Implantación del EGSI de la Versión 2 de la Universidad de las Fuerzas Armadas ESPE.

Narváez Chiriboga, Patricio Alexander y Rosero Mafla, Jhoan Dangely

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de titulación previo, a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Ron Egas, Mario Bernabé

19 de marzo de 2023

Copyleaks

Plagiarism report

TESIS_EGSIv2.docx

Scan details

Scan time:	Total Pages:	Total Words:
August 18th, 2023 at 17:17 UTC	105	26014

Plagiarism Detection

Types of plagiarism		Words
Identical	1%	267
Minor Changes	0.5%	122
Paraphrased	0.3%	73
Omitted Words	0%	0

AI Content Detection

Text coverage
- AI text
- Human text

Plagiarism Results: (31)

Repositorio Institucional de la Universidad Politécn... 0.1%

https://dspace.ups.edu.ec/handle/123456789/16568/simple-...

Skip navigation ...

Repositorio Institucional de la Universidad Politécn... 0.1%

https://dspace.ups.edu.ec/handle/123456789/16560/simple-...

Skip navigation ...

T-ESPE-043688.pdf 0.1%

https://repositorio.espe.edu.ec/bitstream/21000/22145/1/t-e...

Andrea Tipán

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA TRABAJO DE TITULACIÓN, PREVIO A LA...

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de titulación: "Implantación del EGSI de la Versión 2 de la Universidad de las Fuerzas Armadas ESPE" fue realizado por los señores Narváez Chiriboga, Patricio Alexander y Rosero Mafla, Jhoan Dangely; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 09 de septiembre de 2023

Firma:

Firmado electrónicamente por:
MARIO BERNABE RON EGAS

.....

Ing. Ron Egas, Mario Bernabé MSc.

C. C: 1704229747

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Nosotros, Narváez Chiriboga, Patricio Alexander y Rosero Mafla, Jhoan Dangely, con cédulas de ciudadanía n° 1004321137, y n° 0401786140 declaramos que el contenido, ideas y criterios del trabajo de titulación: Implantación del EGSI de la Versión 2 de la Universidad de las Fuerzas Armadas ESPE es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 09 de septiembre de 2023

Narváez Chiriboga, Patricio Alexander
C.C.: 1004321137

Rosero Mafla, Jhoan Dangely
C.C.: 0401786140

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Nosotros, Narváez Chiriboga, Patricio Alexander y Rosero Mafla, Jhoan Dangely, con cédulas de ciudadanía n° 1004321137, y n° 0401786140 autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: Implantación del EGSI de la Versión 2 de la Universidad de las Fuerzas Armadas ESPE en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 09 de septiembre de 2023

Narváez Chiriboga, Patricio Alexander
C.C.: 1004321137

Rosero Mafla, Jhoan Dangely
C.C.: 0401786140

Dedicatoria

Dedico este trabajo a mis padres, familia y amigos.

Agradecimientos

Patricio

Agradezco a mis padres por su apoyo, me agradezco a mí por nunca rendirme, a los amigos que hice a lo largo de la universidad que junto hemos pasado por diversas situaciones y siempre nos hemos apoyado, a los profesores de vocación que si dedicaron tiempo para enseñar y me gustaría decir que el One Piece existe.

Finalmente, agradezco a mi tutor de tesis el Ing. Mario Ron por su apoyo y paciencia para culminar con éxito del presente trabajo.

Dangely

Agradezco a mi padre por el apoyo incondicional que me ha dado desde pequeño, agradezco a mis hermanos, mi familia, a mi novia y a mis amigos que me acompañaron en todo el proceso de aprendizaje sin importar las complicaciones que existieron en el camino. Además, a la institución con todos los profesores que me bridaron conocimientos necesarios para seguir adelante.

Finalmente, agradezco a mi tutor de tesis el Ing. Mario Ron por su apoyo y paciencia para culminar con éxito del presente trabajo.

Índice de contenido

Índice de figuras

Índice de tablas

Resumen

El proyecto del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Universidad de las Fuerzas Armadas ESPE, versión dos, se encuentra actualmente en desarrollo y requiere continuar con su proceso de implementación. Una vez seleccionados los controles siguiendo las normativas internacionales ISO 27002 e ISO 27003, se asegurarán las directrices necesarias para crear un plan de implementación y llevarlo a cabo, seguido de un proceso de evaluación del estado final de la implementación.

El proyecto se fundamenta en un análisis previo de vulnerabilidades que ayudó a determinar los controles basados en la norma ISO 27002, los cuales se utilizaron a lo largo del proyecto de implementación para su posterior evaluación y análisis técnico.

La esencia del proyecto consiste en la generación de un plan que especifique los plazos, los controles y los roles que intervendrán para reducir los riesgos a un punto de control óptimo, competente para cualquier auditoría y preparado para una pre-certificación, si fuese necesaria. Este enfoque llevará a la Universidad de las Fuerzas Armadas ESPE a un nuevo nivel de madurez en el campo de la seguridad de la información.

En resumen, el proyecto EGSI en la Universidad de las Fuerzas Armadas ESPE, versión dos, es un esfuerzo en curso basado en normas internacionales, respaldado por un análisis de vulnerabilidades y centrado en la creación y ejecución de un plan integral de implementación. Esta iniciativa tiene como objetivo mejorar la seguridad de la información y elevar la madurez de la universidad en este campo.

Palabras clave: Esquema gubernamental para la seguridad de la información, seguridad de la información, procesos, Sistemas de Gestión de Seguridad de la Información.

Abstract

The University of the Armed Forces ESPE's Governmental Information Security Scheme (EGSI) project, version two, is currently in development and requires the continuation of its implementation process. After selecting controls based on international standards ISO 27002 and ISO 27003, this will ensure the necessary guidelines for creating an implementation plan and executing it, followed by a process to evaluate the final implementation status.

The project's foundation lies in a previously conducted vulnerability analysis that aided in determining the controls based on ISO 27002, which have been employed throughout the implementation project for subsequent evaluation and technical analysis.

The core of the project involves generating a plan specifying timelines, controls, and roles to be involved to mitigate risks. This will bring them to an optimal control point, well-prepared for any audit and pre-certification, should it be necessary. This approach will elevate Universidad de las Fuerzas Armadas ESPE to a new level of maturity in the field of information security.

In summary, the EGSI project at Universidad de las Fuerzas Armadas ESPE, version two, is a continuing endeavor based on international standards, grounded in vulnerability analysis, and focused on the creation and execution of a comprehensive implementation plan. This initiative aims to enhance information security and bring the university to a heightened level of maturity in this field.

Keywords: Governmental Information Security Scheme, information security, processes, Information Security Management Systems.

Capítulo I

Introducción

Antecedentes

Dentro de la sociedad actual la seguridad de la información se ha vuelto un tema clave para toda empresa, debido a que la tecnología avanza cada día a pasos agigantados a su vez también aumentan los riesgos que conllevan el uso de estas.

Debido a estas razones las empresas ya sean públicas o privadas han comenzado a implantar sistemas que les permiten precautelar su valiosa información de forma que se garantice la disponibilidad, integridad y confidencialidad de esta.

El presente trabajo de titulación se enfocará en aplicar el sistema previamente diseñado para la Universidad de las fuerzas armadas ESPE con el objetivo de evaluar su implantación dentro de la entidad educativa.

El estudio examinará las diferentes medidas de seguridad utilizadas en el sistema, los procedimientos de gestión de riesgos y la política de seguridad de la información, así como los resultados obtenidos después de la implementación.

Con este trabajo se espera determinar como un sistema de la gestión de la seguridad de la información puede mejorar la protección de datos y la capacidad para enfrentar los riesgos que el uso de las tecnologías conlleva.

Planteamiento del problema

La Universidad de las Fuerzas Armadas ESPE, con la finalidad de mejorar la gestión de la información y la seguridad en sus procesos institucionales, ha decido implementar el Esquema Gubernamental de Seguridad de la Información (EGSI) en su versión 2. Este proyecto aborda a una adecuada implantación del EGSI en la Unidad de Seguridad Integral de la ESPE, además considerando desafíos como la falta de cultura de seguridad en la institución, la falta de

capacitación adecuada al personal involucrado, la identificación de los activos y recursos críticos que deben ser protegidos, la definición de políticas y procedimientos de seguridad.

Justificación

Según la norma ISO 27001 un sistema de la gestión de la información SGSI se ha vuelto una necesidad dentro de la organización, que permitirá a la Universidad de las Fuerzas Armadas ESPE proteger la gran cantidad de información sensible que maneja, asegurando la confidencialidad, disponibilidad e integridad de toda la información de cada una de sus unidades orgánicas.

La norma ISO 27003 establece directrices para la implantación del modelo ya creado en base a la normativa ISO 27001 y 27002, de esta manera gestionar los procedimientos necesarios, con esto llevar a cabo un proceso riguroso y estructurado con los controles diseñados previamente, y que serán implantados en las unidades responsables del manejo de la información.

Con la ayuda de la implantación del SGSI se optimizarán las unidades que cuenten con información dentro de la Universidad de las Fuerzas Armadas ESPE, mejorando procesos para que de esta forma la entidad esté preparada para cualquier auditoria de precertificación en el cumplimiento de la normativa.

Objetivos

Objetivo general

Realizar la Implantación de controles de la Versión 2 del EGSI de la Universidad de las Fuerzas Armadas ESPE, en base de las normas ISO 27001, ISO 27002, ISO 27003.

Objetivos específicos

- Establecer el estado del Arte

- Elaborar el plan detallado de implementación de controles y salvaguardas de la Versión 2 del EGSI de la ESPE
- Implementar los controles y salvaguardas del SGSI-ESPE Versión 2, en base del Plan de Implementación.
- Evaluar la Implantación de controles y salvaguardas.

Alcance

Implementar el Esquema Gubernamental de Seguridad de la Información EGSI usando como base la normativa internacional ISO 27000, el mismo que establece normas y procesos para la implantación de salvaguardas y controles de los activos de información de la institución.

Para esto se toma en cuenta los objetivos específicos planteados con los cuales se establecerá un estado del arte que se enfocará en generar un plan detallado donde se describirá los controles que se van a implementar, el tiempo que tomara implementarlos y los recursos necesarios con la responsabilidad de los agente involucrados para posteriormente implementar los controles de acuerdo al plan establecido y por ultimo evaluar el nivel de madurez de estos, a continuación, se muestran los objetivos específicos con cada una de las preguntas de investigación, las mismas que servirán de base para el progreso del proyecto en la **Tabla 1.**

Tabla 1

Objetivos y preguntas

Objetivo específico	Pregunta de investigación
Establecer el estado del Arte	a. ¿Cómo ayudará la implementación del EGSI Versión 2 a la Universidad de las Fuerzas Armadas “ESPE”? b. ¿De qué manera y en que se basará el plan de implementación de los controles del EGSl?
Elaborar el Plan detallado de implementación de controles y salvaguardas de la Versión 2 del EGSI de la ESPE	a. ¿Cómo se va a realizar la planificación de la integración de los controles de la Versión 2 del EGSI? b. ¿Cuáles son los requisitos y estándares específicos que se deben cumplir para la implantación del EGSI en la Universidad de las Fuerzas Armadas ESPE? c. ¿Cuáles son las herramientas y tecnologías más adecuadas para la implementación del EGSI en la Universidad de las Fuerzas Armadas ESPE, y cómo se pueden integrar con los sistemas y plataformas existentes?
Implementar los controles y salvaguardas del SGSI-ESPE Versión 2, en base del Plan de Implementación.	a. ¿Cuáles son los procedimientos específicos para la implementación de los controles y salvaguardas definidos en el Plan de Implementación del EGSI Versión

Objetivo específico	Pregunta de investigación
	2 de la Universidad de las Fuerzas Armadas ESPE? b. ¿Cómo se pueden establecer los roles y responsabilidades necesarios para la implementación de los controles y salvaguardas del EGSI Versión 2, y cómo se puede garantizar la colaboración y coordinación entre los diferentes actores involucrados? c. ¿Cuál es la mejor estrategia para la implementación del EGSI Versión 2 en la Universidad de las Fuerzas Armadas ESPE, teniendo en cuenta el tamaño de la organización, la complejidad de sus procesos y la disponibilidad de recursos?
Evaluación de la Implantación de controles y salvaguardas.	a. ¿Cómo se puede evaluar el nivel de cumplimiento de los controles y salvaguardas implementados en la Universidad de las Fuerzas Armadas? b. ¿Qué parámetros serán considerados para medir la eficiencia y la efectividad de los controles?

Hipótesis

La implantación de los controles y salvaguardas del Esquema Gubernamental de

Seguridad de la Información en la Universidad de las Fuerzas Armadas “ESPE” permitirá reducir los riesgos de vulnerabilidades sobre los activos de información, mejorando la gestión de los procesos de manejo de la información y aumentando la confianza de los usuarios de la institución.

Metodología

Para el presente proyecto la metodología a usar en la implantación de controles se basa en los principios extraídos de la ISO 27001 siguiendo una lógica sistemática y estructurada, con la finalidad de realizar una implantación de manera efectiva, dicha metodología cuenta con seis pasos a seguir:

- Preparación y planificación: En este paso se define el alcance del SGSI y se establecen objetivos.
- Selección de controles: Se usa de base la normativa ISO 27001 y 27002 como guía para la selección de controles adecuados, siguiendo los requerimientos de la Universidad de las Fuerzas Armadas.
- Diseño e Implementación: Generar los procedimientos y políticas necesarias para cada control seleccionado, asegurándose que se encuentren acorde con las operaciones de la Universidad de las Fuerzas Armadas ESPE.
- Prueba y validación: Realizar revisiones y ajustes según las necesidades de la Universidad de las Fuerzas Armadas.
- Monitorización y evaluación: Realizar revisiones técnicas para evaluar el cumplimiento de los controles.
- Mejora continua: Realizar revisiones para considerar cambios necesarios dentro del sistema de la seguridad de la información.

Dicha metodología genera un ciclo de mejora continua que permitirá aumentar los estándares de seguridad de la Universidad de las Fuerzas Armadas.

Capítulo II

Fundamentación teórica y estado del arte

Fundamentación teórica

En el presente proyecto se deben abordar y tomar en cuenta diversas terminologías y elementos de los cuales se fundamentará la investigación entre los cuales se encuentran temas como la ciberseguridad, salvaguardas, controles, metodologías y estándares que se usaran para llevar a cabo dicho proyecto.

Introducción al SGSI y controles de seguridad de la información

Definimos a un SGSI como un conjunto de políticas y procedimientos usados para la gestión de riegos que una organización puede tener al momento de querer salvaguardar sus activos de información más críticos, un SGSI se basa en evaluar los riegos que pueden existir y asignar controles adecuados para cada activo con el fin de reducir los riesgos.

Entre los controles que se pueden aplicar a activos tenemos medidas técnicas, físicas y administrativas para la protección de la información y garantizar la confidencialidad, integridad y disponibilidad, de las cuales se pueden tomar diversas medidas que van desde solicitar identificación a empleados hasta encriptar activos de información y generar monitoreos contantes. (International Organization for Standardization, 2013)

En referencia a esto las normas más comunes para la creación de un SGSI son las ISO 27001 y la NIST 800-53 donde proporcionan una estructura adecuada y con detalle de como implementar este marco para la seguridad de la información.

Antecedentes y evolución del SGSI

El Esquema Gubernamental de Seguridad de la Información (EGSI) es un conjunto de

políticas, procedimientos y controles que permiten proteger la información de organizaciones públicas y privadas.

El concepto de EGSI se presenta por primera vez en el Reino Unido en el año de 1999, con la publicación del documento “Protecting Government’s Information Assets” por el Government Communications Headquarters (GCHQ) y el National Audit Office (NAO) (Johnson, 2013). En este se recalca los requisitos para la seguridad de la información en el sector público del Reino Unido y los cuales fueron la base para el desarrollo del EGSI. Para que posteriormente países como Estados Unidos, Canadá y Australia adoptaran este concepto para desarrollar sus propios marcos de referencia para la gestión de la seguridad de la información en el sector público.

A continuación, los países de América Latina han establecido sus propios EGSI en los últimos años. Por ejemplo, en México se estableció el Esquema Nacional de Seguridad de la Información (ENSI) en 2005 (Secretaría de Gobernación, 2005). En Colombia se estableció el Esquema de Seguridad de la Información (ESI) en 2011, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información en el sector público (Departamento Administrativo de la Función Pública, 2011).

En el contexto de Ecuador, el EGSI fue establecido en el año 2015 con el objetivo de establecer un marco de referencia para la gestión de la seguridad de la información en el sector público (Presidencia de la República del Ecuador, 2015). Este esquema establece los requisitos y controles necesario para garantizar la confidencialidad, integridad y disponibilidad de la información en las entidades del sector público.

Posteriormente en los siguientes años se publicó la versión 2 del EGSI, que incluye nuevos requisitos y controles para adaptarse a las nuevas amenazas y desafíos en el tema de la seguridad de la información (Senescyt, 2019). En esta versión se incluyeron los controles específicos para la gestión de la privacidad de la información, la gestión de incidentes de seguridad de la información y la gestión de la continuidad del negocio.

Normas y marcos de referencia para los SGSI

Para los sistemas de Gestión de la información tenemos algunas normativas relevantes para la creación de esta las cuales se presentarán a continuación:

- ISO/IEC 27001: Norma internacional que establece los requisitos para un SGSI. Proporciona las directrices para la gestión de la seguridad de la información en una organización.
- ISO/IEC 27002: Norma internacional que proporciona los pasos a seguir para la implementación de controles a los activos de información se basa en la norma 27001. (International Organization for Standardization, 2013)
- NIST SP 800-53: Proporcionado por el instituto de estándares y tecnologías de Estados Unidos es un marco que proporciona controles de seguridad de la información para sistemas y organizaciones federales. (Technology, 2020)
- COBIT 5: Un marco de referencia creado por ISACA que proporciona directrices para la implementación de controles de seguridad de la información.
- GDPR (Reglamento General de Protección de Datos). Este es un marco legal de la unión europea que establece requisitos para la protección de datos.

Identificación y evaluación de los riesgos de seguridad de la información.

Para una gestión efectiva de los recursos y preservar la seguridad de estos se debe tomar en cuenta dos puntos sumamente fundamentales que son la identificación y evaluación de los riesgos. Como se señala en la norma internacional ISO 27005 “La evaluación de riesgos es el proceso que consiste en evaluar los riesgos asociados con los activos de información y controles existentes o propuestos para reducir estos riesgos” (International Organization for Standardization, 2013)

Para la identificación y evaluación de riesgos de seguridad existen varios marcos de referencia y metodologías que ayudan en esto. Entre ellas se encuentra el instituto de estándares y tecnologías NIST con la guía NIST SP 800 que proporciona una metodología de evaluación de riesgos.

También existen metodologías como la FAIR (Factor Analysis of information Risk) que se centra en la evaluación cuantitativa de los riesgos de la seguridad de la información y a su vez está el marco de referencia OCTAVE que ayuda a las organizaciones a identificar y abordar los riesgos de seguridad de la información de manera proactiva y sistemática. (Software Engineering Institute)

Por lo cual este proceso de identificación y evaluación de los riesgos de la seguridad de la información es un proceso crítico para la gestión efectiva de la información, de lo cual se puede destacar una gran variedad de marcos y metodologías que se pueden usar de referencia para estas tareas.

Técnicas y metodologías para la implantación de un EGSI.

La implantación de un Esquema Gubernamental de Seguridad de la Información (EGSI) presenta un proceso complejo que necesita una metodología bien estructurada y de la implementación de diferentes técnicas específicas para llegar a una efectiva implementación y aseguramiento de la seguridad de la información en una organización.

Una de las técnicas más utilizadas para la implantación de un EGSI es el análisis de riegos, en la cual consiste en identificar los activos de información críticos de la organización, evaluar las amenazas y vulnerabilidades que pueden afectarlos, y establecer medidas de seguridad adecuadas para minimizar el riesgo (Ameen, 2018). Para realizar el análisis de riegos se pueden utilizar metodologías como la que presenta MAGERIT desarrollada por el Gobierno de España (CCN-CERT, 2019) y el estándar ISO/IEC 27005:2018 (ISO, 2018).

Otra técnica propuesta para la implantación de un EGSI es la gestión de seguridad de la información basada en procesos, la cual consiste en establecer procesos documentados para la gestión de la seguridad de la información, por ejemplo, la gestión de incidentes, la gestión de cambios y la gestión de accesos (Choudhary, Choudhary, & Kaur, 2018). Para llevar a cabo esta técnica se pueden utilizar diversas metodologías, como el estándar ISO/IEC 27001:2013 (International Organization for Standardization, 2013) y el modelo Capability Maturity Model Integration (CMMI) desarrollado por el Instituto de Ingeniería de Software de Carnegie Mellon (Instituto de Ingeniería de Software de Carnegie Mellon, 2019).

En el año 2017, Cárdenas propuso una metodología basada en estándares internacionales para implementar un EGSI en una organización, en este se incluye una fase de análisis y diagnóstico, una fase de diseño y planificación, una fase de implementación y una fase de seguimiento y mejora continua (Cárdenas, 2017).

Por otro lado, Gómez en el año 2018 propuso una metodología de implantación de un EGSI para pequeñas y medianas empresas, la cual consta de cinco fases: análisis, diseño, implementación, operación y mejora continua (Gómez J. A., 2018).

En el año 2019, Espinosa propuso una metodología para implantación de un EGSI basa en la norma ISO/IEC 27001, la cual consta de cuatro fases: planificación, implementación, evaluación y mejora continua (Espinosa, 2019).

En el año 2020, Sánchez propuso una metodología basa en el ciclo Planear-Hacer-Verificar-Actuar para le implantación de un EGSI en una organización, esta metodología incluye la realización de una evaluación de riegos, la definición de una política de seguridad de la información, implementación de controles, realizar auditorías y la mejora continua (Sánchez, 2020).

Implementación y gestión de los controles de seguridad de la información

La implementación y gestión de controles de seguridad de la información es un aspecto critico de la gestión de la seguridad de la información. Para implementar y gestionar los controles de seguridad de la información es necesario seguir un enfoque basado en riesgos, según la norma ISO 27001, “los controles de seguridad deben ser seleccionados e implementados en función de los riesgos identificados y evaluados en la organización” (International Organization for Standardization, 2013).

La norma ISO 27002 proporciona una guía de los pasos a seguir para lograr una implementación de controles dentro de la organización en base a los activos. (International Organization for Standardization.).

