ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Implementación de políticas para la gestión de riesgos de seguridad en el manejo de la información académica de la Empresa Pública ESPOCH CONDUESPOCH EP.

CARLOS ERNESTO GUFFANTTE NARANJO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA- ECUADOR

NOVIEMBRE – 2023

DECLARACIÓN DE AUTENTICIDAD Y CESIÓN DE DERECHOS DE AUTOR

Yo, Carlos Ernesto Guffantte Naranjo, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría, el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, noviembre de 2023

Carlos Ernesto Guffantte Naranjo
No. Cédula. 060215591-3

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y desarrollo**, denominado: **Implementación de políticas para la gestión de riesgos de seguridad en el manejo de la información académica de la Empresa Pública ESPOCH CONDUESPOCH EP.**, de responsabilidad del señor Carlos Ernesto Guffantte Naranjo, ha sido minuciosamente revisado por los Miembros de Tribunal del trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal autoriza su presentación.

Ing. Oswaldo Geovanny Martínez Guashima M. Sc.
PRESIDENTE

Ing. Washington Gilberto Luna Encalada Ph.D.
DIRECTOR

Ing. Raúl Marcelo Lozada Yánez. Mgtr.
MIEMBRO

Ing. Gladys Lorena Aguirre Sailema Mgtr.
MIEMBRO

Riobamba, noviembre de 2023

DEDICATORIA

Dedico este trabajo a mis abuelitos (+) Mamita Pía y Papito Ángel quienes desde un principio se preocuparon por que logre grandes cosas en mi vida. A mi querida madre Charito Naranjo como todos la conocen por ser quien siempre se preocupa de nosotros a mi amado padre (+) Rafel Guffantte, de manera muy especial a mi querida esposa Pilita y a mis dos hijos hermosos Carlitos y Dayanita quienes día a día están junto a mí brindándome su amor y llenándome de orgullo con sus logros.

Carlos.

AGRADECIMIENTO

Con mucho cariño y respeto a mí querida Escuela Superior Politécnica de Chimborazo, a la Escuela de Postgrado y Educación Continua, a todos los docentes que incondicionalmente compartieron sus conocimientos, de manera muy particular al Ing. Oswaldo Martínez coordinador de la maestría por sus atenciones durante todo este proceso, un agradecimiento a mi director de Tesis Ing. Washington Luna. PhD y Miembros de Tribunal Ing. Raúl Lozada. Mgtr. e Ing. Lorena Aguirre. Mgtr.

Carlos.

TABLA DE CONTENIDO

RESUMEN ..... **xii**
SUMMARY ..... **xiii**

CAPÍTULO I **14**
1. INTRODUCCION **14**
1.1 Antecedentes. **14**
1.2 Problema de Investigación. **15**
1.2.1 Planteamiento del problema ***15***
1.3 Formulación del problema. **16**
1.4 Sistematización del Problema. **16**
1.5 Justificación de la investigación. **16**
1.5.1 Justificación Teórica. ***16***
1.5.2 Justificación Metodológica. ***17***
1.5.3 Justificación Práctica. ***17***
1.6 Objetivos. **18**
1.6.1 Objetivo General ***18***
1.6.2 Objetivos Específicos ***18***
1.7 Hipótesis **18**
CAPÍTULO II **19**
2. MARCO TEÓRICO **19**
2.1 Antecedentes del Problema **19**
2.2 Bases Teóricas **20**
2.2.1 Seguridad en la información ***20***
2.2.2 Constitución Política del Ecuador ***21***
2.2.3 Normas de Control interno de la Contraloría General del Estado ***21***
2.2.3. Normas de Seguridad ***22***
2.2.4 Norma ISO ***23***
2.2.4.1 Estudio de las normas ISO 27001 ..... ***23***
2.2.4.2 Estudio de las normas ISO 27002 ..... ***24***
2.2.4.3 Estudio de las normas ISO 27005 ..... ***25***
2.2.4.4 Estudio de la Metodología OWASP ***25***
2.2.4.5 Estudio de MAGERIT ***26***
2.3 Operacionalización de la variable independiente Políticas para la gestión de riesgos de seguridad. **28**
2.4 Operacionalización de la variable dependiente: Seguridad y disponibilidad. . **29**
2.5 Matriz de Consistencia **30**

CAPÍTULO III **31**
3. METODOLOGÍA DE INVESTIGACIÓN **31**
3.1 Tipo y Diseño de la Investigación **31**
3.2 Métodos de investigación **32**
3.3 Enfoque de la investigación **32**
3.4 Alcance de la investigación **32**
3.5 Población de estudio **33**
3.6 Unidad de análisis **33**
3.7 Selección de la muestra **33**
3.8 Tamaño de la muestra **33**
3.9 Técnicas de recolección de datos primarios y secundarios **33**
3.10 Instrumentos de recolección de datos primarios y secundarios **34**
3.11 Instrumentos para procesar datos recopilados **34**
3.12 Hipótesis **34**
3.13 Identificación de variables **34**
3.14 Operacionalización conceptual **35**
3.15 Operacionalización metodológica **35**
CAPÍTULO IV **36**
4. RESULTADOS Y DISCUSIÓN **36**
4.1 Procedimiento General **36**
4.2 Análisis Diferencial **36**
4.2.1 Resultado General del Diagnóstico ***44***
4.3 Identificación y valoración de Activos de la Información **45**
4.3.1 Contexto ***45***
4.3.2 Desarrollo ***45***
4.4 Vulnerabilidades y Exploits. **46**
4.4.1 Análisis de vulnerabilidades. ***51***
4.4.2 Análisis de exploits. ***52***
4.4.3 Recomendaciones ***53***
4.5 Sistema de Gestión de Seguridad de la Información. **53**
4.5.1 Introducción ***53***
4.5.2 Objetivos ***53***
4.5.3 Plan (planificar): PLANIFICACION DEL SGSI ***54***
4.5.4 Do (hacer): IMPLEMENTACION DEL SGSI ***55***
4.5.5 Check (verificar): MONITORIZAR Y SEGUIMIENTO DEL SGSI ***57***
4.5.6 Act (actuar): MANTENER Y MEJORA CONTINUA DEL SGSI ***58***
4.6 Análisis diferencial final. **60**

4.7 Comprobación de la Hipótesis General **61**
CAPITULO V **64**
5. PROPUESTA **64**
5.1 Determinación de la Propuesta **64**
5.2 Manual de Políticas de Seguridad de la Información **64**
5.2.1 Introducción ***64***
5.2.2 Alcance ***64***
5.2.3 Objetivos ***65***
5.2.4 Responsabilidades ***65***
5.2.5 Principales Resultados ***66***
5.3 Políticas de Seguridad de la Información **66**
5.3.1 Políticas sobre Plataformas de Sistemas Operativos ***66***
5.3.2 Políticas sobre instalación de sistemas operativos. ***66***
5.3.3 Políticas sobre actualizaciones a los sistemas operativos ***67***
5.3.4 Políticas sobre Programas antivirus ***67***
5.3.5 Políticas sobre instalación de aplicaciones ***68***
5.3.6 Políticas sobre uso de espacio de disco duro ***68***
5.3.7 Políticas sobre Navegador de Internet ***69***
5.3.8 Políticas sobre el uso del Internet ***70***
5.3.9 Políticas sobre el uso de correo electrónico ***70***
5.3.10 Política de protección de contraseña ***72***
5.3.11 Política de comunicación inalámbrica ***74***
5.3.12 Política de responsabilidad por los activos ***75***
5.3.13 Recomendaciones ***75***
CONCLUSIONES **76**
RECOMENDACIONES **77**
GLOSARIO
BIBLIOGRAFÍA

ÍNDICE DE TABLAS

Tabla 1-2: Operacionalización variable independiente 28
Tabla 2-2: Operacionalización variable dependiente 29
Tabla 3-2: Matriz de consistencia 30
Tabla 1-3: Personal del departamento pedagógico ConduEspoch E.P. 33
Tabla 2-3: Operacionalización Conceptual 35
Tabla 3-3: Operacionalización metodológica 35
Tabla 1-4: Políticas de Seguridad 36
Tabla 2-4: Organización de la Seguridad 37
Tabla 3-4: Administración de activos 38
Tabla 4-4: Seguridad de los Recursos humanos 38
Tabla 5-4: Seguridad física y del ambiente 39
Tabla 6-4: Gestión de comunicaciones y operaciones 40
Tabla 7-4: Control de acceso 41
Tabla 8-4: Desarrollo y mantenimiento de los sistemas 42
Tabla 9-4: Administración de incidentes 43
Tabla 10-4: Gestión de la continuidad de la empresa 43
Tabla 11-4: Cumplimiento 44
Tabla 12-4: Inventario de activos de la información 46
Tabla 13-4: Vulnerabilidades Base de Datos MySQL 46
Tabla 14-4: Exploits Base de Datos MySQL 48
Tabla 15-4: Vulnerabilidades Base de Datos Mariadb 49
Tabla 16-4: Exploits Base de Datos Mariadb 51
Tabla 17-4: Vulnerabilidades comunes en MySQL 52
Tabla 18-4: Vulnerabilidades comunes en Mariadb 52
Tabla 19-4: Exploits comunes para MySQL 52
Tabla 20-4: DTIC: Responsable 56
Tabla 21-4: DTIC: Responsable 56
Tabla 22-4: Dominios de Control 60
Tabla 23-4: Rendimiento alcanzado 61
Tabla 24-4: Resultados Chi-Cuadrado 62
Tabla 25-4: Resultados Generales Obtenidos 63

ÍNDICE DE GRÁFICOS

Gráfico 1-2: Ciclo de desarrollo, mantenimiento y mejora 24
Gráfico 2-2: Modelo PDCA aplicado a los procesos SGSI 26
Gráfico 1-4: Políticas de Seguridad 37
Gráfico 2-4: Organización de la Seguridad 37
Gráfico 3-4: Administración de activos 38
Gráfico 4-4: Seguridad de los Recursos humanos 39
Gráfico 5-4: Seguridad física y del ambiente 39
Gráfico 6-4: Gestión de operaciones y comunicaciones 41
Gráfico 7-4: Control de acceso 42
Gráfico 8-4: Desarrollo y mantenimiento de los sistemas 42
Gráfico 9-4: Administración de incidentes 43
Gráfico 10-4: Gestión de la continuidad de la empresa 44
Gráfico 11-4: Cumplimiento 44
Gráfico 12-4: Resultado General del diagnóstico 45
Gráfico 13-4: Avances, logros obtenidos 61
Gráfico 14-4: Resultados Obtenidos 63

RESUMEN

El objetivo fue implementar políticas para la gestión de riesgos de seguridad en el manejo de la información académica de la Empresa Pública ESPOCH CONDUESPOCH EP, ya que la empresa no cuenta con estas políticas; la investigación inicia con un análisis diferencial basado en el autodiagnóstico de la norma ISO 27001 de la situación inicial de la empresa, se elaboró un inventario de activos de información sensible usando metodología MAGERIT, se realizó la detección de vulnerabilidades y exploits, para luego establecer un sistema de gestión de seguridad de la información SGSI de la empresa y determinar las políticas de seguridad de la información a implementar, finalizando con un análisis de la situación actual basados en la metodología OWASP. Como resultado de la investigación, al aplicar las políticas para la gestión de riesgos de la seguridad de la información del sistema académico de la escuela se logró mejorar de un 32,38% a un 74,6% lo que de cierta manera permite garantizar la confidencialidad, disponibilidad e integridad de los datos. Al levantar la información inicial nos dio como resultado que su principal problema es el no poseer un plan estratégico ni políticas de seguridad de información claras y definidas, por lo tanto, es necesario el implementar este tipo de procesos que ayuden a mejorar el nivel de seguridad de la información basado en un estándar internacional como la norma ISO 27001.

Palabras clave: <SEGURIDAD>, <GESTION DE RIESGOS>, <ANALSIS DIFERENCIAL>, <NORMA ISO 27001>, <INVENTARIO DE ACTIVOS>, <METODOLOGIA MAGERIT>, VULNERABILIDADES>, <EXPLOITS (SOFTWARE)>, <POLITICAS DE SEGURIDAD>, < SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)>

0139-DBRA-UPT-IPEC-2023

27-10-2023

SUMMARY

The objective was to implement policies for the management of security risks in the handling of academic information of the Empresa Pública ESPOCH ConduEspoch EP since the company did not have any such policies. The research begins with a differential analysis based on the self-diagnosis of the ISO 27001 standard of the initial situation of the company, an inventory of sensitive information assets has been made using the MAGERIT methodology, the detection of vulnerabilities and exploits has been carried out, to then establish an ISMS Information Security Management System of the company and determine the information security policies to be implemented, ending with an analysis of the current situation based on the OWASP methodology. As a result of the research, it was possible to improve from 32.38% to 74.6% by applying the information security risk management policy of the school's academic system, which in some way guarantees the confidentiality, availability, and integrity of the data. When the initial information was collected, it was found that the main problem was the lack of a strategic plan and a clear and defined information security policy. Therefore, it is necessary to implement this type of process to help improve the level of information security based on an international standard such as ISO 27001.

Keywords: <RISK MANAGEMENT>, <SECURITY>, <DIFFERENTIAL ANALYSIS>, <ISO 27001>, <ASSET INVENTORY>, <MAGERIT>, VULNERABILITIES>, <EXPLOITS>, <SECURITY POLICIES>, <SGSI>, <OWASP>, <INFORMATION>.

CAPÍTULO I

1. INTRODUCCION

1.1 Antecedentes.

Dentro del ámbito de los Sistemas de Gestión de la Seguridad de la Información encontramos diferentes herramientas como: norma ISO 27005 (Gestión de la Seguridad de la Información), OWASP (Open Web Application Security Project), metodologías como MAGERIT, OCTAVE, etc, que permiten gestionar y administrar la información en una determinada empresa o institución con herramientas de seguimiento y seguridad.

Cuando se hace referencia a la norma ISO 27005, se debe tener en cuenta que la propia norma proporciona diferentes orientaciones que se deben utilizar para la gestión de riesgos, teniendo en cuenta los requisitos establecidos, especialmente para los sistemas de gestión de seguridad de la información (SGSI), en línea con ISO/ CEI 27001.

Además, el estándar no proporciona ninguna metodología para la gestión de riesgos de seguridad de la información de ninguna empresa, y debe ser el estándar el que genere su propia política de acuerdo con el alcance que quiera otorgar.

Si hacemos referencia a MAGERIT, se habla de una de las metodologías más utilizadas para el propósito, pues permite realizar varias actividades que se encaminan a desarrollar una mejor evaluación de los riesgos en la empresa.

El manejo de la información académica en la empresa pública ESPOCH CONDUESPOCH EP, se ha venido manejando de una manera inadecuada, sin respetar procesos mínimos de seguridad y respaldo que garanticen su confidencialidad, integridad y disponibilidad, especialmente de aquellas que se encuentran presentes en la web, lo que evidencia la falta de políticas que garanticen su seguridad.

Existen diferentes estándares, normas, modelos y metodologías a seguir y las mismas son ignoradas, lo que conlleva el riesgo de que la información contenida en las bases de datos empresariales pueda ser vulnerada en cualquier momento y extraída para distintos fines.

Descubrir el valor de los activos y los activos en riesgo es una parte importante de la evaluación de riesgos. Los tokens son activos y su valor en riesgo puede generar riesgos de seguridad y

privacidad. Esto crea un grave riesgo de seguridad de la información, el mismo riesgo da paso a vulnerabilidades al momento de manejar información sensible, poniendo en riesgo los diferentes activos informáticos de la empresa por diferentes factores que pueden derivar en fallas de seguridad, ataques externos, violaciones a la seguridad de la información de la empresa, Fuga de información y otras violaciones de la confidencialidad interna de la empresa.

