UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

TEMA: EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR (IES), DE LA ZONA 1 DEL ECUADOR, MEDIANTE ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN.

Trabajo de grado previo a la obtención del título de Ingeniero en Sistemas Computacionales

Autor:

Edwin Sebastián Echeverría Baldeón

Director:

Daisy Elizabeth Imbaquingo Esparza

Ibarra - Ecuador

2022

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	100387087-8
APELLIDOS Y NOMBRES:	ECHEVERRÍA BALDEÓN EDWIN SEBASTIÁN
DIRECCIÓN:	COTACACHI, QUIROGA 12-42 Y SIMON BOLIVAR
EMAIL:	esecheverriab@utn.edu.ec
TELÉFONO MÓVIL	0988270931

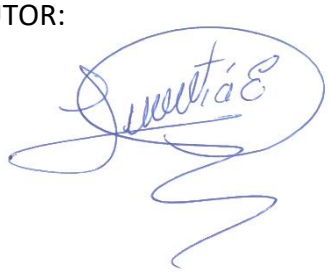
DATOS DE LA OBRA	
TÍTULO:	EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR (IES), DE LA ZONA 1 DEL ECUADOR, MEDIANTE ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN
AUTOR (ES):	ECHEVERRÍA BALDEÓN EDWIN SEBASTIÁN
FECHA:	03/10/2022
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERO EN SISTEMAS COMPUTACIONALES
DIRECTOR:	MSC. DAISY ELIZABETH IMBAQUINGO ESPARZA

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 03 días del mes de octubre de 2022

EL AUTOR:



ECHEVERRÍA BALDEÓN EDWIN SEBASTIÁN
100387087-8

CERTIFICADO DEL DIRECTOR DE TRABAJO DE GRADO

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR

Por medio del presente yo MSc. Daisy Imbaquingo, certifico que el Sr. Edwin Sebastián Echeverría Baldeón, portador de la cédula de ciudadanía Nro. 100387087-8. Ha trabajado en el desarrollo del proyecto de tesis "EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR (IES), DE LA ZONA 1 DEL ECUADOR, MEDIANTE ESTÁNDARES INTERNACIONALES DE SEGURIDAD DE LA INFORMACIÓN", previo a la obtención del título de Ingeniería en Sistemas Computacionales, lo cual ha realizado en su totalidad con responsabilidad y esmero.

Es todo cuanto puedo certificar en honor a la verdad.

En la ciudad de Ibarra, a los 03 días del mes de octubre del 2022

Atentamente

MSc. Daisy Imbaquingo

TUTOR TRABAJO DE GRADO

DEDICATORIA

Dedico este proyecto de titulación a mi madre Rosario de las Mercedes Baldeón Olmedo y mi padre Edwin Rubén Echeverría Terán por darme todo su amor y dejarme los estudios que es la herencia más importante que un hijo puede recibir de sus padres.

A mi hermano Esteban Echeverría y mis hijas Valentina y Mía Echeverría, ellos me motivaron a salir victorioso en cada paso que me llevará al éxito, luchando frente a las adversidades presentadas en el camino, hasta alcanzar mi título profesional.

A mis abuelitos, en especial a mi abuelito Vicente Rubén Echeverría Echeverría (+) quien desde mucho antes de iniciar mi carrera universitaria siempre estuvo al pendiente y me apoyo mientras estuvo a mi lado, y que a pesar de que ya no cuento con su grata compañía se que desde el cielo es mi guía y me ayuda a superar cada obstáculo en mi vida.

A mis tíos, primos, y toda mi familia porque desde el hogar forjaron una persona llena de sueños al cual nunca dejaron solo, siempre estuvo como base el amor, el cariño, y el respeto para formar lo que soy hoy en día, un hombre de bien con principios y conocimientos fundamentados.

Sebastián Echeverría

AGRADECIMIENTO

En primer lugar, quisiera agradecer a Dios por darme salud, guiar mi camino, y poder culminar esta etapa de mi vida.

A mi madre Rosario de las Mercedes Baldeón Olmedo y mi padre Edwin Rubén Echeverría Terán que fueron los pilares fundamentables de mi formación personal y académica. Por darme siempre su bendición y soporte en cada una de las etapas de mi vida.

A mi hermano por su cariño y que a pesar de ser el menor de la casa ha servido en mi como un ejemplo de un buen ser humano, que a pesar de cualquier situación siempre estuvo a mi lado dándome ánimo.

A mis hijas Valentina y Mía Echeverría quienes a pesar de su corta edad han estado ahí conmigo brindándome su cariño incondicional y dándome ánimo para culminar mi vida universitaria.

Un agradecimiento especial a mi tutora MSc. Daisy Imbaquingo, por ser maestra y madre a la vez tanto dentro como fuera de las aulas, por su apoyo, ánimo y por los consejos que siempre me brindo. Sin ella nada de esto sería posible.

Agradezco a mis abuelitos, tíos, primos y amigos que siempre estuvieron al pendiente en todo el transcurso de mi vida personal y universitaria.

A mi segunda familia universitaria, a mis docentes los cuales con sus clases, tutorías, charlas, giras, lograron un cambio positivo en mi vida, y como no a mis amigos universitarios “Tardones” con los cuales hemos compartido un sinnúmero de aventuras y situaciones que siempre nos dejaron una anécdota y nos llenaron de felicidad cuando más la necesitabamos. Los llevo y los llevaré por siempre en mi mente y mi corazón.

Sebastián Echeverría

TABLA DE CONTENIDO

Índice de tablas

Índice de ilustraciones

RESUMEN

La seguridad de la información contribuye a la mejora continua de las organizaciones públicas o privadas debido a que la información actualmente es declarada un activo importante dentro de las instituciones, más ahora con los avances tecnológicos, la seguridad de la información siempre está en riesgo de ser vulnerada, es por esta razón que se deben analizar nuevos métodos para prevenir cualquier tipo de amenazas, los métodos tradicionales de gestión de la seguridad están quedando obsoletos y la transformación digital exige un cambio y actualización en los programas de seguridad. Por lo tanto, en el presente proyecto de investigación se realiza una revisión sistemática de literatura (SRL) sobre la seguridad, los pilares y las métricas para evaluar la seguridad de la información, obteniendo como resultado documentos científicos que permiten identificar conceptos de seguridad, los pilares y las métricas a utilizar en el proyecto. Para identificar los pilares de seguridad y conocer las métricas asociadas a cada pilar se realizó una investigación de tipo cuantitativa con enfoque exploratorio identificando los pilares básicos (integridad, confidencialidad y disponibilidad) y sumado a ellos se tiene la trazabilidad y accesibilidad, cada uno con métricas basadas en la revisión bibliográfica. Como resultado del proyecto de titulación se tiene un método de evaluación de seguridad de la información basado en el análisis e identificación de métricas asociadas a los pilares de seguridad aplicado en 19 Instituciones de Educación Superior de la Zona 1 del Ecuador.

Palabras clave: Seguridad de la información, pilares de la seguridad, métricas de seguridad.

ABSTRACT

Information security contributes to the continuous improvement of public or private organizations because information is currently declared an important asset within institutions, more now with technological advances, information security is always at risk of being violated, it is for this reason that new methods must be analyzed to prevent any type of threat, traditional security management methods are becoming obsolete and digital transformation requires a change and update in security programs. Therefore, in this research project, a systematic review of the literature (SRL) on security, the pillars and the metrics to evaluate information security is carried out, obtaining as results scientific documents that allow identifying security concepts, the pillars and the metrics to be used in the project. To identify the security pillars and to know the metrics associated with each pillar, a productive type of research was carried out with an exploratory approach, identifying the basic pillars (integrity, confidentiality and availability) and added to them, traceability and accessibility, each with metrics based on literature review. As a result of the titling project, there is an information security evaluation method based on the analysis and identification of metrics associated with the security pillars applied in 19 Higher Education Institutions in Zone 1 of Ecuador.

Keywords: Information security, security pillars, security metrics.

INTRODUCCIÓN

Antecedentes

Las organizaciones son cada vez más dependientes de la información, porque incorporan valor agregado a los productos y servicios, por lo tanto, la protección de la información sensible se convierte en una técnica estratégica que garantiza la sostenibilidad empresarial, la rentabilidad y el valor total de una empresa (Hohan et al., 2015).

Además, los trabajadores no conocen los recursos de información existentes en su entorno, su conservación y transferencia. No se encuentran identificadas aquellas áreas con carencias, duplicidades o excesos de información, por lo que no existe una visión clara de cómo ocurre la comunicación y el intercambio de información. Es complejo acceder a los repositorios de información, y no está concebida una política corporativa relacionada con el uso, manejo y transferencia de la información. Todos estos aspectos, alertan sobre la necesidad de iniciar un proceso de auditoría de la información (González Guitián & Ponjuán Dante, 2014).

Las Instituciones de Educación Superior (IES) integran poco a poco tecnologías de la información, donde se gestionan datos críticos que requieren de procesos para evitar riesgos en su seguridad. Son pocas las instituciones que le dan la importancia necesaria, el 17% de las universidades no cuenta con una política de seguridad debidamente formalizada y aprobada, de acuerdo con un informe emitido por la Red Nacional de Investigación y Educación del Ecuador (CEDIA). Asimismo, el 69% tiene un responsable de seguridad de la información y más de la mitad realizan auditorías específicas en este ámbito. El 55% cuenta con el servicio de respuesta a incidentes de seguridad (CSIRT) y un 10% por uno propio (Padilla R., Cadena S., Córdova J., Enríquez R., 2019).

Situación actual

En la actualidad, según una encuesta sobre el estado de la TI realizada por el Instituto Ponemon, la ausencia en la implementación de sistemas de seguridad de la información se relaciona con el liderazgo en las organizaciones, quienes no consideran prioritaria la seguridad de la información dentro de sus estrategias, y a pesar de los recursos, políticas, procedimientos y tecnologías dispuestos para el cumplimiento de los resultados organizacionales, y a pesar de ello, no se complementan con una cultura de seguridad compartida, destinada a comprometer al personal y los recursos para proteger la información como un medio de apoyo para el logro de los objetivos estratégicos de la organización (Ponemon Institute, 2018).

La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información sensible de las organizaciones que principalmente están relacionados con la confidencialidad, integridad y disponibilidad (Tarazona, 2015).

En las IES los sistemas de información aún presentan "insuficiencias en su desempeño integral para contribuir a un control de gestión para la toma de decisiones, que responda a las Normas Técnicas Ecuatorianas (NTE) vigentes en el país". Por lo cual es necesario aplicar evaluaciones de vulnerabilidades para mejorar la seguridad de los productos y procesos que tienen como activo la información. (Altamirano & Luca, 2019).

Planteamiento del Problema

Para poder definir el diagrama de Planteamiento de Problema se utilizó el instrumento de investigación de identificación y clasificación de problemas (Matriz Vester).

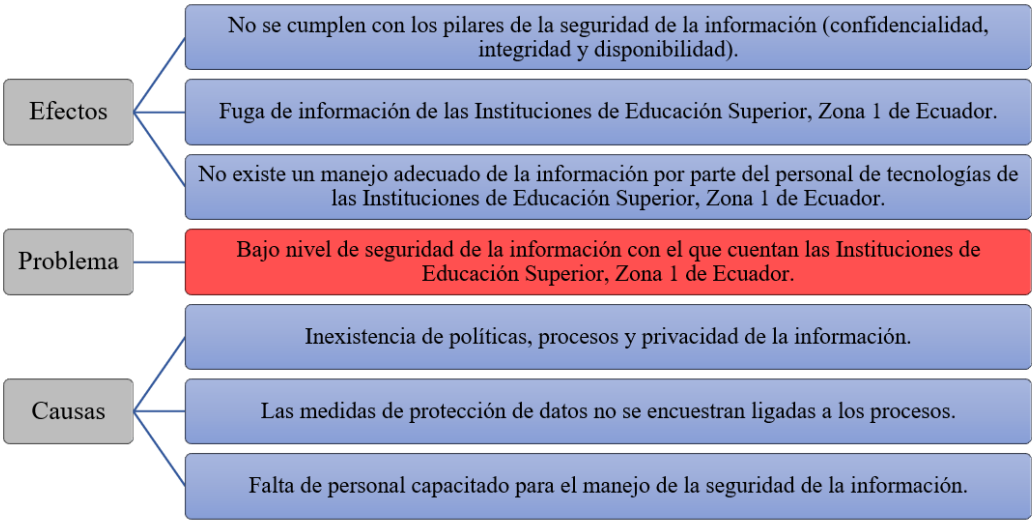


Ilustración 1 Planteamiento del problema.
Fuente: Elaboración propia

Objetivos

Objetivo General

Evaluar la seguridad de la información en Instituciones de Educación Superior (IES), de la Zona 1 del Ecuador, mediante estándares internacionales de seguridad de la información.

Objetivos Específicos

a) Fundamentar el marco teórico sobre seguridad de la información.

b) Describir la situación actual sobre la seguridad de la información en las Instituciones de Educación Superior, de la Zona 1 del Ecuador.

c) Definir métricas y factores de evaluación para las auditorías de la información en las Instituciones de Educación Superior, de la Zona 1 de Ecuador, mediante estándares internacionales de seguridad de la información.

d) Elaborar un informe técnico del nivel de seguridad de la información en las Instituciones de Educación Superior, de la Zona 1 de Ecuador, en base a métricas.

Alcance

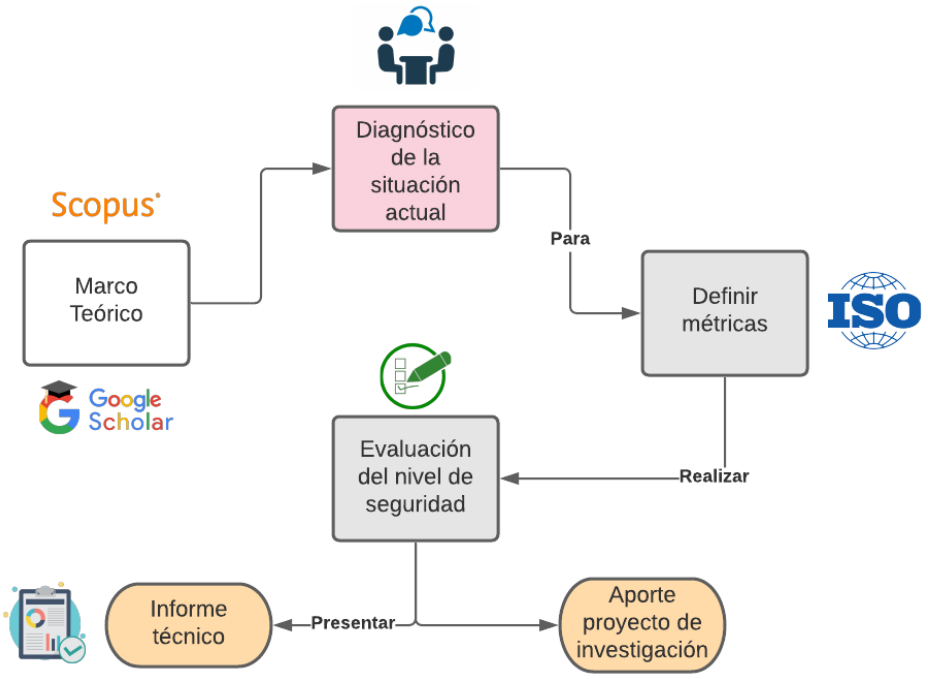


Ilustración 2 Alcance evaluación de seguridad de la información en las IES
Fuente: Elaboración propia

En las IES los sistemas de información aún presentan “insuficiencias en su desempeño integral para contribuir a un control de gestión para la toma de decisiones, que responda a las Normas Técnicas Ecuatorianas (NTE) vigentes en el país”. Por lo cual es necesario aplicar evaluaciones de vulnerabilidades para mejorar la seguridad de los productos y procesos que tienen como activo la información. (Altamirano & Luca, 2019).

Marco teórico: Dentro del marco teórico se realizará una búsqueda sobre auditorías de información, se describirá conceptos de seguridad de la información, así como, la normativa vigente para auditorías informáticas, a continuación, se realizará un diagnóstico de

la situación actual dentro de las IES de la zona 1 del Ecuador; los puntos descritos anteriormente serán extraídos de fuentes bibliográficas con contenido científico.

El marco teórico es un soporte bibliográfico del tema a investigar, por lo que es importante construirlo de manera efectiva para lograr excelentes resultados dentro del proyecto investigativo que se está desarrollando (Gallego Ramos, 2018).

Describir la situación actual sobre la seguridad de la información en las IES: Se realizará una descripción de la situación actual sobre la seguridad de la información en las IES de la Zona 1 del Ecuador.

Definir métricas y factores de evaluación de la seguridad de la información en las IES: Determinar los indicadores que permitirán evaluar la integridad, confidencialidad y la disponibilidad de la información obtenida en el proceso de auditoría. Cada uno de ellos deben ser adecuados para la investigación, de tal forma que se logre la medición, el análisis y la evaluación respectiva (Restrepo Ortiz & Zabala Mendoza, 2016), Se tomará en cuenta los criterios, variables y componentes aplicables en el contexto nacional, además, de estándares internacionales actuales.

Elaborar un informe técnico del nivel de seguridad de la información en las IES: Se procederá a evaluar la seguridad con la que cuenta la información, aplicando la metodología que mejor se ajuste en el contexto nacional en IES de la Zona 1 del Ecuador, para ello se utilizará herramientas seleccionadas durante el proceso investigativo, considerando su pertinencia, eficiencia y eficacia. Con la información obtenida de este proceso se podrá realizar un informe de seguridad que aporte al proyecto de investigación de la autora en su segunda fase.

Justificación

Político

El proyecto se enfoca en el objetivo 9: Industria, innovación e Infraestructura de los Objetivos de Desarrollo Sostenible:

9.5 Aumentar la investigación científica y mejorar la capacidad tecnológica de los sectores industriales de todos los países, en particular los países en desarrollo, entre otras cosas fomentando la innovación y aumentando considerablemente, de aquí a 2030, el número de personas que trabajan en investigación y desarrollo por millón de habitantes y los gastos de los sectores público y privado en investigación y desarrollo.

9.b Apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo, incluso garantizando un entorno normativo propicio a la diversificación industrial y la adición de valor a los productos básicos, entre otras cosas (Naciones Unidas, 2018).

Tecnológico

Los resultados obtenidos acerca del nivel de seguridad de la información necesitan de un estudio objetivo, estándares y marcos referenciales para identificar posibles falencias y garantizar una adecuada gestión de los sistemas de información, para ello se hará el uso de herramientas tecnológicas que permitan el análisis de la seguridad de la información con técnicas avanzadas de datos.

Científico

El proyecto sirve de apoyo a la comunidad de investigadores que trabajan en auditorías y la seguridad de la información, especialmente al Proyecto Doctoral de la Ing. Daisy Imbaquingo, MSc. sobre la creación de un método de auditoría informática para minimizar el riesgo de calidad de los resultados basado en sistemas de procesamiento avanzado de datos. De este modo se contribuirá a que la gestión de los sistemas de información en las IES sea eficiente y efectivo brindando solución a problemáticas detectadas en el proceso sin que exista preocupación por la calidad de los resultados obtenidos.

Método de investigación

Se utilizará el método científico como guía para realizar el procedimiento de la investigación y así dar respuesta a las interrogantes dentro del proyecto.

CAPÍTULO I

Marco Teórico

En la actualidad la información es un factor clave para el éxito y la supervivencia de las empresas y organizaciones (IEEE Staff, 2009). Es por eso que las instituciones, organizaciones y personas responsables eligen implementar métodos de seguridad de la información, los modelos y sistemas deben ser evaluados por su eficiencia y efectividad a través de auditorías que permitan su revisión y análisis a través de estándares y buenas prácticas (Dhillon et al., 2021).

La seguridad de la información trata acerca de la preservación de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, y sobre la protección de la información y de los sistemas que la integran, también controla el acceso, uso, divulgación, interrupción o destrucción no autorizada de la información salvaguardando los intereses de una empresa, organización o una institución de educación superior.

