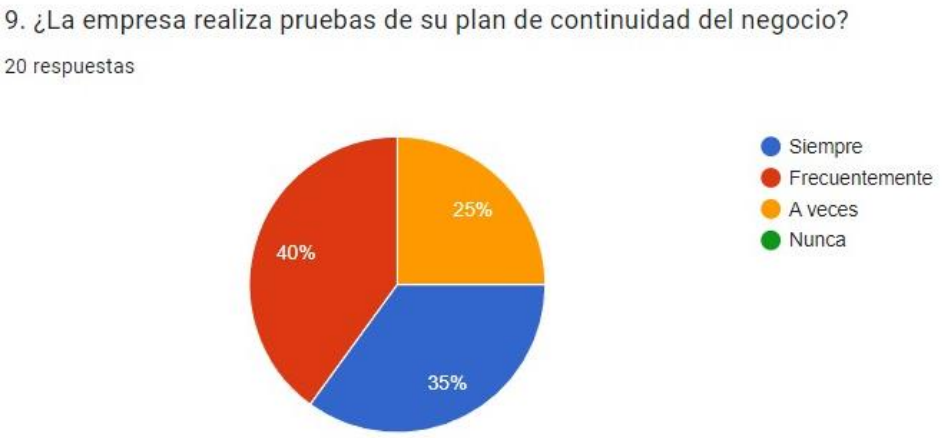



*Figura 17. Pruebas del plan de continuidad del negocio*

4.3.10 Programa de capacitación en las comunicaciones seguras.

El 35% considera que la empresa maneja un muy buen programa de capacitación en las comunicaciones seguras, el otro 35 % también que la empresa tiene un buen manejo de esta capacitación, el 30% asegura que la capacitación de este tema es regular, es decir que las empresas de telecomunicaciones de Guayaquil poseen una reputación positiva en cuanto a la capacitación, ver figura 18.


*Figura 18. Programa de capacitación en comunicaciones seguras*

4.3.11 Capacitación en seguridad para el desarrollo y mantenimiento de sistemas

El 40% considera que la empresa maneja una muy buena capacitación en seguridad y mantenimiento de los sistemas, el otro 40 % también que la empresa tiene un buen manejo de esta capacitación, el 20% asegura que la capacitación de este tema es regular, es decir que las empresas de telecomunicaciones de Guayaquil poseen una reputación positiva en cuanto a la capacitación, ver figura 19.


*Figura 19. Capacitación de seguridad para el desarrollo y mantenimiento de sistemas*

## 5. DISCUSION

En la revisión sistemática se obtuvo 40 artículos seleccionados, el 85% del total se deben implementar protocolos de seguridad SGSI para obtener la certificación basada en la NORMA ISO/IEC 27001 conocida como un estándar internacional con el objetivo de evaluar la seguridad de las tecnologías de la información, el 75% conocer cómo se realiza un análisis exhaustivo sobre la implementación y evaluación de la normas en las redes de telecomunicaciones y sistemas informáticos, el 70% del total solo presento modelos teóricos.

En la encuesta a los 20 expertos en SGSI que trabajan en diferentes empresas de telecomunicaciones, un 80 % están de acuerdo con las diferentes capacitaciones que reciben de reciben referente al tema de la seguridad y sistema de gestión de seguridad que maneja la empresa a la que trabajan, un 85% están de acuerdo que la empresa cumpla con las leyes y regulaciones basada en Normas ISO, el 100% está de acuerdo que las empresas tengan un plan de continuidad del negocio ante un ataque a la entidad lo que da a entender que las empresas están preparadas ante un ataque de gran magnitud.

En esta investigación se trata sobre la evaluación en la seguridad de la información y su calificación por parte de los expertos en SGSI, hacia la arquitectura planteada.

# 6. CONCLUSION

Del total de 40 artículos que fueron seleccionados y analizados para responder las preguntas de investigación se realizó un análisis de datos encontrados como las evaluaciones y protocolos que realizan mediante la Norma ISO/IEC 27001 en los Sistema de Gestión de seguridad de la Información.

Basados en la lectura de los artículos científicos se adoptó elementos para diseñar una arquitectura lógica formada con 3 niveles: Táctica, estratégico y operativo; se utilizaron algunas características de las estructuras presentadas en los 40 artículos que fueron seleccionados, que se ajustan a las evaluaciones que realizan las empresas de telecomunicaciones de Guayaquil.

La encuesta realizada a los 20 expertos en SGSI sirve como validación del trabajo realizado y confirma que están de acuerdo a las características que tiene la arquitectura lógica planteada en la investigación, produce una reducción de riesgos de ataques, mantenimiento, seguridad e integridad de la información que manejan en este tipo de organización.