Cualquier tipo de ataques, deberían ser mitigados para lograr un mayor índice de seguridad de la información, permitiendo mantener un mejor nivel de seguridad de la información empresarial, tomando en consideración que no existe sistema cien por ciento seguro.

La Escuela de Conducción Profesional ESPOCH CONDUESPOCH EP, no ha estado exenta de los riesgos ni vulnerabilidades que se han mencionado, se tiene como antecedente que, en noviembre del año 2018, el servidor sufrió un ataque a su base de datos en donde la información fue borrada en su totalidad y solo quedo un mensaje de un pago en bitcoins que se debía realizar para recuperar dichos datos.

Al no existir políticas que establezcan un nivel de seguridad y responsabilidad que se pueda aplicar para mitigar riesgos de quedar vulnerabilidades expuestas y que sean aprovechadas por atacantes y dada la delicadeza de la información que se maneja en la empresa, se justifica el desarrollo del presente proyecto.

1.2 Problema de Investigación.

1.2.1 Planteamiento del problema

Hoy en día toda Institución sustenta sus actividades de decisión y desarrollo en la información, por ello su validez y transparencia requiere políticas, normas y procedimientos que garanticen su disponibilidad, integridad y seguridad. (ERB, 2019).

El principal problema es la falta de un estándar específico de seguridad informática para la gestión del riesgo que establezca como se menciona anteriormente reglas, normas, controles, políticas y procedimientos para los mismos, con el objetivo de analizar, prevenir, proteger o mitigar las posibles vulnerabilidades y su impacto en los servicios (Areitio, 2008).

En la empresa pública ESPOCH ConduEspoch al no existir políticas que establezcan un nivel de seguridad, que se puedan aplicar para mitigar los riesgos de quedar expuestas vulnerabilidades y

que sean aprovechadas por atacantes, dada la delicadeza de la información académica que se maneja en la Institución, se justifica el desarrollo del presente proyecto.

1.3 Formulación del problema.

¿Cuánto mejoraría la gestión de riesgos de seguridad al implementar políticas para el manejo de la información académica de la empresa ConduEspoch EP?

1.4 Sistematización del Problema.

¿Cuáles son las políticas existentes para la gestión de riesgos de seguridad en el manejo de la información?
¿Cuáles son las coincidencias entre las Normas ISO 27001, 27002, 27005 y OWASP?
¿Cómo evaluar y administrar los riesgos de seguridad de la información?
¿Qué políticas se requieren generar para mejorar la seguridad de la información?

1.5 Justificación de la investigación.

1.5.1 Justificación Teórica.

La fuga de información y ataques hacia activos informáticos de una empresa se dan porque no se toma en consideración, ningún modelo o política existente. (ERB, 2019).

La empresa pública ESPOCH ConduEspoch EP, al no contar con políticas y prácticas para gestionar los riesgos de seguridad en el manejo de la información académica y siendo dicha información importante para sus estudiantes y la Agencia Nacional de Tránsito (ANT) en todo el país, es necesario implementarlas y socializarlas, para procurar mantener lo más seguro posible la información que tiene la empresa en cuanto a su disponibilidad.

La manipulación indebida de la información puede provocar daños irreparables a las personas que estudian en esta empresa, es por lo que, se ha planteado, realizar las políticas de evaluación y administración de los riesgos (gestión de riesgos), que, sin ser una camisa de fuerza, deberán llegar a ser una guía que permitirá mantener segura la información académica.

Además de que, sin ser la solución definitiva para evitar ataques, sustracción de información, y otras vulnerabilidades, permitirá aplacarlas, para poder mantener con menor riesgo los activos sensibles de la institución.

1.5.2 Justificación Metodológica.

La metodología que se va a utilizar en la presente investigación es la metodología MAGERIT, es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica (CSAE), para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. (EcuRed, Política, 2019).

La metodología MAGERIT divide los activos de la organización en varios grupos, lo que permite identificar una mayor cantidad de riesgos y poder tomar medidas para evitar posibles inconvenientes. (Vicente, 2014).

Además, se empleará la metodología OWASP (Open Web Application Security Project ™), metodología de análisis de riesgos cuyo enfoque se basa en que la organización sea capaz de dirigir y enfocar sus evaluaciones de riesgos, tomar decisiones con base en los riesgos, proteger los activos claves de información y comunicar de manera efectiva la información clave de seguridad. (Onur. A, 2018).

El método aprovecha el conocimiento de múltiples niveles de la organización, centrándose en la construcción de los perfiles de amenazas basados en activos, la identificación de la infraestructura de vulnerabilidades y el desarrollo de planes y estrategias de seguridad.

1.5.3 Justificación Práctica.

Es importante el poder establecer una buena seguridad de la información como uno de los activos informáticos que tiene una empresa, hay que considerar que existen varias maneras de vulnerar las seguridades de un sistema de información, llámese esto, DDNS, SQLINJECTION, los que, en muchas de las ocasiones por no decir en la mayoría, son provocados por la falta de políticas y controles.

Para poder brindar una buena protección al sistema académico de la empresa ConduEspoch EP, el primero será, presentar políticas y normativas de seguridad de la información que nos permita mantener un nivel de seguridad adecuado, que por lo menos retrase los intentos de vulnerar las seguridades organizacionales.

En este sentido, se realizará un estudio de las políticas existentes, normas ISO 27001, 27002 y se elaborará un SGSI que permita mediante MAGERIT establecer las vulnerabilidades existentes;

además de establecer las herramientas para evaluar y administrar los riesgos de seguridad de la información, generando con esto las políticas a implementarse para la gestión de riesgos de la información académica, finalizando con un análisis con y sin estas políticas investigadas.

1.6 Objetivos.

1.6.1 Objetivo General

- Implementar políticas para la gestión de riesgos de seguridad en el manejo de la información académica de la Empresa Pública ESPOCH ConduEspoch EP

1.6.2 Objetivos Específicos

- Determinar y analizar las reglamentaciones, proceso y responsabilidades de las normativas y políticas para la gestión de la seguridad de la información existentes en el Ecuador.
- Definir las coincidencias y discrepancias entre las Normas ISO 27001, 27002, 27005
- Establecer las herramientas para evaluar y administrar los riesgos de seguridad de la información.
- Proponer políticas para mejorar la seguridad de la información académica.
- Aplicar las políticas de seguridad investigadas y su funcionalidad.
- Determinar si las políticas implementadas mejoran la gestión de riesgos de la información académica.

1.7 Hipótesis

La implementación de políticas para gestionar los riesgos de seguridad de la información académica, permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes del Problema

Una vez realizada la revisión de trabajos de investigación, existen temas similares que respaldan y sirven de referencia para el desarrollo de la investigación.

La investigación realizada por (Montalvo, 2017) con el tema: "Generación de políticas para la gestión de riesgos de seguridad en el desarrollo de software", en la que se concluye que al evaluar las políticas existentes para el desarrollo de software, se ha podido concluir que, las políticas existentes que se han publicado, y se puedan aplicar para poder realizar esta tarea, se encuentran elaboradas de una manera general para la Seguridad de la Información Empresarial, pero, dichas políticas no particularizan para el Desarrollo de Software, lo cual se debería tener para poder desarrollar Software seguro. (Montalvo, 2017). Como resultado de la investigación, es posible concluir que, aplicar las políticas y utilizarlas durante la etapa de desarrollo de software, logra reducir del 39,2 % al 12,5 % en las pruebas realizadas, de manera que, se pueda seguir mejorando las vulnerabilidades existentes en las aplicaciones desarrolladas. (Montalvo, 2017).

Se recomienda el uso de las Normas creadas para mantener la seguridad de los activos informáticos de cualquier empresa, para desarrollar sus propias aplicaciones de software, se deben tomar en consideración las coincidencias y, dentro de las discrepancias, las que puedan coadyuvar para presentar una aplicación segura, no se las debe descartar, puesto que, no se puede limitar el uso de Normas cuando se trata de la seguridad. (Montalvo, 2017). Siempre será recomendable, desarrollar prototipos para realizar las diferentes pruebas de ataques que puedan determinar las vulnerabilidades existentes, para poder corregir antes y no sufrir ataques fácilmente al ser puestas en producción.

Así mismo se muestra el estudio de (Guevara, 2018) con el tema: "Estudio de las normativas de seguridad de la información de instituciones públicas: propuesta de una normativa en una institución de educación superior", los hallazgos de este trabajo indican que al estudiar las leyes existentes se considera importante organizarlas y estandarizarlas para que puedan ser aplicadas a un departamento de tecnologías y comunicación de cualquier institución, es así que el cuadro que se presenta en este trabajo de investigación permite que pueda ser usado en cualquier caso de estudio en el Ecuador. (Guevara, 2018). Así mismo la implementación de la propuesta en la política de control de acceso ha permitido mostrar que, de manera empírica los trabajadores

usaban su propio conocimiento de lo que no deberían realizar cuantificando esto en un 40% en la seguridad de la información que manejan, al plantear una política basados en controles de la norma ISO 27000 y que estén empatadas con leyes del Ecuador, primeramente concientiza a los trabajadores de la obligatoriedad y el compromiso de usarla de esta manera se incrementa al 60% la seguridad de información. (Guevara, 2018).

En base al estudio realizado las leyes y normativas del Ecuador pueden ir variando durante el transcurso de los gobiernos, por lo que es importante basarse en una norma estandarizada internacional como la ISO 27001 la cual es la única certificable, es escalable y permite cambios continuos y se adapta fácilmente a las necesidades de un departamento de tecnología y comunicación. (Guevara, 2018). La creación del cuadro de las leyes vigentes en el Ecuador versus los controles que se adaptan a estas leyes no solo beneficiará al caso de estudio presentado sino también a cualquier departamento de tecnología que desea acoplar la ISO 27001 para la creación de su sistema de seguridad de la información.

2.2 Bases Teóricas

2.2.1 Seguridad en la información

Según (Salazar, 2008), cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, es por ello la necesidad de una estrategia completa de seguridad, de manera de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas (misma organización), que son un factor de riesgo no menor, y, por lo tanto, existe alta probabilidad de pérdida de datos y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

Se establece que, para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, según (Borghello, 2001) estos son:

- *Confidencialidad:* Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.
- *Integridad:* Busca asegurar: o que no se realicen modificaciones por personas no autorizadas a los datos o procesos, o que no se realicen modificaciones no autorizadas

por personal autorizado a los datos o procesos, o que los datos sean consistentes tanto interna como externamente.

- *Disponibilidad:* Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

La seguridad de la información no es una propiedad funcional de un sistema de información, sino más bien una propiedad emergente ya que a lo largo de los años la percepción de la seguridad de la información ha ido cambiando hasta llegar a nuestros días, nació ligada a los entornos militares, diplomáticos y gubernamentales (Areitio, 2008); a nivel empresarial comenzó siendo un lujo y posteriormente se consideró como una obligación para que las empresas no queden desprotegidas, desde el punto de vista legal, frente a leyes y reglamentos.

2.2.2 Constitución Política del Ecuador

Es importante mencionar algunos artículos de la Constitución del Ecuador en donde hace referencia a la información (Constituyente, 2008):

"Art. 18. Todas las personas, de forma individual o colectiva, tiene derecho a:
2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en caso expresamente establecidos por la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información".
"Art. 389. El estado garantizará el derecho de las personas, las colectividades y la naturaleza a la protección frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objeto de minimizar la condición de vulnerabilidad".

2.2.3 Normas de Control interno de la Contraloría General del Estado

Las normas de control interno hacen referencia explícita a la seguridad de la información en su apartado 410 Tecnologías de la Información en donde según (Contraloria General del Estado, 2010) se puede encontrar:

410-01 Organización informática.

410-02 Segregación de funciones.

410-03 Plan informático estratégico de tecnología.

410-10 Seguridad de tecnología de Información.

En este apartado se dice: “La Unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra perdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:”

1. Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de información y en especial a las áreas de: servicios, desarrollo y bibliotecas”.
2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado.
3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.
4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.
5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;
7. Consideración y disposición de sitios de procesamiento alternativos.
8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

2.2.3. Normas de Seguridad

Entre los aspectos que se deben considerar para la gestión de riesgos se encuentran varios estándares de seguridad que formarán la base del trabajo actual, a través de su estudio, con el objetivo de establecer las mejores políticas que deben utilizarse para garantizar el poder reducir las vulnerabilidades, ya que esto podría significar pérdida de activos de la empresa.

Para ello, se realizarán los estudios de:

- Norma ISO 27001
- Norma ISO 27002
- Norma ISO 27005
- Estudio de las OWAS
- Estudio de MAGERIT

2.2.4 Norma ISO

ISO es una organización internacional independiente, no gubernamental, con una membresía de 164 organismos nacionales de normalización. A través de sus miembros, reúne expertos para compartir conocimientos y desarrollar estándares internacionales voluntarios, basados en el consenso y relevantes para el mercado, que apoyan la innovación y proporcionan soluciones a los desafíos globales. (ISO, 2019).

Los estándares internacionales hacen que las cosas funcionen. Proporcionan especificaciones de clase mundial para productos, servicios y sistemas, para garantizar la calidad, la seguridad y la eficiencia. Son instrumentales para facilitar el comercio internacional. ISO ha publicado 22670 Normas Internacionales y documentos relacionados, que abarcan casi todas las industrias, desde tecnología, seguridad alimentaria, agricultura y atención médica. Las Normas Internacionales ISO impactan a todos, en todas partes. (ISO, 2019)

2.2.4.1 Estudio de las normas ISO 27001

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (ISO, 2019).

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.
Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a) Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) Monitorear y revisar el desempeño y la efectividad del SGSI; y
d) Mejoramiento continuo, en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

En la Figura 1 se puede apreciar el ciclo de desarrollo, mantenimiento y mejora en el cual se basa esta norma para la Seguridad de la información, recalcando que ésta se aplica para un SGSI. (Gómez Orozco, 2013)

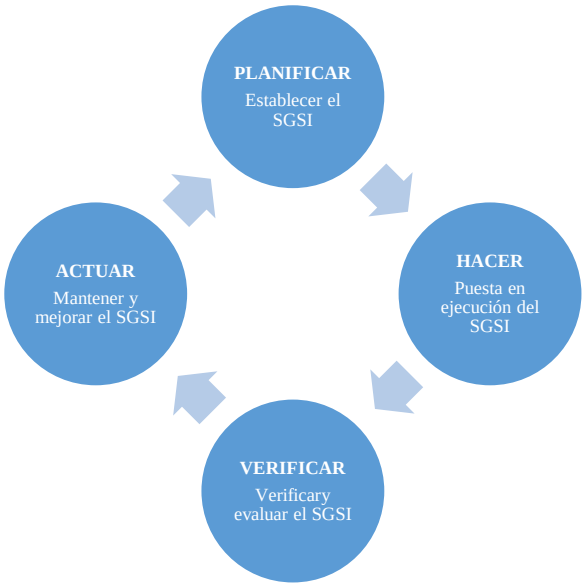

Gráfico 1-2. Ciclo de desarrollo, mantenimiento y mejora

Fuente: Sistema de gestión de seguridad de la información SGSI *(Gómez Orozco, 2013)*

2.2.4.2 Estudio de las normas ISO 27002

Proporciona pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de los controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización. (ISO, 2019).

Está diseñado para ser utilizado por organizaciones que pretenden:

- Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001;
- Implementar controles de seguridad de la información comúnmente aceptados;
- Desarrollar sus propias pautas de gestión de seguridad de la información

Ante todo, lo descrito cabe resaltar que, esta norma no es certificable, y no lo es por una sencilla razón, la ISO 27002 no es una norma de gestión, así como lo es la ISO 27001, para darse cuenta, únicamente se debe ver que, en la norma ISO 27002, los controles tienen la misma denominación que los controles del Anexo A de la ISO 27001.