Uno de los controles de seguridad de la información más importantes, es la política seguridad de la información. Este documento no siempre es fácil de elaborar y luchan con la implementación de lo que constituye una política. Por lo que todos los autores y expertos en el área recurran a las fuentes existentes para orientarse y actualizarse en seguridad de la información. Entre estas fuentes se tienen las normas internacionales de seguridad de la información, que son un buen punto de partida para determinar en qué debe consistir la política, pero no se debe confiar exclusivamente en ellas para la orientación y protección de la información, también se debe identificar los tipos de activos de información que maneja una empresa, organización o una institución de educación superior para conocer cuáles son los más importantes y que tan vulnerables son ante las amenazas (Zhou et al., 2022).

Otro aspecto importante es que las personas deben estar preparadas en la seguridad de la información y deben tener en cuenta diferentes situaciones que puedan volver vulnerables los datos. La seguridad de la información de una empresa u organización depende cada vez más de las actitudes y actividades que realicen sus expertos en seguridad informática, estas personas deben estar lo suficientemente capacitadas para recopilar, analizar y utilizar datos y ser responsables de proteger los datos de los usuarios a los que tienen acceso comprometiéndose a resguardar de manera confiable los datos que tienen a disposición (Ma, 2022).

1. 1 Antecedentes.

El constante y veloz desarrollo tecnológico ha provocado que los sistemas informáticos sean potentes herramientas, aptas para asistir y ser aplicadas en cualquier tipo de organización, tal como indica (E. Gómez, 2015) a partir del siglo XX los sistemas de información se han vuelto necesarios en cualquier organización empresarial. Por otra parte, se ha analizado que la importancia del software empresarial se ha generado por:

- Versatilidad del software.
- Funcionalidades basadas en la razón de ser de las organizaciones.
- Reglas del negocio.
- Sustitución a procesos establecidos.
- Poder de toma de decisiones.

La seguridad informática, tiene una importancia cada vez mayor. Los usuarios, particulares y trabajadores de las empresas, deben ser conscientes de que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros (Muñoz, 2020).

(López, 2014) menciona en su libro “Seguridad Informática” que esta consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. Mientras que (Romero Castro et al., 2018) afirma que se suele confundir estos dos conceptos, seguridad informática y seguridad de la información, podrán sonar muy parecidos, pero tienen puntos clave que hacen la diferencia. La seguridad informática se encarga de toda la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar, almacenar y transmitir la información.

(Kisan & Rao, 2020) señala que el significado ha evolucionado en los últimos años, la idea de la seguridad informática se centraba en la máquina física, protegiendo las instalaciones informáticas por tres razones: evitar el robo o daño del hardware, evitar el robo o daño de la información y evitar la interrupción del servicio.

Según (López, 2014), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

Por otra parte, (Baca Urbina, 2016) señala qué la seguridad informática es la disciplina que, con base en políticas y normas internas y externas, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.

En seguridad informática, es necesario cuidar ciertos aspectos como el control de acceso y la autenticación, aunque éstos podrían incluirse en la característica de apego a estándares (Baca Urbina, 2016).

1.2 Variables de investigación

Las variables intervienen como causa o como efecto en el proceso investigativo. Las variables que se van a investigar quedan identificadas desde el momento en que se define el problema. Son factores que intervienen tanto como causa o como resultado dentro del proceso o fenómeno de la realidad formando parte esencial de la estructura del experimento; las variables adquieren valor para la investigación científica cuando llegan a relacionarse con otras variables, es decir, si forman parte de una hipótesis o una teoría (Espinoza, 2018).

Las variables independientes son aquellas que se manipulan por el investigador para explicar, describir o transformar el objetivo de estudio a lo largo de la investigación. Son las que generan y explican los cambios en la variable dependiente. Mientras que las variables dependientes son aquellas que se modifican por la acción de la variable independiente; constituyen los efectos o consecuencias que dan origen a los resultados de la investigación (Espinoza, 2018).

Teniendo claro los conceptos y la diferencia entre variable dependiente e independiente, a continuación, en la Tabla 1 se puede observar de manera detallada cuales son las variables con las que se va a trabajar durante la investigación.

Tabla 1 Variables que intervienen durante el proyecto de investigación

Variable dependiente	Seguridad de la información
Variable independiente	Estándares internacionales de seguridad de la información Métricas de seguridad de la información

1.3 Escalas de Medida

El uso y origen de la escala como herramienta para recopilar información está relacionada con métodos cuantitativos en encuestas. Es importante conocer el tipo de escala a utilizar en función de las características de los datos a comparar, ya que de ello dependerá la fiabilidad de los resultados (Cajas & Luje, 2019).

1.3.1 Técnicas de escalas

Las técnicas de escalamiento más comunes son: las escalas comparativas o también conocidas como escalas no métricas y escalas no comparativas o escalas métricas. En la siguiente investigación se trabajará con las escalas no comparativas ya que son indicadores que nos ayudaran a evaluar el nivel de seguridad de la información dentro de las IES de la Zona 1 del Ecuador.

1.3.2 Escalas no comparativas

(Rosendo, 2018) señala que las escalas no comparativas o escalas métricas (también llamadas escalas monódicas) son técnicas que consisten en escalas de clasificación continuas y detalladas en las que el objeto de estímulo se escala independientemente de otros objetos. Se evalúa solo un objeto a la vez.

Escala de clasificación continua

Según menciona (Benassini, 2009) se trata de escalas diseñadas para medir la opinión de los entrevistados mediante la presentación de infinitas opciones de respuesta, también pueden usarse clasificaciones numéricas. Mientras que (Rosendo, 2018) señala que los encuestados califican los objetos asignando una marca en la posición apropiada en una línea continua que va de un extremo del criterio a otro, el formato puede incluir muchos puntos de anclaje y descripciones breves.

Escala de clasificación por ítems

Las escalas tienen un número de descriptores breves asociados con cada categoría. Los encuestados deben indicar sus calificaciones sobre un atributo u objeto seleccionando la categoría que mejor describa su posición en el atributo u objeto. Las escalas de clasificación por ítems más utilizadas son las escalas de Likert, las de diferencial semántico y las escalas Stapel.

- Escala de Likert

El autor (Vila López et al., 2000) señala que las escalas de Likert son las más utilizadas en el desarrollo de escalas. El ítem se representa como una afirmación, seguida por alternativas de respuesta que suponen diversos niveles de acuerdo en ella, por otra parte, (Benassini, 2009) señala que en esta escala se requiere que el entrevistado señale un grado de aceptación o desacuerdo con una diversidad de afirmaciones relacionadas con el objeto de la actitud, a continuación, en la tabla 2 se puede observar un ejemplo de la estructura de esta escala.

Tabla 2 Estructura de una escala de Likert

	Completamente de acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Completamente en desacuerdo
La IES cuenta con un SGSI	X				
La IES realiza capacitaciones acerca de la SI			X		
Las políticas de SI son correctas				X	
La información de los usuarios se encuentra protegida		X			

- Escala de diferencial semántico

Es una escala en la que se evalúa el estímulo representado en función de diversos atributos, adjetivos o sentencias bipolares. A fin de diseñar un diferencial semántico se pide a los entrevistados que clasifiquen cada objeto de actitud según varias escalas de cinco o siete puntos, rematados en cada extremo por adjetivos o frases polares (Benassini, 2009).

- Escala de Stapel

Según mencionan (Mtra & Cibrián, 2016) es una escala semejante y simplificada de la escala de diferencial semántico, se considera a esta escala como unipolar para medir un

solo adjetivo en el punto medio de un rango de 10 puntos sin punto neutral, la escala está divida con 5 valoraciones positivas y 5 valoraciones negativas ordenadas verticalmente, el entrevistado debe dar su opinión con respecto a un único adjetivo en medio de un rango de valores que va entre -5 y +5.

1.4 Seguridad de la información

La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información (Escrivá Gema et al., 2013). Y tomando en cuenta que uno de los activos más valiosos para cualquier empresa es la información que maneja puesto que ella da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la ruina; incluso si un adversario obtiene acceso no autorizado podría comprometer la confidencialidad de la información.

(Gladden, 2017) afirma que, la seguridad de la información, también conocida como InfoSec, está definida como la protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para brindar confidencialidad, integridad y disponibilidad. La seguridad de la información no se puede conseguir de primera instancia, sino más bien un objetivo que se debe perseguir continuamente, mediante planes sofisticados que son desarrollados y ejecutados por especialistas dedicados a la tecnología de la información donde se utilizan muchas prácticas de seguridad de la información en un esfuerzo por mantener la información confidencial, privada y segura.

Con el pasar del tiempo la seguridad de la información se ha vuelto importante no sólo dentro del ámbito relacionado con los sistemas bancarios sino también dentro del círculo de la industria y el público en general debido a que “no sólo las pérdidas financieras son un riesgo, sino también las repercusiones legales y de reputación” (Diesch et al., 2020), el éxito de la seguridad de la información depende de los comportamientos adecuados de las prácticas de seguridad de la información por parte de los usuarios finales, así como el intercambio de conocimientos sobre seguridad de la información, la colaboración, la intervención, la experiencia, el compromiso que son elementos importantes de la colectividad social (Rhee et al., 2009).

1.5 Pilares de la seguridad de la información

En el ámbito informativo los pilares de la seguridad son diversos y se clasifican según su importancia, los pilares más conocidos son tres: disponibilidad, confidencialidad e

integridad, aunque con el avance de la informática y el manejo de la información se identifican pilares adicionales igual de importantes como: trazabilidad, autenticación; para muchos desarrolladores es importante la implementación de estas herramientas para la seguridad y evitar los ataques a la información, se utilizan protocolos y servicios para la administración de la seguridad que siempre deben ir en conjunto con la seguridad en redes (Zubareva & Byelovb, 2016).

1.5.1 Confidencialidad

Al hablar de confidencialidad se consideran varias definiciones mencionadas por distintos autores descritos en la Tabla 3, los mismos que concuerdan en que confidencialidad consiste en como los datos o la información de una persona, empresa u organización se encuentran de manera oculta o en secreto y solo debe estar disponibles para los agentes autorizados y de este modo evitar la divulgación no autorizada de dicha información, asegurando que únicamente ellos puedan acceder a la información y la puedan modificar.

Tabla 3 Definiciones de confidencialidad según varios autores.

Autor	Conceptos
(Kisan & Rao, 2020)	Lo califica como un principio, y señala qué: "El principio de confidencialidad especifica que solo el remitente y el destinatario previsto deben poder acceder al contenido del mensaje".
(Alhassan & Adjei-Quaye, 2017)	"Es hacer o garantizar que solo las personas de confianza vean o accedan a la información para garantizar que se mantenga la confianza de la información, también tiene que ver con la tecnología, que ayuda a proteger los datos y también garantizar el acceso solo a las personas adecuadas o de confianza". "Observación limitada y divulgación de conocimientos solo a personas autorizadas."
(Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012)	"La información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como los accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación".

(Instituto Nacional de Ciberseguridad, 2010)	“Implica que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso”.
(Co-operation, 2002)	La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus directrices para la Seguridad de la Información define la confidencialidad como “el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada”.
(A. Fernández & Llorens, 2011)	“Se refiere a la protección de información sensible contra la divulgación no autorizada”.
(Calderon Arateco, 2004)	“En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos, su objetivo es prevenir la divulgación no autorizada de la información”.

1.5.2 Integridad

El término integridad, se refiere a que los datos o información, sea lo que dice ser, manteniéndose tal y como fue almacenada por un usuario autorizado interno o externo, que no haya sido modificada de manera alguna, para que de este modo la información obtenida sea auténtica y precisa, permitiendo de esta forma que dicha información sea exacta y completa. A continuación, en la tabla 4, se presenta las diferentes definiciones de autores que sobresalen en los últimos años en temas de seguridad.

Tabla 4 Definiciones de integridad según varios autores.

Autor	Conceptos
(Kisan & Rao, 2020)	“La información confidencial enviada por A a B a la que C accede sin el permiso o conocimiento de A y B”.
(Alhassan & Adjei-Quaye, 2017)	“Asegurarse que el mensaje no se haya modificado en tránsito y esté protegido durante la transmisión”, también ayuda a garantizar que nuestros datos sean lo que se supone que son, en cualquier momento que los necesitemos y que no han sido modificados sin autorización, integridad y legibilidad de la información,

	y la calidad de no haber cambiado desde un estado de referencia".
(Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012)	"Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta".
(Instituto Nacional de Ciberseguridad, 2010)	"La información sea correcta y esté libre de modificaciones y errores".
(López, 2014)	"Garantiza la autenticidad y precisión de la información sin importar el momento en que se solicita, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado."
(A. Fernández & Llorens, 2011)	"Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio".
(Calderon Arateco, 2004)	"La integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado, su objetivo es prevenir modificaciones no autorizadas de la información".

1.5.3 Disponibilidad

Luego de la revisión y análisis acerca de la definición de disponibilidad, se puede decir que se refiera a que la información sea esta física o se encuentre dentro de un sistema esté disponible para usuarios que tengan la autorización necesaria cuando sea requerida mediante cualquiera de los canales de comunicación sin interrupción alguna, especialmente en caso de información crítica; permitiendo que la información esté disponible cuando los usuarios necesiten. A continuación, en la tabla 5 se detalla, los conceptos más utilizados sobre disponibilidad:

Tabla 5 Definiciones de disponibilidad según varios autores.

Autor	Conceptos
(Kisan & Rao, 2020)	"Los activos son accesibles a las partes autorizadas en los momentos adecuados".
(Alhassan & Adjei-Quaye, 2017)	"Significa que los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerla y los canales de

	comunicación utilizados para acceder deben estar funcionando correctamente y estar disponibles en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallas de hardware y actualizaciones del sistema.”
(Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012)	“Disposición de los servicios a ser usados cuando sea necesario, la carencia de disponibilidad supone una interrupción del servicio, la disponibilidad afecta directamente a la productividad de las organizaciones”.
(Instituto Nacional de Ciberseguridad, 2010)	“La información esté accesible cuando la necesitemos”.
(López, 2014)	“La información ha de estar disponible para los usuarios autorizados cuando la necesiten”.
(Calderon Arateco, 2004)	“La disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos utilizados, su objetivo es prevenir interrupciones no autorizadas/controladas de los recursos informáticos”.
(A. Fernández & Llorens, 2011)	“Se refiere a la disponibilidad de la información cuando esta es requerida, también se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas”.
(Cristiá, 2021)	“Preservar la disponibilidad de datos y programas significa que los usuarios autorizados pueden usar los datos y programas cada vez que necesiten”.

1.5.4 Autenticidad

La autenticación es el acto de confirmar la identidad de un dispositivo, persona o software, la autenticación se ve comprometida si las claves son capturadas por un adversario malintencionado (Gungor & Koksal, 2016). Los autores analizados coinciden en que la autenticidad se trata de que la información es lo que dice ser, también consiste en garantizar la legitimidad. A continuación, en la tabla 6, se presenta las diferentes definiciones de autores que sobresalen en los últimos años en temas de seguridad acerca de autenticidad.

Tabla 6 Definiciones de autenticidad según varios autores.

Autor	Conceptos
(Alhassan & Adjei-Quaye, 2017)	"Validez, conformidad y autenticidad de la información"
(Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012)	"Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación de origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos encontrar suplantación de identidad".
(Szczepaniuk et al., 2020)	"La identidad de un usuario o recurso sea la declarada".
(Calderon Arateco, 2004)	"Verificar que la identidad del usuario, generalmente cuando entra al sistema o la red, o accede a una base de datos".
(Montenegro Marín et al., 2011)	"Es uno de los ejes fundamentales para garantizar la validez de documentos enviados a través de una Red de comunicaciones entre sistemas cliente-servidor y por ende sobre Internet".

1.5.5 Trazabilidad

La trazabilidad es la propiedad que certifica que las acciones de una entidad se pueden rastrear, y así determinar quién hizo qué y en qué momento. Se materializa en la integridad de los registros de las actividades realizadas dentro de una entidad por parte de uno o varios usuarios para de este modo llevar un control completo de las acciones. A continuación, en la tabla 7, se presenta las diferentes definiciones de autores que sobresalen en los últimos años en temas de seguridad.

Tabla 7 Definiciones de trazabilidad según varios autores.

Trazabilidad	Conceptos
(Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012)	"Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento", es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia, se materializa en la integridad de los registros de actividad".
(Internacional Organization for Standardization, 2015)	"Capacidad para seguir el histórico, la aplicación o la localización de un objeto".

(INCIBE, 2018)	“Gracias a esta se puede saber el histórico de un activo a lo largo del tiempo. Por medio de la trazabilidad de un documento se puede saber quién ha sido último en modificar o acceder al mismo”

1.6 Revisión de literatura

La base fundamental dentro de un proyecto de investigación es la revisión de la literatura, los autores (Webster & Watson, 2002) mencionan que para un correcto desarrollo del proyecto es necesario realizar la revisión en cuatro fases: preguntas de investigación, búsqueda de documentos, selección de artículos y la extracción de datos relevantes, tal y como se detalla a continuación.

1.6.1 Preguntas de investigación

Para el desarrollo del proyecto se han planteado 2 preguntas de investigación que constituyen las pautas para el proceso de revisión del tema. A continuación, en la tabla 8 se describen las preguntas utilizadas en el proyecto de investigación.

Tabla 8 Preguntas de investigación

N°	Preguntas de investigación	Motivación
PI1	¿Cuáles son los estándares internacionales de la seguridad de la información?	Comprender cuales son los estándares internacionales de la seguridad de la información.
PI2	¿Cuáles son las métricas para evaluar la seguridad de la información?	Identificar las métricas para evaluar la seguridad de la información.

1.6.2 Búsqueda de documentos

Considerando la cadena de búsqueda: (information AND security AND standards AND metrics AND evaluation OR cybersecurity) y algunas palabras auxiliares como protection e ISO las cuales ayudaron a obtener un mayor número de artículos en las bases de datos bibliográficas, como resultado se obtuvieron un total de 97 documentos de las siguientes bases de datos bibliográficas: IEEE Xplore (18), Springer (17), ScienceDirect (39), Scopus (22) y MPDI (1). En la Ilustración 3 se observa el diagrama de búsqueda de documentos.

Ilustración 3 Diagrama de búsqueda
Fuente: Elaboración propia

1.6.3 Selección de artículos

Se consideraron dos etapas para la selección de artículos. En la primera fase se aplican criterios de inclusión y exclusión. Los criterios de inclusión se basan en consideraciones tomadas por los autores: artículos científicos y revisiones de la literatura relevantes para el estudio. Todo el trabajo se relaciona con las disciplinas de la seguridad, información y sus estándares, publicados durante los últimos 7 años en inglés y español. Criterios de exclusión enfocados en la procedencia de bases de datos científicas certificadas, con esto se asegura que todos los documentos citados en este documento son de cuartil 1, 2, 3 y 4. En la segunda fase se consideraron estándares y métricas según su tipo y que respondan a las preguntas de investigación planteadas, en la Tabla 9 se describen los artículos resultantes después de las dos fases de análisis.

Tabla 9 Selección de artículos

Base de datos	Fase I	Fase II
IEEE Xplore	18	14
Springer	17	3
ScienceDirect	39	37
Scopus	22	10
MPDI	1	1
Total	97	65

En la Tabla 10 se describe la información de los artículos seleccionados en la fase II.