# REFERENCIAS


Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, *12*, 100268. https://doi.org/10.1016/J.RICO.2023.100268

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2023.2251455

Alcívar-Cruz, B., & Llerena-Izquierdo, J. (2023). After-Sales and Customer Loyalty Strategies for Fixed Internet Through the Implementation of Virtual Assistance in the Ecuadorian Context. In V. Robles-Bykbaev, J. Mula, & G. Reynoso-Meza (Eds.), *Intelligent Technologies: Design and Applications for Society* (pp. 139–149). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-24327-1_12

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 3079–3095. https://doi.org/10.1016/J.JKSUCI.2020.09.011

Angelo Edu, M. L., Alexis, G. P., & Lenis, W. P. (2023). Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls. *Iberian Conference on Information Systems and Technologies, CISTI*, *2023-June*. https://doi.org/10.23919/CISTI58278.2023.10211874

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing. *Procedia Computer Science*, *196*, 36–43. https://doi.org/10.1016/J.PROCS.2021.11.070

Ayala Carabajo, R., Llerena Izquierdo, J., Pérez Gosende, P. A., Carrera Jiménez, J. A., Freire Morán, J. F., Morales Navas, M. E., Parra, P., Martillo, D., Romero Romero, B. R., Vega Ureta, N., & others. (2017). *Tercer Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad*.

Ayala, R., Llerena, J., Parra, P., Vega Ureta, N., Hernández, A., Romero, I., & Cueva, J. (2016). *Segundo Congreso Salesiano de Ciencia*. Tecnología e Innovación Para La Sociedad. http://dspace.ups.edu.ec/handle/123456789/12776

Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal. *Procedia Computer Science*, *219*, 121–128. https://doi.org/10.1016/J.PROCS.2023.01.272

Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems 2023, Vol. 11, Page 218*, *11*(5), 218. https://doi.org/10.3390/SYSTEMS11050218

Bounagui, Y., Mezrioui, A., & Hafiddi, H. (2019). Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models. *Computer Standards & Interfaces*, *62*, 98–118. https://doi.org/10.1016/J.CSI.2018.09.001

Carvajal Nagua, K. A., & Solano Cedeño, C. S. (2021). *Desarrollo de una Aplicación Web para el Control de citas y manejo de historial médico en la Unidad Médica Family care de la ciudad de Guayaquil* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/20905

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021a). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202/FULL/PDF

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021b). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021c). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202/FULL/PDF

Dax, A., & Kunnemann, R. (2021). On the Soundness of Infrastructure Adversaries. *Proceedings - IEEE Computer Security Foundations Symposium*, *2021-June*. https://doi.org/10.1109/CSF51468.2021.00039

de la Nube Toral Sarmiento, A., Loaiza Martínez, M. de L., Llerena Izquierdo, J., Ayala Carabajo, R., Torres Toukoumidis, A., Romero-Rodríguez, L. M., Aguaded, I., Vega Ureta, N. T., Fuentes Espinoza, P. G., Peñafiel Caicedo, J. A., & others. (2018). *4to. Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad. Memoria académica*. https://dspace.ups.edu.ec/handle/123456789/16318

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls. *Information and Computer Security*, *28*(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004/FULL/XML

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

Falconi Tamayo, L. F. (2021). *Desarrollo e implementación de una aplicación Web para la Gestión de Boletería de Vilaró Microteatro Restaurante*. https://dspace.ups.edu.ec/handle/123456789/20292

Gaitero, D., Genero, M., & Piattini, M. (2021). System quality and security certification in seven weeks: A multi-case study in Spanish SMEs. *Journal of Systems and Software*, *178*, 110960. https://doi.org/10.1016/J.JSS.2021.110960

Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and E-Business Management*, *21*(3), 699–722. https://doi.org/10.1007/S10257-023-00646-Y/TABLES/1

Kheir, O., Jacoby, A., & Verwulgen, S. (2022). Risk Identification and Analysis in the Development of Medical Devices Among Start-Ups: Towards a Broader Risk Management Framework. *Medical Devices: Evidence and Research*, *15*, 349–363. https://doi.org/10.2147/MDER.S375977

Koulierakis, E. (2023). Certification as guidance for data protection by design. *International Review of Law, Computers and Technology*. https://doi.org/10.1080/13600869.2023.2269498

Lenning, J., & Gremyr, I. (2022). Unleashing the potential of internal audits: a review and research agenda. *Total Quality Management and Business Excellence*, *33*(9–10), 994–1010. https://doi.org/10.1080/14783363.2021.1911635

Lindao Guevara, R. A. (2023). *Desarrollo web para la gestión y control de prevención de riesgos laborales para la empresa Biofactor SA* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/24171

Lopez-Leyva, J. A., Kanter-Ramirez, C. A., & Morales-Martinez, J. P. (2020). Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001. *Proceedings - 2020 8th Edition of the International Conference in Software Engineering Research and Innovation, CONISOFT 2020*, 147–153. https://doi.org/10.1109/CONISOFT50191.2020.00030

Mayayise, T. (2021). Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption

in South Africa. *South African Journal of Information Management*, *23*(1), 9. https://doi.org/10.4102/SAJIM.V23I1.1376

