UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
Creada Ley No. 10 – Registro Oficial 313 de Noviembre 13 de 1985

PROYECTO INTEGRADOR

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA

Sistema de Gestión de Seguridad de la Información para la Tecnología Educativa de las aulas de TI y Software.

AUTOR
Anthony Bladimir Vélez Villavicencio

TUTOR
Ing. Clara Guadalupe Pozo Hernández, MG.

EL CARMEN, 2025

CERTIFICACIÓN DE TUTOR

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría del estudiante Vélez Villavicencio Anthony Bladimir , legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(2)-2025(1), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es "**Sistema de Gestión de Seguridad de la Información para la Tecnología Educativa de las aulas de TI y Software**". La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 18 de agosto del 2025

Lo certifico,

Ing. Clara Guadalupe Pozo Hernández, Mg.
Docente Tutor(a)
Área:

TRIBUNAL DE SUSTENTACIÓN

Universidad Laica Eloy Alfaro de Manabí
Extensión El Carmen
Carrera de Ingeniería en Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Título del Trabajo de Titulación: Sistema de Gestión de Seguridad de la Información para la Tecnología Educativa de las Aulas de TI y Software en la Uleam Extensión El Carmen

Modalidad: Proyector Integrador

Autor: Velez Villavicencio Anthony Bladimir

Tutora: Ing. Pozo Hernandez Clara Guadalupe, Mg.

Tribunal de Sustentación:

Presidente:
Mg. Minaya Macias Renelmo Wladimir. _____

Miembro:
Ing. Mendoza Villamar Rocio Alexandra, Mg. _____

Miembro:
Ing. Reascos Pinchao Raul Saed, Mg. _____

Fecha de Sustentación: 10 de septiembre de 2025

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA TECNOLOGÍA EDUCATIVA DE LAS AULAS DE TI Y SOFTWARE, corresponde exclusivamente a: VÉLEZ VILLAVICENCIO ANTHONY BLADIMIR con CI. 1313538398 y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Vélez Villavicencio Anthony Bladimir
C.I. 1313528398

DEDICATORIA

Le dedico este trabajo a todas las personas que estuvieron a mi lado, en cada momento del desarrollo profesional, brindándome su apoyo y ánimos en los instantes en los que sentía ya no poder, en especial a mis padres y tía, por darme la ayuda que necesite en esos momentos.

Anthony Vélez

AGRADECIMIENTO

Le agradezco a mis padres, hermanos, familia y amigos que estuvieron conmigo, personas que me dieron palabras de aliento en los momentos justos, a los que en el camino no se apartaron, sino que caminaron conmigo.

Y a Dios, por darme las fuerzas necesarias para llegar a donde eh llegado.

El SEÑOR es mi fuerza y mi escudo;
mi corazón en él confía;
de él recibo ayuda.
Mi corazón salta de alegría,
y con cánticos le daré gracias.

Salmos 28:7

Anthony Vélez

ÍNDICE DE CONTENIDOS

ÍNDICE TABLAS

ÍNDICE GRÁFICOS E ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de titulación propone el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para fortalecer la protección de las pantallas electrónicas utilizadas como recurso didáctico en las aulas de las carreras de Tecnologías de la Información y Software de la Universidad Laica “Eloy Alfaro” de Manabí, Extensión El Carmen. La investigación surge de la necesidad de garantizar la confidencialidad, integridad y disponibilidad de estos equipos, considerando la ausencia de políticas claras, controles físicos adecuados y procedimientos normalizados. La investigación tuvo un enfoque descriptivo y aplicado, empleando métodos inductivo, deductivo, analítico y sintético. Para la recolección de datos se aplicaron encuestas a estudiantes y entrevistas al director de carrera, lo que permitió identificar debilidades en la gestión y los principales riesgos de seguridad. La propuesta metodológica se fundamentó en la norma ISO/IEC 27001, utilizada como guía para evaluar el nivel de madurez, analizar los riesgos y diseñar un plan de acciones correctivas y preventivas. Como resultado, se determinó que las pantallas están especialmente expuestas a incidentes de incendio y robo, ambos con un nivel alto de riesgo, por lo que se propuso un plan de medidas de seguridad que incluye la elaboración de un manual de políticas y la instalación de cámaras de videovigilancia, fomentando prácticas seguras y responsables en la comunidad académica.

ABSTRACT

This thesis proposes the design and implementation of an Information Security Management System (ISMS) to strengthen the protection of electronic screens used as teaching resources in the classrooms of the Information Technology and Software programs at the Eloy Alfaro Laica University of Manabí, El Carmen Extension. The research arose from the need to ensure the confidentiality, integrity, and availability of this equipment, given the lack of clear policies, adequate physical controls, and standardized procedures. The research had a descriptive and applied approach, employing inductive, deductive, analytical, and synthetic methods. Data collection involved student surveys and interviews with the program director, which allowed for the identification of management weaknesses and the main security risks. The methodological proposal was based on the ISO/IEC 27001 standard, used as a guide to assess the maturity level, analyze risks, and design a corrective and preventive action plan. As a result, it was determined that the displays are particularly vulnerable to incidents of fire and theft, both of which pose a high risk. Therefore, a security plan was proposed that includes the development of a policy manual and the installation of video surveillance cameras, promoting safe and responsible practices within the academic community.

CAPÍTULO I:

1 INTRODUCCIÓN

1.1 Introducción

Hoy en día, la tecnología ya no es solo un complemento en la educación, sino una parte esencial de cómo se enseña y se aprende. Las universidades y otros centros de estudios superiores están invirtiendo en tecnología de punta para mejorar la formación que ofrecen. No obstante, esta apuesta por la modernización también nos obliga a enfrentar nuevos retos, sobre todo en lo que respecta a cómo gestionamos y protegemos estos recursos. Tanto la información como los equipos tecnológicos son ahora bienes muy preciados, y es crucial cuidar su confidencialidad, integridad y que siempre estén disponibles para no interrumpir las clases y mantener un alto nivel educativo.

Este proyecto de titulación aborda precisamente este desafío en un contexto específico: las aulas de las carreras de Tecnologías de la Información y Software de la Universidad Laica "Eloy Alfaro" de Manabí, en su extensión de El Carmen, vemos que la introducción de modernas pantallas interactivas ha sido un gran paso adelante para la enseñanza, pero al mismo tiempo ha revelado que no existe un plan claro para su uso, cuidado y seguridad. Al no haber reglas definidas, controles de acceso adecuados ni un conocimiento extendido sobre cómo manejarlas correctamente, estos equipos quedan vulnerables a todo tipo de problemas, desde daños físicos y robos hasta fallos técnicos y un mal uso.

Frente a este panorama, la investigación que se presenta busca crear un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como referencia la norma ISO/IEC 27001. La meta es clara: desarrollar un conjunto de políticas, pasos a seguir y controles para reducir los peligros detectados, alargar la vida útil de estos equipos y promover entre alumnos y profesores una mayor conciencia sobre la importancia de la seguridad. En las siguientes páginas, se examinará el problema a fondo, se explicarán las bases teóricas del proyecto, se detallará cómo se recogió la información y, por último, se ofrecerá un plan práctico para poner en marcha el SGSI, junto con los resultados que se esperan y las sugerencias finales.

1.2 Presentación del tema

El tema central de esta investigación es el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Tecnología Educativa de las aulas de TI y Software en la Universidad Laica “Eloy Alfaro” de Manabí, Extensión en El Carmen. Este proyecto surge como respuesta a la necesidad crítica de proteger los activos tecnológicos que la institución ha incorporado para modernizar sus procesos pedagógicos.

1.3 Ubicación y contextualización de la problemática.

El presente proyecto de titulación se desarrolló en la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, ubicada en la ciudad del mismo nombre El Carmen, entre las calles Avenida 3 de Julio y Carlos Alberto Aray, planta central, en el segundo piso de las carreras de TI y Software, en los pasillos del respectivo piso.