La implementación y gestión de los controles para los activos de información es una tarea que garantiza la protección de dichos elementos de información dentro de una organización, por lo cual lo hace esencial al momento de montar un SGSI. Para esto podemos analizar los enfoques que nos brinda la normativa internacional como son la ISO 270002 y 270001 como guías para implantar y gestionar los controles.

Evaluación y mejora continua del SGSI

La evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso fundamental en la implantación del EGSI. Para esta fase, la revisión debe ser constante para identificar posibles brechas de seguridad, analizar los riesgos y tomar medidas preventivas para garantizar la seguridad de la información.

Diversos autores han propuesto metodologías y técnicas para la evaluación y la mejora continua del SGSI, en el año 2018, Castillo propuso una metodología para la mejora continúa basada en la norma ISO/IEC 27001, en la cual se realiza una evaluación interna y externa, identificación de oportunidades de mejora, implementación de acciones correctivas y preventivas, y el monitoreo periódico del SGSI (Castillo, 2018).

Pérez en el año 2019 propuso una metodología para la mejora continua que se basa en la norma ISO/IEC 27004, la cual incluye la definición de objetivos y metas de seguridad, la evaluación del desempeño del SGSI, la identificación de oportunidades de mejora, la implementación de acciones correctivas y preventivas, y el monitoreo y revisión periódica del SGSI (Pérez, 2019).

Otro enfoque para la evaluación y mejora continua del SGSI es la implementación de un modelo de madurez, el cual propone Gómez en el año 2020 con la implementación del modelo Capability Maturity Model Integration (CMMI) para la evaluación y mejora continua del SGSI en la cual se incluye la definición de niveles de madurez la evaluación del desempeño del SGSI, la identificación de áreas de mejora, la implementación de acciones correctivas y preventivas, y el monitoreo y revisión periódica del SGSI (Gómez A. , 2020).

Estado del arte

Se realizo una revisión literaria con el propósito de contextualizar la búsqueda de casos de estudios científicos relevantes para la realización del proyecto, se define los objetivos y una descripción del problema a investigar, así como criterios de inclusión y exclusión.

Estrategia de búsqueda

Para llegar a un acuerdo entre los interesados del proyecto se realizó una validación cruzada entre los miembros del equipo con el fin de determinar qué casos de investigación son relevantes y cuales deben ser excluidos.

Construcción y afinación de la cadena de búsqueda

Para obtener los resultados deseados se usó el siguiente grupo de palabras para generar una cadena de búsqueda: "Information security management systems" AND "information security controls" AND "risk assessment" AND "implementation" AND "continuous improvement"

Selección de estudios

Con la ayuda de la cadena de búsqueda se dio como resultado 82 estudios relacionados con la temática a investigar. Debido al gran número de resultados fue necesario conceder un filtro para seleccionar los artículos que serían útiles a la investigación dando como resultado un numero manejable de 20 artículos.

Parámetros para tomar en cuenta para los artículos seleccionados:

- Artículos publicados desde el año 2019.
- Artículos que hacen referencia a modelos estandarizados con la ISO 27001
- Artículos de muestran metodologías para implementar controles dentro de instituciones.
- Artículos que se encuentren dentro de los idiomas inglés o español.

Parámetros para no tomar en cuenta artículos:

- Artículos con un año de publicación menor a 2019
- Estudios que no tengan un marco guía reconocido como la ISO o NIST.
- Artículos con Idiomas Diferentes a inglés o español

A continuación, en la **tabla 2** se muestran los artículos seleccionados en base al criterio de los responsables del proyecto, estos artículos mencionados fueron estudiados y analizados para resolver las dudas propuestas por los objetivos de investigación propuestos.

Tabla 2

Tabla de selección de estudios.

Código	Titulo	Cita
EP01	Investigación sobre el análisis de la eficacia en los controles de la	(Z. Sun, 2020)

	seguridad de la información	
EP02	Problemas de implementación de sistemas de gestión de seguridad de la información.	(Aleksandrova, Vasiliev, & Aleksandrov, 2020)
EP03	Evaluación de madurez de un sistema de la seguridad de la información basado en la ISO 27001 y ISO 27002	(Monev, 2020)
EP04	Un Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC-ISO/IEC 27001	(Fonseca-Herrera, Rojas, & Florez, 2021)
EP05	Critical Success Factor for Integration of Cyber Security in Context of Managed Services	(Georg Sven Lampe, 2022)
EP06	El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador).	(Janeth Mora Secaira, 2020)
EP07	Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS.	(Recalde, 2019)
EP08	Plan para la implementación de un SGSI en un centro educativo.	(Martínez, 2019)
EP09	Elaboración de una guía de implementación de un SGSI para la	(Orellana Toledo, 2022)

	corporación ecuatoriana para el desarrollo de la investigación y la academia - CEDIA

Nota. La tabla nos indica la selección de estudios realizada para desarrollar el trabajo de titulación.

- **EP01** (Z. Sun, 2020) **Investigación sobre el análisis de la eficacia en los controles de la seguridad de la información.**

  El presente articulo propone un modelo PDCA para el análisis de la efectividad de controles para la seguridad de la información basado en el análisis de los sistemas de la gestión de la seguridad de la información del estándar ISO 27001 para lo cual emplean fórmulas que les permite comparar cuantitativamente y verificar el cumplimiento del trabajo realizado por cada uno de los controles de esta forma demostrar si están cumpliendo con las metas establecidas al momento del diseño del plan o si es necesario darles un mantenimiento para que estén dentro del margen aceptable descrito por el plan previamente creado, en el presente caso de estudio se comenta la comparación de efectividad entre controles antiguos y renovados donde se juzga por medio de un indicador de medición numérico si necesitan alguna actualización o cumplen con los estándares planteados en los objetivos.

- **EP02** (Aleksandrova, Vasiliev, & Aleksandrov, 2020) **Problemas de implementación**

de sistemas de gestión de seguridad de la información.

En el artículo presentado se abordan los desafíos y problemas asociados con la implementación efectiva de sistemas de seguridad de la información (SGSI) en las organizaciones. Los avances de las tecnologías como su uso en la información y la comunicación han hecho que la seguridad de la información sea una preocupación crítica para las empresas de todo el mundo. El artículo se centra en la implementación del estándar internacional ISO/IEC 27001, que establece los requisitos para un SGSI efectivo. Se discuten los problemas comunes que surgen durante la implementación, como la falta de apoyo y compromiso de la alta dirección, la falta de recursos y la falta de conocimientos y experiencias. Además, proporciona recomendaciones para superar los problemas expuestos y lograr una implementación exitosa de in SGSI en una organización.

- **EP03** (Monev, 2020) **Evaluación de madurez de un sistema de la seguridad de la información basado en la ISO 27001 y ISO 27002.**

En este artículo se presenta una metodología practica para evaluar el nivel de madurez de un sistema de la gestión de la seguridad de la información dentro de una organización para lo cual se basa en la ISO 27001 y ISO 27002 dejando en claro que esta metodología está limitada a sistemas que hayan sido creados con este tipo de normativa, con este marco el autor provee una manera eficaz de identificar deficiencias y oportunidades de mejora a los ISMS generando oportunidad de evaluación continua usando métricas por niveles sobre el desempeño de las

estrategias y operaciones de nuestro sistema.

- **EP04** (Fonseca-Herrera, Rojas, & Florez, 2021) **Un Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC-ISO/IEC 27001.**

  El artículo presenta un modelo para implementar un sistema de gestión de seguridad de la información en cualquier organización, basado en la norma internacional NTC-ISO/IEC 27001:2013.

  Utilizaron una combinación de metodologías y técnicas para llevar a cabo la implementación del modelo en una organización que ofrece servicios de gestión y administración técnica de información en el sector de los hidrocarburos. En primer lugar, se identificaron los activos de información, incluyendo los procesos, clientes y proveedores, entre otros. A continuación, se evaluaron los riesgos asociados a los activos de información identificados, utilizando técnicas de análisis de riegos que permitió identificar las amenazas, vulnerabilidades y consecuencias potenciales. Luego se seleccionaron los controles de seguridad adecuados para mitigar los riesgos identificados en la evaluación de riesgos y se implementaron los controles de seguridad seleccionados para proteger los activos de información de la organización. Finalmente, se estableció un ciclo de mejora continua para el sistema de gestión de seguridad de la información, que incluyó una revisión constante de los controles de seguridad implementados y la evaluación periódica de los riesgos.

  Los autores destacaron la importancia de la norma NTC-ISO/IEC 27001:2013 como un marco útil para la gestión de la seguridad de la información en cualquier organización, recalcando la importancia de la mejora continua en un contexto de amenazas constantes como la ciberdelincuencia y el espionaje cibernético.

- **EP05** (Georg Sven Lampe, 2022) **Factor crítico de éxito para la integración de ciberseguridad en el contexto de administración de servicios.**

  Esté articulo presenta un modelo para adaptar a la empresa nuevas tecnologías y servicios los cuales pueden proveer un riesgo potencial hacia ella por lo cual usa estándares de medición y evaluación para determinar el riesgo de los nuevos activos tecnológicos, el impacto que a la infraestructura y a la economía de la empresa que estos puedan tener, en dicha investigación se basan en un modelo de RMP(Identificar, Proteger, Responder, Recuperar) para ayudar a las personas encargadas de la ciberseguridad a reportar los posibles riesgos y las contingencias hacia estos de las nuevas tecnologías.

  Para lograr exitosamente el modelo que se propone se usa un modelo jerárquico con el cual identificar a los responsables y las personas encargadas del manejo de la información dentro de las instituciones dando a concientizar a dichos responsable se pueden tomar medidas sobre las vulnerabilidades y la exposición dentro de la empresa, del modelo se puede destacar como se usa una plantilla con la cual identifican al nuevo elemento de riesgo con una descripción detallada de este la prioridad que tiene y los posibles efectos como sus niveles de riesgo asociados a este.

- **EP06** (Janeth Mora Secaira, 2020) **El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador).**

  El articulo presenta un caso de estudio de la implementación de un sistema de SGSI dentro de una institución educativa superior de Ecuador la idea de este trabajo es describir una metodología para llegar a implementar un SGSI basado en la norma 27001 por lo cual nos muestra los pasos con los que identifican las vulnerabilidades

y los riesgos de cada activo de la institución en la cual están realizando el trabajo por lo cual sigue un estándar de desarrollo basado en PHVA(Planear, Hacer, Verificar y Actuar) con esto plantean un plan para generar mejoras y cambios a las políticas y procedimientos que en ese entonces se llevaban en la UTEQ (Universidad Técnica Estatal de Quevedo) el problema que abordan es de gran interés para cualquier institución estatal del estado Ecuatoriano ya que buscan con esto mejorar los niveles de confidencialidad, integridad y disponibilidad.

- **EP07** (Recalde, 2019) **Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS.**

  En el proyecto se presentó la implementación de un sistema de gestión de seguridad de la información (SGSI) en la empresa GMS, con el objetivo de obtener la certificación de la norma ISO/IEC 27001:2013. Es importante la implementación de controles para gestionar la seguridad de la información utilizada en sus procesos para respaldar la entrega de servicios a los clientes.

  El primer capítulo resume y describe un análisis del SGSI basado en la norma ISO/IEC 27001:2013, el ciclo PDCA y un análisis comparativo de las metodologías para la gestión de riesgos. El segundo capítulo describe la metodología del proyecto y detalla el proceso de evaluación con la gestión de riegos y controles implementados.

  A continuación, evalúan comparativamente los niveles de seguridad inicial y posterior a la implementación de los controles, además de recomendaciones para el mantenimiento del SGSI para los controles críticos en el centro de operaciones de seguridad.

- **EP08** (Martínez, 2019) **Plan para la implementación de un SGSI en un centro educativo.**

  El presente trabajo tuvo como objetivo implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma 27000 y siguiendo la metodología MAGERIT. Los objetivos se dividen en el análisis de la situación actual de la institución y diseñar un plan de seguridad con su respectiva implantación. Gracias a la metodología MAGERIT observaron generalmente los activos importantes para el sistema de información, las amenazas y riesgos, para poder identificar las salvaguardas aplicables.

  El proyecto relacionado diseñó siete programas de seguridad que reducen los riegos a los que están expuesto el sistema de la información y a su vez evaluar la eficiencia de los controles.

- **EP09** (Orellana Toledo, 2022) **Elaboración de una guía de implementación de un SGSI para la corporación ecuatoriana para el desarrollo de la investigación y la academia - CEDIA.**

  El presente trabajo desarrolla una guía de implementación de SGSI para CEDIA la cual abarca a la información en formato digital como formato físico de todas las áreas de la organización, para la realización del proyecto utilizaron la metodología de la ISO/IEC 27001 a razón de que cuenta con la evaluación y tratamiento de riegos. Además, se realizó un análisis de brecha para permitir conocer los límites de la organización con el cumplimiento de la norma ISO/IEC 27001.

  Por otro lado, también se incluyó todos los controles pertinentes con sus respectivos tratamientos de los cuales se llegaron a implementar y analizar socializando el

cumplimiento de las políticas al personal y responsables del Sistema de Gestión de Seguridad de la Información.

Capítulo III

Planificación de implantación del SGSI

Fase 1 Plan de revisión técnica

Introducción y perspectiva general.

Para la primera fase del proceso de implantación es precioso realizar una revisión técnica al estado actual del EGSI de la Universidad de las Fuerzas Armadas, para esto se detallará un plan de revisión el cual se pondrá en marcha posteriormente.

Según los lineamientos establecidos en el plan se realizará diversas revisiones a las políticas establecida actualmente para detectar las mejoras que debe llevar a cabo el sistema de gestión de la seguridad de la información, luego se procederá con la selección y posteriormente la implantación de controles con fallas criticas dando por último paso a una evaluación que compruebe la mejora del sistema.

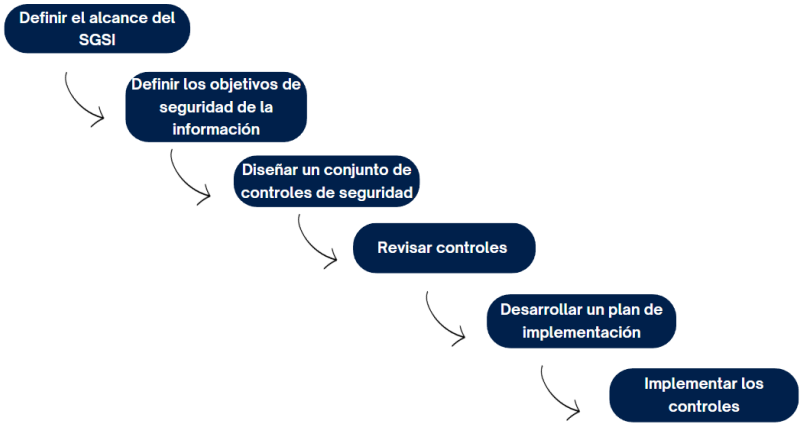
Descripción del Proyecto

Para proceder con la implantación exitosa de un SGSI, se debe contar con la colaboración de la Dirección de la organización que debe aprobar mediante un proyecto institucional donde se detallen las actividades a realizar. Se deberá generar un caso de negocio que describa los objetivos, alcance y la estructura de la organización para llevar a cabo la implantación del SGSI.

Esta fase del proyecto es de suma importancia debido a que en ella se podrá establecer responsables de las actividades y la colaboración de la dirección para llevar a cabo el plan de implantación, el cual se llevará a cabo en el tiempo establecido en el caso de negocio presentado.

Figura 1

Fase para un proyecto de implantación de un EGSI



Nota. El grafico describe los pasos que se deben realizar para hacer un proyecto de ` implantación de un SGSI.

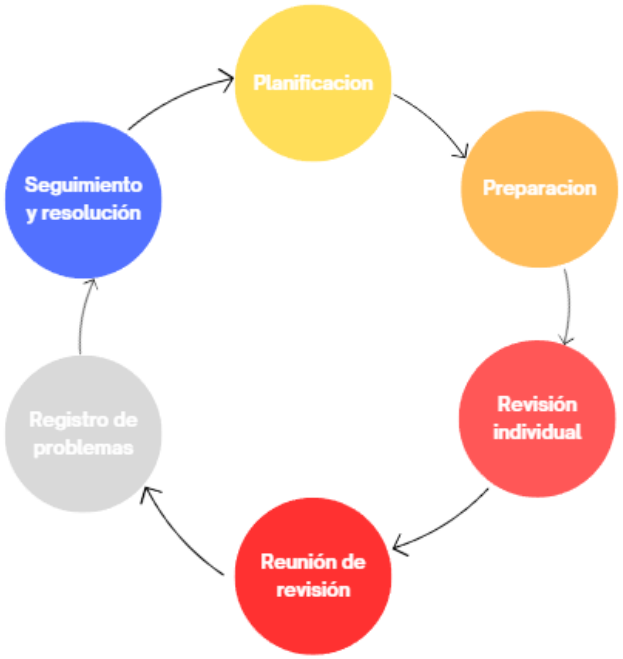
Alcance de la revisión técnica

Establecer el alcance que llevará la revisión de controles es esencial para determinar los componentes a ser analizados e identificar hasta donde se llegará con el análisis, para tener una perspectiva del trabajo que se va a desarrollar y en que componentes se debe realizar mejoras o rehacer por completo.

Para la primera fase se diseñó un plan de revisión con el cual los implicados estuvieran conformes con el fin de llegar a un consenso de que controles necesitan una revisión y cuales se encuentran acorde a la planificación.

Figura 2

Ciclo de revisión y planificación



Nota. El grafico describe las fases para una revisión técnica

Revisión técnica de controles

Para el plan de implantación de controles se ha considerado realizar una revisión técnica para tener un registro de los controles que se encuentra implantados en su totalidad y los controles que cuentan con fallos para su futura corrección.

Dicho plan toma en cuenta y se alinea con los objetivos institucionales para lo cual se estableció los diversos activos de información y mediante los registros de los controles que la dirección dio acceso se determina cuales se deberán dar mayor prioridad que se encuentra en la Evidencia Nro. AI-LI03.

En la siguiente tabla se puede observar los puntos a tomar en cuenta para la revisión técnica:

Tabla 3

Elementos de la revisión técnica

Ítem	Descripción
Activo	Propiedad de información perteneciente a la Universidad de las Fuerzas Armadas ESPE
Clasificación del control	Control basado en la normativa internacional ISO/IEC 27002
Descripción del control	Descripción detallada del control de acuerdo con la normativa internacional ISO/IEC 27002
Elementos de verificación	Preguntas creadas para verificar y sustentar la evidencia mostrada dentro de la documentación del control
Control Implantado	Pregunta de SI y NO para verificar si el control se encuentra implantado o no
Porcentaje Implantado	Valor dado en porcentaje para comprobar en qué nivel de aceptación se encuentra implantado el control.
Responsable	Personal responsable del activo y de los controles que se deben llevar sobre el
Observaciones	Observaciones tomadas de la documentación revisada del control
Evidencia	Enlace de la documentación proporcionada donde se encuentra los registros y manuales del control

Nota. La tabla representa los elementos que se encuentran en la Evidencia Nro. AI-LI03

Activos de información

La Universidad de las fuerzas armadas cuenta con diversos activos de información que

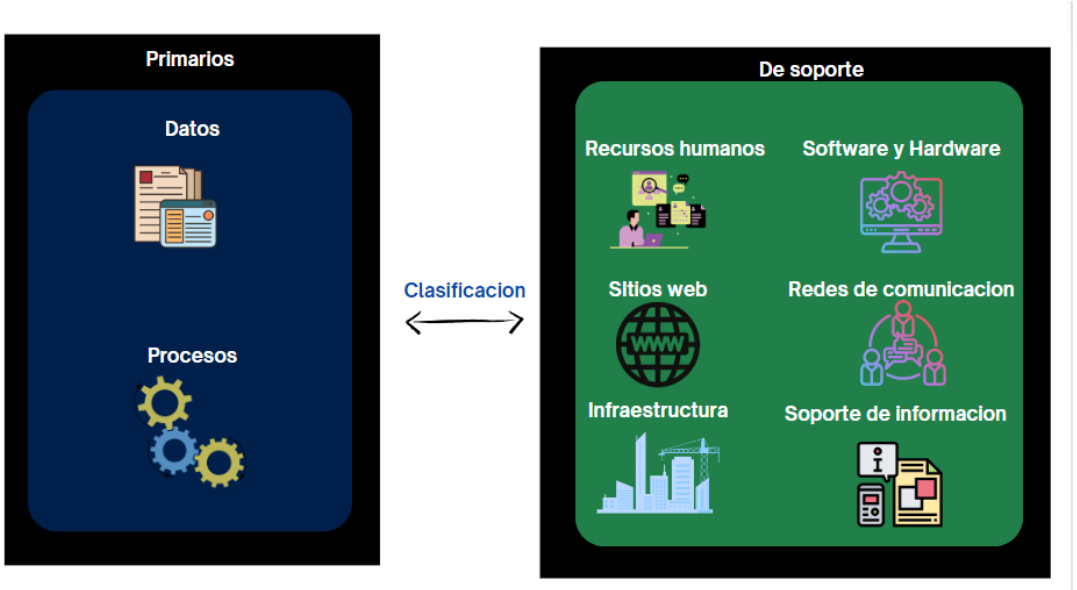
permiten llevar a cabo la misión de la institución que se numeran a continuación:

- Banner -ac 25
- BDD Banner – AC220
- Educativa -ac 49
- BDD educativa ac-222
- Monitoreo y seguridad (aulas y laboratorios) AC-202
- PENTAHO ACT-72
- QUIPUX Act-65
- ESPEMATICO AC-59

Dentro de los activos mostrado se reunirán los esfuerzos para tratar los controles con los que ya cuenta dichos activos de información para preservar la integridad de estos.

Figura 3

Activos de información



Nota. El grafico representa los activos de información que la Universidad de las Fuerzas

Armadas posee.

Descripción del proceso metodológico.

Para esta etapa se usará como referencia el ciclo Deming PDCA (Planear, Hacer, Verificar, Actuar). En este capítulo estaremos concentrados en la parte de planeación y realización.

Como primer punto se debe tomar en cuenta la elaboración de un plan para la implantación de controles con la normativa ISO 27003 para delimitar el alcance de dicho proyecto y posteriormente ser entregado a espera de una aprobación. Hay que tomar en cuenta la estructura que se tiene del proyecto ya que se cuenta con una planificación previamente realizada para seguir.

La planificación de la versión 2 del EGSI aporta con la identificación de los activos relevantes para la Universidad de las Fuerzas Armadas ESPE, así como los controles que se debe implantar basados en las ISO 27001 y ISO 27002.

Como primer paso se tomará estos controles y se tabularán para tener un entendimiento completo de todas las salvaguardas que se han tomado en cuenta por la primera parte del proyecto.