2.2.4.3 Estudio de las normas ISO 27005

Este documento proporciona pautas para la gestión de riesgos de seguridad de la información, respalda los conceptos generales especificados en ISO / IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminologías descritos en ISO / IEC 27001 e ISO / IEC 27002 es importante para una comprensión completa de este documento el mismo que es aplicable a todos los tipos de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que pretenden gestionar riesgos que pueden comprometer la seguridad de la información de la organización. (ISO, 2019).

La comprensión de los conceptos, modelos, procesos y terminología existentes en las normas ISO/IEC 27001 e ISO/IEC 27002 es muy importante para entender de mejor manera la norma ISO/IEC 27005. (F., N.D.)

2.2.4.4 Estudio de la Metodología OWASP

Cada mercado de tecnología vibrante necesita una fuente de información imparcial sobre las mejores prácticas, así como un cuerpo activo que abogue por estándares abiertos. En el espacio de Application Security, uno de esos grupos es Open Web Application Security Project ™ OWASP para abreviar. (OWASP, 2019).

Usar OWASP permite a las organizaciones tomar mejores decisiones sobres sus riesgos de seguridad. Los proyectos OWASP se dividen en dos categorías principales: proyectos de desarrollo y proyectos de documentación. (MOSQUERA, 2015).

Para investigar sobre OWASP, uno debe preguntarse dónde se encontrará el riesgo, dónde se puede determinar que existe riesgo dondequiera que se realicen las actividades y cualquier empresa que mantenga activos es susceptible al riesgo.

Según (MACHACA, N.D.) Una vez determinado donde se encuentra el riesgo, hay que clasificar los riegos existentes en la organización, teniendo varios tipos, de esta manera se puede realizar el Modelo PDCA aplicado a los procesos SGSI como se muestra en la Figura 2.

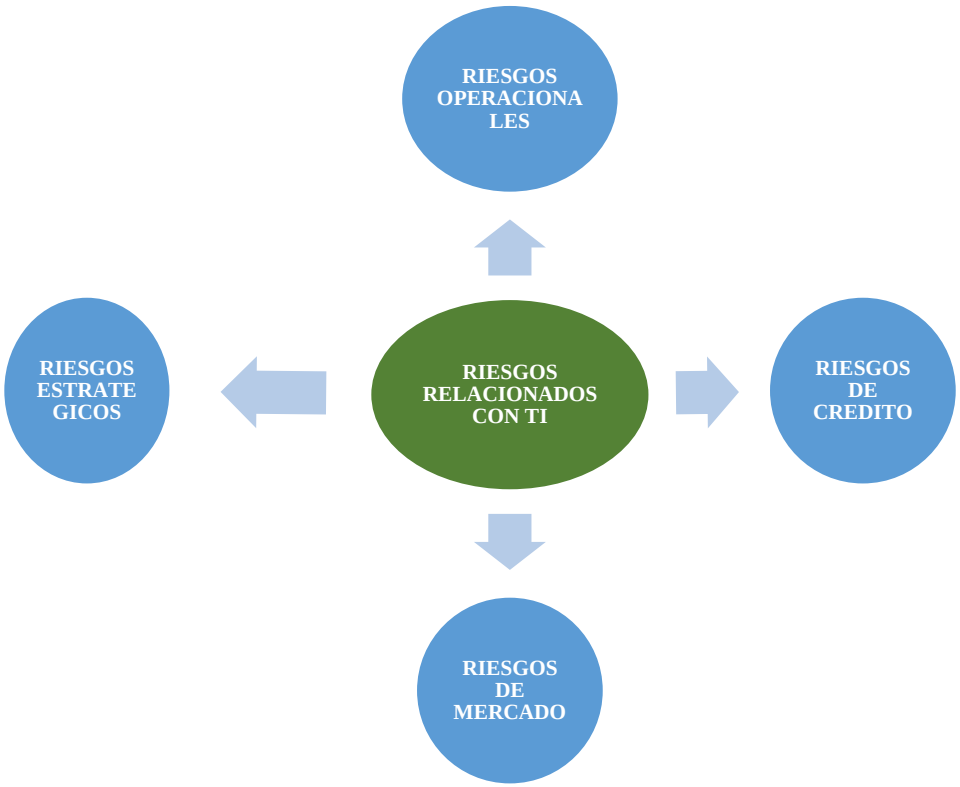

Gráfico 2-2. Modelo PDCA aplicado a los procesos SGSI

Fuente: Análisis de Riesgos usando la Metodología OWASP *(MACHACA, N.D.)*

2.2.4.5 Estudio de MAGERIT

La metodología MAGERIT, permite el análisis y gestión de riesgos de los sistemas de información considerando su ubicación; se manifiesta aún más en la vulnerabilidad física de las organizaciones situadas en zonas bajas, no solo ante inundaciones sino también ante robo de

información o equipos como lo estarían las empresas situadas en zonas altas. Es habitual que las organizaciones tengan pérdidas debido a fallas o agresiones en sus sistemas de TI, los cuales afectan su nombradía. (Gómez, 2019).

Los principales elementos que utiliza MAGERIT son:

- Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio.
- Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.
- Escala alternativa de estimación del riesgo.
- Catálogos de amenazas
- Catálogos de medidas de control (SYALIM, 2009)

El objetivo de MAGERIT es "Estudiar los riesgos que soportan un sistema de información y el entorno asociado a él". (Gómez Orozco, 2013).

Propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización:

- Señala los riesgos existentes, identificando las amenazas que asechan al sistema de información.
- Determina la vulnerabilidad del sistema de prevención de dichas amenazas, generando resultados.

"Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo se potencial o sus posibles perjuicios." (Gómez, 2019).

MAGERIT ofrece un método sistemático para analizar tales riesgos, también ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control, preparando a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.3 Operacionalización de la variable independiente Políticas para la gestión de riesgos de seguridad.

Tabla 1-2: Operacionalización variable independiente

VARIABLE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS	CRITERIO DE MEDICIÓN	TÉCNICA	INSTRUMENTO	ESCALA
Políticas para la gestión de riesgos de seguridad.	Políticas regulatorias y normas que protegen la seguridad de la información académica	Gestión de normas y reglamentaciones establecidas a nivel mundial	Normativas	¿Cuáles son las normativas que se deben aplicar que protegen la seguridad?	Cantidad	Observación	Departamento pedagógico SGSI	Numeración real positiva a partir del 0
			Reglamentaciones	¿Cuántas reglamentaciones aplican a la seguridad?	Cantidad	Observación	Departamento pedagógico SGSI	Numeración real positiva a partir del 0

Fuente: ConduEspoch E.P.

Realizado por: Guffantte, Carlos, 2023

2.4 Operacionalización de la variable dependiente: Seguridad y disponibilidad.

Tabla 2-2: Operacionalización variable dependiente

VARIABLE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS	CRITERIO DE MEDICIÓN	TÉCNICA	INSTRUMENTO	ESCALA
Seguridad y Disponibilidad	Métricas esenciales en cualquier sistema de manejo de información para la garantía de la integridad de los datos.	Seguridad	% de incidentes interceptados	¿Cantidad de eventos que fueron interceptados?	Cantidad	Observación	Software par detección de incidentes	Numeración real positiva a partir del 0
		Disponibilidad	% de incidentes resueltos	¿Cantidad de eventos resueltos?	Cantidad	Observación	Reportes de incidentes resueltos	Numeración real positiva a partir del 0

Fuente: ConduEspoch E.P.

Realizado por: Guffantte, Carlos, 2023

2.5 Matriz de Consistencia

Tabla 3-2: Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTOS
¿Cuánto mejoraría la gestión de riesgos de seguridad al implementar políticas para el manejo de la información académica de la empresa ConduEspoch EP?	Implementar políticas para la gestión de riesgos de seguridad en el manejo de la información académica de la Empresa Pública ESPOCH ConduEspoch EP	H0: La implementación de políticas para gestionar los riesgos de seguridad de la información académica, NO permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch. H1: La implementación de políticas para gestionar los riesgos de seguridad de la información académica, permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch.	**Independiente:** Políticas para la gestión de riesgos de seguridad. **Dependiente:** Seguridad Disponibilidad	Normativas Reglamentaciones Integridad de los datos Acceso a la información académica Confidencialidad de los datos	Observación	Departamento Pedagógico SGSI Software par detección de incidentes Reportes de incidentes resueltos

Fuente: ConduEspoch E.P.

Realizado por: Guffantte, Carlos, 2023

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1 Tipo y Diseño de la Investigación

Existen diferentes tipos de investigación, los mismos que se podrán utilizar dependiendo de las necesidades que se requieren; se pueden definir dos enfoques:

• Cuantitativo y,

• Cualitativo.

El enfoque cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no se puede saltar pasos, el orden es riguroso, aunque, desde luego, se podrá redefinir alguna fase. Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y determinan variables; se desarrolla un plan para probarlas; se miden las variables en un determinado contexto; se analizan las mediciones obtenidas (con frecuencia utilizando métodos estadísticos), y se establece una serie de conclusiones respecto de la(s) hipótesis. (Hernandez, 2010).

El enfoque cualitativo se selecciona cuando se busca comprender la perspectiva de los participantes acerca de los fenómenos que los rodean, profundizar en sus experiencias, perspectivas, opiniones y significados, es decir, la forma en que los participantes perciben subjetivamente su realidad. También es recomendable seleccionar el enfoque cualitativo cuando el tema del estudio ha sido poco explorado, o no se ha hecho investigación al respecto en algún grupo social específico. El proceso cualitativo inicia con la idea de investigación. (Hernandez, 2010).

Aquí se define la estrategia que se utilizará para obtener la mayor cantidad de resultados que se necesitan para que la investigación culmine de la mejor manera.

El trabajo que se realizará toma por diseño uno de los diseños básicos de la investigación cuantitativa, éste es el diseño experimental, por las características presentadas aquí para poder obtener los resultados que lleven a determinar la validez de la hipótesis planteada.

3.2 Métodos de investigación

La investigación científica se encarga de producir conocimiento, el conocimiento científico tiene diferentes características, las mismas que se listan a continuación.

- Sistemático.
- Ordenado.
- Metódico.
- Racional (Reflexivo).
- Crítico.

Para desarrollar el presente trabajo se ha tomado en consideración el método científico el mismo que propone las siguientes etapas:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis
- Difusión de resultados. (Machaca, N.D.)

3.3 Enfoque de la investigación

El presente estudio por su concepción es de tipo cuantitativo, pues utiliza la recolección y el análisis de datos para contestar una o varias preguntas de investigación y probar la hipótesis establecida previamente.

3.4 Alcance de la investigación

El alcance de la presente investigación e implementación es de tipo descriptivo, como dice (Gay, 1996), “La investigación descriptiva, comprende la colección de datos para probar hipótesis o responder a preguntas concernientes a la situación corriente de los sujetos del estudio, pues un estudio descriptivo determina e informa los modos de ser de los objetos.”

3.5 Población de estudio

La población de estudio está en el departamento de pedagogía de la empresa, pues es aquí en donde se manejan la información académica sensible de todos los estudiantes que pretender obtener una licencia profesional de conducir.

A continuación, se detalla el personal que forma parte del departamento de pedagogía con su respectivo cargo.

Tabla 1-3: Personal del departamento pedagógico ConduEspoch E.P.

APELLIDOS Y NOMBRES	CARGO
Ibujes Héctor Galo	Director Pedagógico
Jara Dillon Estefanía Belén	Inspectora

Fuente: ConduEspoch E.P.
Realizado por: Guffantte, Carlos, 2023

3.6 Unidad de análisis

Empresa Pública Escuela de Conducción profesional ESPOCH CONDUESPOCH EP.

3.7 Selección de la muestra

No se realizará muestreo, se trabajará con el personal administrativo del departamento de pedagogía de la Escuela de Conducción profesional ESPOCH CONDUESPOCH E.P.

3.8 Tamaño de la muestra

No se realizará muestreo, se trabajará con el personal administrativo del departamento de pedagogía de la Escuela de Conducción profesional ESPOCH CONDUESPOCH E.P.

3.9 Técnicas de recolección de datos primarios y secundarios

Las técnicas para utilizarse en la presente investigación son las siguientes:

Primarias:

Formulario para Autodiagnóstico (ISO 27001) al personal administrativo referente al tema dentro de ConduEspoch.

Observación.

Secundarias:

Textos referentes al tema de estudio.

3.10 Instrumentos de recolección de datos primarios y secundarios

Primarios:

Cuestionarios del formulario para autodiagnóstico (ISO 27001) y entrevista.

Ficha de observación.

Secundarios:

Fichas bibliográficas.

3.11 Instrumentos para procesar datos recopilados

Los datos recolectados serán procesados en el programa Excel.

3.12 Hipótesis

La implementación de políticas para gestionar los riesgos de seguridad de la información académica, permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH CONDUESPOCH EP.

3.13 Identificación de variables

Variable independiente:

Políticas para la gestión de riesgos de seguridad.

Variables dependientes:

Seguridad
Disponibilidad

3.14 Operacionalización conceptual

Tabla 2-3: Operacionalización Conceptual

VARIABLE	TIPO	CONCEPTO
Políticas para la gestión de riesgos de seguridad.	Independiente	Políticas regulatorias y normas que protegen la seguridad de la información académica
Seguridad Disponibilidad	Dependiente	Métricas esenciales en cualquier sistema de manejo de información para la garantía de la integridad de los datos.

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

3.15 Operacionalización metodológica

Tabla 3-3: Operacionalización metodológica

HIPÓTESIS	VARIABLES	INDICADORES	ÍNDICES	TECNICA
La implementación de políticas para gestionar los riesgos de seguridad de la información académica, permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch.	**Independiente:** Políticas para la gestión de riesgos de seguridad. **Dependiente:** Seguridad Disponibilidad	Normativas Reglamentaciones Integridad de los datos Acceso a la información académica Confidencialidad de los datos	Políticas y reglamentos Salvaguardias físicas y técnicas Requisitos organizacionales y de documentación Seguridad de la información Vulnerabilidades	Observación, análisis Recopilación de información

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Procedimiento General

El presente trabajo de investigación se enfoca en analizar la situación actual de la Escuela de Conducción Profesional ESPOCH ConduEspoch EP, en cuanto a su situación inicial en lo referente al manejo de la seguridad de la información, para poder determinar el estado de operatividad que mantienen, definir el inventario de activos de información, establecer vulnerabilidad y definir las políticas de seguridad que se deberán tomar.

4.2 Análisis Diferencial

El análisis de situación de la empresa respecto a la norma no es obligatorio según la ISO 27001 pero si aconsejable para entender dónde nos encontramos. El análisis diferencial nos permitirá evaluar el grado de cumplimiento de la norma y nos permitirá tener una versión preliminar de la Declaración de aplicabilidad.

La nomenclatura que se va a utilizar en este análisis es la siguiente

- Si: Cumple con el requisito o control.
- No: No cumple con la aplicación del control.