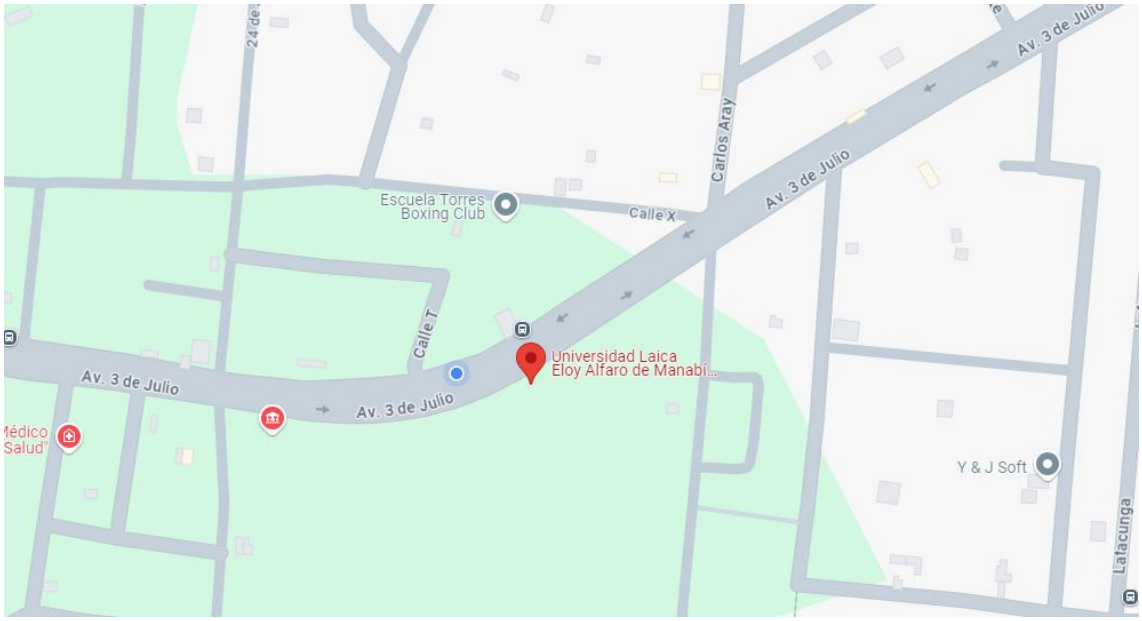


Ilustración 1 Croquis de la ULEAM Extensión el Carmen.

Actualmente se cuenta con 5 aulas en el área de TI y Software, numeradas desde la 201 hasta la 210, desde el año 2022 en el segundo periodo se han entregado estas pantallas inteligentes para ser usadas como material didáctico, teniendo doble sistema operativo, Android y Windows, además de varias conexiones, 5 entradas HDMI, 2 USB C, 5 USB normal, (demás entradas y salidas) contando cada aula con su respectiva pantalla.

1.4 Planteamiento del problema

1.4.1 Problematización

Debido al desconocimiento sobre el uso adecuado de los equipos tecnológicos por parte de los estudiantes y la falta de control de acceso a las áreas implicadas, ha surgido la necesidad de realizar el respectivo trabajo de titulación, el cual es realizar una auditoria informática.

¿Cuál es el nivel de desconocimiento de arte de los estudiantes sobre el buen uso de equipos electrónicos?

¿La aplicación de una auditoria me ayudaría a saber el impacto del uso inadecuado de las pantallas?

¿Cuenta actualmente la universidad un manual de uso para el uso de las pantallas?

1.4.2 Génesis del problema

La génesis del problema se origina en la necesidad de modernizar y optimizar los procesos educativos mediante el uso de pantallas electrónicas como herramienta de apoyo al proceso de enseñanza-aprendizaje. Sin embargo, desde su implementación, la falta de políticas claras de mantenimiento, ausencia de controles físicos y lógicos, y la inexistencia de procedimientos estandarizados de respuesta ante incidentes han incrementado la exposición de estos equipos a diversos riesgos operativos y de seguridad.

Con el paso del tiempo, la ausencia de un programa estructurado de gestión de riesgos y auditoría tecnológica ha permitido la materialización de eventos como fallos por daños físicos, vulnerabilidades frente a ataques de malware, sustracción de equipos y riesgos ambientales como incendios, generando pérdidas económicas y afectando la continuidad académica.

1.4.3 Estado actual del problema

Actualmente, la institución cuenta con pantallas electrónicas distribuidas en varias aulas de la carrera de Tecnologías de la Información. Sin embargo, no existe un manual de procedimientos específicos que oriente al personal docente, técnico y administrativo sobre cómo prevenir, detectar, responder y registrar incidentes relacionados con los riesgos identificados.

La falta de mantenimiento preventivo periódico, controles físicos inadecuados, medidas de seguridad lógica insuficientes y carencia de registros formales han derivado en una alta

dependencia de acciones correctivas improvisadas. Esta situación incrementa el tiempo de inactividad de los equipos, eleva costos de reparación o reemplazo, y expone la información académica a vulnerabilidades que podrían comprometer su integridad, disponibilidad y confidencialidad.

1.5 Diagrama causa – efecto del problema

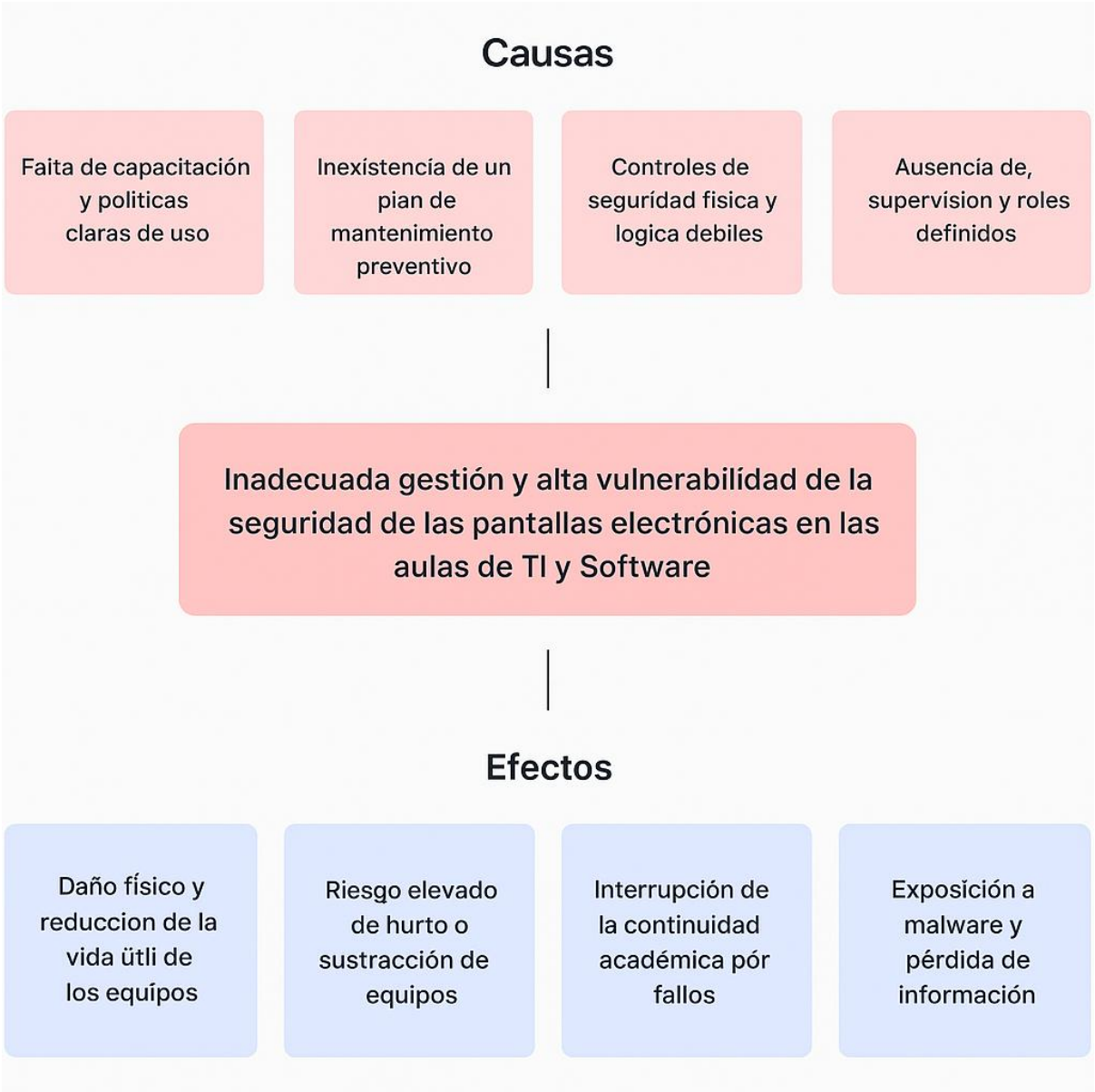


Ilustración 2 Diagrama Causa - Efecto

1.6 Objetivos

1.6.1 Objetivo general

Realizar un Sistema de Gestión de Seguridad de la Información para la Tecnología Educativa de las aulas de TI y Software.