Tabla 10 Descripción de artículos seleccionados

Código	Título	Base de datos	Año	País
A1	"Model-Based Quantitative Network Security Metrics: A Survey" (Ramos et al., 2017)	IEEE Xplore	2017	Estados Unidos
A2	"Dynamic Security Metrics for Measuring the Effectiveness of Moving Target Defense Techniques" (Hong et al., 2018)	ScienceDirect	2018	Reino Unido
A3	"A conceptual framework for resilience: fundamental definitions, strategies and metrics" (Andersson et al., 2021)	Springer	2021	Estados Unidos
A4	"Detection of DDoS Attacks and Flash Events using Information Theory Metrics - An Empirical Investigation" (Behal & Kumar, 2017)	ScienceDirect	2017	Países Bajos
A5	"Technical Privacy Metrics: A Systematic Survey" (Wagner & Eckhoff, 2019)	ScienceDirect	2019	Estados Unidos
A6	"An Approach for Internal Network Security Metric Based on Attack Probability" (Shan et al., 2018)	ScienceDirect	2018	Egipto
A7	"IIoT Cybersecurity Risk Modeling for SCADA Systems" (Falco et al., 2018)	IEEE Xplore	2018	Estados Unidos
A8	"A selective ensemble model for cognitive cybersecurity analysis" (Jiang & Atif, 2021)	ScienceDirect	2021	Estados Unidos
A9	"HARMer: Cyber-Attacks Automation and Evaluation" (Enoch et al., 2020)	IEEE Xplore	2020	Estados Unidos
A10	"Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants" (Cho et al., 2016)	IEEE Xplore	2016	Estados Unidos
A11	"General Confidentiality and Utility Metrics for Privacy-Preserving Data Publishing Based on the Permutation Model" (Domingo-Ferrer et al., 2020)	IEEE Xplore	2020	Estados Unidos

A12	"Cyber security risk assessment for seaports: A case study of a container port" (Gunes et al., 2021)	ScienceDirect	2021	Reino Unido
A13	"An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System" (Kure et al., 2018)	MPDI	2018	Rumanía
A14	"A comprehensive model of information security factors for decision-makers" (Diesch et al., 2020)	ScienceDirect	2020	Reino Unido
A15	"Information security policy non-compliance: Can capitulation theory explain user behaviors?" (McLeod & Dolezel, 2022)	ScienceDirect	2022	Reino Unido
A16	"Learning to upgrade internet information security and protection strategy in big data era" (Guo & Wang, 2020)	ScienceDirect	2020	Países Bajos
A17	"A neo-institutional perspective on the establishment of information security knowledge sharing practices" (Hassandoust et al., 2022)	ScienceDirect	2021	Países Bajos
A18	"IS professionals' information security behaviors in Chinese IT organizations for information security protection" (Ma, 2022)	ScienceDirect	2021	Reino Unido
A19	"Towards quantification and evaluation of security of Cloud Service Providers" (Halabi & Bellaiche, 2017)	ScienceDirect	2017	Reino Unido
A20	"Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs" (Alcaraz Velasco et al., 2021)	ScienceDirect	2021	Países Bajos
A21	"Evaluating the Observability of Network Security Monitoring Strategies With Tomato" (Halvorsen et al., 2019)	IEEE Xplore	2019	Estados Unidos

A22	"Random Forest Bagging and X-Means Clustered Antipattern Detection from SQL Query Log for Accessing Secure Mobile Data" (Dhanaraj et al., 2021)	Scopus	2021	Egipto
A23	"On the improvement of the isolation forest algorithm for outlier detection with streaming data" (Heigl et al., 2021)	Scopus	2021	Suiza
A24	"Secrecy performance analysis of amplify-and-forward cooperative network with relay selection in the presence of multiple eavesdroppers" (Deng et al., 2017)	Scopus	2021	Países Bajos
A25	"A novel technique for speech encryption based on k-means clustering and quantum chaotic map" (Khaleel & Abduljaleel, 2021)	Scopus	2021	Indonesia
A26	"D-FAC: A novel ϕ-Divergence based distributed DDoS defense system" (Behal et al., 2021)	Scopus	2021	Arabia Saudita
A27	"Fast Policy Interpretation and Dynamic Conflict Resolution for Blockchain-Based IoT System" (Fang et al., 2021)	Scopus	2021	Egipto
A28	"Novel security models, metrics and security assessment for maritime vessel networks" (Enoch et al., 2021)	ScienceDirect	2021	Países Bajos
A29	"Side-channel leakage assessment metrics and methodologies at design cycle: A case study for a cryptosystem" (Bokharaie & Jahanian, 2020)	ScienceDirect	2021	Reino Unido
A30	"Contextualising and aligning security metrics and business objectives: A GQM-based methodology" (Philippou et al., 2020)	ScienceDirect	2021	Reino Unido
A31	"A Systematic Approach to Threat Modeling and Security Analysis for Software Defined Networking" (Eom et al., 2019)	IEEE Xplore	2019	Estados Unidos

A32	"False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure" (Ahmed & Pathan, 2020)	Springer	2020	Reino Unido
A33	"Physical layer security over fading wiretap channels through classic coded transmissions with finite block length and discrete modulation" (Baldi et al., 2019)	Scopus	2019	Países Bajos
A34	"A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Consistent Supports for Design, Development, Operation, and Maintenance of Secure Information Systems" (Cheng et al., 2008)	IEEE Xplore	2018	Japón
A35	"Automation of an information security management system based on the ISO/IEC 27001 standard" (de la Rosa, 2021)	Scopus	2021	Ecuador
A36	"Comparative Study of Ontologies Based ISO 27000 Series Security Standards" (Meriah & Arfa Rabai, 2019)	ScienceDirect	2019	Portugal
A37	"Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension" (Mesquida & Mas, 2015)	ScienceDirect	2015	España
A38	"An Engineering Environment Based on ISO/IEC 27000 Series Standards for Supporting Organizations with ISMSs" (Suhaimi et al., 2014)	Springer	2014	Japón
A39	"Risk Assessment Using NIST SP 800- 30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency" (Fikri et al., 2019)	ScienceDirect	2019	Indonesia

A40	"Information security management in ICT and non-ICT sector companies: A preventive innovation perspective" (Mirtsch, Blind, et al., 2021)	ScienceDirect	2021	Alemania
A41	"The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services" (Knight et al., 2007)	ScienceDirect	2007	Canadá
A42	"MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures" (Ranaweera et al., 2022)	ScienceDirect	2021	Irlanda
A43	"Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images" (Zhou et al., 2022)	ScienceDirect	2022	China
A44	"Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity" (Ogbanufe, 2021)	ScienceDirect	2021	Estados nidos
A45	"GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking" (Al-Karaki et al., 2020)	Scopus	2020	Emiratos Árabes Unidos
A46	"Information systems security research agenda: Exploring the gap between research and practice" (Dhillon et al., 2021)	ScienceDirect	2021	Estados Unidos
A47	"Exploring role of moral disengagement and counterproductive work behaviours in information security awareness" (Hadlington et al., 2021)	ScienceDirect	2021	Reino Unido
A48	"Maturity level assessments of information security controls: An empirical analysis of	ScienceDirect	2021	Alemania

	practitioners assessment capabilities" (Schmitz et al., 2021)			
A49	"Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis" (Karlsson et al., 2022)	ScienceDirect	2022	Suecia
A50	“A Review of Security Standards and Frameworks for IoT-Based Smart Environments” (Karie et al., 2021)	IEEE Xplore	2008	Australia
A51	“Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis” (Mirtsch, Kinne, et al., 2021)	IEEE Xplore	2021	Alemania
A52	"Proposal and Validation of a Standard Protection Profile for Homologation of Commercial Videoconferencing Equipment" (Florentino et al., 2021)	IEEE Xplore	2021	Brasil
A53	"Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges" (Gebremichael et al., 2020)	IEEE Xplore	2020	Pensilvania
A54	"Non-Interactive Dealer-Free Dynamic Threshold Secret Sharing Based on Standard Shamir’s SS for 5G Networks" (Hsu et al., 2020)	IEEE Xplore	2020	China
A55	"Integrated installing ISO 9000 and ISO 27000 management systems on an organization" (Wang & Tsai, 2009)	IEEE Xplore	2009	Taiwán
A56	"Defining Information Security" (Lundgren & Möller, 2019)	ScienceDirect	2019	Suecia
A57	"Standardization in Information Technology Security" (O. M. Fal’, 2017)	ScienceDirect	2017	Ucrania

A58	"Standardization in information security management" (A. M. Fal', 2010)	Scopus	2010	Ucrania
A59	"Information security management system standards" (Humphreys, 2011)	ScienceDirect	2011	China
A60	"Information Security Policies, Procedures and Standards" (Peltier, 2001)	ScienceDirect	2001	España
A61	Information security policy – what do international information security standards say? (Höne & Eloff, 2002)	ScienceDirect	2002	Sudáfrica
A62	"Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security" (Breda & Kiss, 2020)	ScienceDirect	2020	Hungría
A63	"Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross country investigation" (Shrivastava et al., 2021)	ScienceDirect	2021	Estados Unidos
A64	"Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards" (Hemphill & Longstreet, 2016)	ScienceDirect	2016	Estados Unidos
A65	"Information security management standards: Problems and solutions" (Siponen & Willison, 2009)	ScienceDirect	2009	Finlandia

1.6.4 Extracción de información

Para dar respuesta a las preguntas propuestas anteriormente se evaluaron 65 fuentes, entre ellas se encuentran artículos científicos, ponencias y discusiones. Existen dos grupos de artículos, para la PI1: ¿Cuáles son los estándares internacionales de la seguridad de la información? se analizaron los estándares más destacados y bajo que normas se manejan en la seguridad de la información, teniendo como resultado los siguientes artículos: A34, A36, A37, A40, A41, A42, A43, A44, A45, A46, A47, A48, A50, A51, A52, A55, A56, A58, A59, A60, A61 y A64.

Mientras que para la PI2: ¿Cuáles son las métricas para evaluar la seguridad de la información?, se seleccionaron 33 artículos, que fueron revisados y escogidos para su respectiva clasificación. Los artículos que están relacionados con más de una métrica han sido agrupados se acuerdo con el pilar de seguridad correspondiente. Los artículos para esta pregunta son: A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A17, A18, A19, A20, A21, A22, A23, A24, A25, A26, A27, A28, A29, A30, A31, A32 y A33.

1.7 Estándares de seguridad de la información

Después de analizar los artículos seleccionados se encontró que los estándares de seguridad de la información más destacados son: ISO/IEC 27000, COBIT e ITIL (Ver Tabla 11).

Tabla 11 Detalle de estándares de Seguridad de la Información

Estándares principales	Artículos seleccionados
ISO 27000	A34, A36, A42, A43, A47, A48, A51, A52, A55, A56, A60, A61, A63, A64, A50
COBIT	A36, A41, A37, A40, A34, A56, A57, A47
ITIL	A45, A58, A52, A53, A54

1.7.1 ISO/IEC 27000

Existen varios estándares de seguridad de la información, iniciando por el grupo de estándares ISO/IEC 27000 que integran un sistema de administración de seguridad de la información, el mismo que está enfocado en la seguridad de la información bajo un explícito control administrativo de la misma (Mesquida & Mas, 2015).

ISO 27000 es una serie de estándares internacionales sobre seguridad de la información que contiene un conjunto de buenas prácticas para establecer, implementar, mantener y mejorar los Sistemas de Gestión de Seguridad de la Información (de la Rosa, 2021). Los principales pilares de la familia 27000 son los estándares 27001 y 27002, la principal diferencia entre estos dos estándares es que el 27001 se basa en la gestión continua de la seguridad, apoyada en la identificación continua de riesgos. Y la 27002 es una guía de buenas prácticas que describe un conjunto de objetivos de control y gestión que una organización debe perseguir (Cheng et al., 2008).

ISO/IEC 27001 es reconocido internacionalmente porque garantiza que una empresa u organización está cumpliendo los requisitos básicos en seguridad de la información y que su sistema de gestión de la información sea adecuado. Estos requisitos incluyen todas las medidas y documentos que son necesarios para proporcionar una protección óptima de los

datos, salvaguardar la integridad de los datos de operaciones y garantizar la disponibilidad de los sistemas informáticos de la empresa, incluyendo sus planes de emergencia y análisis de riesgos (Cheng et al., 2008).

ISO/IEC 27002 es un estándar para la seguridad de la información creada por la organización internacional de normalización y comisión electrotecnia internacional, la misma que brinda diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables. La seguridad de la información se consigue con la implementación de un conjunto de controles que incluyen políticas, procesos, estructuras organizativas y funciones de hardware y software. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización (Guamán, 2019).

1.7.2 COBIT

El modelo COBIT (Control Objectives for In- formation and related Technology) es el marco internacional de buenas prácticas para controlar la información de TI y los peligros que conlleva. COBIT se utiliza para llevar a cabo el régimen de TI y mejorar sus controles (Hsu et al., 2020). Así mismo, tiene fines de control, directrices de aseguramiento, mediciones de funcionamiento y resultados, componentes críticos de triunfo y modelos de madurez (Gebremichael et al., 2020).

Permite a los gerentes cubrir la brecha entre los requisitos de control, los aspectos técnicos y riesgos de negocio (Karie et al., 2021). COBIT hace viable el desarrollo de una política clara y buenas prácticas para los controles de TI a través de las organizaciones (Mesquida et al., 2014). Este estándar hace énfasis en la conformidad de regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de COBIT (Siponen & Willison, 2009).

La nueva versión de esta normativa se basa en cinco principios clave (Breda & Kiss, 2020; Hemphill & Longstreet, 2016):

Principio 1: Satisfacer las necesidades de las Partes Interesadas.

Principio 2: Cubrir la organización de principio a fin. Integrando el Gobierno corporativo con el Gobierno de las TI. Orientación al negocio.

Principio 3: La aplicación de un único marco de trabajo integrado.

Principio 4: Habilitación de un enfoque holístico. Para conseguir una Gestión y Gobierno de las TI con eficiencia y eficacia.

Principio 5: La separación la Gestión de Gobierno.

1.7.3 ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información ITIL está basado en un conjunto de mejores prácticas para la gestión de servicios de tecnologías de la información en lo referente a personas, procesos y tecnología, las cuales fueron desarrolladas por la OGC (Oficina Gubernamental de Comercio) del Reino Unido (Mirtsch, Blind, et al., 2021).

A través de las buenas prácticas detalladas en ITIL se hace posible para departamentos y organizaciones reducir costos, mejorar la calidad del servicio, tanto a clientes externos como internos y optimizar al máximo las habilidades y destrezas del personal mejorando su productividad (Humphreys, 2011).

1.7.4 Ventajas y desventajas de los estándares

Existen varios compendios de normas y estándares internacionales (Cheng et al., 2008). Esto porque, si bien la mayoría de los procesos empresariales son los mismos; no todos los aplican de la misma manera. Por esta razón es que existen varias normas y estándares internacionales que pretenden adaptarse a cada proceso u organización (Meriah & Arfa Rabai, 2019), cada estándar cuenta con ventajas y desventajas en su implementación. En la Tabla 12 se presentan los artículos que permiten comparar los resultados.

Tabla 12 Artículos de ventajas y desventajas de estándares de Seguridad de la Información

Estándares principales	Artículos seleccionados
Ventajas y desventajas de aplicar ISO 27000	A34, A36, A61, A64, A43, A63, A42, A64, A55
Ventajas y desventajas de aplicar COBIT	A56, A57, A47
Ventajas y desventajas de aplicar ITIL	A53, A54

A continuación, se describen cada una de las ventajas y desventajas que presentan los estándares analizados (ver Tabla 13).

Tabla 13 Comparativa de ventajas y desventajas de estándares de Seguridad de la Información

Estándares	Ventajas	Desventajas
ISO 27000	Ideal para PYMES Ideal para procesos de producción y distribución de productos.	Demanda un proceso de cambio para toda la organización.

	Consigue mejoras en un corto plazo y resultados viables. Reduce costos (Hadlington et al., 2021). Incrementa la productividad y la calidad. Elimina las redundancias Los documentos que se requieren se encuentran perfectamente establecidos, ya que se hace referencia a la complejidad y al tamaño. Se reduce sustancialmente el riesgo de fuga o deterioro de la información de clientes, proveedores y trabajadores de la empresa. Se hace mención a todas las acciones preventivas. Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial (Mirtsch, Blind, et al., 2021).	Su puesta en marcha implica una inversión inicial de recursos económicos para hacer frente a los gastos de implantación y auditoría (Siponen & Willison, 2009). Se trata de una abstracción y un elevado nivel, por lo que no está muy detallado. Los requisitos pueden parecer difíciles de interpretar, ya que existen nuevos conceptos (Thuraisingham & Gritzalis, 2010).
COBIT	Es compatible con PYMES. Mejor productividad y la calidad Este marco de referencia proporciona roles y responsabilidades. Proporciona la optimización de los costos de las TI. Asegura el servicio continuo. Este marco no obliga a adoptar todos los procesos (Mesquida et al., 2014). Este estándar integra auditoría.	Requiere un tiempo prudencial para adaptarlos (gestión, seguridad, calidad, desarrollo y continuidad, etc.) (Ranaweera et al., 2022). Produce un abismo entre gerencia y operaciones. Lleva tiempo ver las reducciones de costos y la mejora en la entrega de los servicios (IEEE Staff, 2009). Una implementación exitosa implica compromiso del personal a todos los niveles de la organización.

	Implementa directrices destinados a la alta gerencia para tomar decisiones respecto al servicio que se vaya a implementar o modificar (Peltier, 2001). Ayuda a los ejecutivos a entender y gestionar las inversiones en TI a través de su ciclo de vida, así como también proporcionándoles métodos para asegurarse que TI entregara los beneficios esperados (Höne & Eloff, 2002).	Una introducción demasiado ambiciosa puede llevar a la frustración (Gebremichael et al., 2020).
ITIL	Enfoque en los procesos de negocio. Mayor facilidad de adaptar el ITIL en la empresa. Mejor comunicación entre usuarios (clientes, empleados y finales). Aumento de confiabilidad en la entrega de servicios. Se describen mejor los servicios, en un lenguaje más cómodo para el cliente, y con mayores detalles. La administración tiene más control y los cambios resultan más fáciles de manejar. Se describen mejor los servicios, en un lenguaje más cómodo para el cliente, y con mayores detalles (Humphreys, 2011).	Propensa a fomentar la burocracia cuando hay objetivos no definidos (Osborne, 2006). Compromiso por parte de todos los empleados y niveles de organización. Mayor confusión sobre resultados, métricas y control de rendimiento (Khan et al., 2021).

1.7 Métricas para evaluar la Seguridad de la Información

Para la clasificación de los artículos se han tomado en cuenta los controles para evaluar el cumplimiento de los pilares de seguridad, específicamente: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad (Gómez Enciso & Porras Flores,

2018). En la Tabla 14 se exponen los resultados obtenidos de cada artículo para la segunda pregunta de investigación planteada.

Tabla 14 Detalle pilares de seguridad para la definición de métricas

Pilar de Seguridad	Artículos
Autenticidad	A2, A14, A18, A22, A27, A30
Integridad	A1, A5, A12, A13, A19, A21, A23, A25, A31
Confidencialidad	A10, A11, A15, A16, A17, A20, A24, A33
Disponibilidad	A8, A12, A13, A7, A26, A32
Trazabilidad	A13, A3, A9, A32, A6

La Tabla 15 muestra detalladamente las métricas para evaluar la seguridad de la información que se han encontrado en los artículos analizados.

Tabla 15 Detalle métricas por pilar de Seguridad de la Información

Pilar de Seguridad	Métricas	Artículos
Autenticidad	Esfuerzo de defensa ante ataques	A2
	Seguridad física, control de acceso, concienciación e infraestructura	A14, A22, A6, A26
	Control de amenazas, autorización, autenticación	A18, A8
	Detección de antipatrón	A22
	Control de personal autorizado, efectividad del proceso	A30
Integridad	Seguridad del proceso, software, red y organización	A1, A12, A13, A25
	Privacidad y entropía	A5, A19
	Observación y ataques	A21
	Control de transmisión de datos	A23
	Impacto de ataques	A31
Confidencialidad	Confiabilidad y mantenibilidad	A10, A11, A15
	Validez de datos	A16, A17
	Capacidad de secreto e interrupción del secreto	A24, A33
Disponibilidad	Accesibilidad a activos	A8, A12, A13
	Funcionamiento de sistemas informáticos	A7, A26
	Interrupciones del servicio	A8

	Salvaguarda de recursos	A32
Trazabilidad	Registro de actividades (quién hizo, qué hizo, cuándo lo hizo)	A13
	Control de incidentes	A3, A9, A32
	Control de atacantes	A6, A9

1.8 Situación actual

Para comprender como está la situación actual en las IES se aplicó una encuesta basada en la ISO 27000 a las IES de la Zona 1 del Ecuador con el fin de conocer como manejan la seguridad de la información en general y en función de sus pilares (confidencialidad, integridad y disponibilidad). Para el estudio se descartaron los centros académicos que no cuentan con la implementación de sistemas de información. Entre las universidades e instituciones que está zona comprende y cumplen con el requisito para la investigación se tienen las siguientes (ver Tabla 16):

Tabla 16 IES de la Zona 1 del Ecuador que forman parte del estudio

Institución de Educación Superior	Provincia
Instituto Tecnológico Eloy Alfaro	Esmeraldas
Instituto Superior Tecnológico 17 de Julio	Imbabura
Pontificia Universidad Católica del Ecuador – Sede Ibarra	Imbabura
Universidad Regional Autónoma de los Andes	Carchi - Imbabura
Universidad Politécnica Estatal del Carchi	Carchi
Universidad Técnica del Norte	Imbabura
Universidad Yachay Tech	Imbabura

Se aplicaron 99 preguntas que permiten conocer como las instituciones manejan la seguridad de la información, la técnica ha proporcionado información que permite describir la situación actual de las IES y con lo que cuenta cada una de ellas dentro de esta área, considerando temas como: las políticas de seguridad, gestión de activos, control de acceso, cifrado, cumplimiento de normativa, entre otros.