Una vez identificados estos controles se procederá a realizar una evaluación y filtrado de los mismo para delimitarlos a un número aceptable de controles manejables para la implantación con la intención de implementar el mayor número de salvaguardas en el periodo establecido para lo cual se tomará como referencia los siguientes puntos.

Características de selección:

- Controles que aporten a activos que cumplan con la misión de la Universidad de las Fuerzas Armadas ESPE.
- Controles que en base a evaluación puedan ser implantados dentro del tiempo del presente proyecto.

- Controles que se encuentren dentro del presupuesto establecido.

Una vez realizado el filtrado de los controles se establecerá el límite del proyecto como dicta la ISO 27003 para que pueda ser presentado a la parte administrativa y posteriormente ser aprobada con la ayuda de un documento el cual contenga los siguientes detalles:

- Tiempo de ejecución
- Itinerario de actividades
- Activos
- Presupuesto
- Responsables
- Departamentos interesados

Después de ser aprobado el proyecto se procederá a realizar el proceso de implantación donde se ejecutarán los controles que previamente se seleccionaron para lo cual se tendrá un escrito donde se vayan registrando los activos que ya cuentan con las salvaguardas para futuras auditorías.

Para la implantación de dichos controles se realizará paso a paso lo establecido en el anterior punto que es el plan de implantación, con el manual, los involucrados tendrán la capacidad de realizar una implantación de controles y registrar las nuevas salvaguardas para una futura evaluación.

Selección de controles a implantarse

En la siguiente tabla se especifica cada control seleccionado por parte del plan del EGSI

para cada uno de los activos relevantes de la institución con su respectiva descripción.

Tabla 4

Tabla de clasificación controles

Clasificación Control	Descripción del control
12.1.4. Separación de ambientes de desarrollo, pruebas y producción	Es necesario separar los recursos de desarrollo, pruebas y producción para reducir los riesgos de acceso no autorizado o cambios que existan en producción
9.4.5. Control de acceso al código fuente del programa	El acceso al código fuente de cualquier programa debe ser restringido para cualquier usuario
6.1.2 Separación de funciones	Las responsabilidades y funciones deben tener una separación con el fin de disminuir escenarios de modificar parámetros no autorizados o hacer mal uso de los activos de la institución.
14.2.1 Política de desarrollo seguro	Determinar y asignar reglas en la institución para el desarrollo de sistemas y aplicaciones.
12.3.1. Copias de seguridad de la información	De acuerdo con la política de copias de seguridad establecida se deben realizar los respaldos correspondientes
16.1.5. Respuesta a incidentes de seguridad de la información	De acuerdo con la documentación sobre procedimientos establecidos se debe responder ante incidentes
18.2.3. Comprobación del cumplimiento técnico	Se debe verificar el cumplimiento de las políticas y normas de seguridad de la información y sus activos dentro de la organización
5.1.1 Políticas para la Seguridad de la Información	Se deben establecer las políticas necesarias para cumplimiento de todos los actores que intervienen con los activos
8.2.1. Clasificación de la información	La información de Banner-act25 debe tener una clasificación de acuerdo con el grado de importancia frente al valor, sensibilidad, leyes y criticidad ante una modificación no autorizadas por parte de la dirección.
Clasificación Control	**Descripción del control**
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Se debe considerar la legislación y regulaciones contractuales de forma explícita, documentarse y actualizarse para cada sistema

8.2.2. Etiquetado de la información	Establecer un adecuado proceso de etiquetado en base a las normas establecidas por la organización
12.1.1. Documentación de procedimientos de operación	Todos los procedimientos de operación deben ser documentados y estar disponibles para todos los usuarios
12.2.3 Mensajería electrónica	La información difundida por medios electrónicos debe mantener todas las medidas de seguridad necesarias
7.3.1 Responsabilidades ante el cambio o finalización de empleo	Las responsabilidades continúan vigentes luego de un cambio o finalización de contrato de los empleados
12.1.2. Gestión de cambios	Los cambios, procesos o instalaciones que puedan afectar a la seguridad de la información deben ser controlados de forma eficiente
12.1.3. Gestión de capacidades	Supervisión y asignación de recursos en base al requerimiento, proyección futura de requerimientos para garantizar rendimiento
12.4.1. Registro de eventos	Es necesario un registro sobre las actividades de los usuarios constante, fallos y eventos que afecten la seguridad de la información
12.7.1. Controles de auditoría en los sistemas de información	Se deben planificar comprobaciones en los sistemas operativos para actividades de auditoría evitando interrupciones en los procesos principales
16.1.7 Recopilación de evidencias	Se debe identificar los procesos adecuados para establecer, reunir y conservar la información como parte de la evidencia.
12.4.3. Registros de administración y operación	Registro y revisión de las actividades del administrador del sistema y operadores.
6.1.3 Contacto con las autoridades	Se debe mantener contacto efectivo con las autoridades involucradas

Clasificación Control	**Descripción del control**
6.1.4 Contacto con los grupos de interés especial	Se deba mantener el contacto con los actores especiales con conocimiento en seguridad que pueden tener acceso a los activos de información

9.1.1. Política de control de acceso	El Administrador de aplicaciones especifica formalmente todos los perfiles de acceso a la aplicación solamente a las opciones autorizadas por el manual de descripción de puestos
9.4.1. Restricción del acceso a la información	El Administrador debe determinar las funciones y el acceso a la información en el sistema que deben ser restringidos de acuerdo con lo establecido en la política de control de acceso.
7.1.1 Investigación de antecedentes	La dirección debe verificar cada contratación de acuerdo con reglamentos, leyes y ética del nuevo personal.
7.1.2. Términos y condiciones del empleo	El contrato debe detallar responsabilidades tanto para el nuevo personal como la dirección en seguridad de la información.
9.2.1. Registro y retiro de usuario	Se debe establecer el procedimiento necesario para registro y baja de usuarios en base a asignación de derechos de acceso
9.2.3. Gestión de privilegios de derechos de acceso	Asignación de privilegios controlada y restringida

Clasificación Control	**Descripción del control**
18.1.2. Derechos de propiedad intelectual	Establecer procedimientos que controle la legalidad del uso de software patentados o con derechos de propiedad intelectual

11.2.7 Reutilización o eliminación segura de equipos	Los medios de almacenamiento antes de ser reutilizados o eliminados deben pasar por un proceso de confirmación y verificación de cada aspecto de acuerdo con la sensibilidad y comprobar que se ha eliminado de manera segura
11.2.8 Equipo de usuario desatendido	Se debe garantizar la seguridad de los equipos que se encuentran desatendidos
8.3.2. Eliminación de los medios	Establecer procedimientos para la eliminación de soportes innecesarios
8.1.4. Devolución de activos	A la finalización de un ejemplo o contrato, el empleado debe devolver todos los activos pertenecientes a la organización
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Se debe mantener la seguridad de aquellos equipos que están fuera de las instalaciones por su funcionamiento o desecho del mismo
11.2.5 Eliminación de activos	Debe existir una autorización por parte de los directivos para eliminar o recoger equipos, información o el software de las instalaciones.
9.2.5. Revisión de los derechos de acceso de usuario	Los administradores de los activos deben revisar los derechos de acceso de cada usuario de forma regular
12.5.1. Instalación del software en los sistemas operativos	Establecer procedimientos para instalación de software en sistemas operativos
12.6.1. Gestión de vulnerabilidades técnicas	Oportunamente obtener información sobre las vulnerabilidades técnicas de los sistemas empleados, evaluar la exposición hacia las vulnerabilidades y la adopción de medidas de mitigación
12.6.2. Restricciones en la instalación del software	Se debe normar y regular la instalación de software para los usuarios

Nota. La tabla refleja los controles que se analizaron previamente en la fase 1 de la creación de un SGSI.

Criterios de evaluación

En la presente revisión técnica se debe realizar un análisis de los controles implantados, para esto se debe tomar en cuenta ciertos criterios que permitan determinar si existe o no

problemas con los controles revisados.

La siguiente tabla muestra los criterios de evaluación que se tomó en cuenta:

Tabla 5

Criterios de Evaluación

Criterios de evaluación	Detalles
Documentos legalizados	La documentación presentada para la validación de los controles debe estar legalizada de manera correcta
Manual de procedimientos	Manual de procedimientos donde se encuentran detallado los pasos que se deben hacer para que el control cumpla su objetivo
Registro de actividad	Bitácora o registro donde se pueda evidenciar las actividades

Nota. La tabla muestra los tópicos que se tomaron en cuenta para la evaluación de controles en la revisión técnica.

Estos criterios de evaluación permitirán determinar qué nivel de tratamiento se deberá llevar a cabo para cada control, esto ayuda a identificar que controles necesitan un reajuste.

Reporte de resultados

Según la planificación se realizará un informe de evaluación técnica informática donde se demuestre las observaciones realizadas incluyendo recomendaciones para la evaluación de las autoridades.

El documento contará con criterios donde se podrá analizar cuál es el problema, la descripción de la normativa internacional ISO/IEC 27002, la condición en la que los controles se encuentran y el efecto que podría provocar en la universidad la no revisión de estos, la revisión completa se encuentra dentro del anexo evidencia Nro. AI-Pr05.

La siguiente tabla describe los ítems que se especificaran en el documento de revisión:

Tabla 6

Tabla de reporte de resultados

Item	Descripción
Observación	Problema encontrado dentro de los controles evaluados
Criterio	Basado en la normativa internacional ISO/IEC 27002
Condición	Elemento de verificación y evidencia de los controles
Efecto	Posible evento que podría suceder en caso de no realizar una revisión al control

Nota. Elementos de análisis en el documento evidencia Nro. AI-Pr05

Recursos Humanos

En el mantenimiento de un sistema de la gestión de la información se necesita recursos humanos para realizar las revisiones necesarias y seguir mejorando el sistema continuamente, para lo cual el equipo se apoyará de personal de la institución con el fin de ejecutar el proyecto.

Para el presente proyecto se clasifican los involucrados de la siguiente manera:

Tabla 7

Recursos Humanos del proyecto

CUERPO TECNICO	FUNCION
INGENIEROS DOCENTES	Personal capacitado en procesos de seguridad de la información y normativa internacional ISO 27000. Supervisa las actividades de los estudiantes.
INGENIERO SUPERVISOR	Personal de las UTIC que supervisa las actividades de los estudiantes y otorga soporte a las necesidades de ellos.
ESTUDIANTES OPERATIVOS	Ejecutan las acciones necesarias para realizar la mejora del EGSI de la Universidad de las fuerzas armadas ESPE

Nota. Tabla que hace referencia al equipo técnico conformado por autoridades y estudiantes de la Universidad de las Fuerzas Armadas.

Para un correcto desarrollo de las actividades propuestas se debe contar con los siguientes recursos:

- Material Actualizado.
- Acceso a documentación legal.
- Terminal de trabajo.

Resultados o Hallazgos de la evaluación Técnica informática.

En la siguiente sección se expone los hallazgos de la evaluación técnica a los controles del EGSI de la Universidad de las Fuerzas Armadas con las recomendaciones que se deben tomar en cuenta para la mejora del sistema:

(9.4.5) - Control de acceso al código fuente del programa

Observación:

No presenta dentro de la documentación para el formato de claves o una bitácora de cambios.

Criterio:

NTE ISO/IEC 27002 Control 9.4.5 - El acceso al código fuente de cualquier programa debe ser restringido para cualquier usuario.

Condición:

Según los elementos de verificación se debería integrar un control de acceso al código fuente de cualquier programa desarrollado para la institución el cual debe llevar un registro de cambios o modificaciones el cual no se encuentra dentro de la documentación.

Efecto:

A falta de un registro para la obtención de evidencia tangible la institución carecerá de registros documentados para demostrar el cumplimiento del control y a su vez esto provocará que cuando exista un problema o posibles vulnerabilidades la identificación de este sea complicada por tanto difícil abordar el problema.

Recomendaciones:

Por parte de las UTIC (Unidad de tecnologías de la información y comunicación) de la Información, deberá realizar las siguientes actividades para implantar de manera correcta el control:

Establecer control de versiones: Implementar una solución de control de versiones para rastrear y gestionar las modificaciones realizadas en el código fuente. Esto garantizará la integridad del código y permitirá revertir cambios no autorizados o identificar cualquier actividad sospechosa.

Monitorear y auditar el acceso al código fuente: Implementar mecanismos de monitoreo y registro para registrar todas las actividades relacionadas con el acceso y modificación del código fuente. Esto permitirá realizar auditorías y detectar cualquier actividad sospechosa o no autorizada.

Realizar revisiones periódicas: Realizar revisiones periódicas del acceso al código fuente para asegurarse de que se cumplan los controles establecidos. Esto garantizará que el acceso al código

(14.2.1) - Política de desarrollo seguro:

Observación:

No existe un manual que explique cómo implementar controles de seguridad durante el desarrollo, revisiones de código y pruebas de seguridad, así como un registro de incidentes, lecciones aprendidas y las medidas correctivas.

Criterio:

NTE ISO/IEC 27003 Control 14.2.1 - Determinar y asignar reglas en la institución para el desarrollo de sistemas y aplicaciones.

Condición:

En la documentación presentada para el cumplimiento de dicho control carece de los manuales y registros establecidos en la observación.

Efecto:

Al no estar bien implementado el control aumenta el riesgo de vulnerabilidades de seguridad, exponiendo a la institución a brecha de datos y perdida de información.

Recomendación:

Los encargados de la parte del desarrollo de aplicaciones de la UTIC deben desarrollar y documentar una política clara que establezca los principios y directrices para el desarrollo seguro de aplicaciones y sistemas de información en tu organización. Esta política debe abordar aspectos como la identificación y gestión de vulnerabilidades, la implementación de controles de seguridad durante el desarrollo, la revisión de código y pruebas de seguridad, y la capacitación del personal en prácticas seguras de desarrollo.

(5.1.1) – Clasificación de la información:

Observación:

Dentro del documento 4.2.1 Instructivo Clasificación de la información faltan la firma de aprobación por parte del rectorado, la de supervisión por parte del vicerrectorado y la de revisión por parte de la unidad de seguridad.

Criterio:

NTE ISO/IEC 27002 Control 5.1.1 - La información de Banner-act25 debe tener una clasificación de acuerdo con el grado de importancia frente al valor, sensibilidades, leyes y criticidad ante una modificación no autorizadas por parte de la dirección

Condición:

En la documentación presentada para el cumplimiento de dicho control carece de firmas que validen la documentación que se presentó para el cumplimiento del control.

Efecto:

El control 5.1.1 clasificación de la información no cuenta con un manual valido.

Recomendación:

La UTIC debe proceder con las actividades necesarias para que la documentación se encuentre firmada de manera correcta y de esa forma confirmar su legalización ante las autoridades.

(12.4.1) – Registro de eventos:

Observación:

No presenta un formato o bitácora que muestren las actividades, fallos y eventos que afecten la seguridad de la información.

Criterio:

NTE ISO/IEC 27002 Control 12.4.1 Es necesario un registro sobre las actividades de los usuarios constante, fallos y eventos que afecten la seguridad de la información.

Condición:

En la documentación presentada se encuentra el manual de procedimientos para el cumplimiento del control dejando de lado el registro de los eventos.

Efecto:

A falta de un registro para la obtención de evidencia tangible la institución carecerá de registros documentados para demostrar el cumplimiento del control y a su vez esto provocará que cuando exista un problema o posibles vulnerabilidades la identificación de este sea complicada por tanto difícil de abordar.

Recomendación:

Para el funcionamiento de este control se debe llevar a cabo ciertas actividades:

Definir los eventos a registrar: Identificar y definir los eventos relevantes que deben registrarse en los sistemas de información. Estos eventos pueden incluir accesos no autorizados, cambios en la configuración, intentos de intrusión, fallos del sistema, actividades sospechosas y cualquier otro evento que pueda tener impacto en la seguridad de la información.

Implementar una solución de registro de eventos: Utilizar una solución de registro de

eventos o un sistema de administración de registros que permita recopilar, almacenar y analizar los eventos registrados. Esta solución debe ser capaz de capturar y conservar los registros de manera segura, garantizando la integridad y confidencialidad de la información.

Definir formatos y estándares de registro: Establecer formatos y estándares claros para el registro de eventos. Esto incluye definir los campos de registro requeridos, la estructura del registro y el nivel de detalle necesario para una adecuada auditoría y análisis posterior.

(16.1.7) – Recopilación de evidencias:

Observación:

Falta detallar un subproceso específico para la recopilación de evidencias.

Criterio:

NTE ISO/IEC 27002 Control 16.1.7 Se debe identificar los procesos adecuados para establecer, reunir y conservar la información como parte de la evidencia.

Condición:

No presenta un subproceso específico para la recopilación de evidencias.

Efecto:

La no implantación de este control puede generar dificultad al investigar incidentes.

Falta de trazabilidad al no conocer un registro de eventos no se puede tener un historial de lo ocurrido en términos de seguridad de la información.

Recomendación:

La unidad de Tecnologías de la Información comunicación TICS debe realizar las actividades necesarias para desarrollar de manera correcta un proceso de recopilación de evidencias o de otra forma la institución cuenta con una grave brecha en la seguridad abierta a posibles vulnerabilidades graves, por esto también se debe incluir:

- Manual de procesos para reunir información.
- Evidencias de la información recolectada.

- Plan de conservación de la información.

(6.1.4) – Contacto con los grupos de interés especial:

Observación:

La política de grupos de interés especial se encuentra dentro de un documento de Word el cual no se encuentra firmado.

Criterio:

NTE ISO/IEC 27002 Control 6.1.4 Se deba mantener el contacto con los actores especiales con conocimiento en seguridad que pueden tener acceso a los activos de información.

Condición:

Falta de revisión por parte de las autoridades.

Efecto:

Falta de alineación con las expectativas de los grupos de interés.

Riesgo de incumplimiento normativo y contractual.

Recomendación:

Se debe realizar las respectivas actividades para la legalización de la documentación por parte de la UTIC.

(11.2.5) – Eliminación de activos:

Observación:

No presenta un proceso específico para la eliminación de los activos.

Criterio:

NTE ISO/IEC 27002 Control 11.2.5 Debe existir una autorización por parte de los directivos para eliminar o recoger equipos, información o el software de las instalaciones.

Condición:

Falta de un micro proceso sobre los activos a eliminar.

Efecto:

Brechas de seguridad.

Compromiso de la confidencialidad.

Riesgo de acceso no autorizado.

Riesgo de incumplimiento normativo y contractual.

Recomendación:

Desarrollar una política de eliminación de activos: Establecer una política clara que defina los procedimientos y las mejores prácticas para la eliminación de activos. Esta política debe abarcar diferentes tipos de activos, como hardware, software, medios de almacenamiento y documentos físicos, y debe especificar los pasos requeridos para garantizar una eliminación segura y completa de la información contenida en ellos.

Identificar los activos a eliminar: Realizar un inventario exhaustivo de los activos que deben ser eliminados. Esto implica identificar los activos obsoletos, dañados o fuera de servicio, así como aquellos que contengan información confidencial o sensible que ya no sea necesaria para la organización.

Implementar procesos de eliminación segura: Establecer procesos y procedimientos seguros para la eliminación de activos. Esto puede incluir el borrado seguro de datos, el formateo de medios de almacenamiento, la destrucción física de documentos y la disposición adecuada de hardware y dispositivos electrónicos. Se deben seguir estándares y técnicas reconocidas para garantizar que la información sea irreparablemente eliminada y no pueda ser recuperada.

Documentar y auditar la eliminación de activos: Mantener un registro de las actividades de eliminación de activos, incluyendo detalles como la fecha, el tipo de activo, el método de eliminación utilizado y las personas responsables. Realizar auditorías periódicas para verificar el cumplimiento de los procedimientos de eliminación y asegurarse de que se sigan las políticas

establecidas.

(9.2.5) – Revisión de los derechos de acceso de usuario:

Observación:

No se presenta un formato de registro de los accesos de los usuarios.

Criterio:

NTE ISO/IEC 27002 Control 9.2.5 Los administradores de los activos deben revisar los derechos de acceso de cada usuario de forma regular.

Causa:

No se encontró evidencias de la implantación de este control.

Efecto:

Riesgo de incumplimiento normativo y contractual.

Recomendación:

Se debe dar una revisión a la evidencia que se recopila y almacenarla en el apartado del control con las siguientes actividades:

Establecer criterios de revisión: Definir criterios claros para la revisión de derechos de acceso. Estos criterios pueden incluir la evaluación de la necesidad de acceso, la adecuación de los permisos otorgados, la revisión de los cambios recientes en los roles o responsabilidades del usuario, entre otros aspectos relevantes.

Realizar auditorías internas y externas: Realizar auditorías periódicas tanto internas como externas para evaluar la efectividad del proceso de revisión de derechos de acceso. Estas auditorías pueden identificar áreas de mejora y asegurar que se cumplan los requisitos normativos y las mejores prácticas en materia de seguridad de la información.

Mantener registros y documentación: Mantener registros y documentación adecuada de las revisiones de derechos de acceso realizadas. Esto incluye documentar los resultados de las revisiones, las acciones tomadas para corregir posibles problemas y las fechas de las próximas

revisiones planificadas.

(12.1.2) – Gestión de cambios:

Observación:

Existen los procesos para la gestión de cambio, pero falta el formato de bitácora que llevan a cabo para registrar los cambios.

Criterio:

NTE ISO/IEC 27002 Control 12.1.2 Los cambios, procesos o instalaciones que puedan afectar a la seguridad de la información deben ser controlados de forma eficiente.

Condición:

No se muestra alguna bitácora o formato de bitácora para llevar registro de las actividades que se han realizado con respecto al cambio en los servicios.

Efecto:

Riesgo de introducción de vulnerabilidades.

Falta de control sobre los cambios.

Inconsistencia en la documentación y procedimientos.

Recomendación:

Documentar y comunicar los cambios: Mantener un registro de todos los cambios realizados, incluyendo detalles como la descripción del cambio, la fecha de implementación, los responsables y los resultados obtenidos. Asegurarse de que esta información esté disponible para todas las partes involucradas y sea comunicada de manera efectiva, tanto interna como externamente cuando sea necesario.

Establecer un proceso de revisión posterior a la implementación: Después de que los cambios sean implementados, realizar una revisión posterior para evaluar su efectividad y el cumplimiento.

(13.1.3) – Separación en las redes:

Observación:

Existe solo el excel de VLANs, no tienen registros de configuración y control de acceso.

Criterio:

NTE ISO/IEC 27002 Control 13.1.3 Los sistemas, servicios y usuarios deben separarse en distintas redes.