1.6.2 Objetivos específicos

1. Identificar la problemática de la investigación mediante el análisis de las posibles brechas de seguridad para identificar posibles riesgos.
2. Buscar varias fuentes información relacionada a Sistema de Gestión de Seguridad de la Información para la Tecnología Educativa mediante varios métodos para sustentar mi proyecto de titulación.
3. Aplicación de encuesta y entrevista para identificar los riesgos a los que están expuestas las pantallas.
4. Evaluar la seguridad de las pantallas mediante una auditoría de seguridad informática, para buscar los puntos débiles y peligros existentes.
5. Elaboración un plan de medidas y aplicar el más factible, un manual de uso y políticas de seguridad para disminuir los riesgos a los que están expuestas las pantallas.

1.7 Justificación

La importancia de un Sistema de Seguridad de la Información a nivel mundial radica en su capacidad para proteger la confidencialidad, integridad y disponibilidad de la información, que se ha convertido en uno de los activos más valiosos para individuos, organizaciones e incluso gobiernos. En un contexto global, donde los ataques cibernéticos, las violaciones de datos y las amenazas a la privacidad están en constante aumento, implementar un SGSI efectivo es esencial.

La seguridad informática es vital para resguardar datos delicados, frenar intrusiones virtuales, y asegurar que todo siga funcionando en un planeta más conectado, aparte de cuidar los datos personales y de la empresa no solo esquiva engaños y suplantaciones, sino que también cumple con reglas legales, la defensa de servicios básicos y la fe de los clientes. Usar métodos de protección fuertes es clave para reducir peligros y certificar la firmeza y confianza de los sistemas técnicos.

Los equipos informáticos, los que son usados para la educación por lo que desde la llegada de las pantallas la carrera de TI y Software de la Extensión El Carmen se ha podido constatar que no existe un debido control, norma o sobre el uso de estas, dando con esto que, en algunos casos, estas se descontrolen, por lo que se hace necesario realizar una evaluación de cada una de estas, para así poder determinar el estado en el que se encuentran actualmente y aplicar las correcciones necesarias, al ser un recurso educativo, es muy importante para el desarrollo de los estudiantes y así mismo de la sociedad alrededor.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Como consecuencia de implementar esta auditoría y la entrega de un manual de uso se obtiene una extensión en la vida útil de los equipos y con esto lograr que los estudiantes de las carreras de TI y Software cuenten con estas herramientas educativas actualizadas el mayor tiempo posible.

1.8.2 Impacto social

Al implementar los resultados de la auditoria, los estudiantes aprenderían sobre el buen uso de estas herramientas tan útiles, ya que actualmente se evidencia el uso poco práctico de las pantallas, por la falta de un manual de uso y unas políticas que controlen el mal uso.

También lograr que, al cuidar del equipo tecnológico, la vida útil aumenta, trayendo consigo un beneficio para los futuros estudiantes.

1.8.3 Impacto ecológico

Luego de la realización del siguiente trabajo, podríamos evidenciar a futuro un buen uso de los equipos, trayendo consigo que la universidad no tenga la necesidad de adquirir unos nuevos, disminuyendo como institución, disminuir la contaminación ambiental causada por la basura generada al desechar la basura electrónica, haciendo que nuestra huella digital en el planeta no sea tan elevada.

CAPÍTULO II:

2 MARCO TEÓRICO DE LA INVESTIGACIÓN

2.1 Antecedentes históricos

2.1.1 Sistema de Gestión de Seguridad de la Información (SGSI)

Los Sistema de Gestión de Seguridad de la Información (SGSI) han evolucionado desde la década de 1970, cuando las organizaciones comenzaron a implementar políticas de seguridad para proteger sus datos. La norma ISO/IEC 27001, publicada en 2005, estableció un marco internacional para la gestión de riesgos en la seguridad de la información. Con el aumento de las amenazas cibernéticas, la adopción de un SGSI se ha vuelto esencial, promoviendo una cultura de seguridad donde todos los empleados son responsables. Además, regulaciones como el GDPR han impulsado su implementación para garantizar el cumplimiento normativo (Taylor, Alexander, Finch, & Sutton, 2020).

La historia sobre la seguridad informática se origina en los principios mismos de la computación, cuando se comenzó a identificar así la necesidad de salvaguardar bien la información, las ideas iniciales de seguridad, como la confidencialidad, integridad y disponibilidad de los datos, aparecieron en la década de 1970, con el desarrollo de las primeras redes. La tecnología avanzaba constantemente. Por esto se originaron normas y reglas de seguridad a causa del incremento de los peligros. Con la aparición de virus informáticos en los años 80 además de los 90, se marcó la necesidad por implementar medidas de protección mucho más robustas. Según Avenía (2017), la evolución de la seguridad informática ha sido impulsada por la creciente complejidad de los sistemas y la sofisticación de los ataques.

2.1.2 Tecnología Educativa.

Desde los años 50, la educación ha visto cosas raras, como los laboratorios de idiomas, que parecían magia. En los años 60, la tecnología se puso más interesante con aparatos de audio y video, y formas nuevas de enseñar a muchos a la vez. Se cree que, poco a poco, las computadoras y otras tecnologías más modernas se usarán más para que aprender sea mejor, aunque no tan rápido como quisiéramos (Allen, 1968).

La historia de la tecnología educativa comenzó en el siglo XX con intentos de implementar "máquinas de enseñanza". Sidney Pressey y B.F. Skinner crearon dispositivos para un aprendizaje automatizado y personalizado. A pesar de las expectativas, estas tecnologías no cumplieron completamente su propósito, revelando una desconexión entre la

teoría y la práctica en las aulas. Los medios de comunicación influyeron en las percepciones sobre estas máquinas, mientras que las teorías psicológicas guiaron su desarrollo. Esto muestra que el progreso tecnológico impulsa el cambio educativo, aunque de manera más compleja de lo que se cree comúnmente (Watters, 2019).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

La importancia de la seguridad informática en la educación digital: retos y soluciones

En el artículo se resalta que la seguridad informática en educación digital se protege la información aplicando normas internacionales, buenas prácticas y competencias digitales docentes. Estudios resaltan la importancia de gestionar riesgos y vulnerabilidades, promoviendo un entorno seguro para todos (Guaña, 2023).

Diseño de un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica del Colegio Salesiano basado en Magerit.

En este proyecto, se idea una forma algo extraña de manejar la seguridad de la información en el Colegio Salesiano San Pedro Claver, centrada en cómo se maneja la tecnología. Juntando las reglas internas con ideas globales, usando ISO 27001 como guía y MAGERIT para ver qué cosas podrían salir mal (Rosales, 2019).

Gestión de la seguridad y protección de la información de la UTMACH mediante estándares y buenas prácticas.