De las siete instituciones encuestadas, seis tienen políticas de seguridad de la información, pero sólo en tres instituciones las políticas están debidamente aprobadas, publicadas y comunicadas con todo el personal; asimismo se mantienen en revisiones constantes para garantizar su idoneidad, efectividad e implementación. En conjunto, las tres

instituciones que garantizan la difusión y la mejora de sus políticas de seguridad de la información es porque cuentan con una persona a cargo de esta área en particular, quién es responsable del monitoreo, control y toma de decisiones.

En el aspecto organizativo de la seguridad de la información, se sabe que cinco de las IES encuestadas consideran que la seguridad de la información es importante en la gestión de proyectos y en la adopción de medidas para prevenir los riesgos derivados del uso de recursos móviles. Si bien cuatro de las siete instituciones tienen una comprensión clara de la importancia de definir y asignar responsabilidades para la seguridad de la información, solo tres de ellas tienen un líder o consultan regularmente a un experto en el área. Mientras que solo una de las IES tiene definido un comité que maneja todo lo relacionado con la seguridad de la información, y aunque se reúne temporalmente, se considera relevante para la toma de decisiones, mitigación de riesgos y control de incidentes.

El crecimiento de trabajos desde el hogar ha aumentado considerablemente debido a la emergencia sanitaria por el Covid-19 y para proteger la información a la que se accede, procesa o almacena desde ubicaciones externas a la institución se deben implementar políticas y medidas que garanticen la confiabilidad, integridad y disponibilidad de los datos, sin embargo, ninguna de las IES encuestadas tiene implementado hasta el momento dichas medidas de seguridad.

De las siete instituciones encuestadas, seis informan a todos los empleados, contratistas y terceros sobre la asignación de deberes y responsabilidades al iniciar, cambiar o terminar el empleo al momento de la firma del contrato. Para que los empleados apliquen la seguridad de acuerdo con las políticas y procedimientos institucionales la dirección de cinco IES verifica los antecedentes de su personal en concordancia con las regulaciones, ética y leyes vigentes. En dos de las IES encuestadas las políticas, los procesos formales de seguridad de la información y el control del cumplimiento se comunicaron adecuadamente al personal. Mientras que solo en una institución se brinda capacitación sobre políticas y procedimientos de seguridad de la información organizacional que les permitan estar actualizados para cumplir con su trabajo.

Al hablar de gestión de activos, todas las instituciones encuestadas tienen asignado un responsable del préstamo, devolución y gestión de regulaciones para el manejo adecuado de la información. Seis de las siete instituciones encuestadas tienen sus activos de información clasificados en relación con su valor, requisitos legales y criticidad, y desarrollaron políticas de control de acceso según sus necesidades de seguridad. No obstante, se sabe que solo cuatro de las instituciones encuestadas han implementado

procedimientos para el manejo de la información de acuerdo con sus esquemas de clasificación y políticas de control de acceso. Para el manejo de la información fuera de los límites físicos, sólo dos IES protegen y controlan el acceso, uso o corrupción durante su traslado. Además, se sabe que solo dos de las siete instituciones encuestadas resguardan los activos de información, en consecuencia, las IES restantes están en riesgo constante de pérdida de datos.

Todas las instituciones encuestadas cuentan con un procedimiento formal de acceso a redes y servicios, teniendo en cuenta la asignación de derechos al iniciar, cambiar o finalizar labores, y la definición de roles para todos los sistemas y servicios. El acceso al código fuente de las aplicaciones y el software está restringido únicamente al personal autorizado. Seis IES encuestadas cumplen con procedimientos de inicio de sesión seguros y gestionan adecuadamente las contraseñas de los usuarios a través de herramientas de administración de sistemas totalmente restringidas y controladas. Solamente cinco instituciones requieren que sus usuarios usen buenas prácticas de seguridad para usar dicha información confidencial.

Solamente tres de las instituciones encuestadas han desarrollado e implementado políticas de gestión de claves criptográficas y de regulación de controles en el cifrado para proteger la información.

En temas de seguridad física y ambiental, todas las IES encuestadas utilizan perímetros de seguridad en áreas e instalaciones que contienen y procesan información sensible. Además, los cables eléctricos y de telecomunicaciones que apoyan a los servicios de información están protegidos contra intercepción, interferencia o daños. Seis de las siete instituciones encuestadas restringen el acceso de personal a áreas protegidas y mantienen los equipos protegidos contra cortes de luz e interrupciones con el fin de garantizar su disponibilidad e integridad. En el caso de salida e ingreso de equipos solo cinco de las IES encuestadas tienen procedimientos para su control y uso fuera de las instalaciones. Con la encuesta se pudo determinar que solo una de las instituciones verifica todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

CAPÍTULO II

Desarrollo

2.1 Metodología de investigación

En el proyecto de investigación se sigue una metodología de tipo cuantitativa con enfoque exploratorio, para identificar las métricas que se adapten a la seguridad de la información en IES basadas en los pilares de la ISO 27000 y evaluar la situación en las IES de la Zona 1 del Ecuador. Como resultado se obtendrá la situación actual de las instituciones evaluadas y conocer cómo está la gestión de la información en base a autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad. La metodología cuantitativa sigue los pasos descritos por (C. Fernández & Baptista, 2014) en el libro Metodología de la Investigación presentada en la Ilustración 4, las fases 1, 2, 3, 4 y 5 se desarrollan en el capítulo 1 del presente proyecto de investigación, mientras que las fases siguientes se describen en el capítulo 2 y 3.

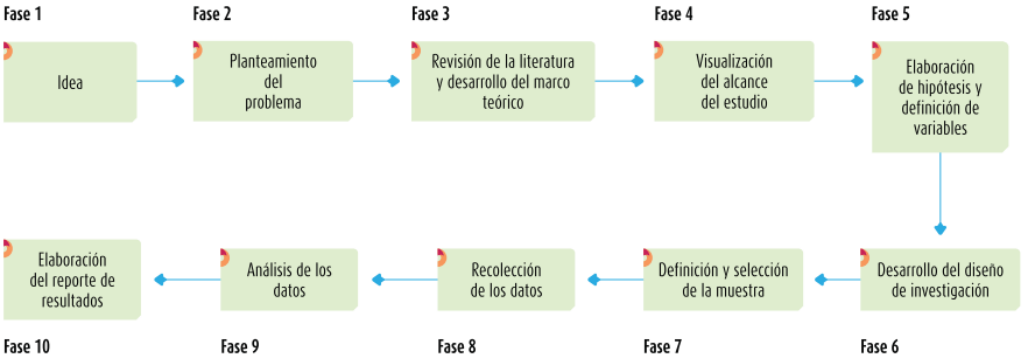


Ilustración 4 Proceso cuantitativo
Fuente: (C. Fernández & Baptista, 2014)

2.1 Desarrollo del diseño de investigación

Una vez definidas las métricas potenciales basadas en la revisión de la literatura de los pilares y características de la seguridad de la información, es necesario describir las preguntas que hacen referencia a cada uno de ellos, con el fin de generar una encuesta dirigida a las IES de la Zona 1 del Ecuador y conocer cómo se encuentran en términos de seguridad, se han considerado un total de 29 preguntas agrupadas en los pilares: autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad. A continuación, en la Tabla 17 se muestran a detalle cada pilar, métricas y posibles preguntas de la encuesta:

Tabla 17 Preguntas de evaluación por métrica y pilar de seguridad

Pilar de seguridad	Métricas	Preguntas
Motivación: Identificar posibles preguntas para evaluación de seguridad de la información en IES relacionadas a las métricas identificadas en cada pilar de seguridad: autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad.		
Autenticidad	Esfuerzo de defensa ante ataques, seguridad física, control de acceso, concienciación e infraestructura, control de amenazas, autorización, autenticación, detección de antipatrón, control de personal autorizado, efectividad del proceso	¿La IES cuenta con políticas para la seguridad de la información?
		¿Se actualizan periódicamente las políticas y procedimientos en seguridad?
		¿Existe un control de acceso a las instalaciones, redes y servicios asociados?
		¿Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad?
		Los servidores cuentan con un acceso controlado
		Se realizan reuniones para tratar temas de la seguridad de la información
		¿Se pueden identificar los usuarios que acceden a la red y lo que hacen?
		Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la institución, según su cargo
		Existe una política de control de accesos
		Se validan los accesos otorgados al personal según su cargo
Integridad	Seguridad del proceso, software, red y organización, privacidad y entropía, observación y ataques, control de transmisión de datos, impacto de ataques	¿Se prueban las vulnerabilidades del sitio web de la institución?
		¿Se monitorea el tráfico de la red?
		Existe una gestión de las contraseñas de usuarios
		¿Se protege la información más sensible?
		¿La institución cuenta con plan de monitoreo y gestión del impacto de incidentes?
Confidencialidad	Confiabilidad y mantenibilidad, validez de datos, capacidad de secreto e interrupción del secreto	¿Se controla que los datos confidenciales no salgan de la red?
		¿Se clasifican y cifran los datos?
Disponibilidad	Accesibilidad a activos, funcionamiento de sistemas informáticos, interrupciones del servicio, salvaguarda de recursos	¿Se tiene documentado y actualizado el inventario de todos los activos de TI?
		Los sistemas cuentan con una acreditación en seguridad
		Controles contra software maligno
		Se realizan copias de seguridad de la información esencial para la institución

Trazabilidad	Registro de actividades (quién hizo, qué hizo, cuándo lo hizo), control de incidentes, control de atacantes	¿Se monitorean las actividades desarrolladas por los usuarios?
		¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?
		¿El procedimiento a seguir frente a incidentes se encuentra documentado?
		¿Se ha tenido pérdidas o daños por incidentes de seguridad?
		¿Se recogen los datos de los incidentes de forma detallada?
		¿Cuándo se identifica un movimiento extraño en la red la institución cuenta con un procedimiento a seguir?
		¿Se realizan auditorías de cumplimiento de seguridad de la información?

2.1.1 Diseño de la encuesta

De acuerdo a las métricas identificadas en la revisión bibliográfica se tienen 29 preguntas presentadas en la Tabla 17, sin embargo, considerando la norma ISO 27000 que tiene como objetivo implementar buenas prácticas vinculadas a la gestión de la seguridad de la información y las necesidades de las IES se redujeron a 19 preguntas seleccionadas por el grupo de investigación del proyecto.

Al identificar y definir las métricas y preguntas se procede a la elaboración de la encuesta basada en una escala de Likert con los siguientes pasos: desarrollar la lista de ítems, definir respuestas con su respectivo puntaje, aplicar la escala, generar y analizar los resultados (Min Shum, 2020) y preguntas con una escala de respuesta de si o no.

2.1.2 Lista de preguntas propuestas

En la Tabla 18 se describen las preguntas elegidas para la evaluación:

Tabla 18 Preguntas para evaluación de la seguridad de la información

N°	PREGUNTA	ESCALAS
1	¿La IES dispone de políticas para la seguridad de la información?	Si / No
2	¿Se actualizan periódicamente las políticas y procedimientos en seguridad en la IES?	Likert
3	¿Existe un control de acceso a la infraestructura y servicios de TI de la IES?	Si / No
4	¿Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad?	Likert
5	¿Con qué frecuencia identifican a los usuarios que acceden a la red y las acciones que ejecutan?	Likert
6	¿Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la IES, según su cargo?	Likert

7	¿Se realiza análisis de vulnerabilidades de los servicios web de la IES?	Likert
8	¿Existen políticas de gestión de contraseñas para los usuarios finales de las IES?	Si / No
9	¿Con qué periodicidad se aplican políticas y acciones de seguridad para la información sensible de las IES?	Likert
10	¿Con qué periodicidad se aplican planes de monitoreo y gestión de impacto de incidentes de seguridad en la IES?	Likert
11	¿Con qué frecuencia las IES actualizan y aplican las políticas de acceso a la información en base a los roles de usuario existentes?	Likert
12	¿Con qué frecuencia las IES clasifican y cifran los datos sensibles?	Likert
13	¿Con qué frecuencia se actualiza y documenta el inventario de todos los activos de TI?	Likert
14	¿La IES dispone de una acreditación en seguridad de la información para todos sus sistemas informáticos?	Si / No
15	¿La IES dispone de aplicaciones para proteger de software malicioso a todas sus soluciones informáticas?	Si / No
16	¿Con qué frecuencia se realizan copias de seguridad de la información esencial para la institución?	Likert
17	¿Con qué frecuencia se monitorean las actividades desarrolladas por los usuarios?	Likert
18	¿Existe un canal y procedimiento documentado a seguir en caso de incidentes de seguridad?	Si / No
19	¿Con qué frecuencia se realizan auditorías de cumplimiento de seguridad de la información?	Likert

2.1.3 Asignación de puntaje

Con la lista de preguntas definida se asigna las respuestas, en este caso se requieren diferentes respuestas para obtener los resultados de acuerdo al tipo de pregunta planteado. Las respuestas y puntajes asignados para la evaluación de la seguridad de la información son los siguientes (ver Tabla 19):

Tabla 19 Escala de respuestas

Preguntas	Escala de respuesta
1, 3, 8, 14, 15 y 18	Si / No
2, 4, 5, 6, 7, 9, 10, 11, 12, 13 y 19	Nunca Raramente Ocasionalmente Frecuentemente Muy frecuentemente
16 y 17	Diario Semanal Mensual Semestral Anual

2.1.4 Población y muestra

La evaluación de la seguridad de la información se aplica a las IES de la Zona 1 del Ecuador, en total son 21 centros académicos de educación superior comprendidos en las provincias de Carchi, Imbabura, Esmeraldas y Sucumbíos, sin embargo, solamente 19 instituciones cumplen con la característica de tener implementado y hacer uso de sistemas de información. En la Tabla 20 se describen las IES que son parte del proyecto:

Tabla 20 Población y muestra

N°	Institución de Educación Superior	Provincia
1	Universidad Politécnica Estatal de Carchi	Carchi
2	Universidad de Investigación de Tecnología Experimental YACHAY	Imbabura
3	Universidad de Otavalo	Imbabura
4	Universidad Técnica del Norte	Imbabura
5	Pontificia Universidad Católica del Ecuador Sede Ibarra	Imbabura
6	Universidad Técnica Luis Vargas Torres de Esmeraldas	Esmeraldas
7	Instituto Tecnológico Superior Vicente Fierro	Carchi
8	Instituto Tecnológico Superior Alfonso Herrera	Carchi
9	Instituto Tecnológico Superior Cotacachi	Imbabura
10	Instituto Tecnológico Superior Luis Ulpiano de la Torre	Imbabura
11	Instituto Tecnológico Superior 17 de Julio.	Imbabura
12	Instituto Tecnológico Superior Luis Tello	Esmeraldas
13	Instituto Tecnológico Superior Quinindé	Esmeraldas
14	Instituto Superior Pedagógico Martha Bucaram De Roldós - Bilingüe Intercultural	Sucumbíos
15	Instituto Tecnológico Superior José Chiriboga Grijalva	Imbabura
16	Instituto Tecnológico Superior Ibarra	Imbabura
17	Instituto Tecnológico Superior Liceo Aduanero	Imbabura
18	Universidad Autónoma Regional de los Andes "Uniandes"	Imbabura
19	Pontificia Universidad Católica Del Ecuador Sede Esmeraldas	Esmeraldas

2.2 Análisis de resultados del instrumento para la evaluación de las IES

Para el análisis de los resultados una vez completada la aplicación del instrumento de evaluación a las 19 IES de la Zona 1 del Ecuador se utiliza el programa estadístico informático SPSS, el mismo que se ajusta al proyecto y ofrece resultados eficientes y minimiza el riesgo de fallas en los datos (IBM, 2021). Se realiza un estudio por pregunta planteada en el instrumento, considerando frecuencias, porcentajes, porcentajes válidos y porcentajes acumulados, los resultados en conjunto brindan una visión de como las IES manejan temas de seguridad de la información actualmente y poder así dar recomendaciones en base a la norma ISO 27000 para garantizar la mejora dentro de las instituciones.

Pregunta 1: ¿La IES dispone de políticas para la seguridad de la información?

De acuerdo con los resultados obtenidos, se puede aseverar que del total de IES encuestadas el 84,21% disponen de políticas enfocadas en la seguridad de la información, mientras que el 15,79% no las posee lo que puede poner en riesgo su información. La diferencia entre las respuestas es estadísticamente significativa, así como se muestra en la ilustración 5.

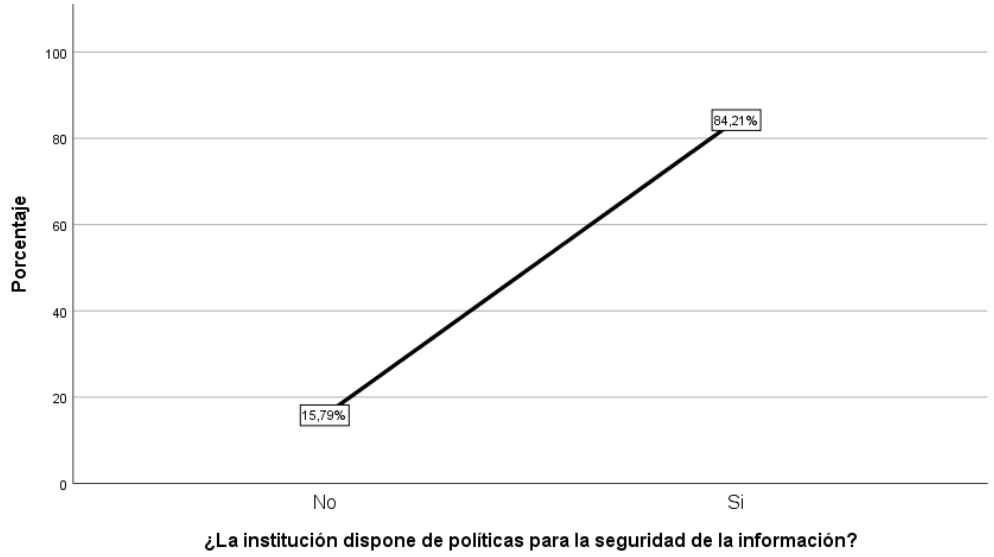


Ilustración 5 Gráfico de líneas pregunta 1

En la Tabla 21 se muestran los valores estadísticos de los resultados obtenidos para la pregunta 1 de las 19 IES evaluadas.

Tabla 21 Valores estadísticos pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	3	15,8	15,8	15,8
	Si	16	84,2	84,2	100,0
	Total	19	100,0	100,0	

Pregunta 2: ¿Se actualizan periódicamente las políticas y procedimientos en seguridad en la IES?

En lo que respecta a la pregunta de la periodicidad con la que se actualizan las políticas y procedimientos en seguridad de la información, se puede observar que las opciones de respuesta que abarcan al menos al 80% del total de encuestados son ocasional y frecuentemente.