Condición:

Existe solo el Excel de VLANs, no tiene un registro de configuración y control de acceso.

Efecto:

Riesgo de introducción de vulnerabilidades.

Falta de control sobre los cambios

Inconsistencia en la documentación y procedimientos

Recomendación:

Aplicar controles de acceso: Establecer políticas y mecanismos de autenticación y autorización para controlar el acceso a las distintas zonas de la red. Utilizar soluciones como VPN, autenticación de dos factores y sistemas de gestión de identidad para garantizar que solo los usuarios autorizados puedan acceder a las zonas correspondientes.

Segmentar la red en zonas de seguridad: Establecer políticas de acceso y comunicación entre las zonas para garantizar una separación efectiva y controlada.

(14.2.7) – Desarrollo externalizado:

Observación:

No tiene un registro de las actividades de usuarios externos.

Criterio:

NTE ISO/IEC 27002 Control 12.6.1 Es necesario un registro sobre las actividades de los usuarios constante, fallos y eventos que afecten la seguridad de la información.

Condición:

No se llevó un registro de actividades de usuarios externos a la institución.

Efecto:

Riesgo de vulnerabilidades y no tiene control de actividades de terceros.

Recomendación:

Se debe realizar un registro de las actividades de usuarios externos al realizar un trabajo dentro de la institución.

(7.2.2) –Concienciación, educación y formación en seguridad de la información:

Observación:

Presenta un plan de concienciación, pero no contiene un registro o cronograma de realización de concienciación al personal.

Criterio:

NTE ISO/IEC 27002 Control 7.2.2 La dirección debe garantizar que el personal reciba un apropiado programa de formación y concienciación, incluyendo actualizaciones frecuentes acerca de los nuevos procedimientos y estándares de seguridad de la información.

Condición:

En la documentación presentada para el cumplimiento de dicho control carece de un registro de realización de capacitación del personal para el cumplimiento del control.

Efecto:

Falta de conocimiento de las políticas de seguridad.

Mayores riesgos de incidentes de seguridad

Menor capacidad de respuestas ante incidentes.

Recomendación:

Las UTIC deberá realizar un plan para llevar a cabo distintas capacitaciones y dar conocimiento a los empleados sobre las políticas con las que cuenta la institución. Además,

mantener un registro de todas las actividades realizadas para la concienciación del personal.

(12.6.2) –Restricciones en la instalación del software:

Observación:

No presenta un registro de evidencias de instalaciones de software anteriores, además las políticas de instalación del software no se encuentran respectivamente legalizadas.

Criterio:

NTE ISO/IEC 27002 Control 12.6.2 Se debe normar y regular la instalación de software para los usuarios.

Condición:

Falta de revisión por parte de las autoridades.

Efecto:

Aumento del riesgo de comprometer la seguridad de los sistemas y la integridad de los datos.

Dificulta la capacidad de rastrear y auditar el software instalado, lo que puede resultar en la presencia de software no autorizado o no actualizado.

Recomendación:

La UTIC de la universidad debe establecer y documentar políticas claras y legalizadas para regular la instalación de software por parte de los usuarios. Estas políticas deben cumplir con el control 12.6.2 de la norma NTE ISO/IEC 27002. Se recomienda que la UTIC asuma la responsabilidad de mantener un registro actualizado de todas las instalaciones de software realizadas en los sistemas.

La UTIC de la universidad, como autoridad competente, debe implementar un proceso de revisión para garantizar el cumplimiento de las políticas de instalación de software establecidas. Esta revisión debe incluir la verificación de que se siguen los procedimientos establecidos por la UTIC y que se cuenta con la debida autorización para cada instalación de software realizada.

Los hallazgos y resultados de estas revisiones deben ser documentados por la UTIC y utilizados para mejorar continuamente el proceso de instalación de software específicamente en su ámbito de acción.

La UTIC de la universidad debe considerar la implementación de herramientas de gestión de activos de software específicas para su uso. Estas herramientas permitirán un seguimiento más eficiente de las instalaciones de software en el ámbito de la UTIC, ayudando a mantener un inventario actualizado de los programas instalados y facilitando la identificación de software no autorizado o desactualizado. Además, estas herramientas pueden proporcionar informes y alertas específicos para el monitoreo y control del software instalado por la UTIC.

La UTIC de la universidad debe brindar capacitación y concientización específicamente a los usuarios de la UTIC sobre las políticas y procedimientos de instalación de software establecidos. Esto garantizará que estén informados y comprendan las restricciones y requisitos específicos aplicados por la UTIC. Además, la UTIC debe promover una cultura de responsabilidad y cumplimiento en relación con la instalación de software, fomentando la comunicación y el reporte de cualquier instalación no autorizada o sospechosa específicamente dentro de su ámbito de acción.

(8.3.3) –Transferencia de Medios Físicos:

Observación:

No presenta un formato de registro de la transferencia de medios físicos, el proceso se encuentra validado y excelente.

Criterio:

NTE ISO/IEC 27002 Control 8.3.3 Los medios físicos que salgan de límite de la universidad deben tener el respectivo control ante accesos no autorizados a la información que estos contienen.

Condición:

Falta de registros de las actividades de transferencia.

Efecto:

el aumento del riesgo de pérdida, robo o acceso no autorizado a la información contenida en dichos medios.

dificulta el seguimiento y la auditoría de las transferencias realizadas, lo que puede dar lugar a la falta de responsabilidad y al desconocimiento de la ubicación y el estado de los medios físicos

la exposición de información confidencial y sensible, así como en la pérdida de activos de información críticos.

Recomendación:

La UTIC de la universidad debe implementar un proceso formal específico para la UTIC, que permita el registro de todas las transferencias de medios físicos que salgan de los límites de la universidad. Este registro debe ser exhaustivo y contener información detallada sobre los medios transferidos, incluyendo el tipo de medio (por ejemplo, discos duros, USB, DVDs), una descripción precisa de los contenidos, el destinatario, la fecha de transferencia y cualquier otra información relevante para el seguimiento y control de los medios físicos.

Se debe capacitar al personal de la UTIC y a aquellos involucrados en las transferencias de medios físicos sobre los procedimientos y políticas establecidas. Esto garantizará que comprendan la importancia de registrar adecuadamente las transferencias y cumplan con los controles de seguridad establecidos.

Realizar auditorías regulares para verificar el cumplimiento de las políticas y procedimientos de transferencia de medios físicos.

(12.1.2) –Controles físicos de entrada:

Observación:

Presenta el procedimiento para la entrada de personas a las instalaciones del Campus Matriz, pero falta la firma de aprobación. Además de la falta de registros como evidencia del control

Criterio:

NTE ISO/IEC 27002 Control 12.1.2 Las áreas seguras deben permitir el ingreso solo a personal autorizado, se debe emplear los controles de entrada adecuados para este caso.

Condición:

El control no ha sido aprobado por el Comité de Seguridad de la Información.

Efecto:

Debilidad en la seguridad de las áreas seguras.

Sin la firma de aprobación, no se puede verificar de manera confiable que solo el personal autorizado tenga acceso a las instalaciones.

La ausencia de registros dificulta la capacidad de rastrear y auditar el acceso de las personas, lo que puede resultar en la entrada no autorizada de individuos.

Recomendación:

La UTIC debe establecer un proceso formal que requiera la firma de aprobación de un supervisor o autoridad competente para el acceso a las áreas seguras. La firma de aprobación debe ser registrada y archivada como evidencia de la autorización y para fines de auditoría.

La UTIC debe implementar un sistema de registro para el control físico de entrada que permita registrar y rastrear el acceso de las personas a las instalaciones. Estos registros deben incluir información como la fecha, hora, nombre de la persona, motivo de la visita y cualquier otra información relevante.

(11.1.3) –Seguridad de oficinas, despachos e instalaciones:

Observación:

Presenta el procedimiento para la entrada de personas a las instalaciones del Campus

Matriz, pero falta la firma de aprobación.

Criterio:

NTE ISO/IEC 27002 Control 11.1.3 Es necesario materializar la seguridad física de las instalaciones donde se encuentren los activos de información.

Condición:

El control no ha sido aprobado por el Comité de Seguridad de la Información.

Efecto:

Debilidad en la seguridad de las áreas seguras.

Sin la firma de aprobación, no se puede verificar de manera confiable que solo el personal autorizado tenga acceso a las instalaciones.

Recomendación:

La UTIC debe establecer un proceso formal que requiera la firma de aprobación de un supervisor o autoridad competente para el acceso a las oficinas, despachos e instalaciones. La firma de aprobación debe ser registrada y archivada como evidencia de la autorización y para fines de auditoría.

(14.2.5) –Principios de ingeniería de sistemas seguros:

Observación:

No presenta un documento o manual general que indique los principios seguros para la implementación de sistemas de información.

Criterio:

NTE ISO/IEC 27002 Control 14.2.5 Se deben establecer y documentar los principios de sistemas seguros a todos los esfuerzos de modificación o implementación de los sistemas de información.

Condición:

No presenta un documento con políticas, procedimientos o manual sobre los principios

de ingeniería en desarrollo de sistemas seguros.

Efecto:

Riesgo de desarrollar sistemas inseguros o vulnerables.

Existe la posibilidad de que los sistemas de información carezcan de los controles necesarios para proteger la información y garantizar la integridad, disponibilidad y confidencialidad de los datos.

Recomendación:

La UTIC de la universidad debe elaborar y documentar un documento o manual específico para su ámbito de acción que defina los principios seguros a seguir en la implementación de sistemas de información. Este documento debe cumplir con el control 14.2.5 de la norma NTE ISO/IEC 27002. Se recomienda que la UTIC asuma la responsabilidad de elaborar y mantener este documento, en colaboración con los profesionales de ingeniería de sistemas y seguridad de la información.

El documento o manual de principios seguros para la implementación de sistemas de información debe abordar prácticas de diseño seguro, autenticación y autorización adecuadas, cifrado de datos, gestión de vulnerabilidades y pruebas de seguridad. Es importante que estos principios estén alineados con los estándares y mejores prácticas reconocidos en el campo de la seguridad de la información, y que sean actualizados periódicamente para adaptarse a las nuevas amenazas y tecnologías emergentes.

La UTIC debe asegurarse de que el documento o manual sea ampliamente difundido y esté accesible para todos los profesionales y equipos involucrados en el desarrollo e implementación de sistemas de información. Se deben proporcionar capacitaciones y sesiones de concientización específicas para garantizar que los principios seguros sean entendidos y aplicados correctamente por todos los miembros del equipo.

La UTIC debe integrar los principios seguros definidos en el documento o manual en los procesos de desarrollo de sistemas de información. Esto implica incorporar controles y

verificaciones durante todas las etapas del ciclo de vida de los sistemas, desde el diseño hasta la implementación y el mantenimiento. Además, se deben establecer mecanismos de revisión y evaluación periódicos para asegurar el cumplimiento de los principios seguros y realizar mejoras continuas en los sistemas implementados.

(14.2.6) –Ambiente de desarrollo seguro:

Observación:

Presenta un diagrama de desarrollo, pero no se identifica de manera clara la separación del ambiente de producción y el desarrollo en general con la seguridad que presenta.

Criterio:

NTE ISO/IEC 27002 Control 14.2.6 Se debe asegurar el ambiente de desarrollo de forma adecuada durante todo el ciclo de vida de desarrollo de sistemas.

Condición:

No presenta un documento donde se identifique claramente la separación del ambiente de desarrollo como su seguridad.

Efecto:

Riesgo de introducir vulnerabilidades y debilidades en el software y las aplicaciones.

Es más probable que las pruebas y las modificaciones realizadas en el ambiente de desarrollo afecten la integridad y seguridad de los sistemas en producción.

Recomendación:

La UTIC de la universidad debe implementar políticas y procedimientos que aseguren una separación adecuada entre los entornos de desarrollo y producción. Esto debe cumplir con el control 14.2.6 de la norma NTE ISO/IEC 27002. Es fundamental garantizar que exista una clara segregación de los ambientes de desarrollo y producción, tanto en términos de infraestructura como de seguridad.

Se debe establecer una infraestructura separada para el ambiente de desarrollo, que esté

física o lógicamente aislada del ambiente de producción. Esto implica utilizar servidores, redes y sistemas de almacenamiento dedicados exclusivamente para el desarrollo y pruebas de software. La UTIC debe garantizar que esta infraestructura cumpla con los estándares de seguridad adecuados y esté protegida contra accesos no autorizados.

Se deben implementar controles de acceso y autorización estrictos para restringir el acceso al ambiente de producción únicamente al personal autorizado. Esto implica establecer políticas claras de gestión de usuarios y privilegios, implementar autenticación fuerte, como el uso de contraseñas robustas o autenticación de dos factores, y realizar un monitoreo continuo de los accesos y actividades en el ambiente de producción.

La UTIC debe establecer políticas y procedimientos para la gestión de cambios en el ambiente de producción. Esto implica tener un proceso formal y controlado para migrar el software desarrollado y probado en el ambiente de desarrollo hacia el ambiente de producción. Se deben establecer revisiones y aprobaciones de cambios, pruebas exhaustivas y controles de calidad para asegurar que los cambios introducidos no comprometan la seguridad y la integridad de los sistemas en producción.

(17.1.1) –Planificación de la continuidad de la seguridad de la información:

Observación:

No presentan un plan de continuidad solo un plan de contingencia.

Criterio:

NTE ISO/IEC 27002 Control 17.1.1 Determinar las necesidades de seguridad de la universidad gestionando la continuidad del proceso de aseguramiento de la información en situaciones adversas.

Condición:

Confusión entre plan de continuidad y plan de contingencia.

Efecto:

Falta de medidas y estrategias para garantizar la continuidad de las operaciones y la protección de la información en situaciones adversas.

La organización puede enfrentar dificultades para mantener la disponibilidad, integridad y confidencialidad de la información, lo que puede resultar en pérdida de datos, daños a la reputación y pérdida de confianza de los clientes y socios.

Recomendación:

La UTIC de la universidad debe elaborar un plan de continuidad de la seguridad de la información que cumpla con el control 17.1.1 de la norma NTE ISO/IEC 27002. Es importante distinguir entre un plan de continuidad y un plan de contingencia, ya que ambos son necesarios para garantizar la protección de la información en situaciones adversas.

El plan de continuidad de la seguridad de la información debe abordar específicamente las necesidades de la universidad y considerar los diferentes escenarios de riesgo que puedan afectar la disponibilidad, integridad y confidencialidad de la información. Se deben identificar los activos críticos, los procesos clave y los sistemas de información relevantes para establecer las estrategias y medidas de continuidad adecuadas.

Es fundamental establecer roles y responsabilidades claros dentro del plan de continuidad. Designar un equipo responsable de la implementación y ejecución del plan, así como de la coordinación de las actividades de respuesta ante situaciones adversas. Este equipo debe contar con los recursos necesarios y estar capacitado para actuar de manera efectiva en caso de incidentes.

El plan de continuidad debe incluir procedimientos para la rápida recuperación de los sistemas y servicios afectados. Se deben establecer protocolos de respaldo y restauración de datos, así como estrategias de redundancia y disponibilidad de los sistemas críticos. También se deben definir los mecanismos de comunicación y notificación tanto interna como externa en caso de interrupciones graves.

(17.1.2) –Implementación de la continuidad de la seguridad de la información:

Observación:

No presentan un plan de continuidad solo un plan de contingencia.

Criterio:

NTE ISO/IEC 27002 Control 17.1.2 Establecer, documentar e implementar los procedimientos y controles necesarios para situaciones adversas.

Condición:

Confusión entre plan de continuidad y plan de contingencia.

Efecto:

Falta de medidas y procedimientos adecuados para garantizar la continuidad de las operaciones en situaciones adversas.

La organización puede enfrentar dificultades para mantener la disponibilidad, integridad y confidencialidad de la información, lo que puede resultar en pérdida de datos, daños a la reputación y pérdida de confianza de los clientes y socios.

Recomendación:

La UTIC de la universidad debe implementar los procedimientos y controles necesarios para garantizar la continuidad de la seguridad de la información en situaciones adversas, de acuerdo con el control 17.1.2 de la norma NTE ISO/IEC 27002. Es importante distinguir entre un plan de continuidad y un plan de contingencia, ya que ambos son necesarios para enfrentar situaciones adversas de manera efectiva.

Una vez que se haya elaborado el plan de continuidad específico, es fundamental implementarlo de manera adecuada en toda la organización. Esto implica poner en práctica los procedimientos y controles definidos en el plan, así como asegurarse de que todos los responsables conozcan sus roles y responsabilidades durante una situación adversa.

Se deben establecer medidas y procedimientos para garantizar la continuidad de las operaciones críticas durante situaciones adversas. Esto puede incluir la implementación de

sistemas de respaldo y redundancia, la asignación de recursos adicionales, la planificación de infraestructuras alternativas y la definición de protocolos de comunicación y coordinación.

(16.1.2) –Notificación de los eventos de seguridad de la información:

Observación:

Necesario un proceso para la notificación de eventos de seguridad de la información.

Criterio:

NTE ISO/IEC 27002 Control 16.1.2 Los eventos deben ser comunicados por los canales establecidos y de manera oportuna.

Condición:

No se presenta un procedimiento o manual para la notificación de los eventos.

Efecto:

La falta de comunicación adecuada puede retrasar la identificación y respuesta a eventos adversos, lo que aumenta el riesgo de que se produzcan daños mayores a la organización.

Recomendación:

La UTIC de la institución debe implementar un proceso formal que establezca los canales de comunicación y los procedimientos para notificar los eventos de seguridad de la información, de acuerdo con el control 16.1.2 de la norma NTE ISO/IEC 27002. Es esencial garantizar una comunicación adecuada y oportuna de los eventos de seguridad para poder identificar y responder rápidamente a situaciones adversas.

La UTIC debe Se deben designar responsables claros para recibir y registrar las notificaciones de eventos de seguridad. Estos responsables deben estar capacitados para manejar la información de manera confidencial y tomar las medidas adecuadas en respuesta a los eventos reportados.

La UTIC debe Definir los plazos y protocolos de comunicación para garantizar una respuesta oportuna a los eventos de seguridad. Establecer tiempos específicos para la

notificación de eventos, tanto internamente dentro de la UTIC como hacia otras partes interesadas relevantes, como la alta dirección y los equipos de respuesta a incidentes.

Implementar un sistema o herramienta para el registro y seguimiento de los eventos de seguridad de la información. Esto facilitará la documentación adecuada de los eventos, el monitoreo de su resolución y la generación de informes para su análisis y mejora continua.

Capacitar al personal de la UTIC y a otros empleados sobre la importancia de notificar los eventos de seguridad de la información de manera oportuna y adecuada. Esto fomentará una cultura de seguridad y colaboración en la organización, promoviendo la detección temprana y la respuesta efectiva a los incidentes de seguridad.

Realizar revisiones periódicas del proceso de notificación de eventos de seguridad para evaluar su eficacia y realizar mejoras continuas. Esto puede incluir la revisión de los canales de comunicación utilizados, los procedimientos establecidos y la retroalimentación recibida de los usuarios del sistema.

(16.1.3) –Notificación de los puntos débiles de la seguridad de la información:

Observación:

Falta definir las políticas y acuerdos específicos de la notificación de los puntos débiles.

Criterio:

NTE ISO/IEC 27002 Control 16.1.3 Los usuarios de los sistemas y los activos de información tienen la obligación de comunicar cualquier punto débil que identifiquen.

Condición:

No se tomó en cuenta este control al momento de la implantación del SGSI por lo cual la carpeta se encuentra completamente vacía.

Efecto:

Los puntos débiles no notificados pueden ser aprovechados por atacantes para comprometer la seguridad de la información, lo que puede resultar en la pérdida, filtración o

alteración de datos sensibles.

Recomendación:

La UTIC de la institución debe implementar un proceso formal que permita a los usuarios identificar y notificar los puntos débiles de seguridad de la información, de acuerdo con el control 16.1.3 de la norma NTE ISO/IEC 27002. Es esencial fomentar una cultura de seguridad en la organización, donde los usuarios sean conscientes de su responsabilidad de comunicar cualquier punto débil que identifiquen.

Establecer un canal de comunicación específico para la notificación de puntos débiles de seguridad. Esto puede ser a través de un sistema de tickets, una dirección de correo electrónico dedicada o cualquier otra herramienta de comunicación que facilite la recopilación y gestión de la información.

Promover la conciencia y capacitación de los usuarios sobre la importancia de identificar y notificar los puntos débiles de seguridad de la información. Esto puede incluir la realización de sesiones de formación, la difusión de material educativo y la integración de la seguridad de la información en los programas de inducción y entrenamiento del personal.

Designar responsables dentro de la UTIC para recibir y gestionar las notificaciones de puntos débiles de seguridad. Estos responsables deben estar capacitados para evaluar la gravedad de las vulnerabilidades reportadas y tomar las medidas adecuadas para su mitigación.

Establecer procedimientos claros para el seguimiento y la resolución de los puntos débiles reportados. Esto incluye establecer plazos para la revisión y acción, así como la comunicación de los resultados y las medidas adoptadas a los usuarios que notificaron los puntos débiles.

Realizar revisiones periódicas del proceso de notificación de puntos débiles de seguridad para evaluar su eficacia y realizar mejoras continuas. Esto implica revisar la calidad y eficiencia de la gestión de las vulnerabilidades reportadas, así como la comunicación y retroalimentación con los usuarios involucrados.

(16.1.4) –Evaluación y decisión sobre los eventos de seguridad de la información:

Observación:

Es importante detallar el proceso por el cual se realizará una evaluación adecuada de los eventos de seguridad de la información para determinar los criterios que cumplen para considerarlos incidentes.

Criterio:

NTE ISO/IEC 27002 Control 16.1.4 Se debe evaluar los eventos de seguridad con el fin de determinar si son considerados incidentes.

Condición:

No se detalla el proceso por el cual se realizará una evaluación adecuada de los eventos de seguridad de la información se encuentra completamente vacía.

Efecto:

Los eventos de seguridad no evaluados pueden pasar desapercibidos o no ser tratados de manera adecuada, lo que podría permitir que los incidentes se agraven y causen daños mayores a los sistemas y la información.

Recomendación:

La UTIC de la institución debe implementar un proceso formal para evaluar todos los eventos de seguridad de la información, de acuerdo con el control 16.1.4 de la norma NTE ISO/IEC 27002. Es importante contar con un mecanismo que permita identificar y determinar si un evento constituye un incidente de seguridad que requiere una respuesta específica.