Esta iniciativa puso en marcha un Sistema para Manejar la Seguridad de la Información en la Universidad Técnica de Machala. Se metió de lleno con los fallos de seguridad y animó a todos a pensar en la seguridad. Al revisar las tecnologías, vimos lo bueno y lo que se podía mejorar, creando así una base fuerte para la seguridad en la universidad. El Sistema demostró ser muy bueno, sirviendo de ejemplo para otros centros educativos. El estudio también ayuda a que se aprenda más sobre seguridad de la información, sumando ideas éticas sobre cómo cuidar los datos importantes (Díaz Quezada, 2024).

Sistemas de gestión en seguridad informática SGSI en universidades públicas del eje cafetero – Colombia.

Este proyecto busca ver cómo se maneja la información en las universidades públicas cafeteras de Colombia, espiando cómo se usan las leyes de aquí y de fuera para poner en marcha un Sistema de Gestión de Seguridad Informática (SGSI). Viendo que cada vez hay más ataques

cibernéticos que ponen en peligro la seguridad de la información, se ve que es clave tener trucos para bajar los riesgos y cuidar lo que tienen las universidades. El estudio mira qué tanto han avanzado en poner en marcha el SGSI, basándose en reglas como la ISO 27001 y la forma de hacer las cosas de MAGERIT (Buitargo Giraldo, 2020).

Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico.

En este proyecto el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) ha establecido directrices para implementar Sistemas de Gestión de Seguridad de la Información (SGSI) en entidades estatales. Este proyecto además analiza los riesgos en las secretarías académicas de instituciones educativas de nivel básico, utilizando la norma ISO 27005 para identificar activos críticos y riesgos asociados, y proponiendo un plan de tratamiento de riesgos (Blandón Jaramillo & Benavides Sepúlveda, 2018).

2.3 Definiciones conceptuales

2.3.1 Sistema de Gestión de Seguridad de la Información

2.3.1.1 Definición de Sistema de Gestión de Seguridad de la Información.

Un SGSI es un conjunto de procesos que permiten gestionar y mejorar continuamente la seguridad de la información en base a los riesgos de la organización. Su implementación implica establecer procesos formales, definir responsabilidades y documentar políticas, planes y procedimientos. Hay dos tipos de procesos: los de gestión, que controlan el sistema y su mejora, y los de seguridad, que se enfocan en proteger la información (Gómez Fernández & Fernández Rivero, 2018).

2.3.1.2 Controles de seguridad y sus tipos.

Al hablar de la vigilancia, es vital nombrar las ideas de activo, vulnerabilidad, amenaza, impacto, probabilidad y riesgo. Un bien es algo preciado; la amenaza es su lado flojo; la amenaza es lo que lo puede tocar; el impacto es el daño hecho; la probabilidad es si algo puede pasar; y el riesgo es ver la chance y la probabilidad juntos.

Las vigilancias, o defensas, buscan bajar o quitar riesgos, jugando con la probabilidad o el impacto. Lo vital es que lo que cueste la vigilancia no debe ser más de lo que vale el bien. En la computación, hay vigilancias con fuerzas y costos distintos, pero ninguna borra el trance del todo. Para cuidar bien, hay que saber qué bienes hay, ver los riesgos y tomar los controles adecuados para cuidarlos (Oviedo Regueros, 2023).

Tipos de controles:

- **Controles básicos.**

Preventivo: Actúa sobre la probabilidad, buscando evitar que ocurra un incidente de seguridad. Según la ISO 27002:2022, es un control diseñado para impedir incidentes de seguridad de la información. Es más económico y efectivo, ya que evita que una amenaza se materialice.

Ejemplos de controles preventivos incluyen: una valla que bloquea el acceso a una zona, un firewall que impide ciertos ataques en la red, un IPS que previene intrusiones descartando paquetes, y los controles de acceso físicos o lógicos, que limitan el acceso a personas autorizadas (DTS Solution, 2022).

Correctivo: Trabaja luego de un golpe tras un fallo de seguridad. La ISO 27002:2022 lo ve como actos de mando puestos tras un suceso. Estos controles suelen costar más y son difíciles de mantener, así que hay que elegir bien la técnica, los bienes y el plan.

Este control no baja el riesgo, pero sí el daño si una pega sale bien. Por ejemplo, copias de resguardo (para volver a tener datos tocados), gente extra (para llenar pegas clave), y actos para bajar o arreglar fallos vistos en los sistemas (Schellman Blog, 2022).

2.3.1.3 Seguridad de la información y la ISO 27001

La seguridad de la información efectiva, según la Norma, implica mantener la confidencialidad, integridad y disponibilidad de los datos, y debe estar alineada con la gestión de riesgos de la organización, sin interferir en sus operaciones. El SGSI incluye estructura organizativa, políticas, procedimientos y recursos, proporcionando un enfoque integral para proteger la información.

La norma ISO/IEC 20000-1 también indica la seguridad de la información, conectándose con ISO 27002. Los requisitos clave de seguridad en 20000-1 incluyen: La aprobación de una política de seguridad por la dirección, la implementación de controles basados en riesgos, la gestión de incidentes, supervisión de mejoras. Un SGSI alineado con ISO 27001 lo hace más fácil de cumplir, lo cual es una razón por la cual integrar dos sistemas es fundamental para la gestión eficaz de la seguridad y el TI servicio (Calder, 2020).

2.3.1.4 Modelo PHVA.

El modelo PHVA es un conjunto de acciones que se componen de las siglas: P (plan: planear), H (hacer, ejecutar), V (verificar, controlar) y, finalmente, A (actuar, actuar de manera correctiva) (Silva Coelho, Segadas de Araújo, & Kowask Bezerra, 2014):

- Planear.

Establecer las reglas, metas, métodos y pasos del SGSI que sirvan para manejar el riesgo y hacer más fuerte la protección de los datos, buscando así obtener logros que vayan de la mano con las metas y reglas principales del lugar de trabajo.

- Hacer.

Poner en marcha y ejecutar las políticas, controles, procesos y procedimientos del SGSI.

- Verificar.

Analizar y, si es necesario, medir el rendimiento de un proceso basado en la política, los objetivos y la experiencia práctica del SGSI, presentando los resultados para la revisión por parte de la dirección.

- Actuar.

Implementar acciones correctivas y preventivas basadas en los resultados de la auditoría interna del SGSI y en la revisión crítica realizada por la dirección u otra información relevante, con el objetivo de lograr la mejora continua del SGSI.

2.3.1.5 Plan de respuesta a incidentes de seguridad física informática.

En general, el Plan de Respuesta a Incidentes de Seguridad Física Informática describe los procesos técnicos, técnicas, listas de verificación y formularios fundamentales que se requieren en la gestión de un incidente de seguridad. En este sentido, éste deber ser detallado y coherente con la prioridad crítica de la organización, de modo que la probabilidad de cometer errores debido a la presión se minimice. Por lo tanto, el uso primordial del plan incluye el mantenimiento de la integridad y la posibilidad de recuperar sistemas críticos en un contexto de seguridad física, tecnología y gestión de materiales cuando la situación lo exige (Atómica Organismo Internacional de Energía, 2018).

2.3.2 Tecnología Educativa.

2.3.2.1 Introducción a la tecnología digital en la educación.

La era digital cambió la enseñanza de forma notoria. Este capítulo muestra cómo lo digital, desde sus inicios hasta hoy, impactó en la educación. Siempre, la educación usó inventos, desde la imprenta a internet, para hacer mejor el enseñar y el aprender.

Aunque usar la tecnología trajo problemas como la falta de acceso y los datos seguros, también dio cosas buenas. La tecnología hizo que la información sea más fácil de hallar y creó lugares para aprender más movidos, donde los alumnos participan más (Araujo Bedoya, Guerra Delgado, Bastidas Santana, Diaz Berruz, & Planta Ulloa, 2024).

2.3.2.2 TIC en la educación inclusiva.

Las Tecnologías de la Información y la Comunicación (TIC) son cruciales al diseñar espacios educativos que integran, colaborando a cubrir las variadas necesidades de los estudiantes. En un planeta donde las aulas son más distintas, con alumnos de diversos inicios, habilidades y retos, las TIC se revelan como herramientas potentes que dejan a los docentes cambiar su enseñanza de forma más eficaz y a medida.