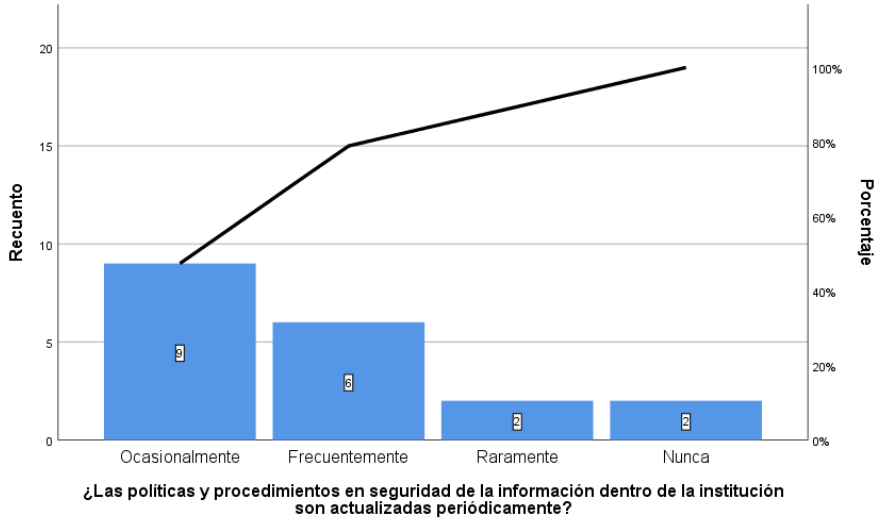


Ilustración 6 Gráfico de Pareto pregunta 2

En la Tabla 22 se presentan los resultados de las IES evaluadas, en las que se puede evidenciar que 9 de las 19 instituciones actualizan ocasionalmente las políticas y procedimientos en seguridad de la información, mientras que el resto no cuenta con actualizaciones continuas.

Tabla 22 Valores estadísticos pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	6	31,6	31,6	31,6
	Nunca	2	10,5	10,5	42,1
	Ocasionalmente	9	47,4	47,4	89,5
	Raramente	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Pregunta 3: ¿Existe un control de acceso a la infraestructura y servicios de TI de la IES?

Del total de instituciones evaluadas el 84,21% cuentan con controles de acceso a la infraestructura y servicios de TI de la institución, lo que garantiza que solo el personal autorizado haga uso de la información presente en las instituciones (Ver Ilustración 7).

En la Ilustración 7 se observa la diferencia de respuestas a la pregunta 3 ya que solamente el 15,79% de IES evaluadas no cuenta con un control de acceso a la infraestructura y servicios de TI, este porcentaje se debe a que no cuentan con un área específica para la gestión de tecnologías de la información.

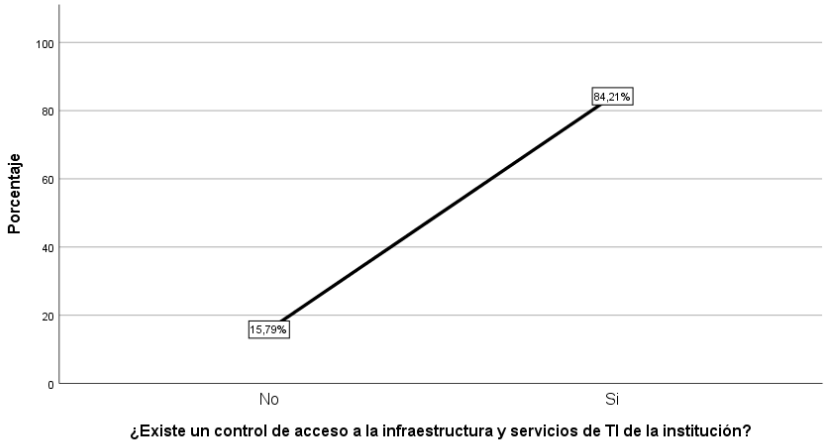


Ilustración 7 Gráfico de líneas pregunta 3

En la Tabla 23 se muestran los resultados estadísticos de la pregunta 3 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 23 Valores estadísticos pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	3	15,8	15,8	15,8
	Si	16	84,2	84,2	100,0
	Total	19	100,0	100,0	

Pregunta 4: ¿Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad?

De acuerdo con la gráfica de Pareto en la Ilustración 10 se puede afirmar que en lo referente a la pregunta se suele capacitar e involucrar a usuarios y personal en temas de seguridad de la información en más del 80% de los casos de forma ocasional, seguida de rara y frecuentemente.

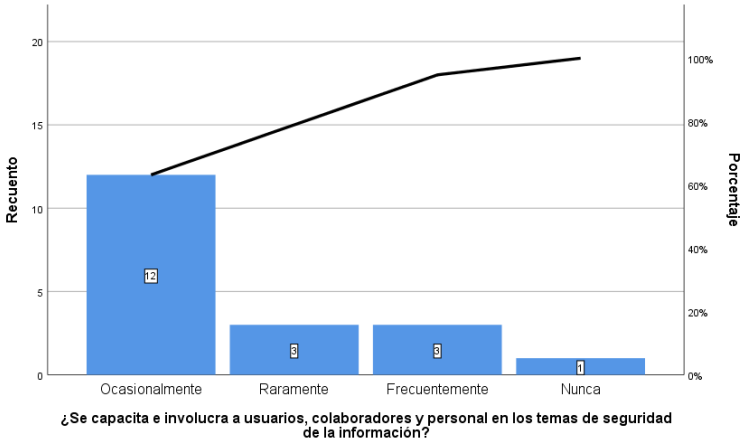


Ilustración 8 Gráfico de Pareto pregunta 4

En la Tabla 24 se muestran los valores estadísticos de los resultados obtenidos para la pregunta 4 de las 19 IES evaluadas.

Tabla 24 Valores estadísticos pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	3	15,8	15,8	15,8
	Nunca	1	5,3	5,3	21,1
	Ocasionalmente	12	63,2	63,2	84,2
	Raramente	3	15,8	15,8	100,0
	Total	19	100,0	100,0	

Pregunta 5: ¿Con qué frecuencia identifican a los usuarios que acceden a la red y las acciones que ejecutan?

El 80% de IES evaluadas afirman que la frecuencia con la que identifican a usuarios que acceden a sus redes y toman acciones en base a las mismas son frecuente y ocasionalmente, tal y como se ve en la Ilustración 9.

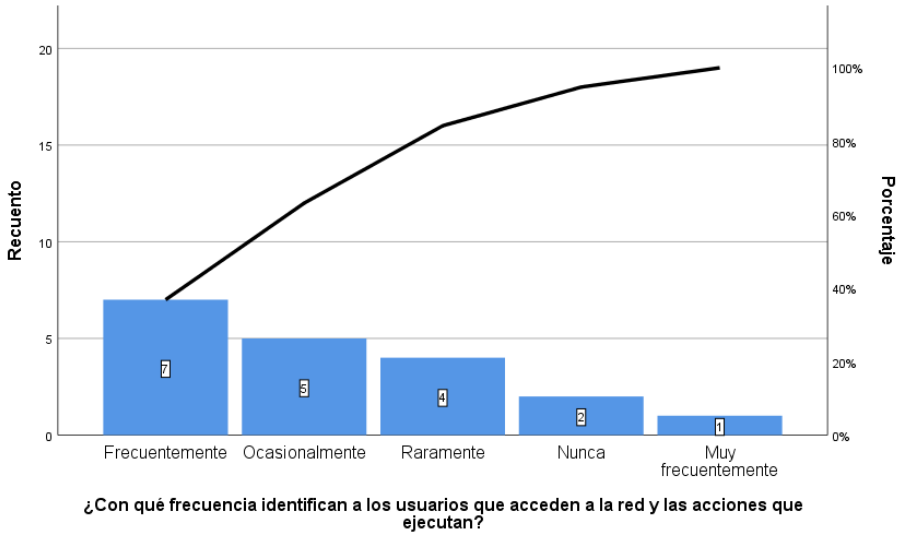


Ilustración 9 Gráfico de Pareto pregunta 5

En la Tabla 25 se presentan los resultados de las IES evaluadas, en las que se puede evidenciar que 7 de las 19 instituciones evaluadas identifican a usuarios que acceden a la red y hacen seguimiento de las acciones que ejecutan.

Tabla 25 Valores estadísticos pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	7	36,8	36,8	36,8
	Muy frecuentemente	1	5,3	5,3	42,1
	Nunca	2	10,5	10,5	52,6

	Ocasionalmente	5	26,3	26,3	78,9
	Raramente	4	21,1	21,1	100,0
	Total	19	100,0	100,0	

Pregunta 6: ¿Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la IES, según su cargo?

De todas las opciones presentadas para esta pregunta, las que abarcan al 80% del total de encuestados son de mayor a menor ocasional, frecuente y raramente, lo que denota que este es un aspecto para mejorar debido a que solo uno de todos los encuestados respondió que esta actividad se realiza muy frecuentemente.

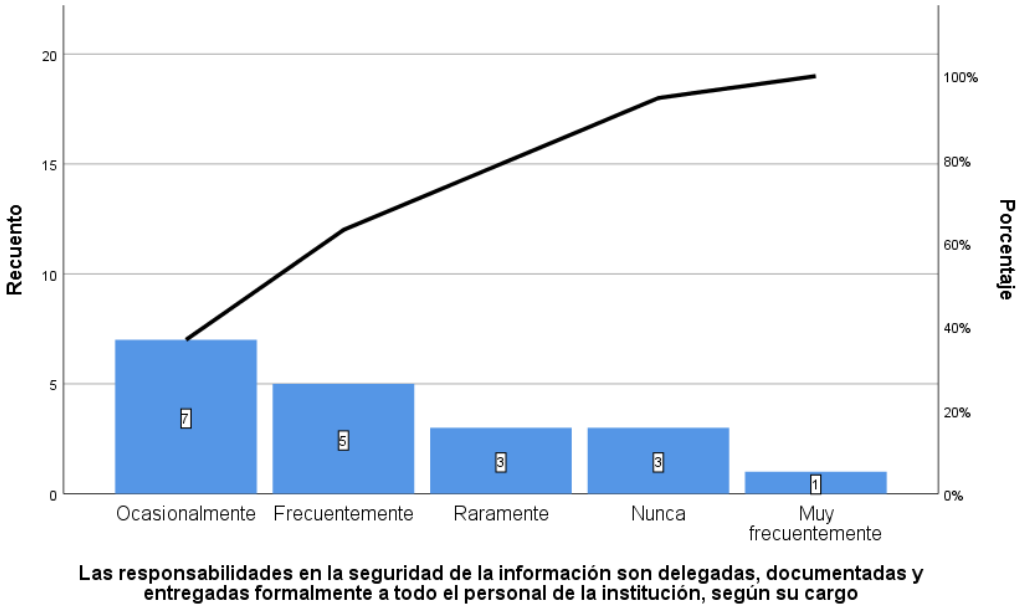


Ilustración 10 Gráfico de Pareto pregunta 6

En la Tabla 26 se muestran los resultados estadísticos de la pregunta 3 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 26 Valores estadísticos pregunta 6

		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	**Frecuentemente**	5	26,3	26,3	26,3
	Muy frecuentemente	1	5,3	5,3	31,6
	Nunca	3	15,8	15,8	47,4
	Ocasionalmente	7	36,8	36,8	84,2
	Raramente	3	15,8	15,8	100,0
	Total	19	100,0	100,0	

Pregunta 7: ¿Se realiza análisis de vulnerabilidades de los servicios web de la IES?

En lo referente a la pregunta 7, el 80% de la respuesta dada por las IES evaluadas son frecuente y ocasionalmente, lo que denota que, pese a que se realizan de forma periódica análisis de vulnerabilidades, puede mejorarse para aumentar de manera considerable la seguridad de la información en las instituciones (Ver Ilustración 11)

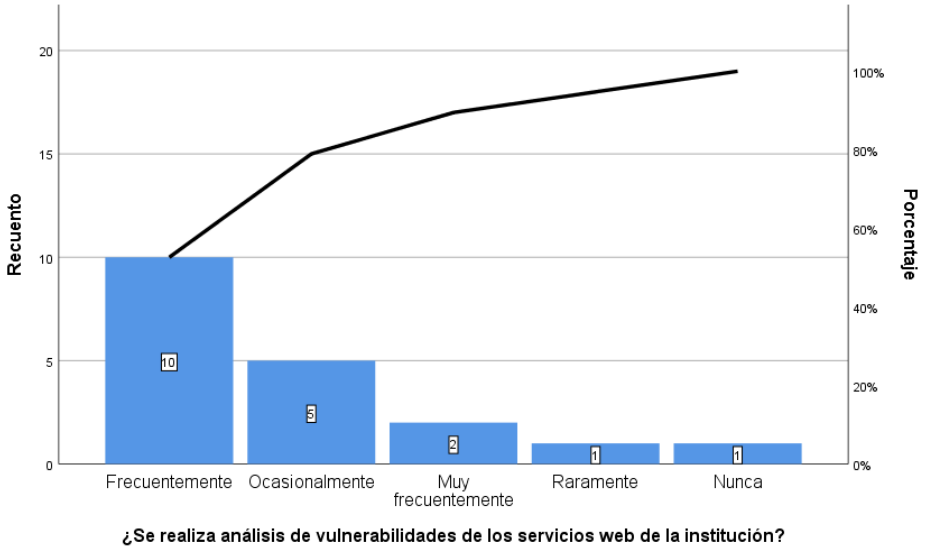


Ilustración 11 Gráfico de Pareto pregunta 7

En la Tabla 27 se presentan los resultados de las IES evaluadas, en las que se puede evidenciar que 10 de las 19 instituciones evaluadas realizan análisis de vulnerabilidades de los servicios web de la institución.

Tabla 27 Valores estadísticos pregunta 7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	10	52,6	52,6	52,6
	Muy frecuentemente	2	10,5	10,5	63,2
	Nunca	1	5,3	5,3	68,4
	Ocasionalmente	5	26,3	26,3	94,7
	Raramente	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Pregunta 8: ¿Existen políticas de gestión de contraseñas para los usuarios finales de las IES?

En lo referente a la pregunta 8, un 73.68% afirma que, si existen políticas para la gestión de contraseñas para usuarios de las instituciones, sin embargo, un 26,32% no las posee lo que puede ser un riesgo en la seguridad de la información, tal y como se muestra en la Ilustración 12.

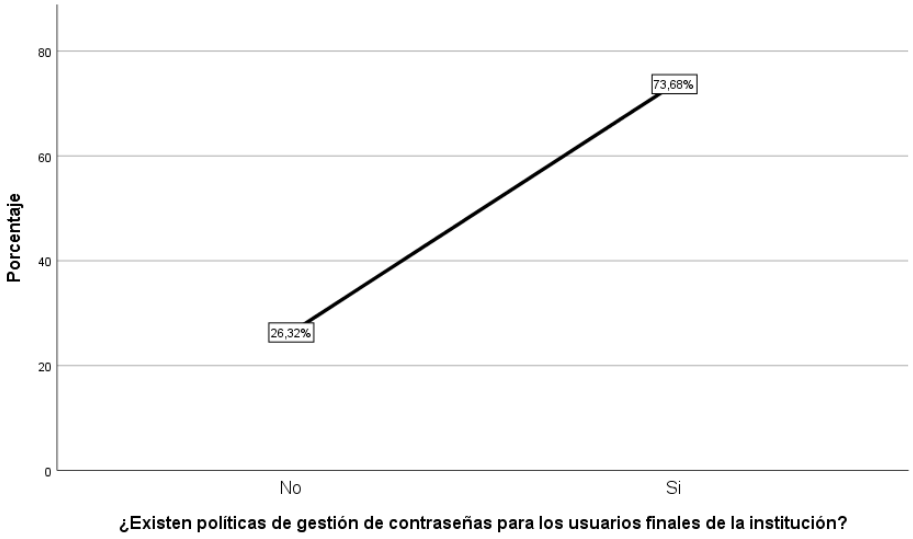


Ilustración 12 Gráfico de líneas pregunta 8

En la Tabla 28 se muestran los valores estadísticos de los resultados obtenidos para la pregunta 8 de las 19 IES evaluadas.

Tabla 28 Valores estadísticos pregunta 8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	5	26,3	26,3	26,3
	Si	14	73,7	73,7	100,0
	Total	19	100,0	100,0	

Pregunta 9: ¿Con qué periodicidad se aplican políticas y acciones de seguridad para la información sensible de las IES?

En esta pregunta, no existe diferencia estadísticamente significativa entre las opciones respondidas por las IES evaluadas, pero se debe considerar que al menos el 30% rara vez aplica políticas en lo referente a la seguridad de la información de carácter sensible de las instituciones, así como se muestra en la Ilustración 13.

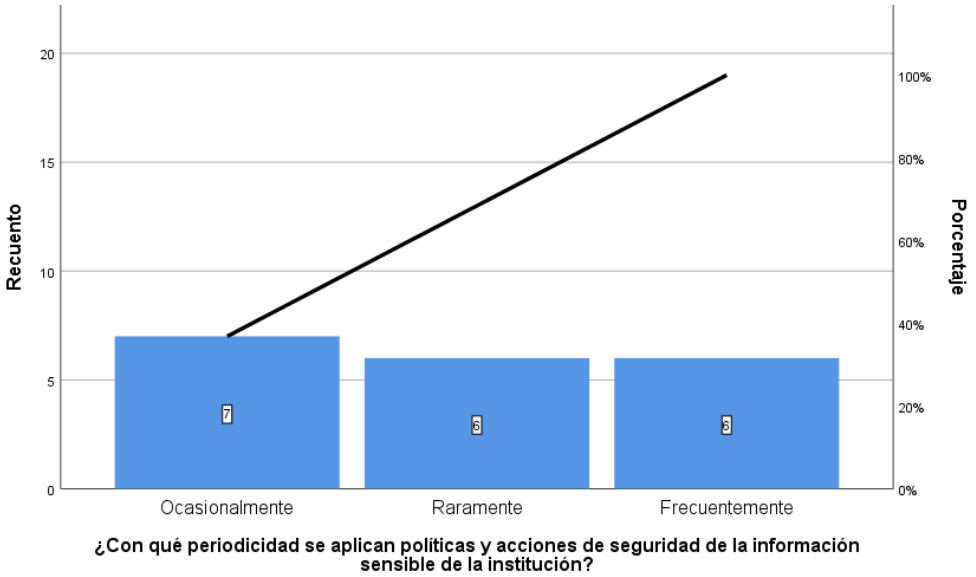


Ilustración 13 Gráfico de Pareto pregunta 9

En la Tabla 29 se muestran los resultados para la escala frecuente, ocasional y raramente, las escalas que no están en la tabla no tuvieron ninguna puntuación por ninguna de las IES evaluadas.

Tabla 29 Valores estadísticos pregunta 9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	**Frecuentemente**	6	31,6	31,6	31,6
	Ocasionalmente	7	36,8	36,8	68,4
	Raramente	6	31,6	31,6	100,0
	Total	19	100,0	100,0	

Pregunta 10: ¿Con qué periodicidad se aplican planes de monitoreo y gestión de impacto de incidentes de seguridad en la IES?

La periodicidad con la que se ejecutan planes de monitoreo y gestión de impacto de incidentes de seguridad en las IES, en el 80% de casos se da de forma ocasional y raramente, esta última es alarmante ya que debería hacerse esto por lo menos de forma ocasional, para asegurar la adecuada gestión de la seguridad de la información (Ver Ilustración 14).

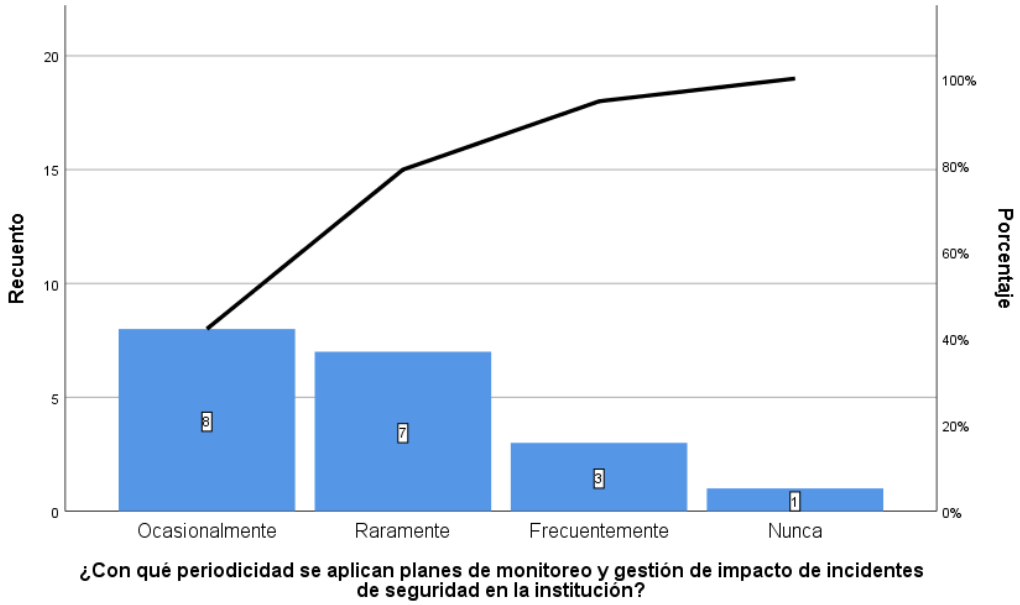


Ilustración 14 Gráfico de Pareto pregunta 10

En la Tabla 30 se muestran los resultados estadísticos de la pregunta 10 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 30 Valores estadísticos pregunta 10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	3	15,8	15,8	15,8
	Nunca	1	5,3	5,3	21,1
	Ocasionalmente	8	42,1	42,1	63,2
	Raramente	7	36,8	36,8	100,0
	Total	19	100,0	100,0	

Pregunta 11: ¿Con qué frecuencia las IES actualizan y aplican las políticas de acceso a la información en base a los roles de usuario existentes?