Los resultados obtenidos son los siguientes:

Formulario para Autodiagnóstico (ISO 27001)

Tabla 1-4: Políticas de Seguridad

POLÍTICAS DE SEGURIDAD	CUMPLE
Existen documento(s) de políticas de seguridad de SI	No
Existe normativa relativa a la seguridad de los SI	No
Existen procedimientos relativos a la seguridad de SI	No
Existe un responsable de las políticas, normas y procedimientos	No
Existen mecanismos para la comunicación a los usuarios de las normas	No
Existen controles regulares para verificar la efectividad de las políticas	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

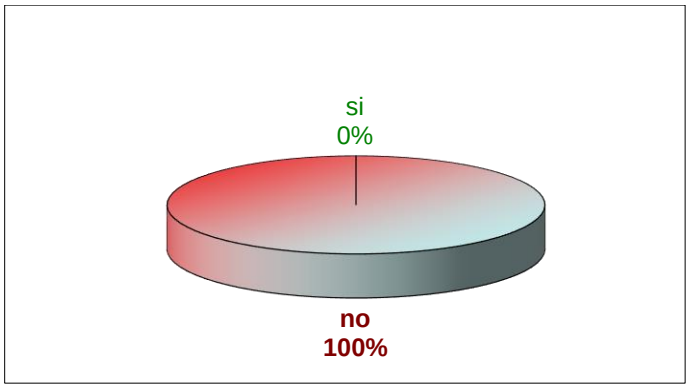

Gráfico 1-4. Políticas de Seguridad

Realizado por: Guffantte, Carlos, 2023

Tabla 2-4: Organización de la Seguridad

ORGANIZACIÓN DE LA SEGURIDAD	CUMPLE
Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	No
Existe un responsable encargado de evaluar la adquisición y cambios de SI	No
La Dirección y las áreas de la Organización participa en temas de seguridad	No
Existen condiciones contractuales de seguridad con terceros y outsourcing	No
Existen criterios de seguridad en el manejo de terceras partes	No
Existen programas de formación en seguridad para los empleados, clientes y terceros.	No
Existe un acuerdo de confidencialidad de la información que se accesa.	No
Se revisa la organización de la seguridad periódicamente por una empresa externa	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

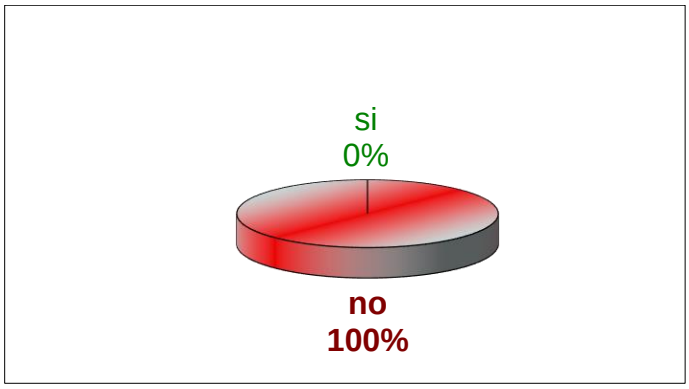

Gráfico 2-4. Organización de la Seguridad

Realizado por: Guffantte, Carlos, 2023

Tabla 3-4: Administración de activos

ADMINISTRACIÓN DE ACTIVOS	CUMPLE
Existen un inventario de activos actualizado	Si
El Inventario contiene activos de datos, software, equipos y servicios	Si
Se dispone de una clasificación de la información según la criticidad de la misma	No
Existe un responsable de los activos	Si
Existen procedimientos para clasificar la información	Si
Existen procedimientos de etiquetado de la información	Si

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

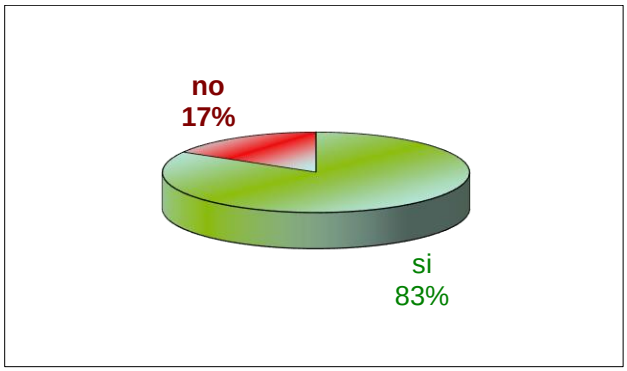

Gráfico 3-4. Administración de activos

Realizado por: Guffantte, Carlos, 2023

Tabla 4-4: Seguridad de los Recursos humanos

SEGURIDAD DE LOS RRHH	CUMPLE
Se tienen definidas responsabilidades y roles de seguridad	No
Se tiene en cuenta la seguridad en la selección y baja del personal	No
Se indica las condiciones de confidencialidad y responsabilidades en los contratos	Si
Se imparte la formación adecuada de seguridad y tratamiento de activos	No
Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	No
Se recogen los datos de los incidentes de forma detallada	No
Informan los usuarios de las vulnerabilidades observadas o sospechadas	Si
Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	No
Existe un proceso disciplinario de la seguridad de la información	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

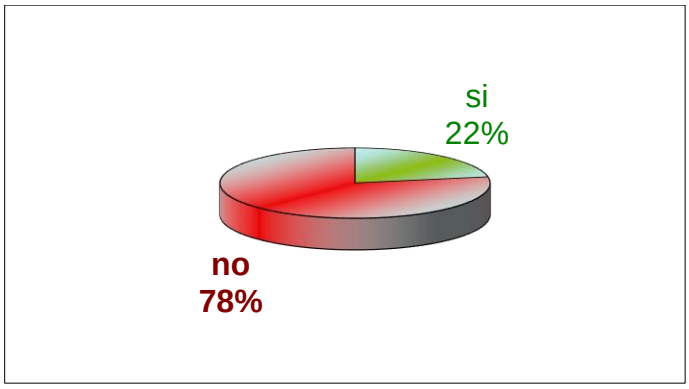

Gráfico 4-4. Seguridad de los Recursos humanos

Realizado por: Guffantte, Carlos, 2023

Tabla 5-4: Seguridad física y del ambiente

SEGURIDAD FÍSICA Y DEL AMBIENTE	CUMPLE
Existe perímetro de seguridad física (una pared, puerta con llave).	Si
Existen controles de entrada para protegerse frente al acceso de personal no autorizado	No
Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	Si
En las áreas seguras existen controles adicionales al personal propio y ajeno	Si
Las áreas de carga y expedición están aisladas de las áreas de SI	Si
La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	No
Existen protecciones frente a fallos en la alimentación eléctrica	Si
Existe seguridad en el cableado frente a daños e intercepciones	Si
Se asegura la disponibilidad e integridad de todos los equipos	No
Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	No
Se incluye la seguridad en equipos móviles	Si

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

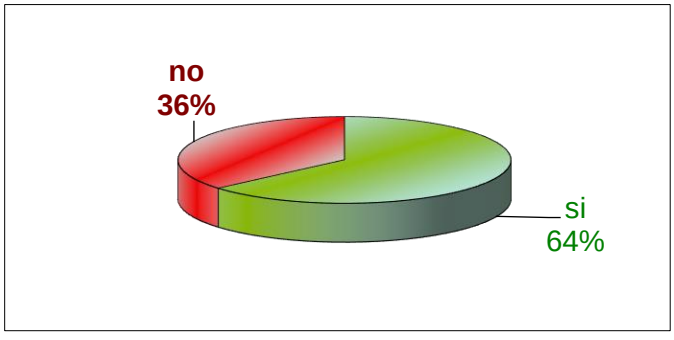

Gráfico 5-4. Seguridad física y del ambiente

Realizado por: Guffantte, Carlos, 2023

Tabla 6-4: Gestión de comunicaciones y operaciones

GESTIÓN DE COMUNICACIONES Y OPERACIONES	CUMPLE
Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	No
Están establecidas responsabilidades para controlar los cambios en equipos	Si
Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	Si
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	Si
Existe una separación de los entornos de desarrollo y producción	No
Existen contratistas externos para la gestión de los Sistemas de Información	No
Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	No
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	No
Controles contra software maligno	Si
Realizar copias de backup de la información esencial para el negocio	Si
Existen logs para las actividades realizadas por los operadores y administradores	Si
Existen logs de los fallos detectados	Si
Existen rastro de auditoría	No
Existe algún control en las redes	Si
Hay establecidos controles para realizar la gestión de los medios informáticos. (cintas, discos, removibles, informes impresos)	No
Eliminación de los medios informáticos. Pueden disponer de información sensible	Si
Existe seguridad de la documentación de los Sistemas	Si
Existen acuerdos para intercambio de información y software	No
Existen medidas de seguridad de los medios en el tránsito	No
Existen medidas de seguridad en el comercio electrónico.	No
Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	No
Existen medidas de seguridad en las transacciones en línea	Si
Se monitorean las actividades relacionadas a la seguridad	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

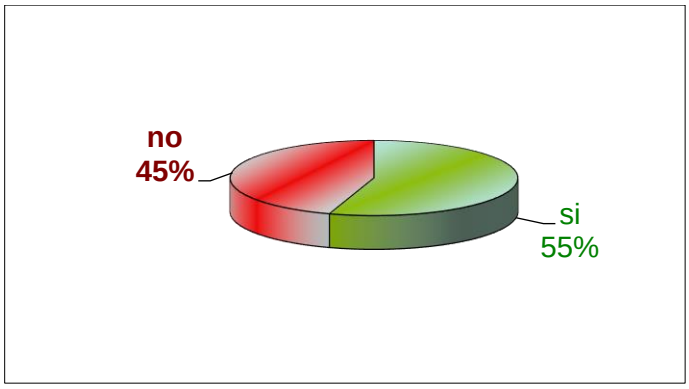

Gráfico 6-4. Gestión de operaciones y comunicaciones

Realizado por: Guffantte, Carlos, 2023

Tabla 7-4: Control de acceso

CONTROL DE ACCESOS	CUMPLE
Existe una política de control de accesos	No
Existe un procedimiento formal de registro y baja de accesos	No
Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	Si
Existe una gestión de los password de usuarios	No
Existe una revisión de los derechos de acceso de los usuarios	No
Existe el uso del password	Si
Se protege el acceso de los equipos desatendidos	No
Existen políticas de limpieza en el puesto de trabajo	Si
Existe una política de uso de los servicios de red	No
Se asegura la ruta (path) desde el terminal al servicio	No
Existe una autenticación de usuarios en conexiones externas	No
Existe una autenticación de los nodos	No
Existe un control de la conexión de redes	Si
Existe un control del routing de las redes	Si
Existe una identificación única de usuario y una automática de terminales	No
Existen procedimientos de log-on al terminal	No
Se ha incorporado medidas de seguridad a la computación móvil	No
Está controlado el teletrabajo por la organización	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

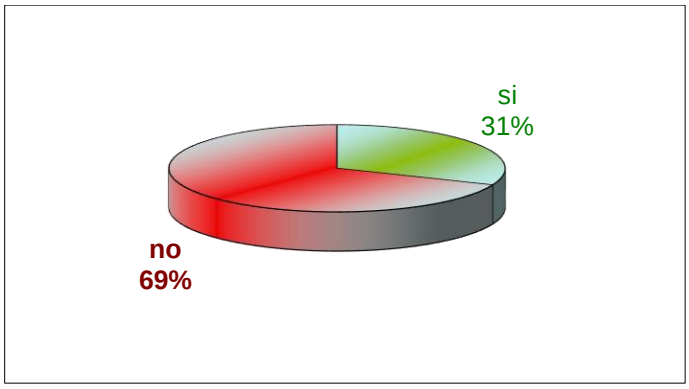

Gráfico 7-4. Control de acceso

Realizado por: Guffantte, Carlos, 2023

Tabla 8-4: Desarrollo y mantenimiento de los sistemas

DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	CUMPLE
Se asegura que la seguridad está implantada en los Sistemas de Información	No
Existe seguridad en las aplicaciones	No
Existen controles criptográficos.	No
Existe seguridad en los ficheros de los sistemas	No
Existe seguridad en los procesos de desarrollo, testing y soporte	No
Existen controles de seguridad para los resultados de los sistemas	No
Existe la gestión de los cambios en los SO.	Si
Se controlan las vulnerabilidades de los equipos	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

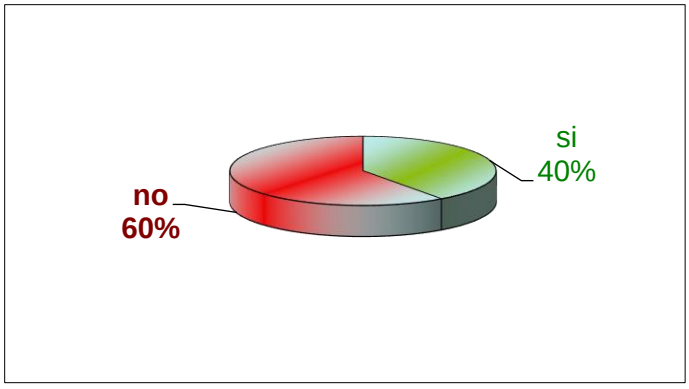

Gráfico 8-4. Desarrollo y mantenimiento de los sistemas

Realizado por: Guffantte, Carlos, 2023

Tabla 9-4: Administración de incidentes

ADMINISTRACIÓN DE INCIDENTES	CUMPLE
Se comunican los eventos de seguridad	Si
Se comunican las debilidades de seguridad	Si
Existe definidas las responsabilidades antes un incidente.	No
Existe un procedimiento formal de respuesta	No
Existe la gestión de incidentes	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

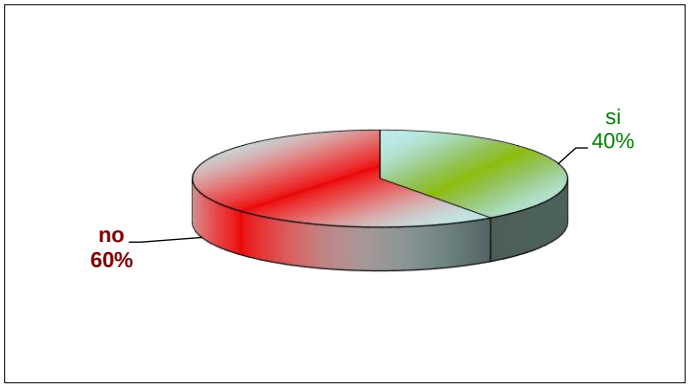

Gráfico 9-4. Administración de incidentes

Realizado por: Guffantte, Carlos, 2023

Tabla 10-4: Gestión de la continuidad de la empresa

GESTIÓN DE LA CONTINUIDAD DE LA EMPRESA	CUMPLE
Existen procesos para la gestión de la continuidad.	No
Existe un plan de continuidad del negocio y análisis de impacto	No
Existe un diseño, redacción e implantación de planes de continuidad	No
Existe un marco de planificación para la continuidad del negocio	No
Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

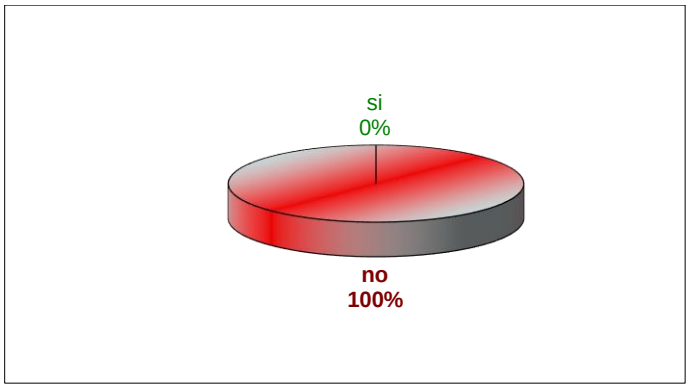

Gráfico 10-4. Gestión de la continuidad de la empresa

Realizado por: Guffantte, Carlos, 2023

Tabla 11-4: Cumplimiento

CUMPLIMIENTO	CUMPLE
Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	Si
Existe el resguardo de la propiedad intelectual	No
Existe el resguardo de los registros de la organización	No
Existe una revisión de la política de seguridad y de la conformidad técnica	No
Existen consideraciones sobre las auditorías de los sistemas	No