A pesar de la actitud positiva de muchos profesores hacia el uso de las TIC, su implementación real en las aulas sigue siendo limitada. Esto se debe, en gran parte, a la falta de formación técnica adecuada. No obstante, se reconoce ampliamente que las TIC ofrecen oportunidades únicas para desarrollar habilidades específicas en los estudiantes y potenciar su

aprendizaje curricular. Desde aplicaciones que facilitan la comunicación para estudiantes con dificultades del habla, hasta programas que permiten personalizar el ritmo y estilo de aprendizaje, las TIC pueden marcar una diferencia significativa, ayudando a que cada estudiante tenga las mismas oportunidades de éxito académico (Colás Bravo & Lozano Martínez, 2011).

2.3.2.3 Los desafíos de las TIC para el cambio educativo.

El uso de las TIC en la educación va más allá de la simple implementación de equipos tecnológicos en las aulas y para aprovechar su potencial transformador, es fundamental que los docentes desarrollen competencias digitales que les permitan integrar las tecnologías de manera efectiva en sus prácticas pedagógicas. Además, la sostenibilidad de estos proyectos requiere una planificación cuidadosa, con contenidos digitales relevantes y accesibles, que promuevan el aprendizaje autónomo y crítico en los estudiantes por esto el acceso equitativo a las TIC tanto en las escuelas como en los hogares es esencial para reducir la brecha digital y garantizar una educación inclusiva y de calidad (Carneiro, Toscano, & Díaz, 2021).

2.3.2.4 Medios, Recursos Didácticos y Tecnología Educativa

Los materiales curriculares, también llamados didácticos, incluyen recursos impresos, audiovisuales y digitales, como libros de texto, videos, infografías y software para PC o móviles. Estos materiales deben estar alineados con los objetivos, contenidos y métodos de enseñanza, y se diseñan según las necesidades de los estudiantes, los objetivos de aprendizaje y el contexto social. No se puede calificar a priori como buenos o malos, sino en función de su adecuación a la propuesta educativa. Los docentes disponen hoy de una amplia variedad de recursos, y aunque estos materiales no sustituyen la creatividad y estrategia docente, facilitan y enriquecen el proceso de enseñanza-aprendizaje. Los recursos no solo sirven para transmitir información, sino también para motivar y estructurar el aprendizaje, y deben estar integrados en el currículo de forma coherente con el contexto cultural y social. Además, el diseño debe cumplir con principios de seguridad, protección de datos y adaptabilidad para ser realmente educativos (Vázquez Cano, 2021).

2.3.2.5 Tipos de tecnología aplicadas en la educación.

1. Tablets.

Ilustración 3 Tablet

Las tabletas digitales están surgiendo como herramientas fundamentales en el ámbito educativo, brindando numerosos beneficios y oportunidades para mejorar el aprendizaje. Según Sánchez (2010), su papel en la educación se puede resumir en los siguientes aspectos:

- Facilitación del Aprendizaje: Las tabletas permiten acceder a una amplia variedad de recursos educativos, como libros digitales, aplicaciones interactivas y contenido multimedia, enriqueciendo así la experiencia de aprendizaje.
- Creación de Contenidos: Orientada a la generación de contenido por parte de los alumnos, no solo de texto, sino de material audiovisual, presentaciones y mapas conceptuales como podcasts, lo que estimula su creatividad y propician la colaboración entre pares.
- Interactividad y Participación: Brindan un entorno dinámico y más divertido para el estudiantado, facilitando su interacción en la clase y adaptándose a su lógica digital como nativo digital.
- Reducción de Cargas Físicas: Permite acceder a materiales digitales, por lo que la mochila debe ser más liviana, los estudiantes no deben cargar libros y fotocopias pesadas. Integración de TIC: Se incorporan en un modelo educativo que utiliza tecnologías de la información y la comunicación (TIC), actuando como herramientas multifuncionales que pueden sustituir libros de texto y cuadernos.
- Desarrollo Profesional del Profesorado: Es vital que los profesores se capaciten bien para usar las tabletas en clase. Se les enseña cómo usarlas y cómo crear un ambiente donde se saquen el mayor provecho a lo que ofrecen.

- Desafíos y Consideraciones: A pesar de sus beneficios, las tabletas no son una solución definitiva. Es importante abordar la escasez de contenido educativo en español y la complejidad en el intercambio de archivos, así como garantizar que su uso esté respaldado por un enfoque pedagógico sólido.

2. Computadoras portátiles.

Ilustración 4 Computadora portátil.

Una computadora portátil es un dispositivo informático compacto y móvil que ofrece a los usuarios opciones para acceder a la información, completar tareas y comunicarse de una manera efectiva en varios entornos, incluidos los espacios educativos. También proporciona un ambiente conveniente para la facilidad de la interacción y colaboración entre alumnos y alumnos o profesores (Ministerio de Educación de la Nación, 2008).

Ventajas para el estudio de los estudiantes:

- Entrada a los datos: Los ordenadores dan a los chicos entrada al instante a una gran cantidad de medios educativos en línea, lo que mejora su forma de estudiar y les permite indagar y ver temas de interés de forma más profunda.
- Impulso del apoyo: Estas computadoras hacen más fácil el trabajo en grupo y el apoyo entre compañeros, dejando que los chicos compartan ideas, medios y trabajos al mismo tiempo, lo que anima a un estudio más activo y que todos tomen parte.
- Ajuste del estudio: Los maestros pueden cambiar las tareas y medios a las peticiones únicas de cada chico, lo que deja una forma más ajustada y buena de estudiar.

- Crecimiento de habilidades digitales: El uso de computadoras ayuda a los chicos a tomar mañas tecnológicas clave, preparándolos para un mundo de trabajo cada vez más con tecnología.
- Estimulación de la creatividad: Los alumnos pueden usar herramientas y programas de computadoras para crear proyectos con fotos y videos, charlas y otras tareas ingeniosas, lo que despierta su fantasía y mañas para mostrar lo que sienten.

3. Pizarras interactivas.
    - **Pizarras digitales interactivas (PDI).**

Ilustración 5 COPIMATIK Pizarras Digitales Interactivas (PDI)

Las pizarras digitales interactivas (PDI), como las Smart Boards, son aparatos que enlazan un computador y un reflector en un panel sensible al tacto, permitiendo a los profesores y alumnos manipular sin intermediarios contenidos digitales. Con estas pizarras, se puede manosear fotos, apuntar notas digitales y tenerlas a buen recaudo para siguientes clases, cosa que pone el aprendizaje más movido e interactivo. Usarlas en las aulas ha evidenciado subir el ánimo y la concentración de los estudiantes, aparte de dar opciones para ocuparse de la diversidad, sobre todo a los que tienen trabas para aprender (Toledo Morales & Sánchez García, 2013).

- **Pantallas electrónicas táctiles.**

Ilustración 6 Pantallas interactivas en la educación.

Las pizarras digitales han transformado la forma de enseñar y aprender, haciendo que las clases sean más dinámicas e interactivas, gracias a estas pantallas táctiles hacen que tanto docentes como estudiantes exploren contenidos multimedia, hagan anotaciones en tiempo real y consulten recursos en línea sin salir del aula con herramientas como gráficos, videos y simulaciones, las pizarras digitales no solo capturan la atención de los estudiantes, sino que también promueven el trabajo en equipo y el aprendizaje práctico. Desde primaria hasta la universidad, su uso apoya metodologías innovadoras como el aprendizaje colaborativo, las clases inversas y los proyectos en equipo, enriqueciendo la experiencia educativa (Johnson & Smith, 2019).

2.3.3 Metodología.

ISO/IEC 27001

Para el desarrollo de la presente investigación se sigue la norma ISO/IEC 27001, cual sendero para instaurar, cuidar y potenciar sin pausa un Sistema de Manejo de la Seguridad de la Información (SGSI). Tal norma, revelada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), da un enfoque metódico que se apoya en el manejo de riesgos, buscando amparar el secreto, entereza y presencia de la información en una entidad (ISO, 2022).