Designar a personas responsables dentro de la UTIC para llevar a cabo la evaluación de los eventos de seguridad. Estas personas deben estar capacitadas y tener el conocimiento necesario para analizar la información disponible, determinar la gravedad del evento y tomar decisiones adecuadas sobre cómo manejarlo.

Establecer criterios claros y predefinidos para determinar si un evento debe ser considerado como un incidente de seguridad. Estos criterios pueden incluir la naturaleza del

evento, su impacto potencial en la confidencialidad, integridad y disponibilidad de la información, y cualquier requisito legal o regulatorio aplicable.

(14.1.2) –Asegurar los servicios de aplicaciones en redes públicas:

Observación:

Solo se encuentra el acuerdo de confidencialidad de evidencia, pero es importante detallar un proceso que permita controlar y asegurar los servicios de aplicaciones en redes públicas.

Criterio:

NTE ISO/IEC 27002 Control 14.1.2 La información que pasan por redes públicas deben estar protegidas de cualquier actividad fraudulenta.

Condición:

Carece de un procedimiento para controlar y asegurar los servicios de aplicaciones en redes públicas.

Efecto:

la información que se transmite a través de estas redes queda expuesta a posibles actividades fraudulentas.

Recomendación:

La UTIC debe implementar sistemas de monitoreo y detección de intrusos en las redes públicas para identificar actividades sospechosas o maliciosas y tomar medidas de respuesta adecuadas.

La UTIC debe brindar capacitación regular sobre seguridad de la información a todo el personal que utiliza servicios de aplicaciones en redes públicas, para aumentar la conciencia sobre los riesgos y promover buenas prácticas de seguridad.

La UTIC debe establecer políticas y procedimientos claros para el uso de servicios de aplicaciones en redes públicas, incluyendo requisitos de seguridad, autenticación de usuarios y

el uso de conexiones seguras.

La UTIC debe evaluar y seleccionar proveedores de servicios de aplicaciones en redes públicas que ofrezcan garantías de seguridad y protección adecuadas.

La UTIC debe establecer acuerdos de confidencialidad y seguridad con los proveedores de servicios de aplicaciones en redes públicas, especificando responsabilidades y medidas de protección adicionales.

Recursos materiales

Con respecto al EGSI de la Universidad de las Fuerzas Armadas por parte de la unidad de tecnologías que cuenta con la documentación necesaria para la revisión técnica y procedimientos necesarias para la implantación, se solicitará acceso a dicha información pertinente para que el equipo de estudiantes operativo tenga la capacidad y las herramientas necesaria para llevar a cabo las actividades planificadas en la culminación del proyecto.

Marco Legal

La implantación del Sistema de Gestión de Seguridad de la Información en la Universidad de las Fuerzas Armadas presenta una iniciativa que busca mejorar la protección, confidencialidad e integridad de la información dentro de la institución. Además, el marco legal desempeña una base importante que incluye las leyes nacionales que rigen la gestión de datos personales.

Legislación Nacional de Ecuador

- **Constitución de la República del Ecuador (2008):** En el Artículo 66 se garantiza el derecho a la intimidad y la protección de los datos personales. (Asamblea Nacional Constituyente., 2008). Lo cual implica la responsabilidad de la Universidad de salvaguardar la privacidad de los datos personales de sus estudiantes, personal y otras partes interesadas.

- **Ley Orgánica de Telecomunicaciones (2019):** Se establece la importancia de la seguridad de la red y los servicios de telecomunicaciones. Este indica la necesidad de mantener la integridad y la confidencialidad de la información en la Institución, específicamente en el entorno en donde las comunicaciones se desempeñan un papel crucial. (Gobierno de Ecuador, 2019).
- **Ley Orgánica de Datos Personales (2018):** Esta ley es importante para la Universidad ya que involucra la gestión de información privada del estudiante y del personal de la institución. En el Artículo 10 se establece los principios para el tratamiento de datos personales. En el Artículo 15 se garantiza el derecho al olvido permitiendo la eliminación de información personal cuando ya no sea necesario para la Universidad. El Artículo 17 nos indica las obligaciones del responsable del tratamiento de datos personales, los cuales garantiza la seguridad de los datos (Asamblea Nacional del Ecuador, 2018).
- **Ley Orgánica de Transparencia y Acceso a la Información Pública (2004):** Esta ley es importante ya que involucra la gestión de información pública y confidencial. En el Artículo 18 se habla de garantizar el derecho a la privacidad y la reserva de la información (Asamblea Nacional del Ecuador, 2004).
- **Ley Orgánica de Comunicación (2013):** En el Artículo 31 se establecen las disposiciones relacionadas con la protección de la privacidad y la confidencialidad de las fuentes de información (Asamblea Nacional del Ecuador, 2013).

En base a las leyes regulatorias del país presentadas anteriormente se designó el uso de las siguientes para cada uno de los controles diseñados:

- Asegurar los servicios de Aplicaciones en redes públicas: se aplican estas leyes debido a que hablan sobre medidas técnicas y adecuadas para preservar la seguridad de la red.
    - Constitución de la República del Ecuador (2008)

- Ley Orgánica de Telecomunicaciones (2019)
- Ley Orgánica de Datos Personales (2018)

- Eliminación de activos: Se contemplan estas leyes ya que describen el tratamiento que deben tener los datos personales en la republica ecuatoriana.
  - Constitución de la República del Ecuador (2008)
  - Ley Orgánica de Datos Personales (2018)
  - Ley Orgánica de Transparencia y Acceso a la Información Pública (2004)
- Evaluación y decisión sobre eventos: Se adjunta estas leyes debido a que el control especifica la manera en la que se toman dichas medidas de respuesta ante eventos que atenten a la seguridad de la información, primeramente, evaluando si estos eventos son incidencias de este tipo o no.
  - Constitución de la República del Ecuador (2008)
  - Ley Orgánica de Datos Personales (2018)
  - Ley Orgánica de Transparencia y Acceso a la Información Pública (2004)
- Recolección de evidencias: Se adjunta estas leyes debido a que se debe dar una transparencia a la evidencia recolectada para una futura auditoria.
  - Constitución de la República del Ecuador (2008)
  - Ley Orgánica de Datos Personales (2018)
  - Ley Orgánica de Transparencia y Acceso a la Información Pública (2004)
  - Ley Orgánica de Comunicación (2013)
- Reporte de eventos: las leyes detallan como se debe tratar a la información relevante de este tipo de eventos y como se debe comunicar a las gamas directivas para una toma de decisión por lo cual se debe dar tratamiento a

datos de índole privado.

- Constitución de la República del Ecuador (2008)
- Ley Orgánica de Telecomunicaciones (2019)
- Ley Orgánica de Datos Personales (2018)
- Ley Orgánica de Comunicación (2013)

- Reporte de puntos débiles: Este control especifica las vulnerabilidades de la institución y la manera de reportar de las cuales en las siguientes leyes especifican temas de comunicación y tratamiento de datos personales.
  - Constitución de la República del Ecuador (2008)
  - Ley Orgánica de Telecomunicaciones (2019)
  - Ley Orgánica de Datos Personales (2018)
  - Ley Orgánica de Comunicación (2013)

De esta forma se cubre lo requerido por las leyes ecuatorianas al formalizar los controles para el EGSI de la Universidad de las fuerzas armadas ESPE.

Políticas y Procedimientos Internos

La Universidad de las Fuerzas Armadas ESPE ha establecidos las políticas y procedimientos internos relacionados con la seguridad de la información, dichas políticas se hacen referencia en el documento de Políticas de Seguridad de la Información (2021), el cual incrementa la seguridad de los recursos de información en la Institución. Estos incluyen políticas de privacidad, políticas de gestión de datos, políticas de acceso a la información y otros documentos que rigen la protección y la seguridad de la información en el entorno universitario.

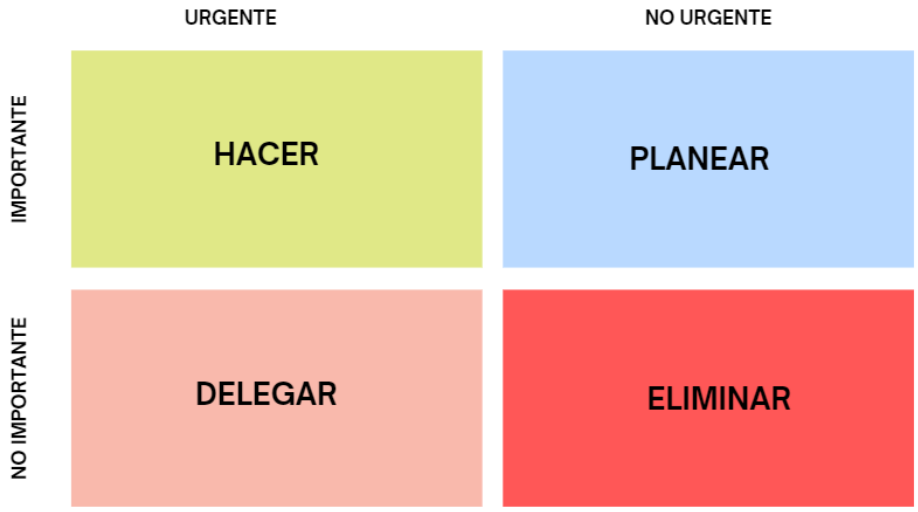
Priorización de controles

Para la selección de controles se usará como base de análisis y herramienta de apoyo

una matriz de priorización, donde se identificarán las incidencias encontradas para decidir si el tratamiento es urgente o no y de alta relevancia para la institución, se llevará a cabo varios análisis para la necesaria intervención al control o no, en la siguiente ilustración se puede observar el tipo de análisis que se dará:

Figura 4

Matriz de Priorización



Nota. La figura representa una matriz de selección y priorización.

Controles seleccionados

En base a los criterios expuestos la revisión técnica se obtuvo como resultado 24 controles que deben ser intervenidos entre los desarrolladores del proyecto y la gente encargada en UTIC los cuales se mostraran en la siguiente tabla sacada de la evidencia Nro. AI-Pr05:

Tabla 8

Priorización de controles.

Controles	Observación	Prioridad

política de desarrollo seguro NTE ISO/IEC 27003 Control 14.2.1 - Determinar y asignar reglas en la institución para el desarrollo de sistemas y aplicaciones.	No existe un manual que explique cómo implementar controles de seguridad durante el desarrollo, revisiones de código y pruebas de seguridad, así como un registro de incidentes, lecciones aprendidas y las medidas correctivas.	ALTA
Registro de EVENTOS NTE ISO/IEC 27002 Control 12.4.1 Es necesario un registro sobre las actividades de los usuarios constante, fallos y eventos que afecten la seguridad de la información.	No presenta un formato o bitácora que muestren las actividades, fallos y eventos que afecten la seguridad de la información	ALTA
Recopilación de evidencias NTE ISO/IEC 27002 Control 16.1.7 Se debe identificar los procesos adecuados para establecer, reunir y conservar la información como parte de la evidencia.	Falta detallar un subproceso específico para la recopilación de evidencia	ALTA
Eliminación de activos NTE ISO/IEC 27002 Control 11.2.5 Debe existir una autorización por parte de los directivos para eliminar o recoger equipos, información o el software de las instalaciones.	No presenta un proceso específico para la eliminación de los activos	ALTA
Revisión de los derechos de acceso de usuario NTE ISO/IEC 27002 Control 9.2.5 Los administradores de los activos deben revisar los derechos de acceso de cada usuario de forma regular.	No se presenta un formato de registro de los accesos de los usuarios	ALTA
Desarrollo externalizado NTE ISO/IEC 27002 Control 12.6.1 Es necesario un registro sobre las actividades de los usuarios constante,	No tiene un registro de las actividades de usuarios externos.	ALTA

fallos y eventos que afecten la seguridad de la información.

Controles	Observación	Prioridad
Concienciación, educación y formación en seguridad de la información NTE ISO/IEC 27002 Control 7.2.2 La dirección debe garantizar que el personal reciba un apropiado programa de formación y concienciación, incluyendo actualizaciones frecuentes acerca de los nuevos procedimientos y estándares de seguridad de la información.	Presenta un plan de concienciación, pero no contiene un registro o cronograma de realización de concienciación al personal	ALTA
Restricciones en la instalación del software NTE ISO/IEC 27002 Control 12.6.2 Se debe normar y regular la instalación de software para los usuarios	No presenta un registro de evidencias de instalaciones de software anteriores, además las políticas de instalación del software no se encuentran respectivamente legalizadas	ALTA
Transferencia de Medios FÍSICOS NTE ISO/IEC 27002 Control 8.3.3 Los medios físicos que salgan de límite de la universidad deben tener el respectivo control ante accesos no autorizados a la información que estos contienen.	No presenta un formato de registro de la transferencia de medios físicos, el proceso se encuentra validado y excelente.	ALTA
Principios de ingeniería de sistemas seguros NTE ISO/IEC 27002 Control 14.2.5 Se deben establecer y documentar los principios de sistemas seguros a todos los esfuerzos de modificación o implementación de los sistemas de información	No presenta un documento o manual general que indique los principios seguros para la implementación de sistemas de información	ALTA

Controles	Observación	Prioridad

Planificación de la continuidad de la seguridad de la información NTE ISO/IEC 27002 Control 17.1.1 Determinar las necesidades de seguridad de la universidad gestionando la continuidad del proceso de aseguramiento de la información en situaciones adversas.	No presentan un plan de continuidad solo un plan de contingencia.	ALTA
Implementación de la continuidad de la seguridad de la información NTE ISO/IEC 27002 Control 17.1.2 Establecer, documentar e implementar los procedimientos y controles necesarios para situaciones adversas.	No presentan un plan de continuidad solo un plan de contingencia.	ALTA
Notificación de los eventos de seguridad de la información NTE ISO/IEC 27002 Control 16.1.2 Los eventos deben ser comunicados por los canales establecidos y de manera oportuna.	Necesario un proceso para la notificación de eventos de seguridad de la información	ALTA
Notificación de los puntos débiles de la seguridad de la información NTE ISO/IEC 27002 Control 16.1.3 Los usuarios de los sistemas y los activos de información tienen la obligación de comunicar cualquier punto débil que identifiquen.	Falta definir las políticas y acuerdos específicos de la notificación de los puntos débiles.	ALTA
Evaluación y decisión sobre los eventos de seguridad de la información NTE ISO/IEC 27002 Control 16.1.4 Se debe evaluar los eventos de seguridad con el fin de determinar si son considerados incidentes.	Es importante detallar el proceso por el cual se realizará una evaluación adecuada de los eventos de seguridad de la información para determinar los criterios que cumplen para considerarlos incidentes.	ALTA

Controles	Observación	Prioridad
Asegurar los servicios de aplicaciones en redes públicas NTE ISO/IEC 27002 Control 14.1.2 La información que pasan por redes públicas deben estar protegidas de cualquier actividad fraudulenta.	Solo se encuentra el acuerdo de confidencialidad de evidencia, pero es importante detallar un proceso que permita controlar y asegurar los servicios de aplicaciones en redes públicas.	ALTA
Clasificación de la información NTE ISO/IEC 27002 Control 5.1.1 - La información de Banner-act25 debe tener una clasificación de acuerdo con el grado de importancia frente al valor, sensibilidades, leyes y criticidad ante una modificación no autorizadas por parte de la dirección	Dentro del documento 4.2.1 instructivo clasificación de la información faltan la firma de aprobación por parte del rectorado, la de supervisión por parte del vicerrectorado y la de revisión por parte de la unidad de seguridad.	MEDIA
Contacto con los grupos de interés especial NTE ISO/IEC 27002 Control 6.1.4 Se deba mantener el contacto con los actores especiales con conocimiento en seguridad que pueden tener acceso a los activos de información.	La política de grupos de interés especial se encuentra dentro de un documento de word el cual no se encuentra firmado.	MEDIA
Gestión de cambios NTE ISO/IEC 27002 Control 12.1.2 Los cambios, procesos o instalaciones que puedan afectar a la seguridad de la información deben ser controlados de forma eficiente.	Existen los procesos para la gestión de cambio, pero falta el formato de bitácora que llevan a cabo para registrar los cambios	MEDIA

Controles	Observación	Prioridad
Controles físicos de entrada NTE ISO/IEC 27002 Control 12.1.2 Las áreas seguras deben permitir el ingreso solo a personal autorizado, se debe emplear los controles de entrada adecuados para este caso.	Presenta el procedimiento para la entrada de personas a las instalaciones del campus matriz, pero falta la firma de aprobación. Además de la falta de registros como evidencia del control	MEDIA

Seguridad de oficinas, despachos e instalaciones NTE ISO/IEC 27002 Control 11.1.3 Es necesario materializar la seguridad física de las instalaciones donde se encuentren los activos de información.	Presenta el procedimiento para la entrada de personas a las instalaciones del campus matriz, pero falta la firma de aprobación.	MEDIA
Ambiente de desarrollo seguro NTE ISO/IEC 27002 Control 14.2.6 Se debe asegurar el ambiente de desarrollo de forma adecuada durante todo el ciclo de vida de desarrollo de sistemas.	Presenta un diagrama de desarrollo, pero no se identifica de manera clara la separación del ambiente de producción y el desarrollo en general con la seguridad que presenta.	MEDIA

Nota. La tabla muestra la priorización de controles a ser tratados.

Plan de implantación

Para el plan de implantación de los controles seleccionados se tomó ciertos puntos basado en la norma ISO/IEC 27001 que se muestran a continuación:

a. Definición de Objetivos y Alcance:

- Establecer los objetivos específicos que se desean lograr con la implementación del SGSI
- Definir el alcance del SGSI, es decir, que activos y procesos estarán incluidos en el sistema

b. Asignación de Responsabilidades:

- Designar un equipo de proyecto responsable de la implantación del SGSI.

c. **Evaluación inicial:**

- Realizar un análisis de riesgos para determinar las amenazas y

evaluar su impacto potencial.

d. Definición de controles de seguridad:

- Identificar y seleccionar los controles de seguridad de la información que serán implementados para mitigar los riesgos identificados.

e. Desarrollo de procedimientos y directrices:

- Crear procedimientos y directrices detallados para cada control de seguridad seleccionado.
- Establecer las normas y reglas que deben seguirse a cada proceso.

f. Implementación y prueba:

- Implementar los controles de seguridad en la infraestructura de la Universidad.
- Realizar pruebas para asegurar la efectividad de los controles.

g. Revisión y Mejora continua:

- Revisión y mejora continua de los controles implementados.

Desarrollo de procedimientos y directrices.

En la siguiente tabla se mostrarán todos los controles revisados y las actividades necesarias para cumplir con su implantación que se encuentra en el anexo Evidencia Nro. AI-Pr05.

Tabla 9

Tabla de actividades por realizar para implantación de controles.

Control	Actividades
Control de acceso al código fuente del programa NTE ISO/IEC 27002 Control 9.4.5	- Política de manejo de versiones - Bitácora de manejo de versiones
Política de desarrollo seguro NTE ISO/IEC 27003 Control 14.2.1	- Identificación y gestión de vulnerabilidades. - Implementación de controles de seguridad durante el desarrollo. - Revisión de código y pruebas de seguridad.

	- Registro de incidentes, lecciones aprendidas y medidas correctivas.
Registro de eventos NTE ISO/IEC 27002 Control 12.4.1	- Definir eventos a registrar. - Implementar una solución de registro de eventos. - Definir formatos y estándares de registros.
Recopilación de evidencias NTE ISO/IEC 27002 Control 16.1.7	- Identificar los procesos relevantes. - Definir Criterios de recolección. - Establecer métodos de recopilación. - Establecer procesos de almacenamiento seguro. - Definir políticas y procedimientos.
Eliminación de activos NTE ISO/IEC 27002 Control 11.2.5 Debe existir una autorización por parte de los directivos para eliminar o recoger equipos, información o el software de las instalaciones.	- Identificar los activos a eliminar. - Establecer procesos de autorización. - Establecer procedimientos de eliminación segura. - Implementar controles de seguimiento. - Mantener Registro.
Revisión de los derechos de acceso de usuario NTE ISO/IEC 27002 Control 9.2.5 Los administradores de los activos deben revisar los derechos de acceso de cada usuario de forma regular.	- Establecer criterios de revisión. - Realizar auditorías. - Mantener registros y documentación.
Desarrollo externalizado NTE ISO/IEC 27002 Control 12.6.1	- Implementar un sistema de registro de actividades de usuarios externos. - Registrar todas las actividades realizadas por usuarios externos. - Registrar cualquier fallo o evento que afecte la seguridad de la información. - Mantener un registro detallado de las actividades y eventos.
Concienciación, educación y formación en seguridad de la información NTE ISO/IEC 27002 Control 7.2.2	- Elaborar un plan de concienciación. - Realizar distintas capacitaciones para dar a conocer las políticas de seguridad. - Mantener un registro de todas las actividades de concienciación realizadas. - Fortalecer una cultura de seguridad dentro de la organización. - Fomentar la comprensión de los riesgos y la importancia de proteger la información.
Restricciones en la instalación del software NTE ISO/IEC 27002 Control 12.6.2 Se debe normar y regular la instalación de software para los usuarios	- Legalizar las políticas - Implementar un proceso de revisión de instalación de software - Mantener un registro de instalaciones de

	software anteriores - Implementar herramientas de gestión de activos de software

Control	Actividades
Transferencia de Medios Físicos NTE ISO/IEC 27002 Control 8.3.3	Registrar todas las transferencias de medios físicos
Principios de ingeniería de sistemas seguros NTE ISO/IEC 27002 Control 14.2.5	- Elaborar un documento o manual de principios seguros - Amplia difusión y accesibilidad del documento o manual - Integrar los principios seguros en los procesos de desarrollo -Monitorear y auditar
Planificación de la continuidad de la seguridad de la información NTE ISO/IEC 27002 Control 17.1.1	- Realizar una evaluación de impacto en el negocio. - Identificar y evaluar riesgos. - Definir objetivos de continuidad. - Desarrollar un plan de continuidad de la seguridad de la información -Establecer equipos de respuesta y roles - Realizar pruebas y ejercicios de continuidad -Capacitar al personal -Revisar y actualizar el plan
Implementación de la continuidad de la seguridad de la información NTE ISO/IEC 27002 Control 17.1.2	- Realizar una evaluación de impacto en el negocio. - Desarrollar un plan de continuidad de la seguridad de la información. - Establecer un equipo de respuesta a incidentes. - Establecer comunicación y coordinación con partes interesadas -Realizar pruebas y ejercicios de continuidad -Mantener actualizado el plan de continuidad
Notificación de los eventos de seguridad de la información NTE ISO/IEC.	- Establecer una política de notificación eventos. - Establecer canales de comunicación. - Establecer procedimientos claros. - Establecer plazos de notificación -Monitorear y auditar la notificación de eventos

Notificación de los puntos débiles de la seguridad de la información NTE ISO/IEC 27002 Control 16.1.3	- Establecer una política de notificación. - Promover una cultura de notificación. - Establecer canales de comunicación. - Establecer un proceso de notificación. - Evaluar y gestionar los puntos débiles -Clasificar y priorizar los incidentes - Realizar auditorías y revisiones regulares

Control	**Actividades**
Evaluación y decisión sobre los eventos de seguridad de la información NTE ISO/IEC 27002 Control 16.1.4.	- Establecer un proceso de gestión de eventos. - Definir criterios para la evaluación. - Identificar y recopilar información. - Analizar el evento - Evaluar si es un incidente -Clasificar y priorizar los incidentes -Documentar y registrar
Asegurar los servicios de aplicaciones en redes públicas NTE ISO/IEC 27002 Control 14.1.2 La información que pasan por redes públicas deben estar protegidas de cualquier actividad fraudulenta.	- Establecer un proceso de gestión de incidentes. - Realizar análisis post-incidente. - Documentar los incidentes. - Realizar análisis de tendencias -Realizar revisiones periódicas
Clasificación de la información NTE ISO/IEC 27002 Control 5.1.1	- Legalizar el control completando las firmas faltantes en la documentación
Contacto con los grupos de interés especial NTE ISO/IEC 27002 Control 6.1.4 Se deba mantener el contacto con los actores especiales con conocimiento en seguridad que pueden tener acceso a los activos de información.	- Legalizar el control completando las firmas faltantes en la documentación
Gestión de cambios NTE ISO/IEC 27002 Control 12.1.2	- Documentar y comunicar cambio. - Mantener registro de todos los cambios realizados.
Separación en las redes NTE ISO/IEC 27002 Control 13.1.3	- Aplicar controles de acceso. - Segmentar la red en zonas seguras.
Controles físicos de entrada NTE ISO/IEC 27002 Control 12.1.2	- Registrar y archivar la firma de aprobación - Implementar controles de entrada adecuados -Monitorear y auditar

Seguridad de oficinas, despachos e instalaciones NTE ISO/IEC 27002 Control 11.1.3	- Establecer un proceso formal de autorización - Implementar medidas de seguridad física - Realizar inspecciones periódicas -Monitorear y auditar
Ambiente de desarrollo seguro NTE ISO/IEC 27002 Control 14.2.6 Se debe asegurar el ambiente de desarrollo de forma adecuada durante todo el ciclo de vida de desarrollo de sistemas.	- Políticas de separación del ambiente de desarrollo seguro - Establecer infraestructura separada - Establecer mecanismos de autenticación segura -Monitorear y auditar

Nota. La tabla representa las tareas por realizar para la implantación y mejoras de controles del sistema actual.