En el 80% de casos esto se realiza de forma ocasional y rara, el resto de las opciones (nunca, muy frecuente y frecuentemente) casi no se realizan, a excepción del 20% de los casos, tal y como se presenta en la Ilustración 15.

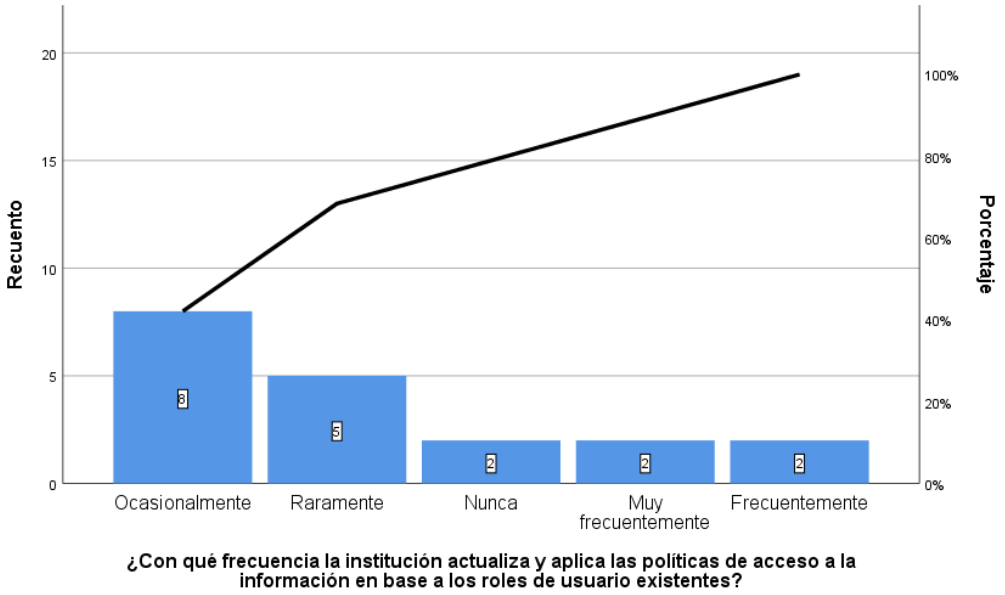


Ilustración 15 Gráfico de Pareto pregunta 11

En la Tabla 31 se muestran los resultados estadísticos de la pregunta 10 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 31 Valores estadísticos pregunta 11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	2	10,5	10,5	10,5
	Muy frecuentemente	2	10,5	10,5	21,1
	Nunca	2	10,5	10,5	31,6
	Ocasionalmente	8	42,1	42,1	73,7
	Raramente	5	26,3	26,3	100,0
	Total	19	100,0	100,0	

Pregunta 12: ¿Con qué frecuencia las IESS clasifican y cifran los datos sensibles?

En los resultados de la pregunta 12 se puede observar que las instituciones clasifican y cifran información con una frecuencia rara u ocasional esto en el 80% de los casos. Los valores estadísticos se presentan en la Ilustración 16.

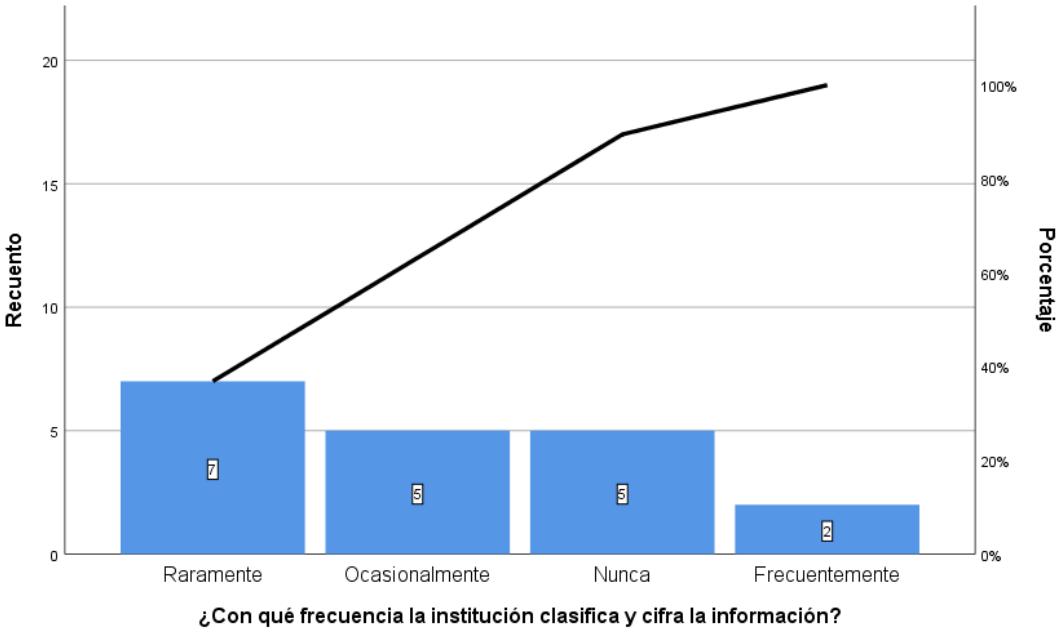


Ilustración 16 Gráfico de Pareto pregunta 12

En la Tabla 32 se presentan los resultados de las IES evaluadas, en las que se puede evidenciar que 7 de las 19 instituciones evaluadas clasifican y cifran la información raramente, lo que es un dato alarmante al momento de administrar y compartir la información.

Tabla 32 Valores estadísticos pregunta 12

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	2	10,5	10,5	10,5
	Nunca	5	26,3	26,3	36,8
	Ocasionalmente	5	26,3	26,3	63,2
	Raramente	7	36,8	36,8	100,0
	Total	19	100,0	100,0	

Pregunta 13: ¿Con qué frecuencia se actualiza y documenta el inventario de todos los activos de TI?

Para la pregunta 13 se obtiene como resultados que la frecuencia con la que se actualiza y documenta el inventario de los activos TI, es frecuentemente en el 80% de casos, lo que indica una adecuada gestión de la seguridad de la información, tal y como se muestra en la Ilustración 17.

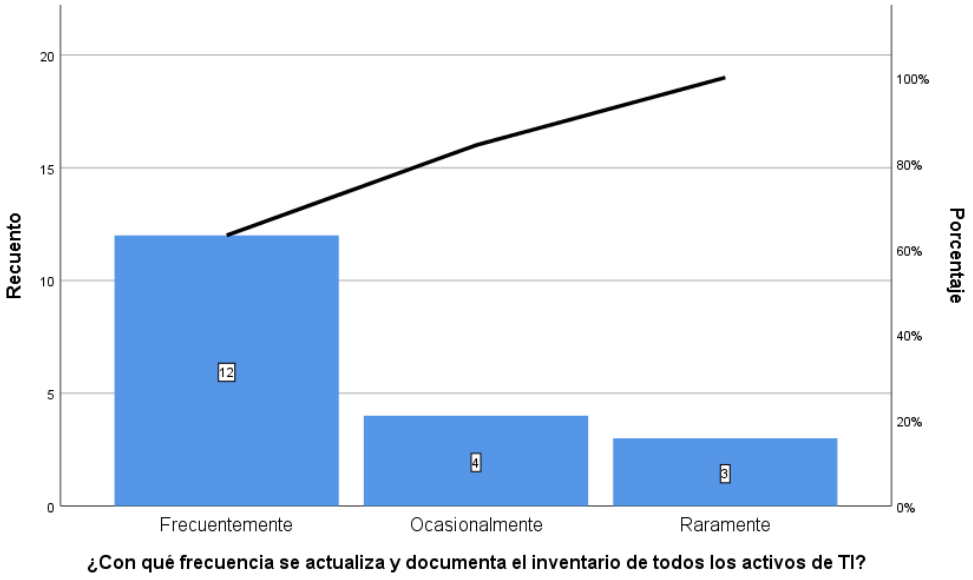


Ilustración 17 Gráfico de Pareto pregunta 13

En la Tabla 33 se presentan los resultados de las IES evaluadas, en las que se puede evidenciar que 12 de las 19 instituciones evaluadas actualizan y documentan el inventario de todos los activos de TI.

Tabla 33 Valores estadísticos pregunta 13

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	**Frecuentemente**	12	63,2	63,2	63,2
	Ocasionalmente	4	21,1	21,1	84,2
	Raramente	3	15,8	15,8	100,0
	Total	19	100,0	100,0	

Pregunta 14: ¿La IES dispone de una acreditación en seguridad de la información para todos sus sistemas informáticos?

En los resultados se puede evidenciar que el 94,74% de los casos la institución dispone de acreditaciones en el tema de seguridad de la información en todos sus sistemas informáticos, solo el 5,26% de los casos no se los posee, los resultados se pueden ver en la Ilustración 18.

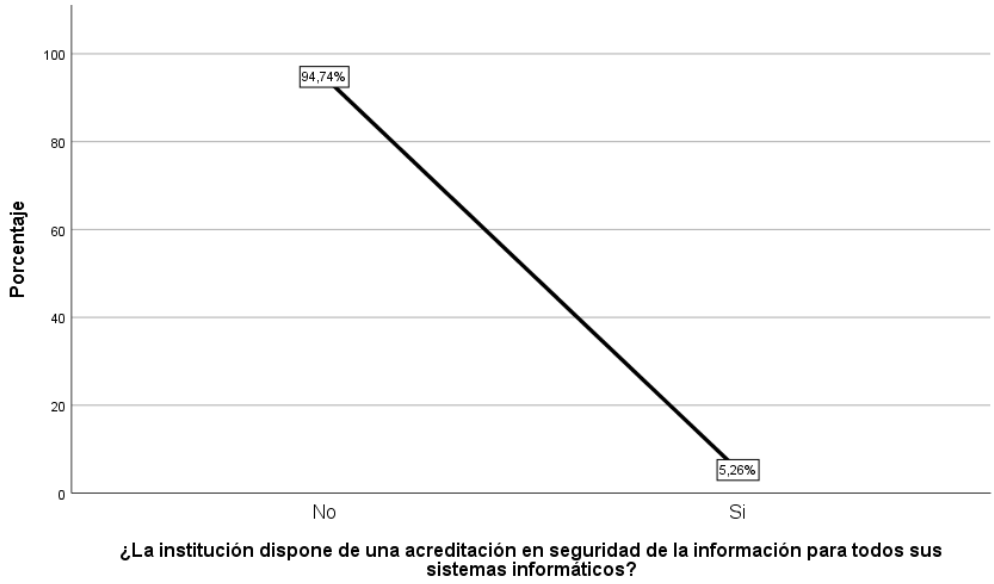


Ilustración 18 Gráfico de líneas pregunta 14

En la Tabla 34 se muestran los resultados estadísticos de la pregunta 14 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 34 Valores estadísticos pregunta 14

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	18	94,7	94,7	94,7
	Si	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Pregunta 15: ¿La IES dispone de aplicaciones para proteger de software malicioso a todas sus soluciones informáticas?

Las IES disponen de aplicaciones especializadas para protegerse de software malicioso en el 57,89% de los casos mientras que en 42,11% de los casos no, lo que es casi una paridad, y este debe ser algo a tomar importancia en la evaluación. Esto se puede ver en la Ilustración 19.

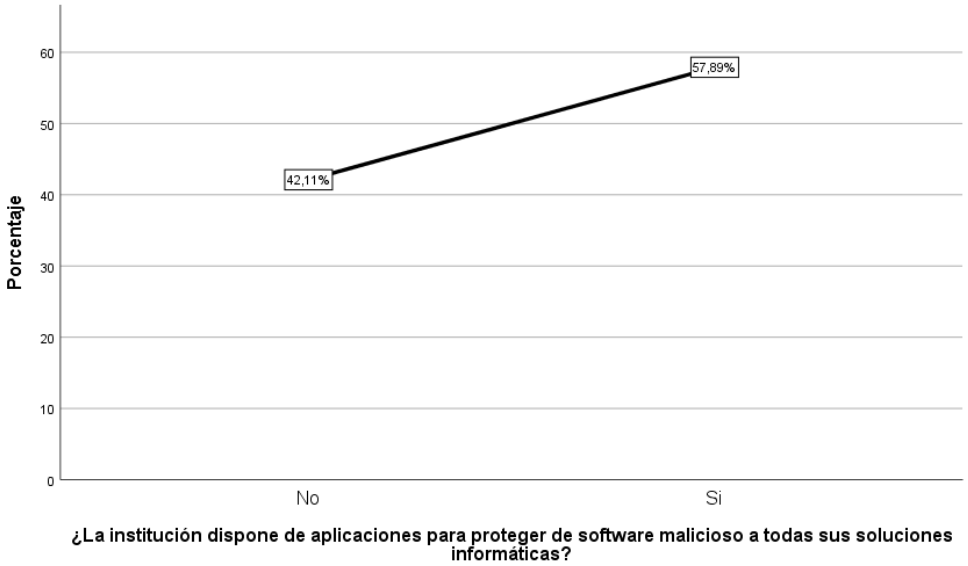


Ilustración 19 Gráfico de líneas pregunta 15

En la Tabla 35 se muestran los resultados estadísticos de la pregunta 15 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 35 Valores estadísticos pregunta 15

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	8	42,1	42,1	42,1
	Si	11	57,9	57,9	100,0
	Total	19	100,0	100,0	

Pregunta 16: ¿Con qué frecuencia se realizan copias de seguridad de la información esencial para la institución?

La frecuencia con la que se realizan copias de seguridad de la información almacenada en las instituciones evaluadas es en al menos el 80% de los casos de forma diaria o semanal, lo cual es un buen indicador (Ver Ilustración 20).

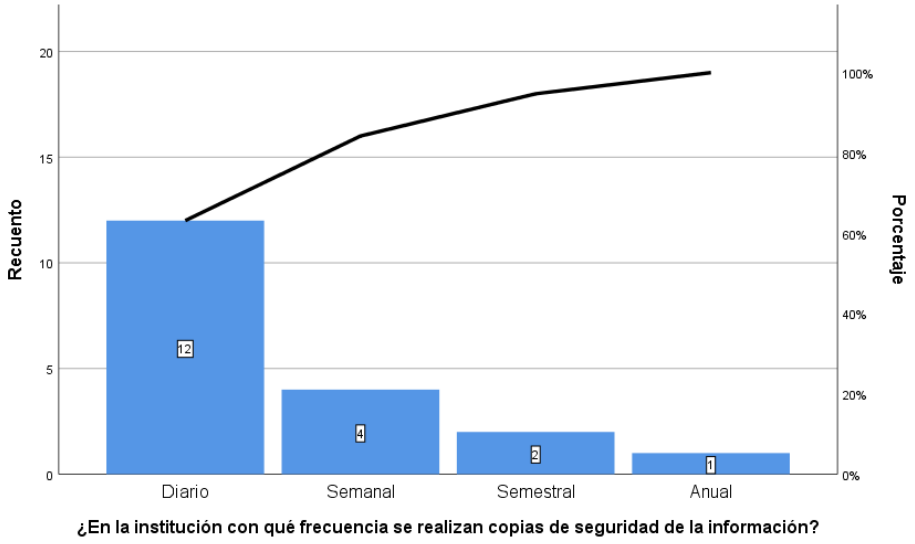


Ilustración 20 Gráfico de Pareto pregunta 16

En la Tabla 36 se muestran los resultados estadísticos de la pregunta 16 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 36 Valores estadísticos pregunta 16

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	**Anual**	1	5,3	5,3	5,3
	Diario	12	63,2	63,2	68,4
	Semanal	4	21,1	21,1	89,5
	Semestral	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Pregunta 17: ¿Con qué frecuencia se monitorean las actividades desarrolladas por los usuarios?

En los resultados para la pregunta 17 se puede observar que se monitorean actividades desarrolladas por usuarios en el 80% de casos, de forma semanal, semestral y mensual (de mayor a menor importancia), tal como se muestra en la Ilustración 21.

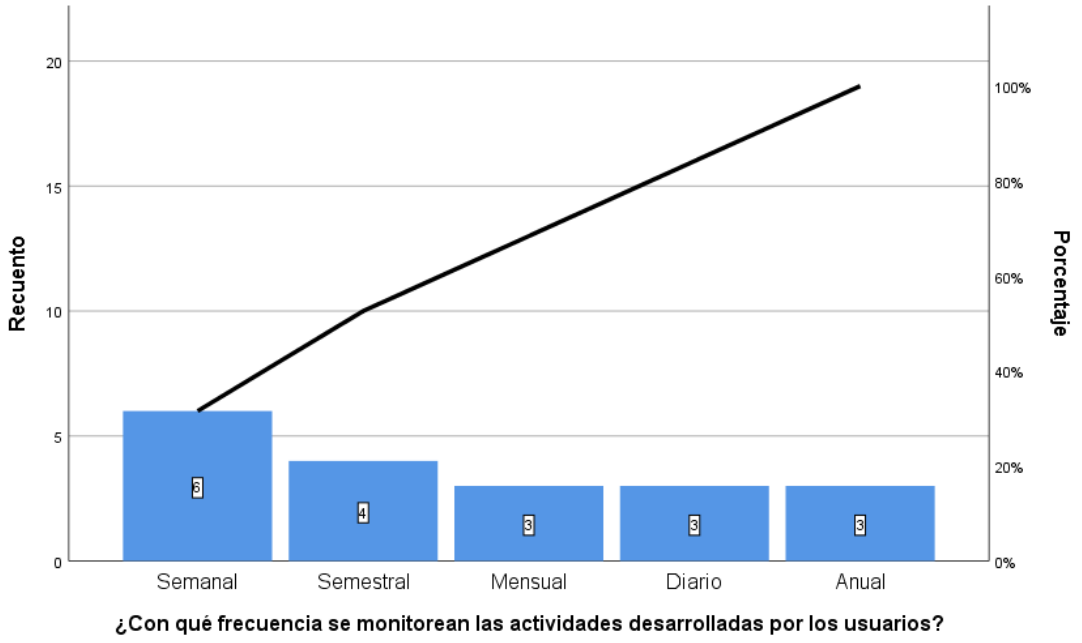


Ilustración 21 Gráfico de Pareto pregunta 17

En la Tabla 37 se muestran los resultados estadísticos de la pregunta 17 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 37 Valores estadísticos pregunta 17

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	**Anual**	3	15,8	15,8	15,8
	Diario	3	15,8	15,8	31,6
	Mensual	3	15,8	15,8	47,4
	Semanal	6	31,6	31,6	78,9
	Semestral	4	21,1	21,1	100,0
	Total	19	100,0	100,0	

Pregunta 18: ¿Existe un canal y procedimiento documentado a seguir en caso de incidentes de seguridad?

En el 84,21% de los casos no existen procedimientos para seguir en caso de que ocurran incidentes de seguridad, lo cual es una grave problemática para la adecuada gestión de la información. Este hecho se puede evidenciar en la Ilustración 22.