La ISO/IEC 27001 se despliega en secciones variadas que contemplan:

Contexto de la organización: Detección de elementos internos y ajenos que impactan la protección de datos, sumado a la precisión de los entes vinculados y los límites del SGSI.

Liderazgo y compromiso: Creación de reglas, oficios, obligaciones y facultades para asegurar que la gerencia superior se involucre con la protección de la información.

Planificación: Reconocimiento de peligros y opciones por medio del estudio de riesgos, así como el diseño de movimientos para manejarlos de la manera correcta.

Soporte: Provisión de los recursos necesarios, competencia del personal, comunicación y control de la información documentada.

Operación: Implementación de controles operativos para tratar los riesgos identificados, en concordancia con el Anexo A de la norma, que detalla un conjunto de controles de seguridad clasificados por objetivos de control.

Evaluación del desempeño: Observar, calcular, estudiar y juzgar qué tan bien funciona el SGSI, usando revisiones internas y chequeos de los jefes.

Mejora continua: Encontrar errores, poner en marcha soluciones y seguir puliendo el SGSI sin parar.

La meta clave de ISO/IEC 27001 es vigilar que los peligros de la protección de datos se manejen de manera organizada y que la empresa pruebe acuerdo con peticiones legales, de reglas y de tratos que sirven, junto con las ilusiones de los grupos de interés.

2.4 Conclusiones.

Se pretende dar un buen comienzo al Sistema de Gestión de Seguridad de la Información (SGSI), aclarando que son pasos vitales para mantener y hacer crecer la seguridad de los datos, según los peligros de cada empresa. Las medidas de seguridad, como las que evitan, arreglan o asustan, son muy importantes para bajar estos peligros.

Mirando esto con cuidado, se notó que los cambios digitales han movido mucho la educación. Poner muchas tecnologías juntas, desde las máquinas de escribir hasta el internet, ha hecho que sea más fácil para todos obtener información y ha formado lugares de aprendizaje más activos y donde todos participan, y también que las TIC son clave para hacer lugares educativos donde todos entran, dejando que los maestros cambien la forma de enseñar a lo que cada estudiante necesita.

CAPÍTULO III:

3 MARCO INVESTIGATIVO

3.1 Introducción

En el marco investigativo, se presenta información sobre los tipos de investigación que se realizarán en el SGSI. Este capítulo tiene como objetivo definir y contextualizar la investigación, proporcionando un marco teórico y metodológico que guiará el estudio, también se busca establecer las bases sobre las cuales se desarrollará, así como los enfoques y métodos que se utilizarán para recopilar y analizar la información relacionada con la seguridad de las pantallas de las aulas de las carreras de TI y Software.

3.2 Tipo de investigación

- **Investigación Cualitativa.**

La investigación cualitativa es como un enfoque que busca entender los misterios de la sociedad y las personas, pero en lugar de números, recolecta pistas en forma de historias y vivencias, dándole mucha importancia a lo que rodea a cada situación y a cómo lo sienten los involucrados (Quecedo & Castaño, 2002).

La investigación cualitativa se usó para comprender los diferentes comportamientos de los estudiantes en cuanto al uso de las pantallas electrónicas.

- **Investigación Cuantitativa.**

El estudio cuantitativo se ve como un método que usa prácticas basadas en datos y patrones numéricos para mirar y calcular elementos en un entorno común, dando paso así a la creación de ideas y la llegada a conclusiones que pueden ser extendidas a todos (Babativa Novoa, 2017).

La investigación cuantitativa impulsó mi proyecto al ofrecer un método ordenado para tasar y estudiar factores vinculados a las pantallas de forma imparcial, además, con este esquema, pude obtener datos reales por medio de sondeos y charlas, logrando así evaluar numéricamente puntos clave, como el uso y la seguridad de estas.

- **Investigación Descriptiva.**

La investigación descriptiva tiene como objetivo describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con la de otras fuentes (Guevara Alban, Verdesoto Arguello, & Castro Molina, 2020).

La investigación descriptiva sirvió para crear una base firme, señalando y organizando los aspectos principales de los fenómenos o las situaciones analizadas. En este caso, la forma en que se recogieron y estudiaron los datos ayudó a lograr una explicación minuciosa de cómo están ahora las pantallas, lo cual apoyó de manera clara las elecciones hechas al crear tu revisión.

3.3 Método(s) de investigación

- **Método Inductivo.**

El razonamiento inductivo busca crear ideas amplias, tomando como base datos reunidos al mirar directamente. Desde sucesos concretos de un grupo, se deducen ideas extendidas sobre el grupo completo. Este modo, que se llama experimental, avanza en pasos que son mirar, crear ideas, comprobar, tesis, norma y teoría (Dávila Newman, 2006).

La investigación comenzó con un enfoque inductivo, basado en la observación directa de las pantallas electrónicas en las aulas de TI y el software de la ULEAM Extensión El Carmen, con este método, se recopilaron datos específicos de su estado físico, la frecuencia de uso y las medidas de seguridad actuales.

- **Método Deductivo.**

El método deductivo confía en la razón para obtener ideas concretas de ideas amplias ya probadas, usándolas en casos particulares como si fueran lentes especiales, siendo el primer método científico utilizado desde la Antigua Grecia, su limitación principal es que garantiza validez lógica, pero no necesariamente veracidad y para superar esto, los científicos verifican hipótesis mediante experimentos alineados con la realidad (Prieto Castellanos , 2017).

Se aplicó un enfoque deductivo partiendo desde las ideas base de la norma ISO 27001 y lo que se sabe de proteger datos. Estas guías amplias se tomaron para analizar los letreros brillantes como cosas valiosas que hay que cuidar.

- **Método Analítico.**

Este proceso cognoscitivo consiste en descomponer un objeto de estudio, separando cada una de las partes del todo para estudiarlas en forma individual (Bernal Torres, 2010).

El enfoque analítico fue crucial para desglosar el objeto de estudio en componentes clave donde se examinaron por separado la seguridad física del hardware, la configuración del software, los procedimientos de uso y el nivel de formación del personal.

- **Método Sintético.**

El método sintético junta piezas e ideas ya vistas para armar una idea grande o teoría que explique bien lo que se estudia. Este método ayuda a unir pedazos sueltos en algo que tenga sentido, haciendo más fácil entender cómo se conectan las cosas y cuáles son las reglas básicas (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

Después de un análisis detallado de cada componente, se integró la información para armar una idea completa. Este modo de hacerlo nos dejó atar los cabos sueltos y crear un plan de revisión de seguridad que mezclaba barreras reales, virtuales y de protocolo.

3.4 Fuentes de información de datos.

Dentro de la ULEAM Extensión El Carmen se pudo identificar que actualmente no cuentan con una política, un manual de uso de las pantallas de las aulas de los estudiantes de las carreras de TI y Software.

3.4.1 Fuentes primarias – Fuentes secundarias

3.4.1.1 Encuesta.

El sondeo o encuesta es un método científico de recolección de datos de carácter cuantitativo que permite recopilar información sobre opiniones, creencias y/o actitudes de los sujetos estudiados e indagar acerca de temas múltiples, tales como pautas de conducta o consumo, prejuicios sociales, trayectorias académicas, laborales, sociales, entre otros aspectos (Maradi, Archenti, & Piovani , 2010).

La encuesta se utilizó como un método masivo de recolección de datos, para así identificar los posibles riesgos y justificar la problemática.

3.4.1.2 Entrevista.

La entrevista se define como "una conversación que se propone con un fin determinado distinto al simple hecho de conversar". Es útil para investigar cosas a fondo, para obtener datos e información detallada sobre un tema en particular, como hurgar en sus rincones más escondidos (Díaz Bravo, Torruco García, Martínez Hernández, & Varela Ruiz, 2013).

La entrevista se usó como un método de recolección de información para corroborar los datos obtenidos de la encuesta, además de proporcionar un punto de vista profesional.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población.