Tratamiento de controles seleccionados.

Para el tratamiento de controles se tomó en cuenta la matriz de prioridad dando mayor importancia a controles que se encontraban sin documentación ni procedimientos establecidos, así como controles que no contaban con registro o bitácoras de actividades que registre la aplicación de estos procedimientos.

Tabla 10

Tabla de Actividades Realizadas

Clasificación del control	Descripción del control	Actividades realizadas
11.2.5 Eliminación de activos	Debe existir una autorización por parte de los directivos para eliminar o recoger equipos, información o el software de las instalaciones.	• Creación de procedimiento • Diseño de un formato de bitácora
16.1.7 Recopilación de evidencias	Se debe identificar los procesos adecuados para establecer, reunir y conservar la información como parte de la evidencia.	• Creación de procedimiento • Diseño de un formato de registro

16.1.2 Notificación de los eventos de seguridad de la información	Los eventos deben ser comunicados por los canales establecidos y de manera oportuna.	• Creación de procedimiento • Diseño de un formato de registro
16.1.3 Notificación de los puntos débiles de la seguridad de la información	Los usuarios de los sistemas y los activos de información tienen la obligación de comunicar cualquier punto débil que identifiquen.	• Creación de procedimiento • Diseño de un formato de registro
16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	Se debe evaluar los eventos de seguridad con el fin de determinar si son considerados incidentes.	• Creación de procedimiento • Diseño de un formato de registro
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	La información que pasan por redes públicas debe estar protegidas de cualquier actividad fraudulenta.	• Creación de procedimiento
12.6.1 Desarrollo externalizado	Es necesario un registro sobre las actividades de los usuarios constante, fallos y eventos que afecten la seguridad de la información.	• Diseño de formato de registro
8.3.3 Transferencia de Medios Físicos	Los medios físicos que salgan de límite de la universidad deben tener el respectivo control ante accesos no autorizados a la información que estos contienen.	• Diseño de formato de registro
12.6.2 Restricciones en la instalación del software	Se debe normar y regular la instalación de software para los usuarios	• Diseño de formato de registro

Nota. Esta tabla representa las actividades realizadas para implementar los controles de mayor prioridad.

Controles Implantados.

En la siguiente sección se describirá los procesos de los controles que se desarrollaron de acuerdo con las actividades de la Tabla 10.

Eliminación de activos.

Tabla 11

Eliminación de activos.

N°.	Actividad	Tarea /Descripción	Responsable	Información Documentada
1	Identificación de Activos para Eliminación	El Propietario del Activo identificará los activos que han alcanzado el final de su ciclo de vida útil o que ya no son necesarios para la Universidad de las fuerzas Armadas	Solicitante/ Propietario	Matriz de inventario
2	Evaluación y clasificación de Activos	Se realizará una evaluación de los activos identificados para determinar su clasificación y la necesidad de implementar medidas especiales de eliminación, como la eliminación segura de datos en medios de almacenamiento.	Comité de cambios	Resultados de evaluación y clasificación
3	Eliminación	Pasos para la eliminación de activos Físicos y digitales de información: 1. Evaluación de la sensibilidad de la información. 2. Respaldo de la información. 3. Eliminación de datos: Para los activos electrónicos, realizar un borrado seguro de los datos almacenados en ellos. Utilizar herramientas y métodos de borrado que garanticen la eliminación completa y permanente de la información. 4. Destrucción física: Para los activos físicos, como discos duros, documentos impresos, etc., realizar una destrucción física segura. Esto puede implicar la trituración, desmagnetización o incineración de los activos para asegurar que la información no pueda ser recuperada.	Área de UTIC	Activos preparados para la eliminación

		5. Registro de eliminación: Mantener un registro detallado de los activos eliminados, incluyendo fechas y hora de eliminación. 6. Gestionar los residuos resultantes de la eliminación de manera ambientalmente responsable.		
N°.	**Actividad**	**Tarea /Descripción**	**Responsable**	**Información Documentada**
4	Implementación de la Eliminación	Se llevarán a cabo las acciones necesarias para eliminar físicamente los activos identificados, incluyendo el borrado seguro de datos en medios de almacenamiento y la disposición adecuada de los equipos y documentos impresos.	Área de UTIC	
5	Registro y Documentación	Se mantendrá un registro de todas las actividades de eliminación de activos, incluyendo la documentación de las acciones realizadas, los resultados obtenidos y cualquier problema o incidente relacionado.	Área de UTIC	Registro de actividades
6	Verificación y Validación	Se realizarán controles y revisiones periódicas para verificar la correcta implementación de los procesos de eliminación de activos y garantizar el cumplimiento de los requisitos de seguridad.	Área de UTIC	Documentos habilitantes

Nota. La tabla representa los procedimientos necesarios y el personal involucrado para la eliminación de activos en la Universidad de las Fuerzas Armadas.

Asegurar servicio de aplicaciones en redes públicas.

Tabla 12

Tabla de procedimientos de servicio de aplicaciones en redes públicas.

N°.	Actividad	Tarea /Descripción	Responsable	Información Documentada
1	**Identificación de Servicios Críticos**	1. Identificar y catalogar los servicios de aplicaciones que requieran acceso a redes públicas, incluyendo aquellos que contengan información crítica o sensible. 2. Priorizar los servicios según su importancia y la sensibilidad de la información que manejen.	Área de UTIC	Listado de servicios de aplicaciones críticos en redes públicas con su nivel de prioridad y la información que manejan.
2	**Evaluación de Riesgos**	1. Realizar evaluaciones periódicas de riesgos para los servicios de aplicaciones en redes públicas, identificando posibles vulnerabilidades y amenazas. 2. Analizar las posibles consecuencias y el impacto de las amenazas sobre la seguridad de la información en redes no confiables.	Área de UTIC	Informes de evaluación de riesgos
3	**Diseño e Implementación de Controles**	1. Diseñar e implementar controles de seguridad adecuados para mitigar los riesgos identificados durante la evaluación. 2. Establecer medidas de protección para garantizar la confidencialidad, integridad y disponibilidad de la información en redes públicas.	Área de UTIC	Plan de controles de seguridad
4	**Monitoreo Continuo**	1. Establecer un sistema de monitoreo continuo para supervisar el tráfico de red y detectar actividades fraudulentas o comportamientos anómalos. 2. Realizar análisis de registro y alertas para identificar posibles incidentes de seguridad en tiempo real.	Área de UTIC	Reportes de monitoreo y análisis de registros
N°.	**Actividad**	**Tarea /Descripción**	**Responsable**	**Información Documentada**

5	**Respuesta a Incidentes**	1. Definir un plan de respuesta a incidentes para actuar rápidamente ante cualquier actividad fraudulenta o ataque que comprometa la seguridad de los servicios de aplicaciones en redes públicas. 2. Establecer procedimientos para contener, mitigar y recuperarse de incidentes de seguridad en redes públicas.	Área de UTIC	Plan de respuesta a incidentes y registros de acciones
6	**Actualización y Mejora**	1. Revisar periódicamente los controles implementados y actualizarlos según sea necesario para adaptarse a nuevas amenazas o cambios en la infraestructura de red. 2. Identificar oportunidades de mejora en el proceso de seguridad y aplicar acciones correctivas y preventivas.	Área de UTIC	Registro de revisiones y mejoras implementadas.
7	**Concienciación y Capacitación**	1. Brindar capacitación regular al personal en prácticas de seguridad para el uso de servicios de aplicaciones en redes públicas. 2. Concientizar a los usuarios sobre la importancia de proteger la información y aplicar las políticas de seguridad.	Área de UTIC	Registros de capacitaciones y material de concienciación.
8	**Auditoría y Certificación**	1. Realizar auditorías internas para verificar el cumplimiento del procedimiento y la eficacia de los controles implementados. 2. Obtener certificaciones de cumplimiento en seguridad para validar el cumplimiento de estándares reconocidos.	Área de UTIC	Informes de auditorías internas y certificaciones de cumplimiento.

Nota. Esta tabla define los procesos a seguir asegurar servicio de aplicaciones en redes públicas.

Reporte de puntos débiles.

Tabla 13

Tabla de procesos de reporte de puntos débiles.

N	Actividad	Tarea /Descripción	Responsable	Información Documentada
1	**Notificación del Punto Débil**	Los usuarios de los sistemas y activos de información deben comunicar de inmediato cualquier punto débil o vulnerabilidad que identifiquen en la seguridad de la información.	Empleado/ Contratista/ Tercero	Descripción detallada del punto débil identificado.
2	**Evaluación y Registro del Punto Débil**	El área de UTIC evalúa el punto débil de seguridad y lo registra en un sistema de seguimiento de eventos y vulnerabilidades.	Área de UTIC	Registro detallado de los puntos débiles identificados
3	**Clasificación y Priorización**	El equipo de seguridad de la información clasifica el punto débil según su gravedad para priorizar la respuesta y asignar los recursos adecuados.	Área de UTIC	Documento de categorización de los puntos débiles según su severidad
4	**Comunicación y Acciones correctivas**	1. El área de UTIC comunica el punto débil a las partes interesadas relevantes, incluyendo a la alta dirección y las áreas afectadas. 2. Se implementan acciones correctivas para abordar y resolver el punto débil identificado.	Área de UTIC	Notificación a partes interesadas y registro de acciones correctivas
5	**Seguimiento y Reporte**	1. Se realiza un seguimiento continuo del punto débil hasta su resolución completa. 2. Se genera un informe sobre el punto débil de seguridad identificado y acciones tomadas, y se presenta a la alta dirección y el equipo de seguridad de la información.	Área de UTIC	Documentos habilitantes/ Registro de seguimiento

Nota. Procesos de reporte de puntos débiles dentro de Universidad de las fuerzas armadas.

Reporte de puntos débiles.

Evaluación y decisión sobre eventos de seguridad.

Tabla 14

Tabla de procesos de evaluación y decisión sobre eventos de seguridad.

N°.	Actividad	Tarea /Descripción	Responsable	Información Documentada
1	**Registro de Eventos**	Recopilar información sobre eventos de seguridad detectados o reportados, registrarlos en el sistema de incidentes designado.	Área de UTIC	Formularios de registro de eventos.
2	**Evaluación Inmediata**	El área de UTIC evaluará los eventos registrados para determinar la gravedad y el posible impacto en la seguridad de la información y los activos aplicando criterios de clasificación establecidos previamente.	Área de UTIC	Criterios de clasificación de eventos
3	**Comunicación de incidentes**	1. Si un evento es clasificado como incidente de seguridad significativo, notificar de inmediato a las partes involucradas. 2. Incluir detalles sobre el incidente, sus posibles consecuencias y los responsables de la gestión de incidentes.	Área de UTIC	Plantilla de notificación de incidentes
4	**Investigación Detallada**	1. Llevar a cabo una investigación exhaustiva del incidente. 2. Determinar el origen, causas y alcance del incidente. 3. Analizar los sistemas y datos afectados. 4. Identificar posibles vulnerabilidades que haya permitido el incidente.	Área de UTIC	Informe de investigación de incidentes
5	**Respuesta y Mitigación**	1. Implementar una respuesta adecuada al incidente. 2. Tomar medidas de mitigación para reducir el impacto y evitar la propagación o recurrencia.	Área de UTIC	Plan de respuesta a incidentes, acciones tomadas y su resultado

		3. Coordinar con los equipos relevantes para corregir las vulnerabilidades identificadas.		
N°.	**Actividad**	**Tarea /Descripción**	**Responsable**	**Información Documentada**
6	**Análisis de lecciones aprendidas**	1. Realizar un análisis de lecciones aprendidas sobre el incidente. 2. Identificar áreas de mejora en el proceso de evaluación y decisión de eventos de seguridad. 3. Proponer acciones correctivas y preventivas para futuros incidentes.	Área de UTIC	Informe de lecciones aprendidas

Nota. Tabla de procesos de evaluación y decisión sobre eventos de seguridad.

Recolección de evidencias.

Tabla 15

Tabla de recolección de evidencias.

N°.	Actividad	Tarea /Descripción	Responsable	Información Documentada
1	Identificación de los requisitos de evidencia	Identificar los requisitos de evidencia establecidos por la norma ISO 27002 y otros estándares o regulaciones aplicables. Definir los tipos de evidencia requeridos para respaldar los controles de seguridad de la información.	Solicitante/ Propietario	Registro de evento
2	Definición de procedimientos de recopilación de evidencias	Establecer procedimientos claros y detallados para recopilar la evidencia requerida. Especificar los métodos y técnicas de recopilación de evidencias a utilizar. Definir los roles y responsabilidades de las personas involucradas en el proceso de recopilación de evidencias.	Área de UTIC	Manual de procedimientos

3	Identificación y selección de fuentes de evidencia	Identificar las fuentes de evidencia disponibles, como registros, informes, documentos, registros de auditoría, entre otros. Determinar qué fuentes de evidencia son relevantes y apropiadas para respaldar los controles de seguridad de la información.	Área de UTIC	Matriz de selección

N°.	**Actividad**	**Tarea /Descripción**	**Responsable**	**Información Documentada**
4	Recopilación de evidencias	Para la recopilación de evidencias se deben seguir los siguientes pasos: 1. Realizar la recopilación de las evidencias de acuerdo con los procedimientos establecidos. 2.Aplicar los métodos y técnicas definidos para asegurar la integridad y autenticidad de las evidencias recopiladas. 3.Registrar y documentar adecuadamente el proceso de recopilación de evidencias	Área de UTIC	Informe de recopilación
5	Almacenamiento y conservación de evidencias	1.Establecer un sistema adecuado de almacenamiento y conservación de las evidencias recopiladas. 2. Definir medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de las evidencias almacenadas. 3.Establecer un periodo de retención adecuado para las evidencias, de acuerdo con los requisitos legales y regulatorios.	Área de UTIC	Registro de actividades

6	Gestión de la evidencia	Implementar un sistema de gestión de evidencias que permita organizar, indexar y acceder de manera eficiente a las evidencias recopiladas. Establecer procedimientos para el seguimiento, análisis y uso de las evidencias en el contexto de la seguridad de la información	Área de UTIC	Documentos habilitantes

Nota. La tabla describe los procedimientos a seguir para la recolección de evidencias en la Universidad de las fuerzas armadas.

Reporte de eventos.

Tabla 16

Tabla de procedimiento de Reporte de eventos

N°.	Actividad	Tarea /Descripción	Responsable	Información Documentada
1	**Notificación del Evento**	Cualquier empleado, contratista o tercero que identifique o sospeche de un evento de seguridad de la información debe notificarlo de inmediato al equipo de seguridad de la información.	Empleado/ Contratista/ Tercero	Descripción detallada del evento.
2	**Registro del Evento**	El área de UTIC registra el evento en la bitácora centralizada de eventos, incluyendo la descripción del evento, la fecha y hora, la fuente y las acciones inmediatas tomadas.	Área de UTIC	Registro de evento
3	Evaluación del evento	El equipo de seguridad de la información evalúa el evento para determinar si se trata de un incidente real o una alerta falsa.	Área de UTIC	Documento de evaluación
4	Clasificación y gestión del evento	Para la clasificación y gestión del evento se deben seguir los siguientes pasos: 1. Se asigna una categoría de severidad al evento	Área de UTIC	Documento de categorización del evento según su severidad

		para priorizar la respuesta. 2. Si se confirma que es un incidente de seguridad de la información, se inicia la gestión del incidente según los procedimientos establecidos.		
N°.	**Actividad**	**Tarea /Descripción**	**Responsable**	**Información Documentada**
5	Comunicación y notificación	1. Se notifica a las partes interesadas relevantes sobre el evento, incluyendo la alta dirección y las áreas afectadas. 2. La notificación incluye la descripción del evento, las acciones tomadas y las medidas adicionales que se tomarán.	Área de UTIC	Notificación a partes interesadas
6	**Seguimiento y Reporte**	1. Se realiza un seguimiento continuo del evento hasta su resolución completa. 2.Se genera un informe periódico sobre los eventos y los incidentes ocurridos, sus causas y acciones tomadas, y se presenta a la alta dirección y el equipo de seguridad de la información.	Área de UTIC	Documentos habilitantes

Nota. La tabla describe los procedimientos a seguir para el reporte de eventos en la Universidad de las fuerzas armadas.

Capitulo IV.

Evaluación e informe de implantación de controles

Introducción

El presente capitulo está destinado a mostrar los resultados de la implantación de nuevos controles y la corrección de controles. Para esto se definió métricas y un plan de evaluación para dar a conocer si los controles implantados cubren con los requerimientos básicos y necesarios para tomarlos en cuenta.

Los controles implantados cuentan con una medida porcentual el cual dictamina las tareas que sea han realizado para su implantación y las tareas que quedan pendientes para una completa implantación.

Definición de controles y métricas de evaluación.

En el marco del desarrollo de la versión 2 del Entorno de Gestión de Seguridad de la Información (EGSI) de la Universidad de las Fuerzas Armadas ESPE, se han implementado diversos controles de seguridad para abordar las áreas críticas de riesgo y garantizar la protección de la información y la integridad del sistema. A continuación, en la **Tabla 11** se detallan los controles seleccionados y las preguntas de evaluación asociadas, así como las métricas utilizadas para medir su efectividad:

Tabla 11

Tabla de evaluación de controles

Control	Preguntas de Evaluación	Métricas de evaluación
11.2.5 Eliminación de activos	• ¿Existe un procedimiento documentado para la eliminación de activos que incluya la autorización por parte de los directivos? • ¿Se ha designado a un responsable o comité para aprobar y supervisar la eliminación de activos?	• Porcentaje de eliminaciones de activos con autorización documentada. • Tiempo promedio desde la solicitud de eliminación hasta la autorización por parte de los directivos.

	• ¿Se mantiene un registro de las autorizaciones para la eliminación o recogida de equipos, información o software? • ¿Se verifica que el personal encargado de la eliminación o recogida de activos tenga la debida autorización antes de realizar la acción?	• Número de incidentes relacionados con eliminaciones no autorizadas.
16.1.7 Recopilación de evidencias	• ¿Existe una política o procedimiento documentado que describa los procesos para la recopilación de evidencias? • ¿Se ha designado a un responsable o equipo encargado de llevar a cabo la recopilación de evidencias? • ¿Los procesos identificados abarcan todas las áreas relevantes de la organización que puedan requerir recopilación de evidencias? • ¿Los procesos identificados aseguran la integridad y autenticidad de la evidencia recopilada? • ¿Los procesos definen claramente qué tipo de información se debe recopilar como evidencia en diferentes situaciones (por ejemplo, incidentes de seguridad, auditorías, reclamaciones legales)?	• Porcentaje de cumplimiento en la aplicación de los procesos de recopilación de evidencias. • Tiempo promedio para completar la recopilación de evidencias en casos de incidentes de seguridad. • Número de casos en los que se detectó falta de integridad o autenticidad de la evidencia recopilada.