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

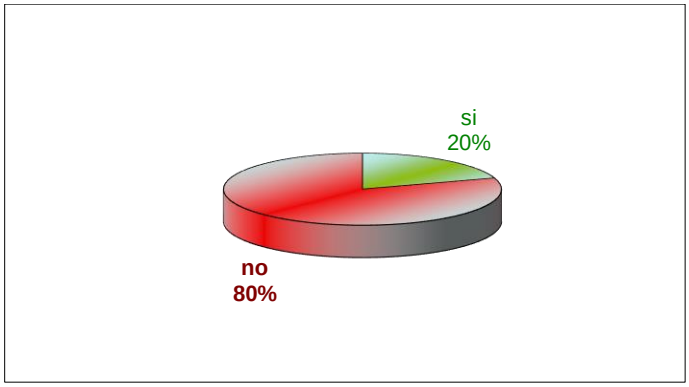

Gráfico 11-4. Cumplimiento

Realizado por: Guffantte, Carlos, 2023

4.2.1 Resultado General del Diagnóstico

Una vez desarrollado el análisis diferencial, podemos observar que en un 67,62 % no se cumplen con los estándares de seguridad de la información, tan solo un 32,38% son cumplidos, esto permite afirmar que no existen normativas que garanticen la confidencialidad, integridad y

disponibilidad de la información en la Escuela de Conducción profesional ESPOCH ConduEspoch EP:

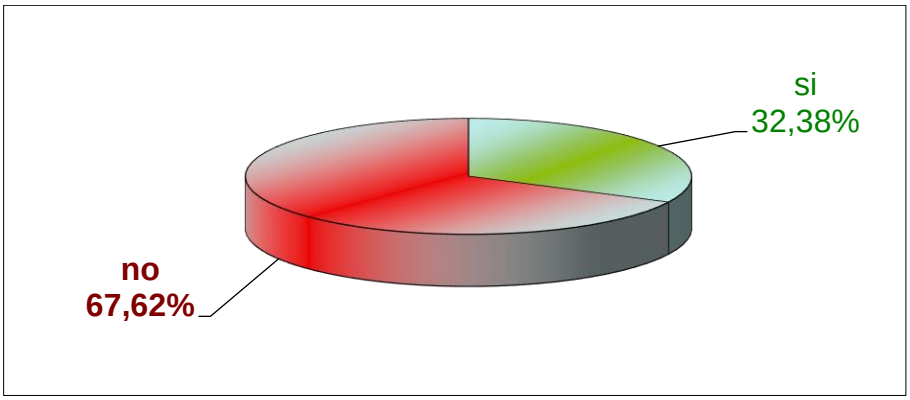

Gráfico 12-4. Resultado General del diagnóstico

Realizado por: Guffantte, Carlos, 2023

4.3 Identificación y valoración de Activos de la Información

4.3.1 Contexto

Realizar una guía que permita identificar en la Escuela de conducción Profesional ESPOCH CONDUESPOCH EP cuales son los activos de información valiosa y que se deba resguardar. Además, el de establecer la propiedad de los activos; cual es el criterio de confidencialidad, integridad y disponibilidad; identificar los activos, clasificar y definir cuál de éstos deben tener un mejor tratamiento.

4.3.2 Desarrollo

La información académica es considerada como un activo valioso de la Escuela de conducción Profesional ESPOCH CONDUESPOCH EP, pues contiene información de todos los estudiantes que han obtenido su licencia de conducir profesional tipo C, la misma que es revisada y validada por la Agencia Nacional de Tránsito, para ello es importante generar un inventario de estos activos tomando como referencia la metodología MAGERIT.

Tabla 12-4: Inventario de activos de la información

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
Información personal de docentes y estudiantes	ALTA	ALTA	MEDIA
Registro de Calificaciones	ALTA	ALTA	MEDIA
Registro de Asistencias	ALTA	ALTA	MEDIA
Registro de Actas de Grado	ALTA	ALTA	MEDIA
Información de estudiantes graduados	MEDIA	ALTA	MEDIA
Registro de promociones	MEDIA	ALTA	MEDIA

Realizado por: Guffantte, Carlos, 2023

Fuente: Dirección Pedagógica CONDUESPOCH EP.

4.4 Vulnerabilidades y Exploits.

Se han detectado las siguientes vulnerabilidades y exploits a los que están expuestos principalmente las bases de datos MySQL y Mariadb, mismas que almacenan la información sensible de la escuela de conducción ESPOCH ConduEspoch EP, tanto para los sistemas académicos GENETRIX de tipo local y SACON de tipo local y Web, para ello se ha utilizado el aplicativo web Vulnerability & Exploit Database.

Tabla 13-4: Vulnerabilidades Base de Datos MySQL

BASE DE DATOS	VULNERABILIDAD	DESCRIPCION
MySQL	CVE-2019-2530	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones compatibles que están afectadas son 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).
	CVE-2019-2494	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: DDL). Las versiones compatibles que están afectadas son 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio

		con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector
	CVE-2019-2536	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Packaging). Las versiones compatibles que están afectadas son 8.0.13 y anteriores. La vulnerabilidad difícil de explotar permite que un atacante con privilegios altos inicie sesión en la infraestructura donde se ejecuta el servidor MySQL para comprometer el servidor MySQL. Los ataques exitosos requieren la interacción humana de una persona que no sea el atacante y mientras la vulnerabilidad está en el servidor MySQL, los ataques pueden impactar significativamente en productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 5.0 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: L / AC: H / PR: H / UI: R / S: C / C: N / I: N / A: H).
	CVE-2019-2482	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: PS). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS:
	CVE-2019-2539	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Connection). Las versiones compatibles que están afectadas son 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples

		protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).

Realizado por: Guffantte, Carlos, 2023

Fuente: http://www.metasploit.com/modules/

Tabla 14-4: Exploits Base de Datos MySQL

BASE DE DATOS	EXPLOIT	DESCRIPCION
MySQL	Oracle MySQL for Microsoft Windows MOF Execution	Este módulo aprovecha un problema de configuración errónea de privilegios de archivos específicamente contra servidores MySQL de Windows (debido al uso de un archivo .mof). Esto puede resultar en la ejecución de código arbitrario en el contexto de SISTEMA. Este módulo requiere una cuenta MySQL válida en la máquina de destino.
	Oracle MySQL for Microsoft Windows FILE Privilege Abuse	Este módulo aprovecha un problema de configuración errónea de privilegios de archivos específicamente contra servidores MySQL de Windows. Este módulo hace uso indebido del privilegio de ARCHIVO para escribir una carga útil en el directorio de Todos los Usuarios de Inicio de Microsoft que se ejecutará cada vez que un usuario inicie sesión. El directorio predeterminado de Todos los Usuarios de Inicio utilizado por el módulo está presente en Windows 7.
	MySQL Authentication Bypass Password Dump	Este módulo explota una vulnerabilidad de omisión de contraseña en MySQL para extraer los nombres de usuario y los hashes de contraseña cifrados de un servidor MySQL. Estos hashes se almacenan como botín para su posterior agrietamiento.
	MySQL yaSSL CertDecoder::GetName Buffer Overflow	Este módulo explota un desbordamiento de búfer de pila en la implementación de yaSSL (1.9.8 y anterior) empaquetada con MySQL. Al enviar un certificado de cliente especialmente diseñado, un atacante puede ejecutar un código arbitrario. Esta vulnerabilidad está presente dentro de la función CertDecoder :: GetName dentro de "taocrypt / src / asn.cpp". Sin embargo, el búfer de pila en el que se escribe existe dentro del marco de pila de una función principal. NOTA: Esta

		vulnerabilidad requiere una configuración no predeterminada. Primero, el atacante debe poder pasar la autenticación basada en host. A continuación, el servidor debe configurarse para escuchar en una interfaz de red accesible. Por último, el servidor debe haberse configurado manualmente para usar SSL. El binario de la versión 5.5.0-m2 fue construido con / GS y / SafeSEH. Durante las pruebas en Windows XP SP3, estas protecciones evitaron con éxito la explotación. Las pruebas también se realizaron con mysql en Ubuntu 9.04. Aunque el código vulnerable está presente, tanto la versión 5.5.0-m2 construida a partir de la fuente como la versión 5.0.75 de un paquete binario no se pudieron explotar debido al uso de la función FORTIFY del compilador. Aunque suse11 se mencionó en la publicación del blog original, el paquete binario que proporcionan no contiene yaSSL ni es compatible con SSL.
	Oracle MySQL UDF Payload Execution	Este módulo crea y habilita un UDF personalizado (función definida por el usuario) en el host de destino a través de SELECT ... en el método DUMPFILE de inyección binaria. En las instalaciones predeterminadas de Microsoft Windows de MySQL (= <5.5.9), los permisos de escritura del directorio no se aplican, y el servicio MySQL se ejecuta como LocalSystem. NOTA: Este módulo dejará un ejecutable de carga útil en el sistema de destino cuando finalice el ataque, así como la DLL de UDF, y definirá o redefinirá las funciones sys_eval () y sys_exec ().

Realizado por: Guffantte, Carlos, 2023

Fuente: http://www.metasploit.com/modules/

Tabla 15-4: Vulnerabilidades Base de Datos Mariadb

BASE DE DATOS	VULNERABILIDAD	DESCRIPCION
Mariadb	(CVE-2018-2767) CESA-2018:2439	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Security: Encryption). Las versiones compatibles que están afectadas son 5.5.60 y anteriores, 5.6.40 y anteriores y 5.7.22 y anteriores. La vulnerabilidad difícil de explotar permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos

		de esta vulnerabilidad pueden resultar en un acceso de lectura no autorizado a un subconjunto de datos accesibles del Servidor MySQL. CVSS 3.0 Base Score 3.1 (Impactos de confidencialidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: L / UI: N / S: U / C: L / I: N / A: N).
	(CVE-2018-2781) CESA-2018:2439	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones admitidas que están afectadas son 5.5.59 y anteriores, 5.6.39 y anteriores y 5.7.21 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).
	(CVE-2018-2813) CESA-2018:2439	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: DDL). Las versiones admitidas que están afectadas son 5.5.59 y anteriores, 5.6.39 y anteriores y 5.7.21 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en un acceso de lectura no autorizado a un subconjunto de datos accesibles del Servidor MySQL. CVSS 3.0 Base Score 4.3 (Impactos de confidencialidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: L / I: N / A: N).
	(CVE-2018-2771) CESA-2018:2439	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Servidor: Bloqueo). Las versiones admitidas que están afectadas son 5.5.59 y anteriores, 5.6.39 y anteriores y 5.7.21 y anteriores. Una vulnerabilidad difícil de explotar permite a los atacantes con privilegios altos con acceso a la red a través de múltiples protocolos para comprometer el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un

		bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.4 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: H / UI: N / S: U / C: N / I: N / A: H).
	(CVE-2018-2755) CESA-2018:2439	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Replication). Las versiones admitidas que están afectadas son 5.5.59 y anteriores, 5.6.39 y anteriores y 5.7.21 y anteriores. Una vulnerabilidad difícil de explotar permite que un atacante no autenticado inicie sesión en la infraestructura donde se ejecuta el servidor MySQL para comprometer el servidor MySQL. Los ataques exitosos requieren la interacción humana de una persona que no sea el atacante y mientras la vulnerabilidad está en el servidor MySQL, los ataques pueden impactar significativamente en productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de MySQL Server. CVSS 3.0 Base Score 7.7 (Impactos de confidencialidad, integridad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: L / AC: H / PR: N / UI: R / S: C / C: H / I: H / A: H).

Realizado por: Guffantte, Carlos, 2023

Fuente: http://www.metasploit.com/modules/

Tabla 16-4: Exploits Base de Datos Mariadb

BASE DE DATOS	EXPLOIT	DESCRIPCION
Mariadb	No results for: Mariadb	No hay resultados de búsqueda

Realizado por: Guffantte, Carlos, 2023

Fuente: http://www.metasploit.com/modules/

4.4.1 Análisis de vulnerabilidades.

Una vez revisadas las vulnerabilidades de las bases de datos MySQL y Mariadb, que se encuentran en el servidor CENTOS 6.0 y almacenan toda la información de la Escuela de Conducción profesional ESPOCH CONDUESPOCH EP, es importante definir aquellas que son más factibles de suceder.

Tabla 17-4: Vulnerabilidades comunes en MySQL

BASE DE DATOS	VULNERABILIDAD	SUBCOMPONENTE	DESCRIPCION
MySQL	CVE-2019-2530	Server: Optimizer	Permiten que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySqL.
	CVE-2019-2494	Server: DDL	
	CVE-2019-2539	Server: Connection	

Realizado por: Guffantte, Carlos, 2023

Fuente: http://www.metasploit.com/modules/

Tabla 18-4: Vulnerabilidades comunes en Mariadb

BASE DE DATOS	VULNERABILIDAD	DESCRIPCION
Mariadb	(CVE-2018-2767) CESA-2018:2439	Permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL
	(CVE-2018-2755) CESA-2018:2439	Permite que un atacante no autenticado inicie sesión en la infraestructura donde se ejecuta el servidor MySQL para comprometer el servidor.
	(CVE-2018-2771) CESA-2018:2439	Es una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo).

Realizado por: Guffantte, Carlos, 2023

Fuente: http://www.metasploit.com/modules/

4.4.2 Análisis de exploits.

Es importante conocer que un exploit es un software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto. (Bitdefender, 2023)

Tabla 19-4: Exploits comunes para MySQL

BASE DE DATOS	EXPLOIT	DESCRIPCION
MySQL	Oracle MySQL for Microsoft Windows MOF Execution	Aprovecha un problema de configuración errónea de privilegios de archivos específicamente contra servidores MySQL de Windows.
	MySQL Authentication Bypass Password Dump	Explota una vulnerabilidad de omisión de contraseña en MySQL para extraer los nombres de usuario y contraseñas.

	Oracle MySQL UDF Payload Execution	Crea y habilita un UDF personalizado (función definida por el usuario) en el host de destino a través de SELECT ... en el método DUMPFILE de inyección binaria.

Realizado por: Guffantte, Carlos, 2023
Fuente: http://www.metasploit.com/modules/

4.4.3 Recomendaciones

- Muchas son las vulnerabilidades y exploits que se presentan en MySql, esto permite que los atacantes puedan establecer ciertos parámetros que comprometen la base de datos, por tal motivo se debe tener un cuidado extremo con este servicio con el fin de que la información no sea modificada, alterada o manipulada y al mismo tiempo que esté disponible y con el acceso asignado a personal autorizado.
- Mariadb presenta dificultades similares es decir puede ser vulnerable, no presenta exploits que podrían ser empleados para realizar ataques.

4.5 Sistema de Gestión de Seguridad de la Información.

4.5.1 Introducción

Una vez finalizado el análisis diferencial inicial de la empresa, desarrollado el Inventario de activos de la información y haber detectado las vulnerabilidades a las que está expuesta la información del sistema académico de ConduEspoch se requiere elaborar el Sistema de Gestión de Seguridad (SGSI).

ConduEspoch EP, al ser una empresa pública adjunta a la Escuela Superior Politécnica de Chimborazo que se dedica a la capacitación de profesionales para la obtención de la Licencia Profesional Tipo C, es importante entender que la seguridad de la información se refiere a la protección de los activos de información fundamentales para el éxito de cualquier organización; por tal razón es imprescindible que ConduEspoch posea este tipo de sistemas que garanticen la confidencialidad, integridad y disponibilidad de su información.

4.5.2 Objetivos

- Implementar un sistema de gestión de seguridad de la información, que permita brindar confianza a todo el personal de la empresa y sus estudiantes durante el tratamiento de los datos que aquí se gestiona.

- Lograr el compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.

4.5.3 Plan (planificar): PLANIFICACION DEL SGSI

Alcance del SGSI

El alcance es para todos los sistemas dirigidos al manejo de la información del proceso académico de la empresa. Quedan excluidas los demás departamentos de dirección, contabilidad y asesoría vial.

Políticas de Seguridad

La política de seguridad es un conjunto de normas y procedimientos de obligado cumplimiento para el tratamiento de los riesgos de seguridad empresariales. Nuestra empresa ConduEspoch EP entiende los riesgos que conlleva la seguridad de la información y por eso ha decidido implantar el SGSI basado en ISO 27001.

Todos los empleados de la organización deben de conocer, aceptar y cumplir dichas normas incluidos los que tengan una relación temporal, así como docentes y estudiantes que hagan uso de los sistemas o herramientas de la empresa.