El *universo* o *población* es el conjunto de elementos estudiados para extraer conclusiones estadísticas o teóricas. La *población marco* es el grupo concreto del que se toma la muestra, y la *población objetivo*, el conjunto al que se extrapolan los resultados. El tamaño poblacional se denota como *N* (López Roldán & Fachelli, 2015).

La Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen cuenta con varias carreras, desde licenciaturas, ingenierías, tecnologías, etc. Para la realización de mi investigación me enfocare en las carreras de Ingeniería en TI y Software, que se encuentran en el segundo piso de la planta central, dando un total de **242** estudiantes de población.

3.5.2 Muestra.

El muestreo es el proceso de seleccionar un conjunto de individuos de una población con el fin de estudiarlos y poder caracterizar el total de la población (Ochoa, 2015).

La muestra se tomó de los estudiantes de la ULEAM Extensión el Carmen, teniendo así solo a los estudiantes de las carreras de TI y Software.

El tipo de muestra fue una muestra de población finita, que es aplicable cuando conocemos nuestra población, la cual es de **242**, la formula a usar fue la siguiente:

$$n = \frac{N * p * q * Z^2}{e^2(N-1) + p * q * z^2}$$

Ilustración 7 Fórmula para calcular la Muestra

Donde **n** es el tamaño de la muestra, **N** es el tamaño de la población total (es decir, el número total de elementos en la población), **p** es la proporción esperada de la característica que

se está estudiando (normalmente se utiliza p=0.5 si no se conoce), **q** es el complemento de p, calculado como q=1−p, **Z** es el valor crítico de la distribución normal asociado al nivel de confianza deseado (por ejemplo, para un nivel de confianza del 95 %, Z≈1.96Z), mientras que **e** es el margen de error aceptable (también conocido como precisión), generalmente expresado como un porcentaje (por ejemplo, e=0.05 para un error del 5 %).

Usando un nivel de confiabilidad del 90% y un nivel de error del 5%, arrojo un total de 128 para el tamaño de la muestra.

Nivel de confiabilidad:

ERROR CON UN NIVEL DE CONF. DEL 90%	5,0%

Cálculo de la muestra:

INTRODUZCA EL MARGEN DE ERROR DESEADO **e**	5,0%
INTRODUZCA EL TAMAÑO DE LA POBLACION **(N)**	242
INTRODUZCA EL VALOR DE **p**	0,5
INTRODUZCA EL VALOR DE **q**	0,5

TAMAÑO DE LA MUESTRA DE ACUERDO AL ERROR Y AL NIVEL DE CONFIANZA DESEADO	
TAMAÑO DE LA MUESTRA PARA UN N. DE CONF. DEL 90%=	128

3.5.3 Técnica de muestreo.

Se utilizó para este tipo de estudio el muestreo aleatorio simple puesto que el muestreo aleatorio simple se aplica, fundamentalmente, en investigaciones sobre poblaciones pequeñas, plenamente identificables (Rodríguez Osuna, 2001).

3.5.4 Tamaño de la muestra.

La muestra según Elsa y Marigina (2023), el muestreo es un procedimiento por el cual algunos miembros de una población se seleccionan como representativos de la población completa.

El tamaño de la muestra se sacó de una población de **242** dando como resultado al aplicar la fórmula una muestra de **128.**

3.5.5 Análisis de las herramientas de recolección de datos a utilizar.

Las técnicas que se utilizaron en la presente investigación son la entrevista y la encuesta. Para la recopilación de información se utilizaron las técnicas de la encuesta tipo cuestionario

que son encuestas estructuradas con preguntas cerradas y entrevista usando como instrumento un cuestionario.

Se aplicaron las encuestas a los estudiantes y la entrevista al director de carrera del área de TI y Software.

3.5.5.1 Entrevista.

Dirigida a: Director de carrera de la carrera de TI y Software de la ULEAM Extensión El Carmen.

Objetivo: Realizar un diagnóstico acerca de la situación actual y uso de las pantallas.

3.5.5.2 Encuesta.

En la respectiva investigación se aplicó una encuesta a los estudiantes de TI y Software para diagnosticar el estado actual y uso de las pantallas de las aulas de las carreras de TI y Software. Se empleó mediante la plataforma Forms de Google.

Dirigida a: Estudiantes de las carreras de TI y Software.

Objetivo: Realizar un diagnóstico acerca del uso y estado actual de las pantallas.

3.5.5.3 Estructura de los instrumentos de recolección de datos aplicados.

La encuesta cuenta con un total de 13 preguntas, siendo 10 preguntas de si y no, una pregunta de orden numérica, donde 5 es el nivel más bajo y uno el más alto en cuanto a seguridad, además de dos preguntas con 3 opciones a elegir, donde las respuestas son NUNCA, AVECES y SIEMPRE.

La entrevista cuenta con un total de 13 preguntas, al igual que la encuesta, con la diferencia que las respuestas son más abiertas, dando la capacidad al entrevistado de argumentar sus respuestas.

3.5.6 Plan de recolección de datos.

Actividad	Fecha	Descripción
Encuesta	11/12/24	Se encuesto mediante un formulario en Forms, con un conjunto de 13 preguntas.
Entrevista	22/12/24	Se realizo una entrevista de forma presencial al director de carrera de TI y Software,

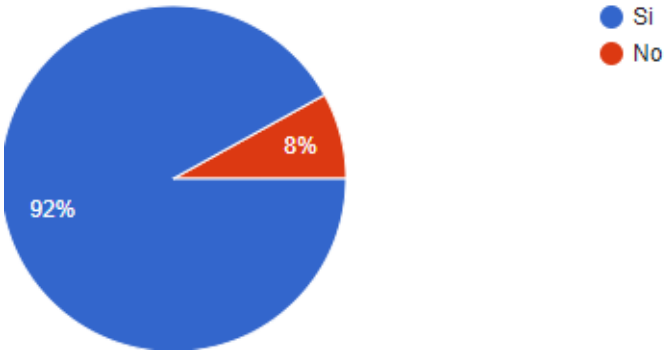
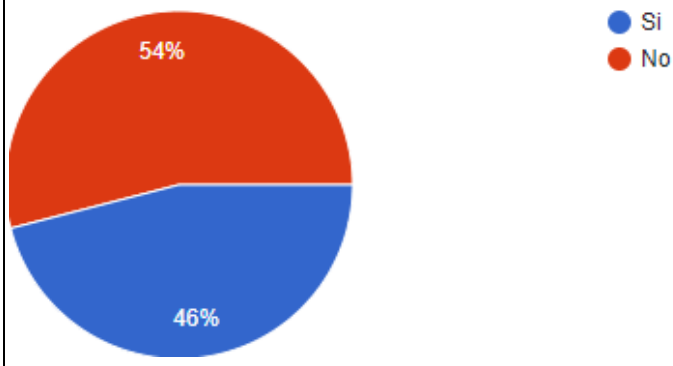
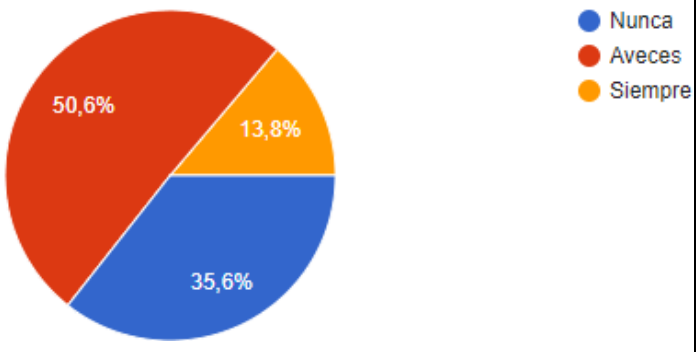
		mediante un conjunto de preguntas pre formuladas.