Meriah, I., & Rabai, L. B. A. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Computer Science*, *160*, 85–92. https://doi.org/10.1016/J.PROCS.2019.09.447

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security*, *109*, 102383. https://doi.org/10.1016/J.COSE.2021.102383

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100. https://doi.org/10.1109/TEM.2020.2977815

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *International Conference on Information Technology*. https://doi.org/10.1109/INFOTECH49733.2020.9211066

Montalvo, A., & Morán, P. (2012). *Propuesta de un Sistema de Gestión del conocimiento para el Departamento de Tecnología de la Información y la incidencia Económica para el Grupo MAVESA*. https://dspace.ups.edu.ec/handle/123456789/3653

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

Olkiewicz, M., Dyczkowska, J., Chamier-Gliszczynski, N., & Królikowski, T. (2023). Quality management in organizations within the framework of standardized management systems. *Procedia Computer Science*, *225*, 4101–4109. https://doi.org/10.1016/J.PROCS.2023.10.406

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, 103744. https://doi.org/10.1016/J.COMPIND.2022.103744

Putra, D. S. K., Tistiyani, S., & Sunaringtyas, S. U. (2021). The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries. *Proceeding - 2021 2nd International Conference on ICT for Rural Development, IC-ICTRuDev 2021*. https://doi.org/10.1109/IC-ICTRUDEV50538.2021.9656529

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, *23*(3), 383–404. https://doi.org/10.1016/J.EIJ.2022.03.001

Reinoso Ordóñez, L. A. (2021). *Desarrollo de sistema informático para la gestión de pagos de cuotas de los residentes de la Urbanización Belo Horizonte*. https://dspace.ups.edu.ec/handle/123456789/20332

Robles Balaz, G. J. (2021). *Desarrollo de la aplicación web para el registro de matrículas y gestión de conducta e incidencias en la Escuela José Martí*. http://dspace.ups.edu.ec/handle/123456789/20951

Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2024). Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Information Security Journal*, *33*(1), 54–72. https://doi.org/10.1080/19393555.2023.2195577

Salazar Guzmán, B. J. (2021). *Desarrollo de una aplicación bajo android para el control y monitoreo de unidades vehiculares en la empresa TCPLUMESAL SA*.

Sánchez-García, I. D., Feliu Gilabert, T. S., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. *Computers & Security*, *128*, 103170. https://doi.org/10.1016/J.COSE.2023.103170

Santos, E., & Amon, M. (2023). Maritime Education and Training (met) Cybersecurity and iso/iec 27001:2022 from Maritime Academy of Asia and the Pacific (maap) Perspectives and Traditions. *Pedagogika-Pedagogy*, *95*(6s), 79–92. https://doi.org/10.53656/PED2023-6S.08

Sengupta, T., Narayanamurthy, G., Moser, R., & Hota, P. K. (2019). Sharing app for farm mechanization: Gold Farm's digitized access based solution for financially constrained farmers. *Computers in Industry*, *109*, 195–203. https://doi.org/10.1016/J.COMPIND.2019.04.017

Shojaeshafiei, M., Etzkorn, L., & Anderson, M. (2020). *multiple layers of fuzzy logic to quantify vulnerabilies in iot*. 169–187. https://doi.org/10.5121/csit.2020.100914

Soto Eras, W. M. (2021). *Desarrollo del portal web de la fundación nuestra Señora del Cisne para la gestión de servicios en el Cantón Durán*. http://dspace.ups.edu.ec/handle/123456789/20947

Spencer, M. (2022). Characterising assurance: scepticism and mistrust in cyber security. *Journal of Cultural Economy*. https://doi.org/10.1080/17530350.2022.2098515

Suorsa, M., & Helo, P. (2023). Information security failures identified and measured–ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal*. https://doi.org/10.1080/19393555.2023.2270984

Syreyshchikova, N. V., Pimenov, D. Y., Mikolajczyk, T., & Moldovan, L. (2019). Information Safety Process Development According to ISO 27001 for an Industrial Enterprise. *Procedia Manufacturing*, *32*, 278–285. https://doi.org/10.1016/J.PROMFG.2019.02.215

Tout, A., Sharafeddine, S., & Abbas, N. (2023). UAV-assisted multi-tier computing framework for IoT networks. *Ad Hoc Networks*, *142*, 103119. https://doi.org/10.1016/J.ADHOC.2023.103119

Vera Cuesta, E. A. (2023). *Desarrollo de una aplicación web para la gestión de matriculación y control de notas para el Instituto Nacional De Tecnologías* [{B.S.} thesis].

Wu, W., Shi, K., Wu, C.-H., & Liu, J. (1 C.E.). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/JGIM.20220701.Oa2*, *30*(3), 1–16. https://doi.org/10.4018/JGIM.20220701.OA2

Yigit Ozkan, B., & Spruit, M. (2023). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. *Journal of Computer Information Systems*, *63*(4), 965–987. https://doi.org/10.1080/08874417.2022.2119442