Establecer responsabilidades, roles y funciones para el sistema de seguridad de la información; la política de seguridad de la información se debería revisar con planificación o en el caso que se produzcan cambios significativos para asegurar la idoneidad, adecuación y la eficacia de la continuidad.

La información debe estar clasificada según su valor, requisitos legales y criticidad para la organización, todos los empleados deberán recibir una formación adecuada y actualizada referente a las políticas y procedimientos de seguridad.

Metodología de evaluación de riesgos

Se establece que el proceso de evaluación de riesgos se llevara a cabo bajo las siguientes directrices:

- Elaborar los objetivos de la evaluación
- Definir el alcance de cada evaluación

- Establecer los criterios para seleccionar el equipo evaluador
    - Validar las competencias de los evaluadores
    - Aspectos éticos y morales.
- Especificar herramientas y procedimientos a utilizar en la evaluación
- Documentar y registrar las actividades realizadas
- Evaluar las competencias del personal de la empresa.

Identificar amenazas y vulnerabilidades

Procederemos a identificar las amenazas que pueden afectar a nuestros activos. Una amenaza es cualquier acción o acontecimiento que puede atentar contra nuestra seguridad.

- Nos enfocaremos en el control de acceso de usuarios a los sistemas informáticos

Identificar impactos

- Acceso indebido a información no asignada al usuario
- Mal uso de la información
- Perdida y mala manipulación de la información
- Daño de los equipos informáticos

Análisis y evaluación de riesgos

- El mal uso de contraseñas implica que la información no esté segura y se pueda provocar manipulación inadecuada de la misma, especialmente en el sistema de calificaciones de los estudiantes.
- La falta de control del acceso de los usuarios del sistema puede provocar perdida de la información y mal uso de los servicios de los equipos informáticos.

4.5.4 Do (hacer): IMPLEMENTACION DEL SGSI

En esta etapa definiremos como se implementarán los controles del documento de aplicabilidad, se asignarán responsables y los recursos. Las prioridades en la gestión de los riesgos deben quedar especificada.

Controles del SGSI

Los controles que se aplicarán en este apartado permitirán llevar un registro de las diferentes actividades para el manejo de contraseñas establecidas en las políticas de seguridad de la información, estos controles serán verificados por el Jefe del Departamento de Tecnologías.

Implementar los controles

- Entregar claves de acceso solo a personal autorizado
- No compartir las contraseñas
- Actualizar las contraseñas cada tres meses
- Limitar el acceso a los sistemas informáticos

Formato Creación de contraseñas

Tabla 20-4: DTIC: Responsable

Fecha	Responsable	Sistema	Usuario	Contraseña
10/10/2018	Galo Ibujes	Genetrix	academico	xxxxxxxxx
14/11/2108	Cristian Pilaguano	Genetrix	secretria	xxxxxxxxx
17/11/2019	Elvis Espinoza	Sacon	gerencia	xxxxxxxxx

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

Formato Cambio de contraseñas (cada 3 meses)

Tabla 21-4: DTIC: Responsable

Fecha	Responsable	Sistema	Usuario	Contraseña
10/01/2019	Galo Ibujes	Genetrix	academico	xxxxxxxxx
14/02/2019	Cristian Pilaguano	Genetrix	secretria	xxxxxxxxx
17/02/2019	Elvis Espinoza	Sacon	gerencia	xxxxxxxxx

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

Plan de tratamiento de riesgos

- Establecer contraseñas seguras para los usuarios
- Responsabilizar de la seguridad de las contraseñas a los usuarios asignados para el efecto
- Delimitar el acceso a determinados servicios del sistema informático.

Implantar el plan de tratamiento de riesgos

No todos los riesgos tienen el mismo origen, se debe enfocar en los más importantes como:

- Aplicar controles de seguridad para disminuir el riesgo como contraseñas seguras.
- Transferir el riesgo a otras personas entregando claves seguras personales.
- Evitar riegos al detener la ejecución de la actividad que genera un elevado riesgo como la asignación o entrega de claves a muchos usuarios.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Formación y concienciación

- Capacitar al personal sobre el uso de contraseñas
- Responsabilizar a los usuarios del servicio informático para evitar su mal uso
- Capacitar de los riesgos del mal uso del acceso al sistema para evitar plagio o daños del sistema

Operar el SGSI

- Establecer la operatividad del sistema de seguridad de la información a todos los miembros de la empresa para futuros monitoreo y seguimiento.

4.5.5 Check (verificar): MONITORIZAR Y SEGUIMIENTO DEL SGSI

La empresa deberá ejecutar procedimientos de monitorización y revisión para:

- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
- Identificar brechas e incidentes de seguridad.
- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación con lo previsto.

- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Revisar el SGSI

- Realizar revisiones periódicas del funcionamiento total del sistema de gestión de la información, para determinar nuevas vulnerabilidades.

Auditorías internas

- Establecer auditorías al sistema de gestión de la información anules para control su uso y funcionalidad en las áreas que se determinase necesario, para lo cual se deberá establecer un cronograma y personal que realice dicha actividad.

Registro de acciones y eventos

- Todas las actividades, acciones o tareas que se presenten en el sistema de gestión de la información deberán ser registradas y documentadas mediante un formato específico para cada actividad, la misma que deberá constar con la firma de responsabilidad de las áreas pertinentes.

4.5.6 Act (actuar): MANTENER Y MEJORA CONTINUA DEL SGSI

El Sistema de Gestión de Seguridad de la Información debe ser revisado periódicamente para asegurar que se cumplan los objetivos marcados por la organización.

Para realizar este seguimiento es necesario establecer una serie de indicadores que nos permitan determinar el estado del sistema. El análisis de indicadores requiere que cada uno de los controles implantados esté asociado a una serie de registros que recopilen la información necesaria para el estudio del control.

La empresa deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas necesarias.

- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

El sistema contiene multitud de entradas y salidas que deben ser revisadas, alguna de ellas por la dirección. En concreto la dirección de la empresa debe revisar los siguientes documentos:

- El informe de las auditorías internas que recoge el estado del sistema y de las incidencias detectadas.
- Los informes que el comité de gestión dirige al comité de dirección. Estos documentos son una fuente muy valiosa para el seguimiento del proyecto, ya que reflejan el estado del sistema y los puntos que requieren la supervisión de la dirección.
- El informe sobre las acciones realizadas por parte de los diferentes actores involucrados en el sistema.
- El resumen sobre el estado de las incidencias reportadas y la solución a las mismas.
- La revisión de los objetivos propuestos en cada una de las fases, así como el grado de cumplimiento de estos.
- Y el resumen sobre los cambios sufridos en la empresa.

Tras la revisión del Sistema de Gestión de Seguridad de la Información por parte de la dirección, se deberán ejecutar una serie de acciones como las siguientes:

- En primer lugar, hay que decidir si es necesario realizar mejoras dentro del sistema, cuáles se van a llevar a cabo y su repercusión económica y laboral dentro de la organización.
- En segundo lugar, se tendrá que actualizar la evaluación y la gestión de riesgos. En el caso de que se hayan observado cambios significativos en la organización, es necesario realizar un nuevo Análisis de Riesgos y un plan de tratamiento de estos.
- Por último, hay que realizar una actualización de los procedimientos y controles si estos han dejado de ser útiles o están obsoletos.

Es muy importante también realizar anualmente una auditoría interna que puede ser realizada por personal de la propia empresa, con el fin de elaborar un listado de todos los controles a revisar y todos los aspectos del sistema que necesitan ser analizados, con este listado el auditor realizará una revisión del sistema e indicará aquellos aspectos de mejora que se han detectado, así como la prioridad o gravedad de cada uno de ellos.

Las acciones preventivas se deben implementar poco a poco para conseguir que el sistema sea cada vez más robusto.

4.6 Análisis diferencial final.

Luego de la aplicación de los parámetros establecidos en el sistema de gestión de seguridad de la información y de la ejecución del manual de políticas de seguridad se ha considerado los siguientes dominios de control para realizar un análisis final mediante OWASP de la situación de la Escuela de Conducción profesional ESPOCH CONDUESPOCH EP.

Tabla 22-4: Dominios de Control

NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	6	5	1	0	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	8	6	2	0	0
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	9	6	2	1	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	6	4	2	0	0
DOMINIO 9 - CONTROL DE ACCESO	18	11	5	2	0
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	11	9	1	0	1
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	23	17	4	2	0
DOMINIO 14 – ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	8	4	2	1	1
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	5	4	1	0	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	5	3	2	0	0
DOMINIO 18 – GESTION DE CUMPLIMIENTO	5	3	1	0	1

Realizado por: Guffantte, Carlos, 2023

Fuente: CONDUESPOCH EP.

Los resultados obtenidos, permiten indicar que se ha podido lograr reducir el riesgo en cuanto a la seguridad de la información académica de la empresa alcanzando niveles muy aceptables de ejecución como se muestra a continuación.

Tabla 23-4: Rendimiento alcanzado

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	28,5%
LOGRO2	HACER	40%	23,6%
LOGRO3	VERIFICAR	15%	10,0%
	ACTUAR	15%	12,5%
	TOTAL	100%	74,6%

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

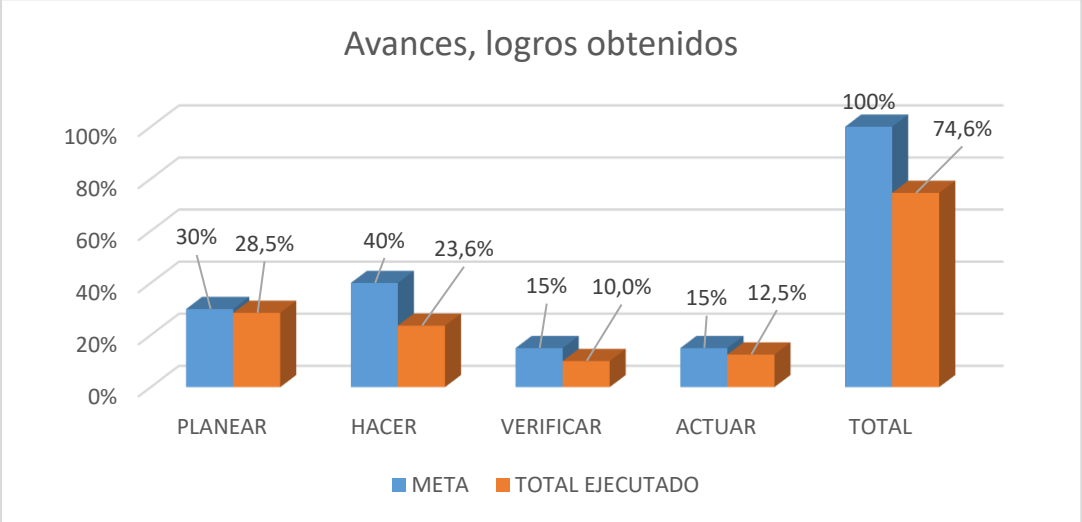

Gráfico 13-4. Avances, logros obtenidos

Realizado por: Guffantte, Carlos, 2023

4.7 Comprobación de la Hipótesis General.

Una vez realizado los diferentes análisis de la seguridad de la información de la Escuela de Conducción profesional ESPOCH CONDUEPSPOCH EP, se presentará el sistema de hipótesis comenzando con la especificación de hipótesis nula y la hipótesis de investigación.

Hipótesis Nula H_0: La implementación de políticas para gestionar los riesgos de seguridad de la información académica, no permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch.

Hipótesis de investigación H_1.: La implementación de políticas para gestionar los riesgos de seguridad de la información académica, permitirán mejorar la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch.

La representación estadística de la hipótesis nula y la de investigación sería el de un caso unilateral, tal como sigue:

$$H_0: \mu 2 \leq \mu 1$$

$$H_1: \mu 2 > \mu 1$$

Luego de establecer las Hipótesis, se procede a realizar el método de Chi-cuadrado, y se obtiene los siguientes resultados, para lo cual se ha considerado el análisis diferencial establecido antes y después de aplicar las políticas para la gestión de la seguridad de la información académica de la empresa.

Tabla 24-4: Resultados Chi-Cuadrado

DOMINIOS	ANTES		DESPUES		CHI CUADRADO	
	si	no	si	no		
POLÍTICAS DE SEGURIDAD	0	6	5	1	30	
ORGANIZACIÓN DE LA SEGURIDAD	0	8	6	2	24	
ADMINISTRACIÓN DE ACTIVOS	5	1	4	2	1	
SEGURIDAD DE LOS RRHH	2	7	6	3	8	
SEGURIDAD FÍSICA Y DEL AMBIENTE	7	4	9	2	2	
GESTIÓN DE COMUNICACIONES Y OPERACIONES	11	12	17	6	8	
CONTROL DE ACCESOS	5	13	11	7	8	
DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	1	7	4	3	8	
ADMINISTRACIÓN DE INCIDENTES	2	3	4	1	5	
GESTIÓN DE LA CONTINUIDAD DE LA EMPRESA	0	5	3	2	8	
CUMPLIMIENTO	1	4	3	2	3	
	Chi-Cuadrado TOTAL				105,14	**
	Chi-Cuadrado al 0,05, 10				18,31	
	Chi-Cuadrado al 0,01, 10				23,21	
	Prob. Chi-Cuadrado				5,0661E-18	

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

Como se puede observar el cálculo del Chi-Cuadrado determina una alta significancia (**) así como su probabilidad, obteniéndose los siguientes resultados:

Nivel de significancia = 5% = 0,05
Grados de libertad = 10
Chi-Cuadrado Total = 1 al 0,05,10 = 18,31

Nivel de significancia = 1% = 0,01
Grados de libertad = 10
Chi-Cuadrado Total = 1 al 0,01,10 = 23,21

Chi-Cuardado Total = 105,14 (**)

Prob. Chi-Cuadrado = 5,0661E-18

Estos resultados nos permiten determinar que, si hubo un cambio significativo una vez implementadas las políticas de gestión de riesgos para la seguridad de la información, de tal forma se rechaza la hipótesis nula y se demuestra la validez de la hipótesis de investigación la misma que influye en la mitigación de vulnerabilidades existentes en la empresa pública ESPOCH ConduEspoch

A continuación, se presentan los resultados obtenidos de forma general:

Tabla 25-4: Resultados Generales Obtenidos

ACTIVIDAD	ANTES		DESPUES	
	SI	NO	SI	NO
Políticas para la gestión de riesgos de seguridad en el manejo de la información académica.	32,38%	67,62%	74,6%	25,4%

Realizado por: Guffantte, Carlos, 2023

Fuente: Propia

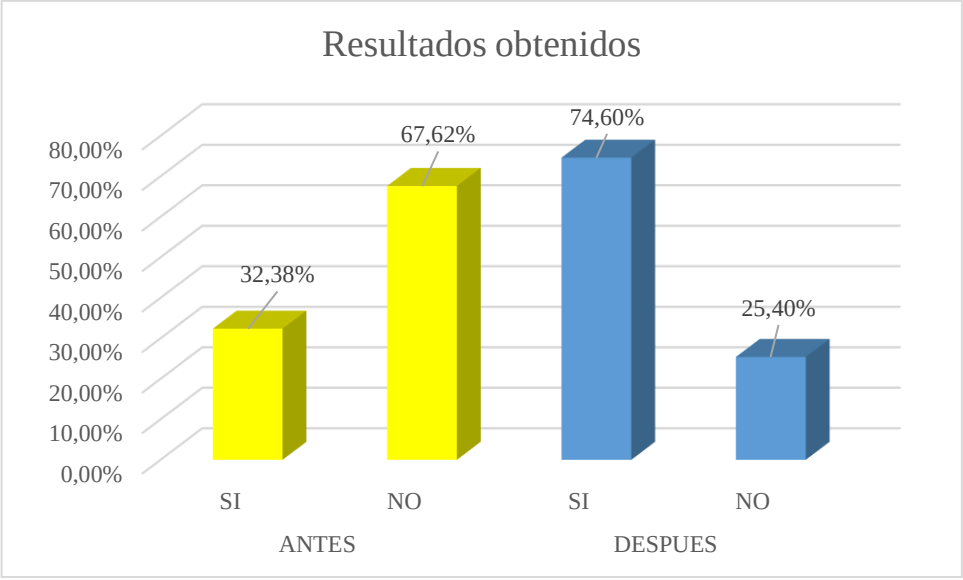

Gráfico 14-4. Resultados Obtenidos

Realizado por: Guffantte, Carlos, 2023

CAPITULO V

5. PROPUESTA

5.1 Determinación de la Propuesta

En el presente capítulo se presenta una propuesta para la elaboración de políticas de seguridad de la información para la empresa pública ESPOCH CONDUESPOCH EP, es pertinente que regule o norme ciertos parámetros que permitirán garantizar la seguridad, integridad y confidencialidad de los datos académicos que la empresa posee.