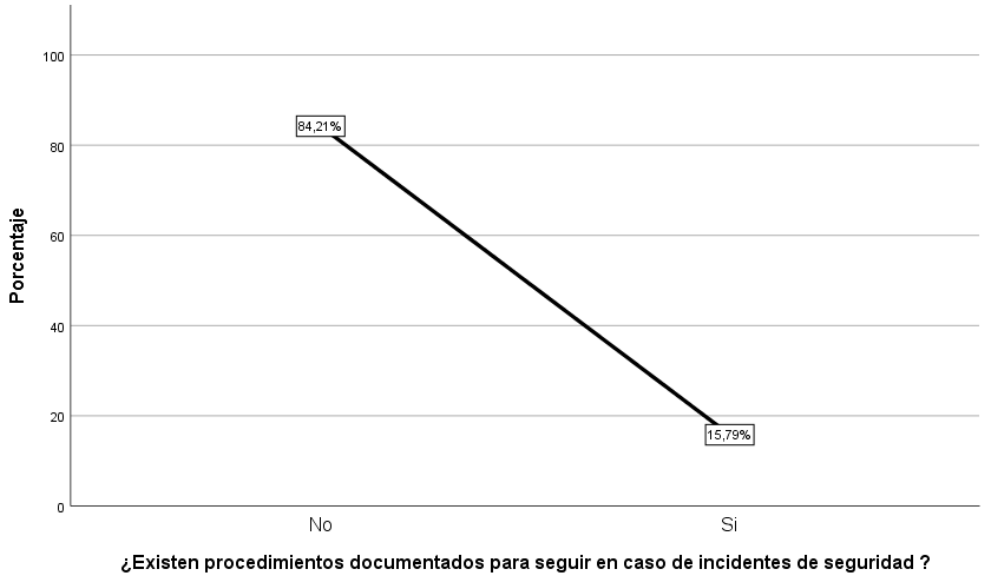


Ilustración 22 Gráfico de líneas pregunta 18

Mientras que en la Tabla 38 se muestran los resultados estadísticos de la pregunta 18 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 38 Valores estadísticos pregunta 18

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	16	84,2	84,2	84,2
	Si	3	15,8	15,8	100,0
	Total	19	100,0	100,0	

Pregunta 19: ¿Con qué frecuencia se realizan auditorías de cumplimiento de seguridad de la información?

La frecuencia con la que se realizan auditorias de cumplimiento de seguridad de la información, en al menos el 80% de los casos es rara o nunca, lo que denota una grave falta para la adecuada gestión de la información y debe ser algo a considerar (Ver Ilustración 23).

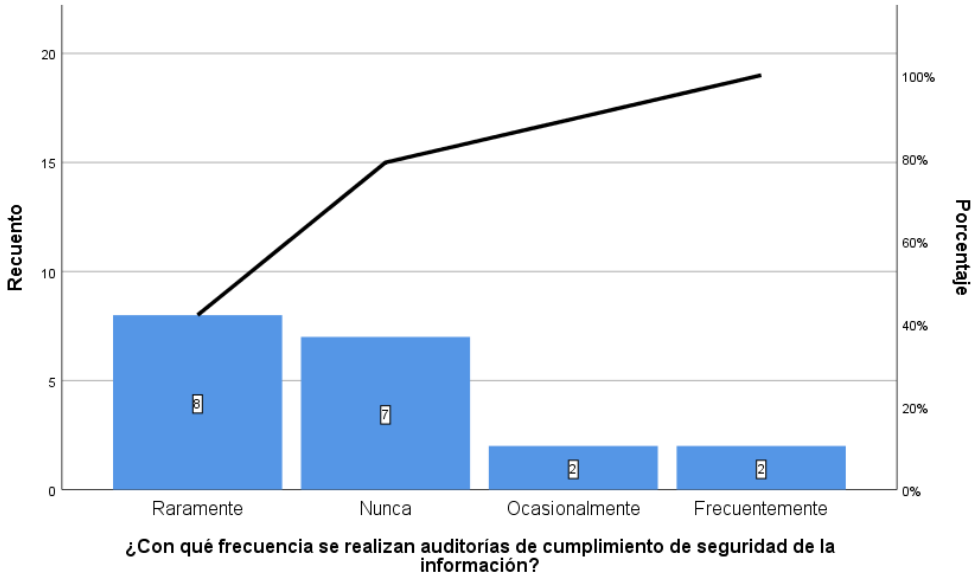


Ilustración 23 Gráfico de Pareto pregunta 19

En la Tabla 39 se muestran los resultados estadísticos de la pregunta 19 con respecto a la respuesta de las 19 IES evaluadas.

Tabla 39 Valores estadísticos pregunta 19

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Frecuentemente	2	10,5	10,5	10,5
	Nunca	7	36,8	36,8	47,4
	Ocasionalmente	2	10,5	10,5	57,9
	Raramente	8	42,1	42,1	100,0
	Total	19	100,0	100,0	

2.3 Análisis de Correlación

En el siguiente análisis y tabla, se presenta la correlación existente entre todas las preguntas en torno a la seguridad de la información existente en las IES, de todas las preguntas solo 4 tienen relevancia estadística fuerte las cuales se detallan a continuación (Ver Tabla 40).

Las preguntas que son estadísticamente significativas y poseen correlación con la pregunta principal de si las instituciones disponen de políticas para la seguridad de la información son:

- ¿Las políticas y procedimientos en seguridad de la información dentro de la institución son actualizadas periódicamente?

Esta con una significancia bilateral de 0,021, cuyo coeficiente de correlación es de 0,472, lo que indica una correlación positiva considerable, es decir que mientras posean políticas en torno a la seguridad se realizan con mayor frecuencia procedimientos de seguridad y actualización de forma más frecuente, es directamente proporcional la correlación.

- ¿Existen políticas de gestión de contraseñas para los usuarios finales de la institución?

Esta con una significancia bilateral de 0,046, cuyo coeficiente de correlación es de 0,397, lo que indica una correlación positiva baja o directamente proporcional.

- ¿Con qué periodicidad se aplican políticas y acciones de seguridad de la información sensible de la institución?

Esta con una significancia bilateral de 0,008, cuyo coeficiente de correlación es de 0,545, lo que indica una correlación positiva considerable la cual es directamente proporcional. Es decir, a mientras se posea políticas para la gestión de la información la periodicidad con la que se ejecutan acciones en torno a dicha seguridad de la información es más frecuente.

- ¿Con qué frecuencia se realizan auditorías de cumplimiento de seguridad de la información?

Esta con una significancia bilateral de 0,032, cuyo coeficiente de correlación es de 0,434, lo que indica una correlación positiva considerable la cual es directamente proporcional. Es decir, a mientras se posea políticas para la gestión de la información la frecuencia con la se realizan auditorias de cumplimiento de la seguridad de la información es mayor.

Tabla 40 Análisis de correlación de Pearson

		¿La institución dispone de políticas para la seguridad de la información?
Correlación de Pearson	¿La institución dispone de políticas para la seguridad de la información?	1,000
	¿Las políticas y procedimientos en seguridad de la información dentro de la institución son actualizadas periódicamente?	,472

	¿Existe un control de acceso a la infraestructura y servicios de TI de la institución?	-,188
	¿Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad de la información?	-,064
	¿Con qué frecuencia identifican a los usuarios que acceden a la red y las acciones que ejecutan?	,021
	Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la institución, según su cargo	,088
	¿Se realiza análisis de vulnerabilidades de los servicios web de la institución?	,114
	¿Existen políticas de gestión de contraseñas para los usuarios finales de la institución?	,397
	¿Con qué periodicidad se aplican políticas y acciones de seguridad de la información sensible de la institución?	,545
	¿Con qué periodicidad se aplican planes de monitoreo y gestión de impacto de incidentes de seguridad en la institución?	,190
	¿Con qué frecuencia la institución actualiza y aplica las políticas de acceso a la información en base a los roles de usuario existentes?	,335
	¿Con qué frecuencia la institución clasifica y cifra la información?	,248
	¿Con qué frecuencia se actualiza y documenta el inventario de todos los activos de TI?	-,303
	¿La institución dispone de una acreditación en seguridad de la información para todos sus sistemas informáticos?	,102
	¿La institución dispone de aplicaciones para proteger de software malicioso a todas sus soluciones informáticas?	,215
	¿En la institución con qué frecuencia se realizan copias de seguridad de la información?	,264
	¿Con qué frecuencia se monitorean las actividades desarrolladas por los usuarios?	-,251
	¿Existen procedimientos documentados para seguir en caso de incidentes de seguridad?	-,208
	¿Con qué frecuencia se realizan auditorías de cumplimiento de seguridad de la información?	,434
Sig. (unilateral)	¿La institución dispone de políticas para la seguridad de la información?	.

	¿Las políticas y procedimientos en seguridad de la información dentro de la institución son actualizadas periódicamente?	,021
	¿Existe un control de acceso a la infraestructura y servicios de TI de la institución?	,221
	¿Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad de la información?	,398
	¿Con qué frecuencia identifican a los usuarios que acceden a la red y las acciones que ejecutan?	,466
	Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la institución, según su cargo	,360
	¿Se realiza análisis de vulnerabilidades de los servicios web de la institución?	,322
	¿Existen políticas de gestión de contraseñas para los usuarios finales de la institución?	,046
	¿Con qué periodicidad se aplican políticas y acciones de seguridad de la información sensible de la institución?	,008
	¿Con qué periodicidad se aplican planes de monitoreo y gestión de impacto de incidentes de seguridad en la institución?	,218
	¿Con qué frecuencia la institución actualiza y aplica las políticas de acceso a la información en base a los roles de usuario existentes?	,081
	¿Con qué frecuencia la institución clasifica y cifra la información?	,153
	¿Con qué frecuencia se actualiza y documenta el inventario de todos los activos de TI?	,104
	¿La institución dispone de una acreditación en seguridad de la información para todos sus sistemas informáticos?	,339
	¿La institución dispone de aplicaciones para proteger de software malicioso a todas sus soluciones informáticas?	,188
	¿En la institución con qué frecuencia se realizan copias de seguridad de la información?	,137
	¿Con qué frecuencia se monitorean las actividades desarrolladas por los usuarios?	,150
	¿Existen procedimientos documentados para seguir en caso de incidentes de seguridad?	,196
	¿Con qué frecuencia se realizan auditorías de cumplimiento de seguridad de la información?	,032

CAPÍTULO III

Resultados

3.1 Informe técnico de la evaluación de la seguridad de la información de las IES

El capítulo tres aborda los puntos estratégicos de la ISO 27000 con los que se evaluó a las IES y resume los problemas y recomendaciones asociados a políticas para la seguridad de la información, control de acceso, seguridad ligada a los recursos humanos, seguridad en la operativa, gestión de incidentes, cifrado, gestión de activos y cumplimiento.

3.1.1 Políticas para la seguridad de la información.

De acuerdo con la evaluación aplicada a las IES de la Zona 1 del Ecuador, el 15,79% de instituciones no cuenta con políticas para la seguridad de la información, lo que conlleva a una serie de riesgos asociados a daños físicos, pérdida de servicios esenciales, afectaciones por radiación, acceso a la información, fallos técnicos, acciones no autorizadas y/o errores de las funciones. Todo esto se debe a que el usuario no conoce qué se puede hacer o cómo hacer sus labores sin vulnerar la información y actuarán bajo distintos comportamientos según su propio criterio.

Para las IES que no cuentan con políticas para la seguridad de la información se recomienda la implementación de políticas que deben estar aprobadas por la dirección, publicadas y comunicadas con todo el personal interno, así como a todo al personal externo que sea relevante, las políticas deben ser revisadas y actualizadas con regularidad para garantizar su idoneidad, adecuación y efectividad (Internacional Organization for Standardization, 2013f).

El 84,21% de IES que disponen de políticas enfocadas en la seguridad de la información se debe asegurar que los directores garanticen que todos los procedimientos de seguridad dentro del área tecnológica se llevan a cabo correctamente para lograr el cumplimiento de las políticas y normas de seguridad vigentes, considerando acciones de control en los sistemas de información con el fin de verificar periódicamente que se cumplan e implementen las políticas de seguridad (Benítez, 2016).

En este contexto, de las instituciones que cuentan con políticas se conoce que el 31,6% de IES actualiza periódicamente las políticas y procedimientos en seguridad de la información, mientras que el 10,5% nunca o raramente lo hace, lo que significa que la

información y procedimientos para la seguridad no están actualizados reduciendo así la efectividad de las políticas.

3.1.2 Control de acceso

El objetivo de este punto es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento (Internacional Organization for Standardization, 2013b). En el estudio se puede observar que el 15,79% de IES evaluadas no cuenta con un control de acceso a infraestructura y servicios de TI de la institución, esto genera una falta de control de accesos a la información, los recursos de tratamiento de la información y los procesos de negocio y permite la materialización de potenciales amenazas como la pérdida de servicios esenciales, compromete la seguridad de la información y abuso de funciones.

El 84,21% de IES cuenta con los controles necesarios para el cumplimiento de este punto como: requisitos del negocio para el control de acceso, gestión del acceso de usuarios, responsabilidades de los usuarios, control de acceso a redes, control de acceso a aplicaciones e información y control de acceso en computación móvil y trabajo remoto. De esta manera las IES controlan el acceso a la información, aseguran el acceso solamente a usuarios autorizados a infraestructura, área tecnológica y sistemas de información, fomentan las buenas prácticas de seguridad en los usuarios, evitan el acceso no autorizado a servicios de red y garantizan la seguridad de la información cuando se usan dispositivos móviles o se hace trabajo remoto (Benítez, 2016).

3.1.3 Seguridad ligada a los recursos humanos

En este apartado se tiene la concienciación, educación y capacitación a usuarios, colaboradores y personal en temas de seguridad de la información, con el fin de educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad (Internacional Organization for Standardization, 2013b).

En este contexto se logró determinar que sólo el 15,8% de IES evaluadas capacita a los involucrados de forma frecuente y existe el 5,3% de instituciones que nunca lo han hecho, las IES deben trabajar más en reducir los riesgos relacionados al error humano que la mayoría de veces se cometen por el desconocimiento de los procedimientos y políticas de seguridad, como requisito se debería recalcar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Para asegurar el cumplimiento de este apartado todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

3.1.4 Seguridad en la operativa

Es importante controlar y evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, para ello se realizan análisis de vulnerabilidades y monitoreo de necesidades de capacidad de los sistemas en operación (Internacional Organization for Standardization, 2019).

En este apartado el 80% de respuestas proporcionadas por las instituciones evaluadas son frecuente y ocasionalmente, lo que significa que se podría mejorar realizando estos controles de forma periódica, ya que dentro de este grupo el 52,6% de IES evaluadas hace análisis y control de vulnerabilidades de servicios web de manera frecuente y el 26,3% ocasionalmente. También se puede observar que el 5,3% de IES nunca han hecho una valoración de sus sistemas desde su implementación, por lo que se reduce la seguridad y no se considera los peligros de los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización.

3.1.5 Gestión de incidentes de seguridad de la información

La gestión de incidentes tiene como objetivo garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados oportunamente para aplicar acciones correctivas a tiempo. Las IES cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad por lo que resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares (Internacional Organization for Standardization, 2013e).

En las IES evaluadas, el 80% ejecutan planes de monitoreo y gestión de impacto de incidentes de seguridad en la institución de forma ocasional y raramente, esta última es alarmante ya que se debería hacer por lo menos de forma ocasional, para que todos los empleados, contratistas y terceros estén al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales.

Dentro de los controles que las IES deben considerar para cumplir con el apartado están los relacionados a las responsabilidades y procedimientos de gestión, notificación de eventos de seguridad, notificación de puntos débiles, valoración de eventos de seguridad, respuesta a los incidentes de seguridad, aprendizaje de los incidentes de seguridad y la recopilación de evidencias.

3.1.6 Cifrado

El uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado asegura una adecuada protección de su confidencialidad e integridad. La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas (Internacional Organization for Standardization, 2013a).

En las IES evaluadas los resultados son alarmantes porque solo el 10,5% clasifica y cifra la información de manera frecuente, mientras que las restantes los hacen con menos frecuencia y el 26,3% nunca lo hace, lo que genera una falta de protección o control en la gestión de la información y permite la materialización de potenciales amenazas como pérdida de servicios esenciales principalmente telecomunicaciones, intercepción, espionaje en remoto, robo de equipos, recuperación desde medios reciclados o desechados, divulgación, manipulación de software y acciones no autorizadas.

Como recomendaciones se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información y gestionar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas.

3.1.7 Gestión de activos

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada por la propia institución (Internacional Organization for Standardization, 2013d).

En este apartado el 63,2% de IES evaluadas actualiza y documenta el inventario de todos los activos de TI, el resto de las instituciones lo hace de forma ocasional y raramente, con este índice se puede asegurar que la falta de inventario de activos de información y un proceso de actualizado asociado permite el descontrol ya que no se sabe qué activos son de

la organización, su estado y las personas a su cuidado específico. Para mejorar este aspecto se recomienda que todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

3.1.8 Cumplimiento

En este aspecto el objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la institución y/o al personal que incurra en responsabilidad civil o penal como resultado de incumplimientos, para ellos se debe revisar la seguridad de la información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información (Internacional Organization for Standardization, 2013c).

En consecuencia, el porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados son un indicador de cumplimiento y en este contexto solamente el 10,5% de las IES evaluadas realizan auditorías de cumplimiento de forma frecuente y ocasional, lo que denota una grave falta para la adecuada gestión de la información y debe ser algo a considerar.

CONCLUSIONES

La seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio. A los riesgos hay que analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso, por lo que es importante tomar en cuenta todo lo que se debe proteger y el procedimiento a seguir para garantizar la seguridad, desde identificar los mecanismos de seguridad informática y su clasificación, así como los tipos de vulnerabilidades y riesgos considerando los pilares de la seguridad que en conjunto protegen los activos informáticos de las organizaciones y sus usuarios.

Conocer la situación actual sobre la seguridad de la información en las IES de la Zona 1 del Ecuador permitió aclarar el panorama e identificar los puntos estratégicos del manejo de la seguridad y con lo que cuenta cada una de ellas dentro de esta área, considerando temas como: las políticas de seguridad, gestión de activos, control de acceso, cifrado, cumplimiento de normativa, entre otros. A partir de aquí se estableció las preguntas de evaluación ejecutadas en este proyecto.

La identificación de los pilares y las métricas que influyen en la seguridad de la información brindan a los departamentos de tecnologías de las IES una guía para evaluar, controlar y gestionar los aspectos relevantes para que en un futuro se implementen medidas y toma de decisiones con resultados óptimos en la gestión de la información, lo que asegura confiabilidad y eficiencia en los procesos.

Al analizar los resultados obtenidos e identificar las métricas de seguridad, se concluye que sirven para identificar y evaluar la seguridad dentro de las diferentes instituciones en las cuales se resguardan una gran cantidad de datos; además del gran impacto que generan a la hora de identificar vulnerabilidades para así realizar un correcto seguimiento de auditoría y evaluaciones de riesgo, lo cual permite la toma de decisiones pertinentes para mantener una seguridad eficiente dentro las instituciones.

RECOMENDACIONES

Todos los involucrados en la seguridad informática deben conocer y garantizar que los procedimientos y actividades a seguir brinden resultados óptimos y eficientes en la toma de decisiones para salvaguardar la información crítica de la Institución y sus usuarios, por lo que se recomienda la implementación de estándares de seguridad informática en los que se consideren las métricas obtenidas en el proyecto de investigación, con el fin de garantizar la seguridad de la información bajo los pilares que aseguran la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Se recomienda hacer un análisis de la situación actual dentro de las IES para lograr identificar puntos clave que garanticen el cumplimiento de los objetivos dentro del proyecto de investigación, además conocer cómo se manejan y gestionan las instituciones todos los aspectos relevantes a la seguridad de la información.

Una evaluación de seguridad informática debe ser usado por todos los involucrados en el proceso, como instrumento para considerar los puntos de mejora en base al hallazgo de vulnerabilidades y amenazas. La omisión de ciertas métricas en la seguridad informática altera considerablemente el nivel de seguridad que manejan en las instituciones.

Se recomienda el diseño e implementación de una aplicación web o/y móvil de la propuesta de evaluación de la seguridad de la información como trabajo futuro y continuación del proyecto de investigación del que es parte este trabajo de titulación.