Control	Preguntas de Evaluación	Métricas de evaluación
16.1.2 Notificación de los eventos de seguridad de la información	• ¿Existe un procedimiento documentado que establezca cómo se deben notificar los eventos de seguridad de la información? • ¿El procedimiento define claramente qué tipos de eventos deben ser notificados? (por ejemplo, intrusiones, intentos de acceso no autorizado, malware, pérdida de datos) • ¿Se han designado responsables o un equipo encargado de recibir	• Porcentaje de eventos de seguridad notificados de acuerdo con el procedimiento establecido. • Tiempo promedio entre la detección de un evento y su notificación formal. • Número de incidentes en los que hubo demoras significativas en la notificación.

	y gestionar las notificaciones de eventos de seguridad? • ¿Los canales de notificación están claramente definidos y son conocidos por todos los empleados y personal relevante? • ¿El procedimiento especifica los plazos para la notificación de eventos, asegurando que se realice de manera oportuna? • ¿Se verifica regularmente que los canales de notificación estén funcionando correctamente y sean accesibles?	
Control	**Preguntas de Evaluación**	**Métricas de evaluación**
16.1.3 Notificación de los puntos débiles de la seguridad de la información	• ¿Existe una política o normativa documentada que establezca la obligación de los usuarios de reportar puntos débiles de seguridad de la información? • ¿La política define claramente qué se considera un "punto débil" en el contexto de la seguridad de la información? • ¿Se ha establecido un proceso claro y accesible para que los usuarios puedan realizar notificaciones de manera efectiva? • ¿Los usuarios son informados sobre los canales a través de los cuales pueden reportar puntos débiles de seguridad? (por ejemplo, un equipo de respuesta a incidentes, un departamento de TI, un buzón de sugerencias) • ¿Se garantiza la confidencialidad y anonimato de los usuarios que realizan notificaciones, si así lo desean? • ¿Los reportes de puntos débiles recibidos se registran adecuadamente para su seguimiento y resolución?	• Porcentaje de cumplimiento en la notificación de puntos débiles de seguridad. • Número de puntos débiles reportados y resueltos en un período determinado. • Nivel de satisfacción de los usuarios con el proceso de notificación de puntos débiles.
16.1.4 Evaluación y decisión sobre	• ¿Existe un procedimiento documentado para evaluar los	• Tiempo promedio para la evaluación de

los eventos de seguridad de la información	eventos de seguridad de la información? • ¿El procedimiento define claramente los criterios que se utilizan para determinar si un evento debe ser considerado como un incidente de seguridad? • ¿Se ha designado a un equipo o a personal responsable de realizar la evaluación de los eventos de seguridad? • ¿El proceso de evaluación se inicia de manera oportuna una vez que se ha detectado un evento de seguridad? • ¿Se notifica adecuadamente a las partes interesadas, incluyendo a la alta dirección, sobre los eventos que están siendo evaluados como posibles incidentes de seguridad? • ¿Se realiza un seguimiento y documentación adecuados de la evaluación de los eventos, incluyendo los resultados y las acciones tomadas? • ¿Se mantiene un registro de los eventos que han sido considerados como incidentes de seguridad, junto con las medidas correctivas aplicadas?	eventos de seguridad desde su detección. • Porcentaje de eventos considerados como incidentes de seguridad después de la evaluación. • Número de incidentes resueltos con éxito y su tiempo promedio de resolución.

Control	Preguntas de Evaluación	Métricas de evaluación
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	• ¿Existe un procedimiento documentado para garantizar la seguridad de los servicios de aplicaciones en redes públicas? • ¿Se han identificado y evaluado los riesgos asociados con el uso de servicios de aplicaciones en redes públicas? • ¿Se implementan medidas de seguridad adecuadas, como firewalls, cifrado y autenticación, para proteger la información que pasa por redes públicas? • ¿Los servicios de aplicaciones en redes públicas son monitoreados de manera regular para detectar	• Nivel de cumplimiento en la implementación de las medidas de seguridad en servicios de aplicaciones en redes públicas. • Número de incidentes de seguridad relacionados con redes públicas detectados y resueltos.

	actividades fraudulentas o inusuales?	
12.6.1 Desarrollo externalizado	• ¿Existe un registro documentado que recoja las actividades realizadas por los usuarios en el contexto del desarrollo externalizado? • ¿Se registran de manera constante las acciones realizadas por los usuarios, incluyendo las fechas y horas de inicio y finalización de sus actividades? • ¿El registro incluye información detallada sobre las acciones específicas que los usuarios realizaron durante el desarrollo externalizado? Por ejemplo, cambios en el código fuente, configuraciones, pruebas, entre otros. • ¿Se registran y documentan los fallos y errores que ocurrieron durante el desarrollo externalizado, así como las medidas tomadas para abordarlos?	• Nivel de cumplimiento en el registro y documentación de actividades de desarrollo externalizado. • Tiempo promedio para la resolución de fallos y errores identificados en el desarrollo externalizado.

Control	Preguntas de Evaluación	Métricas de evaluación
8.3.3 Transferencia de Medios Físicos	• ¿Existe un proceso establecido para autorizar y rastrear la transferencia de medios físicos fuera de la universidad? • ¿Se asigna la responsabilidad a personal designado para autorizar la transferencia de medios físicos y asegurar que se cumplan los controles establecidos? • ¿Se mantiene un registro actualizado de los medios físicos que salen de la universidad, incluyendo detalles como el tipo de medio, su contenido y la persona responsable de su custodia?	• Porcentaje de transferencias de medios físicos con autorización documentada. • Tiempo promedio para registrar las transferencias de medios físicos fuera de la universidad. • Número de incidentes relacionados con accesos no autorizados a medios físicos.
12.6.2 Restricciones en la	• ¿Existe una política o procedimiento que regule la instalación de software para los usuarios?	• Porcentaje de cumplimiento en la solicitud y aprobación

instalación del software	• ¿Se requiere autorización o aprobación previa para instalar software en los sistemas? • ¿Se han designado responsables o un equipo encargado de supervisar y autorizar la instalación de software? • ¿Se mantiene un registro de las solicitudes y autorizaciones de instalación de software realizadas por los usuarios? • ¿El personal encargado de la autorización de instalación de software verifica la legitimidad y seguridad de las aplicaciones antes de aprobar su instalación?	de instalación de software. • Número de incidentes relacionados con la instalación de software no autorizado o malicioso.

Nota. Esta tabla nos indica las preguntas y las métricas de evaluación de los controles que han sido implementados.

Plan de evaluación

El plan de implantación del proyecto cuenta con una revisión técnica donde se recaban todos los controles seleccionado anteriormente con los cuales se midió en base a métricas que dictaminen en qué nivel se encuentran implantados y que mejoras se deben realizar en futuros trabajos, todo la información referente a esto se encuentra descrita en el informe final de revisión técnica el cual muestra observaciones, recomendaciones y la condición en la que se encuentran actualmente los procesos y controles creados.

Instrumentos de evaluación

Para realizar la evaluación de los controles del Esquema Gubernamental de Seguridad de la Información (EGSI), se desarrolló como principal instrumento la “Revisión Documental”. Esta metodología fue seleccionada debido a la disponibilidad de una amplia documentación que se relaciona con la seguridad de la información del EGSI.

La revisión documental consistió en una lectura y análisis de las políticas, normativas,

manual de procedimientos, guía, contratos y formatos de registros pertenecientes a los controles del EGSI. Se evaluó la existencia e implementación de los controles de seguridad, su adecuada descripción, responsabilidades asignadas y los registros de cumplimiento.

Es importante mencionar que, aunque la revisión documental fue el principal instrumento utilizado en esta evaluación, se reconoce que otros métodos de evaluación, como pruebas técnicas, auditorías, simulaciones de incidentes o encuestas de satisfacción, podrían proporcionar perspectivas adicionales y complementarias. Sin embargo, debido a limitaciones de tiempo y recursos, la revisión documental fue considerada como una metodología sólida y confiable para obtener una evaluación inicial del esquema.

Informe Final de revisión

El presente informe de evaluación que se encuentra en el **anexo AI-IN07** aborda el sistema de información del Esquema Gubernamental de Seguridad de la Información (EGSI) de la Universidad de las Fuerzas Armadas ESPE. Esta institución es una universidad pública que ofrece servicios de educación superior en varias provincias y cuenta con una Unidad de Seguridad Integrada (USIN), encargada de gestionar la seguridad en diferentes ámbitos.

El objetivo del proyecto es evaluar el sistema de gestión de seguridad de la información implementado, utilizando como referencia la Norma NTE INEN-ISO/IEC 27001, la cual proporciona un marco de referencia para establecer, implementar, mantener y mejorar un SGSI.

Las áreas auditadas en la evaluación incluyen la Unidad de Seguridad Integrada, la Unidad de Tecnologías de la Información y la Unidad de Planificación y Desarrollo de la universidad. El informe se enfoca en la revisión documental como principal instrumento de evaluación para verificar el cumplimiento de los controles implementados en el EGSI.

Con esta evaluación, se busca identificar fortalezas y áreas de mejora en la seguridad de la información de la institución, con el propósito de contribuir a la protección de la integridad de la comunidad universitaria, los bienes e infraestructura de la universidad, y asegurar el cumplimiento de las normativas vigentes.

Resumen ejecutivo del informe de evaluación técnica

El informe presenta los resultados de la Evaluación Técnica Informática del Esquema Gubernamental de Seguridad de la Información (EGSI) en su Fase 2. Se utiliza como referencia las normas ISO 27001, 27003 y 27002 para evaluar la implementación del Sistema de Gestión de Seguridad de la Información. El análisis identificó observaciones relevantes relacionadas con no conformidades, criterios normativos, causas y efectos en el ámbito de seguridad de la información de la institución. Se presentan recomendaciones para corregir y mejorar los aspectos identificados en el EGSI versión 2.

La evaluación permitió contextualizar el estado actual del EGSI en proceso de implementación, evidenciando la falta de algunos documentos en cada una de las fases del esquema. El informe tiene como objetivo contribuir a la eficacia del sistema de gestión de seguridad de la información y al cumplimiento de los requisitos de la Norma ISO 27001 en el EGSI versión 3.

Alcance del informe de evaluación técnica.

El informe describe la evaluación realizada en la Fase 2 del Esquema Gubernamental de Seguridad de la Información (EGSI) de la institución. Se analizó la implementación del Sistema

de Gestión de Seguridad de la Información con base en las normas ISO 27001, 27003 y 27002. Se identificaron observaciones relevantes relacionadas con no conformidades, criterios normativos, causas y efectos en el ámbito de seguridad de la información. Se presentan recomendaciones para corregir y mejorar los aspectos evaluados en el EGSI versión 2. El informe tiene como objetivo mejorar la eficacia del sistema de seguridad de la información y contribuir al cumplimiento de los requisitos de la Norma ISO 27001 en la siguiente versión del EGSI.

Objetivos del informe de la evaluación técnica informática

Los objetivos de la presente Evaluación Técnica Informática son: determinar el estado de la implementación del Esquema Gubernamental de Seguridad de la Información EGSI de la Universidad de las Fuerzas Armadas “ESPE” fase 2, utilizando como criterios de referencia las normas internacionales NTE ISO/IEC 27001, NTE ISO/IEC 27002 y NTE ISO/IEC 27003; detectar las no conformidades y oportunidades de mejora asociadas al EGSI con respecto a las Normas antes mencionadas y finalmente, desarrollar un informe de hallazgos de la Evaluación Técnica donde se presente un conjunto de recomendaciones enfocadas en la facilitación de toma de decisiones gerenciales dentro de la institución.

Metodología del informe de la evaluación técnica informática

Planificación de la Evaluación Técnica Informática.

La planificación del informe de evaluación técnica del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Universidad de las Fuerzas Armadas "ESPE" se llevó a cabo de manera estructurada y meticulosa. En esta fase, se realizaron una serie de pasos clave para determinar el alcance y los objetivos de la evaluación.

Inicialmente, se definieron los objetivos específicos de la evaluación, los cuales estaban

alineados con los propósitos del EGSI y las necesidades institucionales. Luego, se delimitó el alcance de la evaluación, identificando claramente las áreas o unidades de la institución que serían objeto de revisión para asegurar una cobertura integral.

La planificación también involucró la asignación de recursos, como tiempo y personal, y se estableció un cronograma detallado para la evaluación. Se evaluaron los costos asociados con la realización del informe y se identificaron posibles riesgos, desarrollando planes de contingencia para abordarlos.

La rigurosa planificación realizada aseguró que la evaluación técnica del EGSI fuera exhaustiva y cubriera todos los aspectos relevantes del sistema de gestión de seguridad de la información en la universidad. Los resultados obtenidos a través de esta planificación permitieron llevar a cabo una evaluación precisa y completa, contribuyendo así a la mejora y protección del EGSI de la Universidad de las Fuerzas Armadas "ESPE".

Ejecución de la Evaluación

La evaluación se realizó en base a las normas internacionales NTE ISO/IEC 27001, NTE ISO/IEC 27003 y el Método de Auditoría Informática para Instituciones de Educación Superior SIIES.

Resultados del informe de la evaluación

En la siguiente sección se expone de manera detallada los resultados obtenidos de la presente evaluación con sus respectivas recomendaciones y respuestas de la gerencia, mismas que se encuentran agrupadas en base a las cinco fases del proceso de planificación e implementación del EGSI, de acuerdo con las normas NTE ISO/IEC 27001 y NTE ISO/IEC 27003.

(11.2.5) – Eliminación de activos

Observación:

Es importante definir cómo verificar si el encargado de la eliminación tenga la debida atorización antes de que realice la acción. Además, el proceso se encuentra en revisión para

aprobación.

Criterio:

NTE ISO/IEC 27002 Control 11.2.5 Debe existir una autorización por parte de los directivos para eliminar o recoger equipos, información o el software de las instalaciones.

Condición:

El procedimiento debe definir claramente que el encargado de la eliminación debe contar con la debida autorización por parte de los directivos antes de llevar a cabo la acción.

Efecto:

La falta de autorización apropiada también puede dar lugar a una toma de decisiones inadecuada o descontrolada sobre qué activos se eliminan, lo que podría impactar negativamente en la eficiencia y funcionamiento de la organización.

Recomendación:

Definir y documentar claramente el procedimiento de eliminación de activos que incluya el proceso de obtención de autorización por parte de los directivos antes de llevar a cabo la eliminación.

Capacitar al personal encargado de la eliminación de activos sobre la importancia de obtener la autorización adecuada y los riesgos asociados con la eliminación de activos sin la debida aprobación.

Implementar un mecanismo de seguimiento y control para verificar que la autorización se obtenga antes de realizar cualquier acción de eliminación de activos.

(16.1.7) – Recopilación de evidencias

Observación:

Es importante indicar el manual de procedimientos, como también cuales son estos con su funcionalidad. Además, hay que indicar que tipos de información se debe recopilar en distintas situaciones, describirlas. No obstante, el proceso se encuentra en revisión para su aprobación.

Criterio:

NTE ISO/IEC 27002 Control 16.1.7 Se debe identificar los procesos adecuados para establecer, reunir y conservar la información como parte de la evidencia.

Condición:

El manual de procedimientos debe detallar la funcionalidad de cada proceso, es decir, cómo se lleva a cabo cada actividad de recopilación de evidencias.

Efecto:

La falta de un manual de procedimientos detallado puede llevar a inconsistencias en los procesos de recopilación de evidencias, lo que podría afectar la calidad y confiabilidad de la información recopilada.

Recomendación:

Elaborar y documentar un manual de procedimientos que describa en detalle los procesos de recopilación de evidencias, incluyendo la funcionalidad de cada actividad y los responsables de llevarlas a cabo.

Especificar claramente los tipos de información que deben recopilarse en diferentes situaciones, como incidentes de seguridad, auditorías internas o investigaciones, asegurándose de que se capturen datos relevantes para cada caso.

(16.1.2) – Notificación de los eventos de seguridad de la información

Observación:

Es importante identificar los tipos de eventos que pueden ser notificados, aclarar los canales de comunicación que existen, el proceso se encuentra en revisión para aprobación.

Criterio:

NTE ISO/IEC 27002 Control 16.1.2 Los eventos deben ser comunicados por los canales establecidos y de manera oportuna.

Condición:

El procedimiento debe establecer claramente los canales de comunicación que existen para la notificación de eventos de seguridad, indicando quiénes son los responsables de realizar la notificación.

Efecto:

La falta de claridad en los tipos de eventos que deben ser notificados puede llevar a una comunicación inadecuada o incompleta, lo que podría resultar en la omisión de eventos importantes y afectar la respuesta a incidentes de seguridad.

Recomendación:

Especificar los canales de comunicación que se deben utilizar para la notificación de eventos, como correos electrónicos, sistemas de tickets, reuniones de equipo, o cualquier otro medio apropiado.

Elaborar y documentar un procedimiento que defina claramente los tipos de eventos de seguridad de la información que deben ser notificados, como intrusiones, malware, intentos de acceso no autorizado, pérdida de datos, entre otros.

Designar y capacitar al personal responsable de llevar a cabo la notificación de eventos, asegurándose de que comprendan los procedimientos y plazos para la comunicación oportuna.

(16.1.3) – Notificación de los puntos débiles de la seguridad de la información

Observación:

No se detalla los canales de notificación para los usuarios, además hace falta las políticas que obliguen a notificar un punto débil de seguridad y qué se puede clasificar como este. El proceso se encuentra en revisión.

Criterio:

NTE ISO/IEC 27002 Control 16.1.3 Los usuarios de los sistemas y los activos de información tienen la obligación de comunicar cualquier punto débil que identifiquen.

Condición:

Se debe contar con políticas y procedimientos documentados que establezcan la obligación de los usuarios de notificar cualquier punto débil de seguridad de la información que identifiquen.

Efecto:

La falta de canales de notificación específicos puede llevar a que los usuarios no sepan cómo reportar los puntos débiles de seguridad que encuentren, lo que podría resultar en la no detección oportuna de problemas de seguridad.

La ausencia de políticas claras y obligatorias puede generar una falta de conciencia sobre la importancia de reportar los puntos débiles, lo que podría llevar a que los usuarios no tomen en serio la responsabilidad de notificarlos.

Recomendación:

Definir claramente qué se considera como un punto débil de seguridad y proporcionar ejemplos concretos para ayudar a los usuarios a identificar y comprender qué situaciones deben notificar.

Establecer canales de notificación claros y accesibles para que los usuarios puedan reportar los puntos débiles de seguridad de manera fácil y segura.

Capacitar al personal sobre la importancia de notificar los puntos débiles de seguridad y cómo utilizar los canales de notificación establecidos.

(16.1.4) – Evaluación y decisión sobre los eventos de seguridad de la información

Observación:

El procedimiento no define claramente qué criterios se utilizan para determinar si un evento es incidente de seguridad. Además, el proceso se encuentra en revisión.

Criterio:

NTE ISO/IEC 27002 Control 16.1.4 Se debe evaluar los eventos de seguridad con el fin

de determinar si son considerados incidentes.

Condición:

El procedimiento debe definir claramente los criterios que se utilizarán para determinar si un evento se considera un incidente de seguridad.

Efecto:

La falta de criterios claros para evaluar los eventos de seguridad puede llevar a una toma de decisiones inconsistente o subjetiva, lo que podría afectar la identificación oportuna de incidentes de seguridad graves.

Recomendación:

Definir criterios objetivos y medibles para determinar si un evento debe ser considerado como un incidente de seguridad, como el impacto en la confidencialidad, integridad o disponibilidad de la información.

Capacitar al personal involucrado en la evaluación de eventos sobre los criterios y procedimientos establecidos, asegurándose de que comprendan cómo identificar y clasificar adecuadamente los incidentes de seguridad.

(14.1.2) – Asegurar los servicios de aplicaciones en redes públicas

Observación

identificar los riesgos asociados con el uso de servicios de aplicaciones en redes públicas, además de conocer que medidas de seguridad tienen implementados, para poder evidenciar la seguridad en este control.

Criterio:

NTE ISO/IEC 27002 Control 14.1.2 La información que pasan por redes públicas deben estar protegidas de cualquier actividad fraudulenta.

Condición:

Se debe llevar a cabo una evaluación detallada de los riesgos asociados con el uso de

servicios de aplicaciones en redes públicas.

Es necesario identificar las medidas de seguridad implementadas para proteger la información que pasa por redes públicas.

Efecto:

La falta de una evaluación de riesgos podría dejar a la universidad vulnerable a actividades fraudulentas y otras amenazas que afecten la confidencialidad, integridad y disponibilidad de la información transmitida a través de redes públicas.

Sin conocer las medidas de seguridad implementadas, es difícil garantizar la protección adecuada de la información y demostrar la seguridad en este control.

Recomendación:

Realizar una evaluación exhaustiva de los riesgos asociados con el uso de servicios de aplicaciones en redes públicas, considerando posibles amenazas y vulnerabilidades que puedan afectar la seguridad de la información.

Implementar medidas de seguridad apropiadas para proteger la información que pasa por redes públicas, como el uso de VPN (Redes Privadas Virtuales) para cifrar la comunicación y asegurar la autenticación de los usuarios.

(12.6.1) – Desarrollo externalizado

Observación:

Cabe destacar que el formato de registro falta validar para su uso, este contiene lo más importante que se debe guardar.

Criterio:

NTE ISO/IEC 27002 Control 12.6.1 Es necesario un registro sobre las actividades de los usuarios constante, fallos y eventos que afecten la seguridad de la información.

Condición:

Es necesario validar y asegurarse de que el formato de registro sea adecuado para

capturar la información más importante que se debe guardar, como detalles sobre actividades, incidentes y cambios realizados por los usuarios externos.

Efecto:

La falta de un formato de registro validado podría llevar a la omisión de información relevante o a la captura incorrecta de datos, lo que afectaría la integridad y utilidad del registro para identificar riesgos y analizar eventos de seguridad.

Recomendación:

Validar y revisar el formato de registro para asegurarse de que capture de manera adecuada y completa la información relevante para el control 12.6.1 y la seguridad de la información en general.

Capacitar al personal involucrado en el desarrollo externalizado sobre cómo utilizar y completar correctamente el formato de registro.

(8.3.3) – Transferencia de Medios Físicos

Observación:

El formato de registro se encuentra a espera de confirmación para su uso con el personal correspondiente para guardar la información necesaria.

Criterio:

NTE ISO/IEC 27002 Control 8.3.3 Los medios físicos que salgan de límite de la universidad deben tener el respectivo control ante accesos no autorizados a la información que estos contienen.

Condición:

Es necesario contar con un formato de registro documentado que permita tener el respectivo control de los medios físicos que salen de los límites de la universidad.

Efecto:

La falta de un formato de registro confirmado podría llevar a la omisión de información

crítica sobre la transferencia de medios físicos, lo que podría generar dificultades para rastrear y recuperar dichos medios en caso de pérdida o acceso no autorizado.

Recomendación:

Confirmar y validar el formato de registro para asegurarse de que esté completo y capture la información esencial para el control 8.3.3 y la seguridad de la información.

(12.6.2) – Restricciones en la instalación del software

Observación:

Hay que destacar que se ha creado un formato de bitácora para registrar las solicitudes y autorizaciones de instalación de software, pero falta la validación y aprobación para el uso.

Criterio:

NTE ISO/IEC 27002 Control 12.6.2 Se debe normar y regular la instalación de software para los usuarios.

Condición:

El formato de bitácora debe ser validado y aprobado para su uso por parte de las autoridades competentes.

Efecto:

La falta de validación y aprobación del formato de bitácora podría llevar a la no utilización o a la utilización incorrecta del mismo, lo que afectaría la capacidad de normar y regular la instalación de software para los usuarios.