Se considera para esta propuesta los lineamientos revisados en el marco teórico de este documento, considerando como base fundamental la aplicación del sistema de gestión de seguridad de la información SGSI.

5.2 Manual de Políticas de Seguridad de la Información

5.2.1 Introducción

La Gerencia de ConduEspoch, determina a la información como un activo de alta importancia para la empresa, que permite el desarrollo continuo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El departamento de tecnologías DTIC, diseña y establece las políticas, las cuales deben ser adoptadas por el personal administrativo, docente, estudiantes y terceros que presten sus servicios o tengan algún tipo de relación con la empresa.; estas se encuentran enfocadas y basadas en la norma ISO 27001. [1]

5.2.2 Alcance

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los Directivos, personal administrativo,

[1] ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

docente, estudiantes y terceros que presten sus servicios o tengan algún tipo de relación con la empresa, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, además es necesario aportar en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas.

5.2.3 Objetivos

- Establecer las políticas que regulan la seguridad de la información en la empresa ConduEspoch y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todo el personal administrativo, docente, estudiantes y terceros que presten sus servicios o tengan algún tipo de relación con la empresa, bajo el liderazgo del Departamento de Tecnologías de Información.
- Implementar un sistema de gestión de seguridad de la información, que permita brindar confianza a todo el personal de la empresa y sus estudiantes durante el tratamiento de los datos que aquí se gestiona.
- Lograr el compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.

5.2.4 Responsabilidades

En esta etapa definiremos como se implementarán los controles, se asignarán responsables y los recursos. Las prioridades en la gestión de los riesgos deben quedar especificada.

- Los controles que se aplicarán en este apartado permitirán llevar un registro de las diferentes actividades para el manejo de los datos establecidos en las políticas de seguridad de la información, estos controles serán verificados por el jefe del Departamento de Tecnologías.
- La dirección tiene la responsabilidad de garantizar que sea establecidos los objetivos y planes del SGSI y que estos sean revisados de forma anual.
- Cada ejecutivo tiene la responsabilidad de garantizar que las personas que tiene a su cargo protejan la información de sus procesos asignados.
- Los empleados de la empresa deben ser conscientes de los riesgos de seguridad de la información dentro de sus actividades diarias.

5.2.5 Principales Resultados

- Controlar los posibles riesgos de seguridad de la información a los que se encuentra expuesta la información de la empresa
- Que los incidentes de seguridad de la información no darán lugar a costos considerables e inesperados a los procesos, productos y servicios de la empresa.
- Las posibles pérdidas por fraude se conocerán y estarán dentro de los umbrales aceptables.

5.3 Políticas de Seguridad de la Información

5.3.1 Políticas sobre Plataformas de Sistemas Operativos

El propósito de esta política sobre plataformas de sistemas operativos es garantizar el uso correcto de los sistemas operativos instalados en los equipos de la escuela de conducción ConduEspoch EP, tanto en las estaciones de trabajo como en el servidor de información.

- El sistema operativo deberá tener su licencia original para evitar problemas de copyright, salvo el caso de que la empresa utilice software libre.
- El sistema operativo deberá estar actualizado.
- El sistema operativo debe permitir compartir los recursos justamente.
- Debe proteger a todos los procesos de los demás procesos.
- Deberá proteger a los datos de todos los usuarios de los demás usuarios.
- Asegurar la integridad de la información

5.3.2 Políticas sobre instalación de sistemas operativos.

El propósito de esta política sobre la instalación de sistemas operativos es establecer los requerimientos mínimos que se deben considerar al momento de realizar dicho proceso, determinando responsables.

- Responsabilizar al departamento de tecnología de la información como único responsable de la instalación de sistemas operativos.
- Reportar a la dirección de tecnologías sobre el proceso de instalación de un nuevo sistema operativo.
- Verificar que el equipo cuente con los requerimientos mínimos en hardware para que soporte la versión del sistema operativo que se desea instalar.

- Para la instalación de un sistema operativo se deberá considerar primero los requisitos mínimos de instalación como son las descargas de los controladores del equipo, crear los medios de controladores de almacenamiento masivo que se utilizará en el proceso de instalación y la configuración del BIOS.
- Utilizar software original para la instalación del sistema operativo.
- Se recomienda aplicar la guía de instalación según sea el caso.
- Instalar los controladores de los diferentes dispositivos hardware de los que disponga el equipo.

5.3.3 Políticas sobre actualizaciones a los sistemas operativos

El propósito de esta política sobre las actualizaciones de sistemas operativos es establecer los requerimientos mínimos que se deben considerar al momento de realizar dicho proceso, determinando responsables y evidenciar por qué se realizará la actualización.

- Se deberá realizar una prueba de validación de la versión que se desea instalar para evitar posibles tiempos de inactividad o pérdida de datos.
- Se actualizará un sistema operativo cuando se detecte un problema existente, como una revisión por errores de programación o un parche de seguridad.
- Consultar las políticas de instalación de parches de seguridad a fin de obtener información detallada sobre cómo aplicarlo en sus sistemas.
- Se actualizará el sistema operativo en caso de necesitar un mantenimiento o mejora de sus funciones.
- Realizar actualizaciones periódicas de toda nuestra infraestructura tecnológica tanto para solventar bugs (errores de software), como para mejorar el rendimiento de los servicios o permitir la aparición de nuevas aplicaciones.
- El departamento de tecnología de la información será el único responsable de realizar las actualizaciones de sistemas operativos en la empresa tanto en equipos de trabajo como en servidores.

5.3.4 Políticas sobre Programas antivirus

El propósito de esta política sobre programas antivirus es garantizar el buen funcionamiento de los equipos informáticos de la empresa y evitar la pérdida de información.

- Los usuarios de cada uno de los Sistemas de información son responsables de reportar inmediatamente en caso de encontrar situaciones sospechosas en el sistema, como por

ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades anormales.

- Siempre que se requiera del uso de USB u otros medios de almacenamiento en cualquier computador de la empresa, debe verificarse previamente que están libres de virus u otros agentes dañinos.
- Cualquier equipo que se conecte a la red, debe ser escaneado con un sistema antivirus actualizado antes de tener acceso a la misma.
- La responsabilidad de evaluar la posible existencia de virus en forma adecuada y con el software antivirus en toda la información que provenga de Internet, recae directamente sobre el usuario. Este proceso debe ser realizado antes de abrir o ejecutar los archivos, así como antes de divulgarlos a través de la red, con el fin de no propagar virus informáticos u otros programas.

5.3.5 Políticas sobre instalación de aplicaciones

El propósito de esta política sobre la instalación de aplicaciones es regular que software será instalado en los equipos informáticos de la empresa, lo que será determinado según el área de trabajo respectiva.

- Todo el personal que accede a los Sistemas de Información de la entidad debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
- Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- También se tiene prohibido borrar cualquiera de los programas instalados legalmente.
- Solo se pueden utilizar aplicaciones que la empresa considere adecuada para las funciones que se asignen a desempeñar.

5.3.6 Políticas sobre uso de espacio de disco duro

El propósito de esta política sobre el uso de espacio de disco duro permitirá determinar la cantidad de información almacenada en este dispositivo.

- Precautelar la información y evitar el destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos, almacenados en los discos duros.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo de manera identificada.

- Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas al control de virus.
- Solicitar la autorización respectiva en el departamento de tecnologías para eliminar información que se crea no necesaria.
- Realizar tareas de respaldo de la información de manera periódica.
- Se debe verificar periódicamente, la integridad de los respaldos que se están almacenando
- La información sensible, crítica o valiosa almacenada en medios magnéticos durante tiempo prolongado, debe ponerse a prueba al menos cada 2 o 3 meses para asegurarse de que la información aún es recuperable o debe copiarse a un medio nuevo.
- Es obligación del departamento de tecnologías almacenar y precautelar la información que se respalde en cada área de la empresa.
- Establecer normas de backup respectivo para mantener la seguridad de la información.

5.3.7 Políticas sobre Navegador de Internet

El propósito de esta política sobre el navegador de internet es el indicar cuáles serán los navegadores escogidos para acceso a internet que deberán ser utilizados por el personal de la empresa.

- Los usuarios deben acceder a internet usando el navegador que viene preinstalado (por defecto) con el sistema operativo. Para casos especiales de navegación o utilización de algunos programas se autoriza el uso de otros navegadores como Google Chrome o Mozilla, los cuales serán instalados por el departamento de Tecnología.
- La configuración y puesta a punto de los navegadores será responsabilidad exclusiva del departamento de tecnologías y siempre estará orientado a asegurar el buen uso del ancho de banda para el acceso a las aplicaciones de interés de la Organización
- Cada usuario será responsable por cualquier afectación no deseada que provoque al intentar instalar algún navegador de internet que no esté preestablecido.
- Se deberá periódicamente controlar el historial y las cookies de navegación que pueden provocar errores en el acceso a los datos.

5.3.8 Políticas sobre el uso del Internet

El propósito de esta política sobre el uso de internet es normar el proceso de navegación de los empleados de la empresa, restringiendo accesos a sitios no permitidos y determinando el uso adecuado de este servicio.

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo.
- Todos los colaboradores de la empresa tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma.
- No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.
- En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada.
- El uso de Internet podrá ser registrado y revisado por el Departamento de Tecnología ante cualquier requerimiento de Contraloría Interna o Gerencia de tal forma que sirva como antecedente ante una investigación.

5.3.9 Políticas sobre el uso de correo electrónico

El propósito de esta política de correo electrónico es garantizar el uso correcto del sistema de correo electrónico de ConduEspoch EP. y hacer que los usuarios conozcan lo que la empresa considera un uso aceptable e inaceptable de su sistema de correo electrónico. Esta política describe los requisitos mínimos para el uso del correo electrónico dentro de la red de ConduEspoch EP.

- Todo uso del correo electrónico debe ser coherente con las políticas y procedimientos de ConduEspoch EP de conducta ética, seguridad, cumplimiento de las leyes aplicables y prácticas comerciales adecuadas.

- La cuenta de correo electrónico de ConduEspoch EP debe utilizarse principalmente para fines relacionados con el negocio de ConduEspoch EP; la comunicación personal está permitida de forma limitada, pero los usos comerciales no relacionados con ConduEspoch EP están prohibidos.
- Todos los datos de ConduEspoch EP contenidos en un mensaje de correo electrónico o un archivo adjunto deben estar protegidos de acuerdo con el estándar de protección de datos.
- El correo electrónico identificado como un registro comercial de ConduEspoch EP se conservará de acuerdo con el Programa de retención de registros de ConduEspoch EP
- El sistema de correo electrónico ConduEspoch EP no debe utilizarse para la creación o distribución de mensajes molestos u ofensivos, incluidos comentarios ofensivos sobre raza, género, color de cabello, discapacidades, edad, orientación sexual, pornografía, creencias y prácticas religiosas. Creencias políticas, u origen nacional. Los empleados que reciban correos electrónicos con este contenido de cualquier empleado de ConduEspoch EP deben informar el asunto al departamento de tecnologías.
- Se prohíbe a los usuarios reenviar automáticamente el correo electrónico de ConduEspoch EP a un sistema de correo electrónico de terceros. Los mensajes individuales que son reenviados por el usuario no deben contener información confidencial o superior de ConduEspoch EP.
- Se prohíbe a los usuarios utilizar sistemas de correo electrónico y servidores de almacenamiento de terceros, como Google, Yahoo y MSN Hotmail, etc., para realizar negocios de ConduEspoch EP, crear o memorizar cualquier transacción vinculante, o almacenar o retener correo electrónico en nombre de ConduEspoch EP. Dichas comunicaciones y transacciones deben realizarse a través de los canales adecuados utilizando la documentación aprobada por ConduEspoch EP.
- El uso de una cantidad razonable de recursos de ConduEspoch EP para correos electrónicos personales es aceptable, pero los correos electrónicos no relacionados con el trabajo se guardarán en una carpeta separada del correo electrónico relacionado con el trabajo. Está prohibido enviar cartas en cadena o correos electrónicos de broma desde una cuenta de correo electrónico de ConduEspoch EP.
- Los empleados de ConduEspoch EP no deben esperar privacidad en nada de lo que almacenan, envían o reciben en el sistema de correo electrónico de la empresa.
- ConduEspoch EP puede monitorear mensajes sin previo aviso. ConduEspoch EP no está obligado a controlar los mensajes de correo electrónico.

5.3.10 Política de protección de contraseña

El propósito de esta política es establecer un estándar para la creación de contraseñas seguras y la protección de dichas contraseñas.

Creación de contraseña

- Todas las contraseñas de nivel de usuario y de sistema deben cumplir con las pautas para la construcción de contraseñas.
- Los usuarios deben usar una contraseña única y separada para cada una de sus cuentas relacionadas con el trabajo. Los usuarios no pueden usar contraseñas relacionadas con el trabajo para sus propias cuentas personales.
- Las cuentas de usuario que tienen privilegios de nivel de sistema otorgados a través de membresías deben tener una contraseña única de todas las demás cuentas que posee ese usuario para acceder a los privilegios de nivel de sistema. Además, se recomienda encarecidamente que se utilice algún tipo de autenticación multifactor para cualquier cuenta privilegiada,

Cambio de contraseña

- Las contraseñas deben cambiarse de manera periódica o cuando haya motivos para creer que una contraseña se ha comprometido.
- El departamento de Tecnología puede realizar el descifrado o el cálculo de contraseñas de forma periódica o aleatoria. Si se adivina o rompe una contraseña durante una de estas exploraciones, el usuario deberá cambiarla para cumplir con las pautas para la construcción de contraseñas.

Protección de contraseña

- Las contraseñas no deben compartirse con nadie, incluidos supervisores y compañeros de trabajo. Todas las contraseñas deben tratarse como información confidencial ConduEspoch EP.
- Las contraseñas no se deben insertar en mensajes de correo electrónico, casos de alianza u otras formas de comunicación electrónica, ni se deben revelar por teléfono a nadie.
- Las contraseñas se pueden almacenar solo en los "administradores de contraseñas" autorizados por la organización.
- No utilice la función "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web).

- Cualquier usuario que sospeche que su contraseña pudo haber sido comprometida debe reportar el incidente y cambiar todas las contraseñas

Desarrollo de aplicaciones

- Los desarrolladores de aplicaciones deben asegurarse de que sus programas contengan las siguientes precauciones de seguridad:
- Las aplicaciones deben admitir la autenticación de usuarios individuales, no de grupos.
- Las aplicaciones no deben almacenar contraseñas en texto claro o en forma fácilmente reversible.
- Las aplicaciones no deben transmitir contraseñas en texto claro a través de la red.
- Las aplicaciones deben proporcionar algún tipo de gestión de roles, de modo que un usuario pueda asumir las funciones de otro sin tener que conocer la contraseña del otro.

Autenticación multifactor

- La autenticación multifactor es altamente recomendable y debe usarse siempre que sea posible, no solo para cuentas relacionadas con el trabajo, sino también para cuentas personales. [2]

Responsabilidades de los usuarios finales.