BIBLIOGRAFÍA

Ahmed, M., & Pathan, A.-S. K. (2020). False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, *8*(1), 4. https://doi.org/10.1186/s40294-020-00070-w

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2020). 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*. https://doi.org/10.1016/j.jksuci.2020.09.011

Alcaraz Velasco, F., Palomares, J. M., & Olivares, J. (2021). Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs. *Computer Networks*, *199*, 108470. https://doi.org/10.1016/j.comnet.2021.108470

Alhassan, M. M., & Adjei-Quaye, A. (2017). Information Security in an Organization. *International Journal of Computer (IJC)*, *February*.

Altamirano, M., & Luca, D. (2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. 21*(2), 248–263.

Andersson, J., Grassi, V., Mirandola, R., & Perez-Palacin, D. (2021). A conceptual framework for resilience: fundamental definitions, strategies and metrics. *Computing*, *103*(4), 559–588. https://doi.org/10.1007/s00607-020-00874-x

Baca Urbina, G. (2016). *Introducción a la Seguridad informática* (Primera ed). Grupo Editorial Patria.

Baldi, M., Maturo, N., Ricciutelli, G., & Chiaraluce, F. (2019). Physical layer security over fading wiretap channels through classic coded transmissions with finite block length and discrete modulation. *Physical Communication*, *37*, 100829. https://doi.org/10.1016/j.phycom.2019.100829

Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using information theory metrics–An empirical investigation. *Computer Communications*, *103*, 18–28. https://doi.org/10.1016/j.comcom.2017.02.003

Behal, S., Kumar, K., & Sachdeva, M. (2021). D-FAC: A novel ϕ-Divergence based distributed DDoS defense system. *Journal of King Saud University - Computer and Information Sciences*, *33*(3), 291–303. https://doi.org/10.1016/j.jksuci.2018.03.005

Benassini, M. (2009). Introdución a la Investigación de mercados. In *McGraw-Hill Interamericana*.

Benítez, D. (2016). *Revisión bibliográfica de la Norma ISO 27001 y sus componentes*. https://repository.usta.edu.co/bitstream/handle/11634/22099/2016davidbenitez.pdf?sequence=1&isAllowed=y

Bokharaie, V. S., & Jahanian, A. (2020). Side-channel leakage assessment metrics and methodologies at design cycle: A case study for a cryptosystem. *Journal of Information Security and Applications*, *54*, 102561. https://doi.org/10.1016/j.jisa.2020.102561

Breda, G., & Kiss, M. (2020). Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. *Procedia Manufacturing*, *46*, 580–590. https://doi.org/10.1016/j.promfg.2020.03.084

Cajas, F., & Luje, A. (2019). *EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA INFORMÁTICA BASADO EN SU RIESGO INHERENTE*. Universidad de las Fuerzas Armadas ESPE.

Calderon Arateco, L. L. (2004). Seguridad informatica y Seguridad de Informacion. *Universidad Piloto de Colombia.*

Cheng, J., Goto, Y., Morimoto, & Horie, D. (2008). A security engineering environment based on ISO/IEC standards: Providing standard, formal, and consistent supports for design, development, operation, and maintenance of secure information systems. *Proceedings of the 2nd International Conference on Information Security and Assurance*, 350–354. https://doi.org/10.1109/ISA.2008.106.

Cho, C.-S., Chung, W.-H., & Kuo, S.-Y. (2016). Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *46*(3), 356–369. https://doi.org/10.1109/TSMC.2015.2452897

Co-operation, O. F. O. R. E. (2002). GUÍAS DE LA OCDE PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y REDES. *ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT*, 12.

Cristiá, M. (2021). *Seguridad Informática*.

de la Rosa, M. (2021). *Automation of an information security management system based on the ISO / IEC 27001 Standard*.

Deng, D., Li, X., Fan, L., Zhou, W., Qingyang Hu, R., & Zhou, Z. (2017). Secrecy Analysis of Multiuser Untrusted Amplify-and-Forward Relay Networks. *Wireless Communications and Mobile Computing*, *2017*, 1–11. https://doi.org/10.1155/2017/9580639

Dhanaraj, R. K., Ramakrishnan, V., Poongodi, M., Krishnasamy, L., Hamdi, M., Kotecha, K.,

& Vijayakumar, V. (2021). Random Forest Bagging and X-Means Clustered Antipattern Detection from SQL Query Log for Accessing Secure Mobile Data. *Wireless Communications and Mobile Computing*, *2021*, 1–9. https://doi.org/10.1155/2021/2730246

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4). https://doi.org/10.1016/J.JSIS.2021.101693

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*. https://doi.org/doi.org/10.1016/J.COSE.2020.101747

Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. *Ministerio de Hacienda y Administraciones Publicas*, *3*, 127.

Domingo-Ferrer, J., Muralidhar, K., & Bras-Amoros, M. (2020). General Confidentiality and Utility Metrics for Privacy-Preserving Data Publishing Based on the Permutation Model. *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/TDSC.2020.2968027

Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2020). HARMer: Cyber-Attacks Automation and Evaluation. *IEEE Access*, *8*, 129397–129414. https://doi.org/10.1109/ACCESS.2020.3009748

Enoch, S. Y., Lee, J. S., & Kim, D. S. (2021). Novel security models, metrics and security assessment for maritime vessel networks. *Computer Networks*, *189*, 107934. https://doi.org/10.1016/j.comnet.2021.107934

Eom, T., Hong, J. B., An, S., Park, J. S., & Kim, D. S. (2019). A Systematic Approach to Threat Modeling and Security Analysis for Software Defined Networking. *IEEE Access*, *7*, 137432–137445. https://doi.org/10.1109/ACCESS.2019.2940039

Escrivá Gema, Romero Rosa, Ramada David, & Onrubia Ramón. (2013). *Seguridad Informática* (Ramos Luis Ángel (ed.)). MACMILLAN IBERIA.

Espinoza, E. E. (2018). Las variables y su operacionalización en la investigación educativa. Parte I. *Revista Conrado*, *14*(65), 39–49.

Fal', A. M. (2010). Standardization in information security management. *Cybernetics and Systems Analysis*, *46*(3), 512–515. https://doi.org/10.1007/s10559-010-9227-9

Fal', O. M. (2017). Standardization in Information Technology Security. *Cybernetics and Systems Analysis*, *53*(1), 78–82. https://doi.org/10.1007/s10559-017-9908-8

Falco, G., Caldera, C., & Shrobe, H. (2018). IIoT Cybersecurity Risk Modeling for SCADA Systems. *IEEE Internet of Things Journal*, *5*(6), 4486–4495. https://doi.org/10.1109/JIOT.2018.2822842

Fang, Y., Jian, Z., Jin, Z., Xie, X., Lu, Y., & Li, T. (2021). Fast Policy Interpretation and Dynamic Conflict Resolution for Blockchain-Based IoT System. *Wireless Communications and Mobile Computing*, *2021*, 1–14. https://doi.org/10.1155/2021/9968743

Fernández, A., & Llorens, F. (2011). *Gobierno de las TI para universidades*. Conferencia de Rectores de las Universidades Españolas (CRUE).

Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación*. McGraw Hill Education.

Fikri, M. Al, Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Florentino, A. C. B., Barbalho, S. C. M., & Machado, R. C. S. (2021). Proposal and Validation of a Standard Protection Profile for Homologation of Commercial Videoconferencing Equipment. *IEEE Access*, *9*, 24288–24304. https://doi.org/10.1109/ACCESS.2021.3056491

Gallego Ramos, J. R. (2018). Cómo se construye el marco teórico de la investigación. *Cadernos de Pesquisa*, *48*(169), 830–854. https://doi.org/10.1590/198053145177

Gebremichael, T., Ledwaba, L., Eldefrawy, M., Hancke, G., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access*, 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937

Gladden, M. E. (2017). An Introduction to Information Security in the Context of Advanced Neuroprosthetics. In *The Handbookof Information Security for Advanced Neuroprothestics* (Second Edi, Issue February).

Gómez Enciso, E., & Porras Flores, E. E. (2018). Modelo de evaluación de seguridad para transmitir datos usando Web Services. *Industrial Data*, *21*(1), 123.

https://doi.org/10.15381/idata.v21i1.14927

González Guitián, M. V., & Ponjuán Dante, G. (2014). Metodologías y modelos para auditar la información: Análisis reflexivo. *Revista General de Informacion y Documentacion*, *24*(2), 233–253. https://doi.org/10.5209/rev_RGID.2014.v24.n2.47402

Guamán, V. (2019). *EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3* [Universidad Técnica del Norte]. http://repositorio.utn.edu.ec/bitstream/123456789/9535/2/04 ISC 524 TRABAJO DE GRADO.pdf

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, *103*, 102196. https://doi.org/10.1016/j.cose.2021.102196

Gungor, O., & Koksal, C. (2016). On the basic limits of rf- fingerprint-based authentication. *IEEE Transactions on Information Theory*, *62*(8), 4523–4543. https://doi.org/10.1109/TIT.2016.2572725

Guo, J., & Wang, L. (2020). Learning to upgrade internet information security and protection strategy in big data era. *Computer Communications*, *160*, 150–157. https://doi.org/10.1016/j.comcom.2020.05.043

Hadlington, L., Binder, J., & Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, *114*, 106557. https://doi.org/10.1016/j.chb.2020.106557

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications*, *33*, 55–65. https://doi.org/10.1016/j.jisa.2017.01.007

Halvorsen, J., Waite, J., & Hahn, A. (2019). Evaluating the Observability of Network Security Monitoring Strategies With TOMATO. *IEEE Access*, *7*, 108304–108315. https://doi.org/10.1109/ACCESS.2019.2933415

Hassandoust, F., Subasinghage, M., & Johnston, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information & Management*, *59*(1), 103574. https://doi.org/10.1016/j.im.2021.103574

Heigl, M., Anand, K. A., Urmann, A., Fiala, D., Schramm, M., & Hable, R. (2021). On the Improvement of the Isolation Forest Algorithm for Outlier Detection with Streaming

Data. *Electronics*, *10*(13), 1534. https://doi.org/10.3390/electronics10131534

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society*, *44*, 30–38. https://doi.org/10.1016/j.techsoc.2015.11.007

Hohan, A. I., Olaru, M., & Pirnea, I. C. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, *32*(15), 352–359. https://doi.org/10.1016/s2212-5671(15)01404-5

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Hong, J., Enoch, S., Kim, D., Nhlabatsi, A., Fetais, N., & Khan, K. (2018). Dynamic security metrics for measuring the effectiveness of moving target defense techniques. *Computers & Security*, *79*, 33–52. https://doi.org/10.1016/J.COSE.2018.08.003

Hsu, C., Harn, L., Xia, Z., & Zhang, M. (2020). Non-Interactive Dealer-Free Dynamic Threshold Secret Sharing Based on Standard Shamir's SS for 5G Networks. *IEEE Access*, *8*, 203965–203971. https://doi.org/10.1109/ACCESS.2020.3035278

Humphreys, E. (2011). Information security management system standards. *Datenschutz Und Datensicherheit - DuD*, *35*(1), 7–11. https://doi.org/10.1007/s11623-011-0004-3

IBM. (2021). *Software IBM SPSS*. https://www.ibm.com/es-es/analytics/spss-statistics-software

IEEE Staff. (2009). *International Carnahan Conference on Security Technology*.

INCIBE. (2018, December). *Sigue estas recomendaciones para almacenar tu información en la nube* | *INCIBE*. INCIBE.

Instituto Nacional de Ciberseguridad. (2010). *Colección Protege tu Empresa*.

Internacional Organization for Standardization. (2013a). *Cifrado*. Anexo 10 - ISO 27001. https://www.iso27000.es/iso27002_10.html

Internacional Organization for Standardization. (2013b). *Control de accesos*. Anexo 9 - ISO 27001. https://www.iso27000.es/iso27002_9.html

Internacional Organization for Standardization. (2013c). *Cumplimiento*. Anexo 18 - ISO 27001. https://www.iso27000.es/iso27002_18.html

Internacional Organization for Standardization. (2013d). *Gestión de activos*. Anexo 8 - ISO

27001. https://www.iso27000.es/iso27002_8.html

Internacional Organization for Standardization. (2013e). *Gestón de incidentes de seguridad de la información*. Anexo 16 - ISO 27001. https://www.iso27000.es/iso27002_16.html

Internacional Organization for Standardization. (2013f). *Políticas de Seguridad*. Anexo 5 - ISO 27001. https://www.iso27000.es/iso27002_5.html

Internacional Organization for Standardization. (2015). ISO 9000:2015 Sistemas de Gestion de la calidad. —Fundamentos y vocabulario. *Secretaria Central de ISO*, *2015*, 58.

Internacional Organization for Standardization. (2019). *Seguridad en la Operativa*. Anexo 12 - ISO 27001. https://www.iso27000.es/iso27002_12.html

Jiang, Y., & Atif, Y. (2021). A selective ensemble model for cognitive cybersecurity analysis. *Journal of Network and Computer Applications*, *193*, 103210. https://doi.org/10.1016/j.jnca.2021.103210

Karie, N., Sahri, N., Yang, W., Valli, C., & Kebande, V. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE*, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886

Karlsson, F., Kolkowska, E., & Petersson, J. (2022). Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis. *Computers & Security*, *114*, 102578. https://doi.org/10.1016/j.cose.2021.102578

Khaleel, A. H., & Abduljaleel, I. Q. (2021). A novel technique for speech encryption based on k-means clustering and quantum chaotic map. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 160–170. https://doi.org/10.11591/eei.v10i1.2405

Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *International Journal of Information Management Data Insights*, *1*(2), 100015. https://doi.org/10.1016/j.jjimei.2021.100015

Kisan, S., & Rao, D. C. (2020). *Information Security Lecture Notes for Bachelor of Technology in Information Technology*.

Knight, S., Buffett, S., & Hung, P. C. K. (2007). The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services. *International Journal of Information Security*, *6*(5), 285–286. https://doi.org/10.1007/s10207-007-0036-8

Kure, H., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management

Approach for a Cyber-Physical System. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

López, A. (2014). Seguridad Informática. In *2014*. RA-MA.

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, *112*, 102526. https://doi.org/10.1016/j.cose.2021.102526

Meriah, I., & Arfa Rabai, L. Ben. (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

Mesquida, A., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers and Security*, *48*, 19–34. https://doi.org/10.1016/j.cose.2014.09.003.

Mesquida, A., Mas, A., Feliu, S., & Arcilla, M. (2014). Integración de Estándares de Gestión de TI mediante MIN-ITs. *Revista Iberica de Sistemas e Tecnologias de Informacao*, 31–45. https://doi.org/10.4304/risti.e1.31-45

Min Shum, Y. (2020, May 27). *Escala de Likert – ¿Qué es? ¿Cómo se usa? ¿Dónde se utiliza?* Yi Min Shum Xie. https://yiminshum.com/escala-likert-investigacion/

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers and Security*, *109*. 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

Montenegro Marín, C. E., Gaona García, E. E., & Gaona García, P. A. (2011). Plataforma de seguridad basado en autenticidad de contenidos sobre conjunto de especificaciones SCORM. *Ingeniería Y Competitividad*, *12*(2), 51–68. https://doi.org/10.25100/iyc.v12i2.2693

Mtra, T., & Cibrián, C. (2016). Escalas de actitud para evaluar la personalidad de los personajes publicitarios. *Revista Digital de Diseño Gráfico*, *16*, 10.

Muñoz, I. (2020, July 10). *La importancia de la Seguridad de la Información*. Posgrados IBERO. https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Naciones Unidas. (2018). *La Agenda 2030 y sus Objetivos de Desarrollo Sostenible*.

Ogbanufe, O. (2021). Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computers & Security*, *108*, 102340. https://doi.org/10.1016/j.cose.2021.102340

Osborne, M. (2006). Information Security Standards and Audits. In *How to Cheat at Managing Information Security* (pp. 87–110). Elsevier. https://doi.org/10.1016/B978-159749110-5/50012-9

Padilla R., Cadena S., Córdova J., Enríquez R., L.-L. F. (2019). *Estado De Las Tecnologías De Información Y Comunicación (Tic) En El Sistema Universitario Ecuatoriano – Uetic 2018* (Vol. 2).

Peltier, T. (2001). *Information Security Policies, Procedures, and Standardss: Guidelines for ...* Thomas R. Peltier. https://books.google.com.ec/books?hl=es&lr=&id=mM_LsS-W4f4C&oi=fnd&pg=PP1&dq=standards+in+information+security&ots=WhTYn3jAgg&sig=D7GOca3Eh_BT-%0AjQGyADaU6eYXP0&redir_esc=y#v=onepage&q=standards in information security&f=false

Philippou, E., Frey, S., & Rashid, A. (2020). Contextualising and aligning security metrics and business objectives: A GQM-based methodology. *Computers & Security*, *88*, 101634. https://doi.org/10.1016/j.cose.2019.101634

Ponemon Institute. (2018). *2018 Study on Global Megatrends in Cybersecurity*. *February*.

Ramos, A., Lazar, M., Filho, R., & Rodrigues, J. (2017). Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys and Tutorials*, *19*(4), 2704–2734. https://doi.org/10.1109/COMST.2017.2745505

Ranaweera, P., Jurcut, A., & Liyanage, M. (2022). MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. *ACM Computing Surveys*, *54*(9), 1–37. https://doi.org/10.1145/3474552

Restrepo Ortiz, G. E., & Zabala Mendoza, D. E. (2016). Indicadores de gestión para proyectos de investigación y extensión en instituciones de Educación Superior. *Revista Ciencias Estratégicas*, *24*(36), 451–461. https://doi.org/10.18566/rces.v24n36.a13

Rhee, H., Kim, C., & Ryu, Y. (2009). Self-efficacy in information security: Its influence on end

users' information security practice behavior. *Comput. Secur.*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. In *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Primera Ed). https://doi.org/10.17993/ingytec.2018.46

Rosendo, V. (2018). *Investigación de mercados* (E. EDITORIAL (ed.); Primera ed).

Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers & Security*, *108*, 102306. https://doi.org/10.1016/j.cose.2021.102306

Shan, C., Jiang, B., Xue, J., Guan, F., & Xiao, N. (2018). An Approach for Internal Network Security Metric Based on Attack Probability. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/3652170

Shrivastava, U., Song, J., Han, B. T., & Dietzman, D. (2021). Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *International Journal of Medical Informatics*, *148*, 104401. https://doi.org/10.1016/j.ijmedinf.2021.104401

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Suhaimi, A. I. H., Goto, Y., & Cheng, J. (2014). *An Engineering Environment Based on ISO/IEC 27000 Series Standards for Supporting Organizations with ISMSs* (pp. 195–201). https://doi.org/10.1007/978-3-642-55038-6_30

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers and Security*, *90*, 101709. https://doi.org/10.1016/j.cose.2019.101709

Tarazona, C. H. (2015). *Amenazas Informáticas y seguridad de la informacion*. 137–146.

Thuraisingham, B., & Gritzalis, S. (2010). Information and communications security, privacy and trust: Standards and regulations. *Computer Standards & Interfaces*, *32*(5–6), 229. https://doi.org/10.1016/j.csi.2010.04.001

Vila López, N., Küster Boluda, I., & Aldás-Manzano, J. (2000). Desarrollo y validación de

escalas de medida en Marketing. *Análisis de Datos Multivariable*, *January*, 1–22.

Wagner, I., & Eckhoff, D. (2019). Technical Privacy Metrics. *ACM Computing Surveys*, *51*(3), 1–38. https://doi.org/10.1145/3168389

Wang, C.-H., & Tsai, D.-R. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. *43rd Annual 2009 International Carnahan Conference on Security Technology*, 265–267. https://doi.org/10.1109/CCST.2009.5335527

Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2). http://www.misq.org/misreview/announce.html

Zhou, G., Tian, X., & Zhou, A. (2022). Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images. *Frontiers of Computer Science*, *16*(4). https://doi.org/10.1007/s11704-021-0450-5

Zubareva, E., & Byelovb, S. (2016). New tools of cybernetics, informatics, computer engineering, and systems analysis: Electronic government system of ukraine and a method for increasing its security. *IEEE*. https://doi.org/10.1007/s10559-015-9739-4