Recomendación:

Validar y aprobar el formato de bitácora de registro de solicitudes y autorizaciones de instalación de software por parte de las autoridades responsables de la seguridad de la información.

Conclusión del informe de evaluación técnica

La auditoría incluyó una evaluación documental. A lo largo de la aplicación de esta se tomó como criterios referenciales, las diferentes clausulas contenidas en las normas internacionales NTE ISO/IEC 27001, NTE ISO/IEC 27002 y NTE ISO/IEC 27003.

Al evaluar los controles del EGSI versión 2 que se implementaron se concluyó que se encuentran controles con falta de aprobación para su implantación.

Al evaluar el total de controles en proceso de implantación se pudo constatar que existe un número limitado de controles que no constan con la aprobación correspondiente o no se tomaron en cuenta dentro de la USIN lo cual genera un conflicto de inconsistencia en la documentación y procedimientos dejando vulnerable a la institución.

Al realizar todo el análisis técnico a los controles en proceso de implantación del EGSI versión 2 se determinó como conclusión que se debe dar una revisión a los controles para dar un ciclo de mejora a estos y mejorando los controles restantes que se encuentran con dudas justificadas sobre su implantación para dar una mejora sustancial al sistema actual y estar preparados para una auditoría externa.

Comparativa de la evaluación inicial y la evaluación final

A continuación, se presenta una la tabla que resalta las diferencias entre la evaluación inicial y la evaluación final después de la implantación de los controles. Esta comparación abarca aspectos clave en la evolución del proceso, enfocado en la mejora de la seguridad y preparación para auditorías externas, de acuerdo con los estándares internacionales NTE ISO/IEC 27001, NTE ISO/IEC 27002 y NTE ISO/IEC 27003.

Tabla 17

Tabla comparativa de evaluación

Aspecto	Evaluación Inicial	Evaluación Final

Controles Evaluados	Controles del EGSI con falta de documentación que sustenten su implantación.	Controles del EGSI versión 2 con falta de aprobación para su implantación.
Manuales de Controles	Ciertos controles cuentan con un número limitado de firmas para su legalización.	Los controles se encuentran en el proceso de legalización con la unidad de seguridad.
Total, de Controles Implantados	Existe un número limitado de controles que no constan con documentación o no se tomaron en cuenta dentro de la USIN, generando conflicto de inconsistencia en la documentación y procedimientos.	Existe un número limitado de controles en proceso de implantación que no cuentan con la aprobación correspondiente o no se tomaron en cuenta dentro de la USIN, generando conflicto de inconsistencia en la documentación y procedimientos.
Conclusión sobre Controles	Se debe revisar los controles actuales, completar los que no están implantados y mejorar los que tienen dudas justificadas sobre su implantación para prepararse para una auditoría externa.	Se debe revisar los controles en proceso de implantación, mejorar los controles restantes con dudas justificadas sobre su implantación para prepararse para una auditoría externa.
Enfoque de Evaluación	Se consideró el análisis técnico de los controles existentes.	Se consideró el análisis técnico de los controles en proceso de implantación del EGSI versión 2.

Nota. Esta tabla comparativa nos indica las diferencias entre la evaluación inicial de los controles y la evaluación final de los controles implantados en el EGSI versión 2.

Análisis de impacto de la implementación de Controles de Seguridad.

La implantación de los controles de seguridad como parte del Sistema de Gestión de Seguridad de la Información (SGSI) en la Universidad de las Fuerzas Armadas ESPE ha presentado un impacto significativo en la institución. Es importante destacar que, si bien la implantación no garantiza una seguridad de información con un nivel de excelencia alto, este proporciona una base sólida para el desarrollo de una cultura de seguridad de la información a largo plazo en futuros proyectos, gracias a las evaluaciones y reportes técnicos realizados. A continuación, se presenta un análisis de impacto que se enfoca en los aspectos cualitativos:

- **Mejora en la Seguridad de la Información:** La implementación de los controles de seguridad ha generado una percepción de mayor seguridad entre los usuarios, fortaleciendo la confianza en la protección de los activos de información y el resguardar de sus datos.
- **Eficiencia Operativa Reforzada:** La introducción de controles y procedimientos de seguridad ha permitido una respuesta más rápida a incidentes y una coordinación mejor en la gestión de la seguridad de la información, gracias a los con nuevos controles agregados que simplifica la identificación y mitigación de riesgos de seguridad.
- **Mayor cumplimiento Legal y Normativo:** La implementación de controles específicos otorga las bases para un mayor cumplimiento legal y normativo en el futuro. La Universidad se encuentra en una buena posición al momento de cumplir con las regulaciones de seguridad y también para adaptarse a los cambios normativos, permitiendo reforzar la importancia de la seguridad de la información en la cultura organizacional.
- **Protección de Datos Personales Mejorada:** Con los controles implantados se ha reforzado la capacidad de proteger los datos personales de estudiantes y el personal, en especial cumpliendo las regulaciones de privacidad de datos.
- **Mayor Conciencia de Seguridad:** El desarrollo de controles y procedimientos de

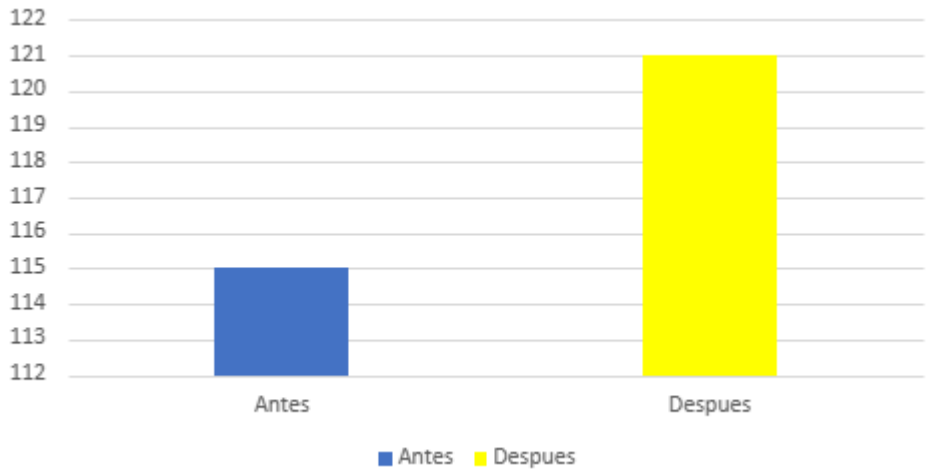
seguridad aumenta la conciencia entre los estudiantes, docentes y personal respectivo. Además, se muestra un mayor compromiso con las prácticas de seguridad de la información por parte de los trabajadores de la institución.

- **Imagen Institucional Reforzada:** La implantación exitosa de los controles del EGSI versión 2, contribuye a una mejora en la imagen institucional, gracias a la percepción de la comunidad académica que demuestran un entorno más seguro y confiable para la gestión de la información. Esto genera un gran paso para la construcción de una cultura de seguridad de la información.

Dado el análisis que se hizo como resultado final de 115 controles establecidos en la versión anterior de EGSI, se llegó a aumentar 6 controles dando como resultado 121 controles, aumentando de forma sustancial la seguridad de la información de la institución.

Figura 5

Controles implantados



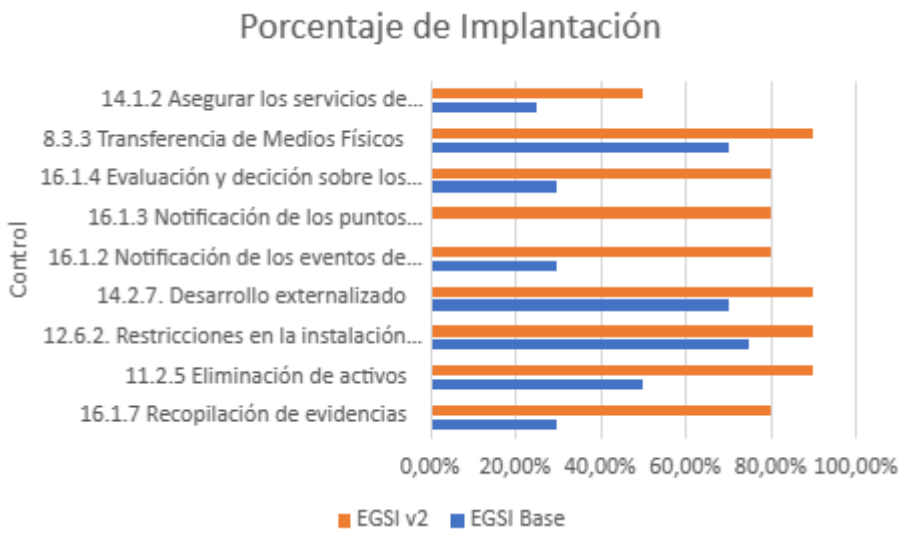
Nota. El gráfico muestra una comparación del número de controles implantados.

El siguiente grafico nos muestra una comparativa entre las dos versiones del EGSI desde el punto de vista inicial al punto de vista final indicando el porcentaje de

implantación en el que se encontraban los controles y como se encuentran en este momento.

Figura 6

Porcentaje de implantación de controles

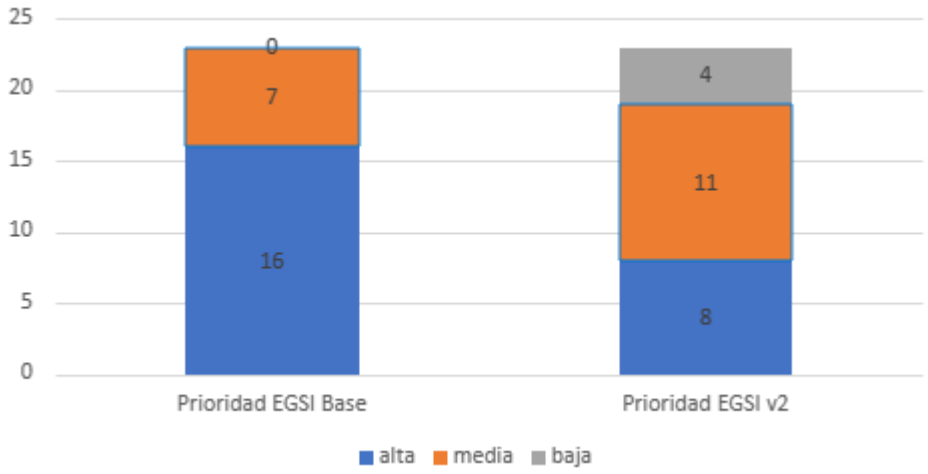


Nota. La figura representa la comparativa del porcentaje de implantación por cada control.

Analizado lo anterior se muestra en que porcentaje se redujo las incidencias graves y que necesitaban un tratamiento inmediato pasando de un numero significativo de falencias a reducirse a incidencias de nivel medio o bajo.

Figura 7

Clasificación de controles por prioridad

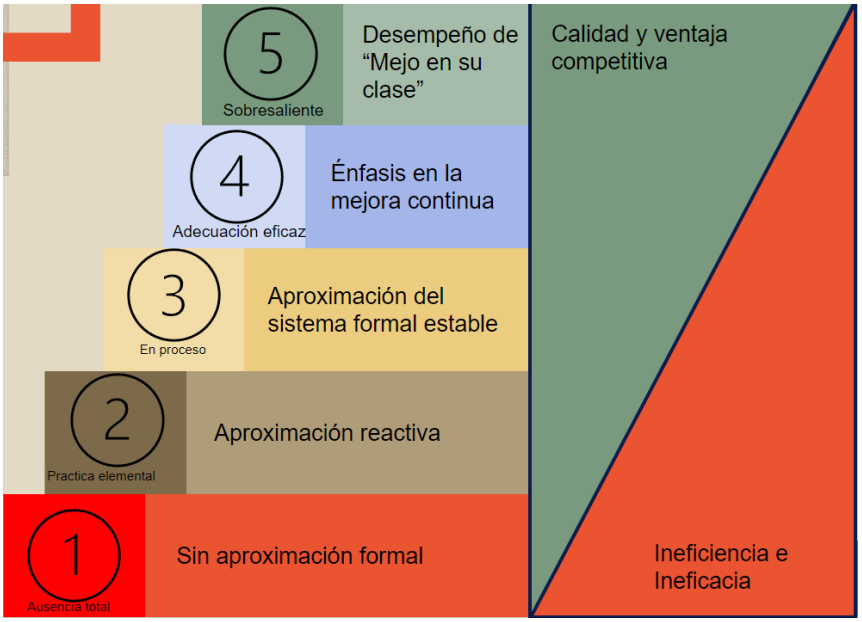


Nota. La figura muestra una comparativa del número de controles por su prioridad.

Gracias a esto se puedo establecer un nivel de madurez mayor al presentado al inicio del proyecto donde la Universidad de las fuerzas armadas se encontraba con una versión del EGSI donde cumplía con lo establecido con el Mintel pero a medida que el proyecto avanzo se pudo denotar un crecimiento sustancial, donde se realizaron diversas actividades con el fin de incrementar la confidencialidad, integridad y disponibilidad dando como resultado un nivel más competitivo de la organización en el ámbito de la seguridad de la información, empezando en un estrato de nivel 3 escalando a uno de nivel 4, siendo aun no suficiente lo que se hizo para estar en el tope de la escala.

Figura 8

Escala de nivel de madurez



Nota. La figura muestra los cinco niveles de madurez que puede tener un EGSI.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

La normativa internacional ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27003 usada como referencia para la ejecución del presente trabajo, permitió de forma objetiva completar la implementación de los controles que se desarrollados con anterioridad y tomar medidas correctivas para agregar nuevos o desarrollar mejoras necesarias para el sistema de la gestión de la seguridad de la información y dar como resultado un mayor nivel de aceptabilidad al sistema que actualmente se encuentra en funcionamiento.

La elaboración de un estado del arte permitió comprender precisamente el contexto y los retos que conlleva la implementación de controles de seguridad de la información en el entorno de la universidad. A partir de esto, se desarrolló detalladamente el plan de implementación de los controles y salvaguardas, tomando en cuenta las acciones necesarias para la ejecución exitosa del proyecto.

Apoyándonos en base a la normativa ISO 27000 se estableció un plan de implantación el cual permitió detallar tiempos, roles y actividades que se realizarían para la correcta implantación de controles, esto conllevaría hacer un análisis técnico al estado actual del EGSI de la Universidad de las Fuerzas Armadas y determinar la criticidad de los controles para posteriormente proceder a la implantación y mejora de los controles.

En concordancia al plan de implantación se logró definir un número de controles específicos con mayor grado de importancia a los cuales mediante diferentes tareas realizadas se les dio tratamiento para mitigar las vulnerabilidades que puedan afectar a las actividades de la Universidad de las Fuerzas Armadas, dando como resultado una mejora en la seguridad de la información.

Finalmente, en base al plan de implantación se realizó una evaluación de los controles donde se comparó con el EGSI inicial como línea base y el sistema con los controles implantados en el presente proyecto. Además, se utilizó la metodología de la revisión documental debido a su accesibilidad y tiempo con relación a los distintos métodos de evaluación.

Recomendaciones

Establecer una práctica de revisión y actualización periódica de las políticas y procedimientos del EGSI garantizará que la documentación esté siempre alineada con los cambios que se presentan en la Universidad de las Fuerzas Armadas ESPE y también mejorando las prácticas en la seguridad de la información.

En futuros trabajos se recomienda insistir a la unidad de tecnologías para realizar entrevistas a los encargados de los activos de información para la comprobación del buen funcionamiento de los controles.

Es recomendable enfocarse en la recolección de datos sobre el funcionamiento de los controles implantados para la evaluación de eficiencia y eficacia que presenta el sistema de gestión de seguridad de la información.

Se debe fortalecer la cultura de seguridad de la información, mediante la sensibilización y formación del personal en este conocimiento. Además, generar una inversión en programas de capacitación garantizará que todos los usuarios tengan claro las políticas y procedimientos de seguridad, lo que contribuye a reducir los riesgos asociados a errores humanos.

Bibliografía

Aleksandrova, S. V., Vasiliev, V. A., & Aleksandrov, M. N. (2020). Problems of Implementing Information Security Management Systems. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 78-81.

Alghamdi, A. M. (2017). Business continuity management: A review of applications, methodologies and frameworks. *Journal of Theoretical and Applied Information Technology*, 3188-3206.

Ameen, N. e. (2018). An approach for implementation of information security management system: A case study of higher educational institutions in Pakistan. *Computers & Security*, 51-64.

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador. Artículo 66.*

Asamblea Nacional del Ecuador. (2004). *Ley Orgánica de Transparencia y Acceso a la Información Pública.*

Asamblea Nacional del Ecuador. (2013). *Ley Orgánica de Comunicación.*

Asamblea Nacional del Ecuador. (2018). *Ley Orgánica de Datos Personales Artículo 10.*

Cárdenas, R. A. (2017). Propuesta metodológica para la implementación de un sistema de gestión de seguridad de la información (EGSI) en organizaciones. *Revista de Investigación Académica*, 1-16.

Castillo, J. (2018). Metodología para la mejora continua del sistema de gestión de seguridad de la información. . *Revista de Seguridad Informática*, 1-12.

Cataldo, A. (2015). *Design Science Research (DSR).* Obtenido de https://www.researchgate.net/profile/Alejandro-Cataldo/publication/283018388_Design_science_research_Una_breve_introduccion/link

s/5626d5ee08aeedae57dc7d20/Design-science-research-Una-breve-introduccion.pdf

CCN-CERT. (2019). *Guía de gestión de riesgos de la información con MAGERIT v3.* Obtenido de https://www.ccn-cert.cni.es/gestion-de-riesgos/guia-de-gestion-de-riesgos-de-la-informacion-con-magerit-v3.html

Choudhary, V., Choudhary, S., & Kaur, S. (2018). Process-oriented approach towards information security management system. *Procedia Computer Science*, 946-954.

Departamento Administrativo de la Función Pública. (2011). *Secretaría Senado*. Obtenido de Resolución No. 2964 de 2011: http://www.secretariasenado.gov.co/senado/basedoc/resolucion_2964_2011.html

Espinosa, J. L. (2019). Metodología para la implantación de un sistema de gestión de seguridad de la información (EGSI) basada en la norma ISO/IEC 27001. *Revista de Investigación Científica*, 29-36.

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, 213-222.

Georg Sven Lampe, M. O. (2022). Critical Success Factor for Integration of Cyber Security in Context of Managed Services. *International Conference on New Trends in Sustainable Business and Consumption*.

Gobierno de Ecuador. (2019). *Ley Orgánica de Telecomunicaciones.*

Gómez, A. (2020). mplementación del modelo CMMI para la evaluación y mejora continua del sistema de gestión de seguridad de la información. *Revista de Investigación en Seguridad de la Información*, 10-23.

Gómez, J. A. (2018). Metodología para la implementación de un sistema de gestión de seguridad de la información (EGSI) en una pequeña y mediana empresa (PME). *Revista Científica del Colegio de Contadores Públicos del Estado Lara*, 9-20.

Instituto de Ingeniería de Software de Carnegie Mellon. (2019). *Capability Maturity Model*

Integration (CMMI). Obtenido de https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=12166

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements.*

International Organization for Standardization. (s.f.). ISO/IEC 27002:2013. *Information technology -- Security techniques -- Code of practice for information security controls.*

ISO. (2018). *ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management.* Obtenido de https://www.iso.org/standard/75281.html

Janeth Mora Secaira, R. D. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). *revista científico - educacional de la provincia Granma.*

Johnson, D. (2013). "A case study of the implementation of the UK Government's security policy framework". *Journal of Information Warfare*, 24-36.

Martínez, J. V. (2019). Plan para la implementación de un SGSI en un centro educativo. 1-143.

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies (InfoTech)*.

Moreira, E. (2023). Afrontando los Desafíos de la Seguridad de la Información: Implementación de un SGSI en un Instituto Superior Universitario. 1-12.

Orellana Toledo, M. A. (2022). Elaboración de una guía de implementación de un SGSI para la corporación ecuatoriana para el desarrollo de la investigación y la academia -CEDIA. 1-160.

Pérez, L. (2019). Metodología para la mejora continua del sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27004. *Revista Internacional de Seguridad de la Información*, 22-35.

Presidencia de la República del Ecuador. (2015). *Acuerdo Ministerial No. 0893*. Obtenido de https://www.redseguridad.com/images/files/ega/Resolucion_0893_-_Esquema_Gubernamental_de_Seguridad_de_la_Informacion_-_Ecuador.pdf

Recalde, J. P. (2019). PLAN DE IMPLEMENTACIÓN DE UN SGSI Y APLICACIÓN DE CONTROLES CRÍTICOS EN EL CENTRO DE OPERACIONES DE SEGURIDAD EN LA EMPRESA GMS. 1-104.

Sánchez, M. A. (2020). Metodología para la implementación de un sistema de gestión de seguridad de la información (EGSI) basada en el ciclo PHVA. *Revista de Investigación Tecnológica*, 18-29.

Secretaría de Gobernación. (29 de Septiembre de 2005). *Acuerdo por el que se establece el Esquema Nacional de Seguridad de la Información*. Obtenido de Diario Oficial de la Federación: http://www.dof.gob.mx/nota_detalle.php?codigo=801217&fecha=29/09/2005

Senescyt. (2019). *Esquema Gubernamental de Seguridad de la Información Versión 2.0*. Obtenido de https://www.redseguridad.com/images/files/ega/EGSI_Version_2.0.pdf

Software Engineering Institute. (s.f.). *OCTAVE Allegro.* Obtenido de https://www.sei.cmu.edu/our-work/initiatives/octave-allegro/index.cfm.

Technology, N. I. (2020). *NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.*

Z. Sun, J. Z. (2020). Research on the Effectiveness Analysis of Information Security Controls. *IEEE 4th Information Technology, Networking*.

Apéndices

A continuación, se anexa los documentos de evidencia de acuerdo con el siguiente Índice:

- Evidencia Nro. AI-PL01
  - Plan de proyecto de implantación EGSI v2
- Evidencia Nro. AI-LI2
  - Cuestionario aplicado al personal encargado de UTIC con la lista de controles implantados
- Evidencia Nro. AI-LI03
  - Revisión técnica de controles implantados.
- Evidencia Nro. AI-IN04
  - Informe ejecutivo inicial de evaluación EGSI
- Evidencia Nro. AI-Pr05
  - Matriz de priorización de controles de EGSI
- Evidencia Nro. AI-Pr06
  - Matriz de Evaluación de controles
- Evidencia Nro. AI-IN07
  - Informe final de evaluación EGSI v2