Un usuario final de los sistemas de información de ConduEspoch EP., tiene las siguientes responsabilidades:

- El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada.
- La cuenta es para uso personal e intransferible.
- La cuenta de usuario se protegerá mediante una contraseña
- Debe conservar su contraseña segura
- No debe guardar las contraseñas de forma legible en medios impresos expuestos a otros usuarios o terceros en la empresa.
- No deben entregar su contraseña a nadie, incluso a los administradores o personal de soporte técnico de la escuela en caso de que ellos lo soliciten como condición para realizar un servicio.
- No se debe utilizar en sistemas externos incluyendo bancos y redes sociales una clave que se esté usando en los sistemas de ConduEspoch EP.

[2] La autenticación multifactor (MFA) es un sistema de seguridad que requiere más de una forma de autenticación para verificar la legitimidad de una transacción.

- No se debe utilizar la función “Recordar contraseña” en los navegadores
- No se deben prestar las contraseñas y no se deben utilizar las credenciales de acceso de usuarios retirados o en período de vacaciones.

Remoción de cuentas y permisos de usuarios

- En el momento en que un usuario termina su vinculación laboral, contractual o convenio con la empresa se deben remover todos sus permisos en los sistemas de información y se debe desactivar el acceso del usuario a los mismos.

5.3.11 Política de comunicación inalámbrica

El propósito de esta política es proteger los activos de información que son propiedad de ConduEspoch EP, proporciona dispositivos informáticos, redes y otros sistemas de información electrónica para cumplir misiones, objetivos e iniciativas. ConduEspoch EP otorga acceso a estos recursos como un privilegio y debe administrarlos de manera responsable para mantener la confidencialidad, integridad y disponibilidad de todos los activos de información.

Esta política especifica las condiciones que deben cumplir los dispositivos de infraestructura inalámbrica para conectarse a la red de ConduEspoch EP. Solo aquellos dispositivos de infraestructura inalámbrica que cumplen con los estándares especificados en esta política o que reciben una excepción del Departamento de Tecnología de la Información están aprobados para la conectividad a una red de ConduEspoch EP.

- Utilizar los protocolos de cifrado aprobados por ConduEspoch EP.
- Mantener una dirección de hardware (dirección MAC) que se pueda registrar y rastrear.
- No interferir con las implementaciones de acceso inalámbrico mantenidas por otras organizaciones de soporte.
- Los dispositivos de infraestructura inalámbrica que brindan acceso directo a la red corporativa de ConduEspoch EP, deben cumplir con los Requisitos de dispositivos inalámbricos domésticos como se detalla en el Estándar de comunicación inalámbrica.
- Los dispositivos de infraestructura inalámbrica que no cumplan con los requisitos de dispositivos inalámbricos domésticos deben instalarse de manera que prohíba el acceso directo a la red corporativa de ConduEspoch EP. El acceso a la red corporativa de ConduEspoch EP a través de este dispositivo debe utilizar la autenticación de acceso remoto estándar.

5.3.12 Política de responsabilidad por los activos

El propósito de esta política de responsabilidad por los activos es para concientizar al personal de la empresa sobre la importancia y seguridad que se debe tener sobre la información que se maneja, pues es de carácter muy sensible, misma que es auditada por la Agencia Nacional de Tránsito.

- ConduEspoch EP como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.
- La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de ConduEspoch EP, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del negocio.
- Toda la información sensible de ConduEspoch EP, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Gerencia. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

5.3.13 Recomendaciones

- Aplicar las normas establecidas en el presente manual de seguridad de la información para precautelar los datos de la empresa.
- Difundir este manual para conocimiento de todo el personal de la empresa y su compromiso de acatar las disposiciones establecidas en el mismo.
- Elaborar un Sistema de Gestión de Seguridad de la Información SGSI para la empresa ConduEspoch.

CONCLUSIONES

- La coincidencia entre las normas ISO 27001, 27005 y OWASP están diseñadas para mantener a las empresas seguras mientras siguen los estándares de calidad, así mismo, cada norma utiliza parámetros para mantener seguros los activos de la empresa, y finalmente la diferencia más destacada es que solo la ISO 27001 es una norma de certificación, para su implementación se utilizan otros estándares, si bien OWASP no es un estándar, es un método que permite mantener el control sobre las vulnerabilidades existentes en una institución.

- Como resultado de la investigación se puede concluir que la implementación de políticas para gestionar los riesgos de seguridad de la información académica logra la mitigación de vulnerabilidades existentes en la Escuela de Conducción profesional ESPOCH ConduEspoch de un 74,60% a un 25,4% según los análisis realizados, teniendo en cuenta que se debe llegar a la máxima mitigación de riesgos para así llegar al nivel más alto de seguridad.

- La implementación de las políticas de seguridad de la información permitió evidenciar que, con base en la experiencia, los empleados utilizan sus propios conocimientos para saber lo que no deben hacer, al proponer una política basada en los controles del estándar ISO y afines a la ley ecuatoriana, permite sensibilizarlos, de esta manera, con sus obligaciones y compromisos, la seguridad de la información aumenta de 0% a un 28,5%.

- Al implementar una política de control de seguridad de información se puede demostrar que la Escuela de Conducción Profesional ESPOCH CONDUESPOCH EP, mejorará la calidad de la seguridad de la información siempre que la gerencia y los empleados estén comprometidos con su uso continuo.

- El personal administrativo, docentes y estudiantes de la Escuela de conducción profesional ESPOCH CONDUESPOCH EP no disponen de conocimientos mínimos en seguridad de la información lo que es una vulnerabilidad más en el servicio.

- Las vulnerabilidades más frecuentes que se pueden dar a las bases de datos Mariadb, que almacena la información web de la escuela son: (CVE-2018-2767) CESA-2018:2439, compromete el servidor MySQL, (CVE-2018-2755) CESA-2018:2439 se dé un inicio de sesión no autorizado y (CVE-2018-2771) CESA-2018:2439 puede causar un DOS completo.

RECOMENDACIONES

- Es importante basarse en una norma estandarizada internacional como la ISO 27001 la cual es la única certificable, es escalable y permite cambios continuos y se adapta fácilmente a las necesidades de cualquier empresa.

- El uso de las políticas propuestas en este trabajo de investigación permitirá a la Escuela de Conducción profesional ESPOCH CONDUESPOCH EP controlar mejor la seguridad de la información, con base en las normas ISO, lo que permitirá, en referencia a la calidad de los servicios que brinda, garantizar a sus potenciales usuarios el adecuado tratamiento de la información.

- Con el fin de evaluar y gestionar los riesgos de seguridad, considere la conveniencia que la herramienta brinda a sus usuarios, así como la información existente y si existen aplicaciones que puedan identificar de manera más fácil y rápida las vulnerabilidades que se pueden encontrar de esta manera para ayudar a corregir y mitigar los resultados de las vulnerabilidades.

- A más de identificar las vulnerabilidades es recomendable que la empresa esté preparada para superar cualquier eventualidad que dificulte las actividades diarias del personal, esto se logra siempre y cuando el Departamento de Tecnologías de la Información y Comunicaciones regule el cumplimiento y evaluación en cuanto a la aplicación de las políticas de seguridad.

GLOSARIO

TERMINO	SIGNIFICADO
ANT	Agencia Nacional de Tránsito
Antivirus	Programa que detecta la presencia de un virus informático en una computadora y lo elimina.
Apartado 410-01	Organización informática.
Apartado 410-02	Segregación de funciones.
Apartado 410-03	Plan informático estratégico de tecnología.
Apartado 410-10	Seguridad de tecnología de Información
Autodiagnóstico	Acción que permite a las organizaciones hacer una revisión de sus procesos internos para conocer su situación
Backup	Proceso de hacer copias de datos para poder restaurar el original en caso de pérdida
BIOS	Sistema básico de entrada / salida, responsable de iniciar el sistema
Bitcoin	Es una moneda digital descentralizada y un sistema de pago sin banco central o administrador único
CENTOS	Community ENTerprise Operating System, es una distribución Linux
Chrome	Es un navegador web de código cerrado desarrollado por Google
Confidencialidad	Busca prevenir el acceso no autorizado a la información
Control	Función que permite la supervisión y comparación de los resultados obtenidos contra los resultados esperados originalmente
Cookies	Son pequeños fragmentos de texto que los sitios web que visitas envían al navegador para recordar información sobre tu visita
Copyright	Expresión utilizada para referirse a los derechos que protegen la propiedad intelectual de un autor
CSAE	Consejo Superior de Administración Electrónica
Database	Una base de datos es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático.
DDL	El lenguaje de definición de datos perite describir los datos y sus relaciones en una base de datos
DDNS	Dynamic Domain Name System, sirve de ayuda a la hora de reenviar las direcciones IP de tu red doméstica, que cambian constantemente, a un nombre de dominio fijo.
Disponibilidad	Busca asegurar acceso confiable y oportuno a los datos
DOS	Es una capacidad no autorizada para causar un bloqueo
DTIC	Departamento de tecnología de la información y comunicación
Encriptado	Pilar fundamentales de la ciberseguridad y sirve para proteger los datos y evitar que se roben, cambien o se vulneren
Exploit	Software, fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto
Genetrix	Sistema académico de escritorio
Integridad	Busca asegurar que no se realicen modificaciones a la información
ISO	Organización Internacional de Normalización, se trata de un órgano cuya principal función es la de crear normas de carácter internacional

ISO 27001	Establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información
ISO 27002	Utilizado como referencia para los controles al implementar un Sistema de Gestión de Seguridad de la Información
ISO 27005	Suministra las directrices para gestionar los riesgos que puede sufrir la información de una empresa
MAC	Identificador único para un dispositivo de red, en ocasiones conocida también como la dirección física
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
Mariadb	Sistema de gestión de base de datos de código abierto que ofrece una mayor eficiencia, un mejor rendimiento de la base de datos y soporte para varios tipos de datos mediante múltiples motores de almacenamiento.
MFA	Autentficación multifactor
Módem	Dispositivo que envía información entre el mundo exterior o red de área extensa (WAN) y el hogar
Mozilla	Navegador gratuito de código abierto cuyo desarrollo es supervisado por Mozilla Corporation
MySQL	Sistema de gestión de bases de datos relacional de código abierto respaldado por Oracle y basado en el lenguaje de consulta estructurado (SQL)
Oracle	Herramienta cliente/servidor para la gestión de Bases de Datos
Outsourcing	Proceso de subcontratar tareas o áreas de una empresa a proveedores externos
OWASP	Open Web Application Security Project
Password	Método de autentificación que se utiliza para controlar el acceso a información, espacios o recursos
Path	Especifica las rutas en las cuales el intérprete de comandos debe buscar los programas a ejecutar
PDCA	Planear-Hacer-Chequear-Actuar
Políticas	Conjunto de actividades que se asocian con la toma de decisiones en grupo, u otras formas de relaciones de poder entre individuos, como la distribución de recursos o el estatus
Riesgo	Es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo
Routing	Proceso de selección de rutas en cualquier red
SACON	Sistema académico web
SGSI	Sistema de gestión de seguridad de la información
SI	Sistema de información
SO	Sistema Operativo
SQL	Lenguaje de programación para almacenar y procesar información en una base de datos relacional.
SQLINJECTION	Es un tipo de vulnerabilidad en la que un atacante usa un trozo de código SQL para manipular una base de datos y acceder a información potencialmente valiosa.
SSL	Tecnología estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web
Testing	Método para verificar si al diseñar un producto digital este cumple con los requisitos esperados y se encuentra libre de errores y brechas
TI	Tecnología de información

UDF	Función definida por el usuario
USB	Universal Serial Bus, dispositivo de almacenamiento masivo que utiliza memoria flash para guardar la información que puede requerir
Vulnerabilidad	Es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre
Web	World Wide Web, sistema interconectado de páginas web públicas accesibles a través de Internet

BIBLIOGRAFÍA

Areitio, J. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* Madrid: Ediciones Paraninfo S.A.

Bitdefender. (17 de 01 de 2023). *Bitdefender*. Obtenido de https://www.bitdefender.es/consumer/support/

Borghello, C. (2001). *"Seguridad Informática: sus implicacncias e implementación".* Argentina.

Constituyente, A. (2008). *Constitución de la República del Ecuador.* Obtenido de https://s3.amazonaws.com/academia.edu.documents/45208547/constitucion-ecuador.pdf?response-content-disposition=inline%3B%20filename%3DConstitucion-ecuador.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190704%2Fus-east-1%2F

Contraloria General del Estado, E. (22 de Octubre de 2010). *Lexis.* Obtenido de https://www.quito-turismo.gob.ec/descargas/septiembre2013/baselegal/NORMAS%20TECNICAS%20DE%20CONTROL%20CGE.pdf

DerechoEcuador. (04 de 07 de 2019). *El Delito Informático*. Obtenido de https://www.derechoecuador.com/el-delito-informatico

EcuRed. (04 de 07 de 2019). *Información*. Obtenido de https://www.ecured.cu/Información

EcuRed. (04 de 07 de 2019). *Política*. Obtenido de https://www.ecured.cu/Política

ERB, M. (16 de 07 de 2019). *Gestión de Riesgos en la Seguridad Informáica*. Recuperado el 6 de 29 de 2019, de https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

F., M. (N.D.). *Norma Iso-27005.* Español.

Gay, L. (1996). *Educational Research Neu Jersey.* Estados Unidos: Prentice Hall Inc.

Gómez Orozco, A. D. (2013). Sistema de gestión de seguridad de la información SGSI. *Bachelor's thesis, Universidad Piloto de Colombia*.

Gómez, E. F. (2019). Plan de contignecia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, 34-41.

Guevara, L. (Marzo de 2018). *Repositorio Institucional Escuela Superior Politécnica de Chimborazo.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/8347

Hernandez, S. F. (2010). *Metodología de la INvestigación.* Mexico: McgrawHill.

ISO. (04 de 07 de 2019). *International Organization for Standardization*. Obtenido de https://www.iso.org/about-us.html

Machaca, A. (N.D.). *Analisis de Riesgos usando la metodología OWASP*.

Montalvo, R. (Julio de 2017). *Respoitorio Institucional Escuela Superior Politécnica de Chimborazo.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/7224

MOSQUERA, D. F. (2015). *Control Inteligente Para El Servicio Crítico De Un Sistema De Información En Línea Enmarcado En Un Dominio De La Iso/Iec 27002.*

Nieves, A. C. (2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI)* . Obtenido de SISNAB: http://alejandria.poligran.edu.co/handle/10823/994

Onur. A, O. O. (2018). *Science Dircet.* Obtenido de www.elsevier.com: https://reader.elsevier.com/reader/sd/pii/S2213624X17303474?token=23F8B8FBE6F7A3F3969AD673835728B35827D28C5ED394C672E12E533BCEADED220DEC87B1E9A3A7D98913C336FDAD60

OWASP, F. (04 de 07 de 2019). *OWASP*. Obtenido de https://www.owasp.org/index.php/Main_Page

Salazar, J. B. (2008). *Modelo para Seguridad de la Información en TIC.* Concepción, Chile: Universidad del Bío-Bío.

SYALIM, A. H. (2009). *Comparison Of Risk Analysis Methods: Mehari, Magerit, Nist800-30 And Microsoft's Security Management Guide.* Ares '09. International Conference On: Ieee.

Urbina, G. B. (2016). *Introducción a la seguridad informática.* Editorial PATRIA.

Vicente, E. M. (2014). *Risk analysis in information systems: A fuzzification of the MAGERIT methodology.* Obtenido de Science Direct: https://reader.elsevier.com/reader/sd/pii/S0950705114000732?token=66FC62105E361AC0D256B1697D72E27FCEA5BD72F0C1F13F2564020B6ABF2B6987AC312C8702425320F59C085525110A