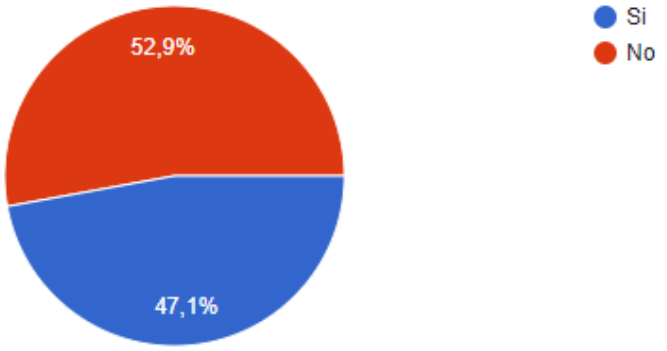
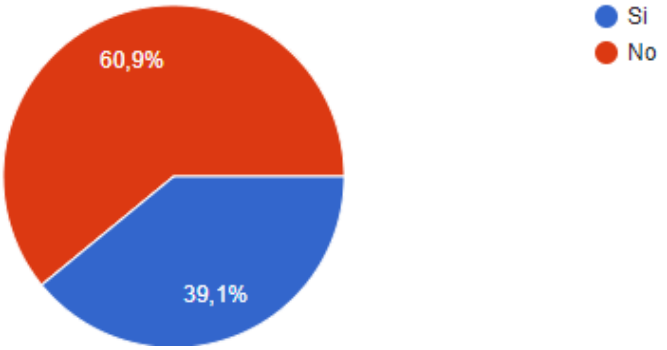
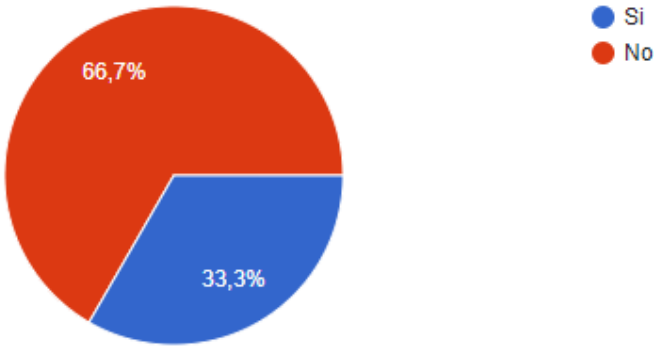
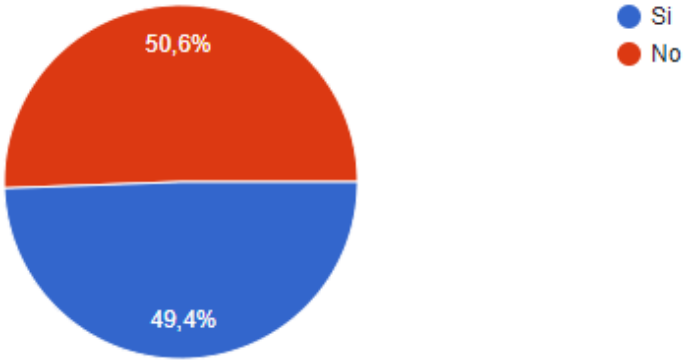
Tabla 1 Plan de recolección de datos

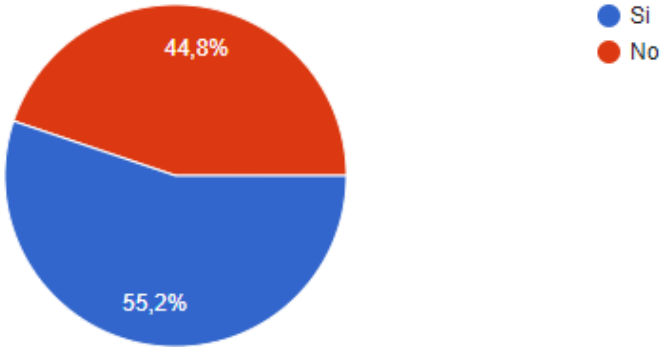
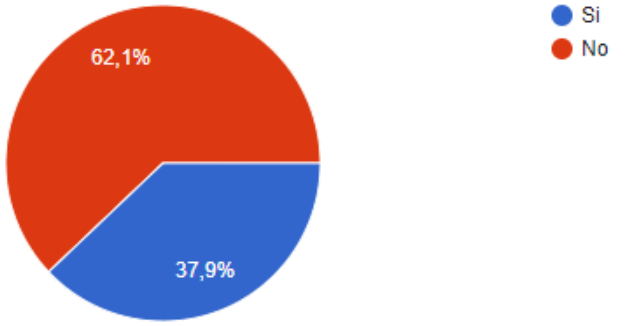
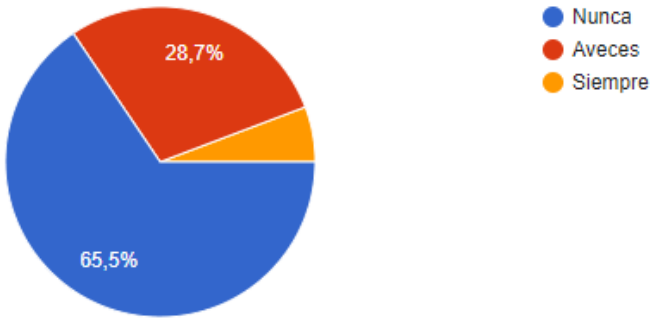
3.6 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos

Encuesta:

Pregunta	**Grafico**	**Interpretación**
¿Usa regularmente las pantallas electrónicas de las aulas como método de enseñanza y/o aprendizaje?		Casi el total de los encuestados supieron declarar que usan las pantallas propósitos educativos.
¿Conoce de la existencia de un manual de uso exclusivo de las pantallas electrónicas?		Un poco más de la mitad de los encuestados supieron decir que conocen de la existencia de un manual de uso de las pantallas.
¿Al momento de ingresar a las aulas, encuentra encendidas o apagadas las pantallas electrónicas?		Un poco más de la mitad indicaron que encuentran a veces encendidas las pantallas, mientras que una tercera parte dice que nunca.

Pregunta	Grafico	Interpretación
¿Ha usado las pantallas para otra actividad que no sea académica?		Mas de la mitad de los encuestados no ha usado las pantallas para una actividad que no sea académica.
¿Conoce usted sobre el tiempo de vida útil de cada pantalla electrónica?		Mas de la mitad de las respuestas indicaron que no conocen el tiempo de vida útil de las pantallas.
¿Ha recibido capacitaciones para el uso y manejo de las pantallas electrónicas?		Mas de la mitad de los encuestados dicen no haber recibido capacitaciones para manejar las pantallas.
¿Ha recibido alguna recomendación o directriz sobre el uso y manejo de las pantallas electrónicas?		Un poco más de la mitad de las repuestas indican que no han recibido alguna recomendación para el manejo de las pantallas.

Pregunta	Grafico	Interpretación
¿Se han registrado incidentes en cuanto al uso y funcionamiento de las pantallas electrónicas?		Más de la mitad de los encuestados expresó que han presenciado incidentes en las pantallas.
¿Existe algún método de seguridad en las pantallas para evitar que sean manipuladas y/o hurtadas?		Un poco más de la mitad indican que no existe un método para mantener las pantallas seguras.
¿En alguna ocasión ha llegado y la pantalla de su aula no está?		Más de la mitad de las respuestas dicen que cuando han llegado al salón encuentran las pantallas ahí, mientras que cerca de la tercera parte dice que a veces.

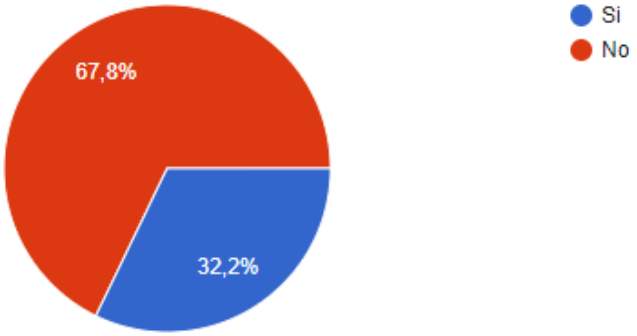
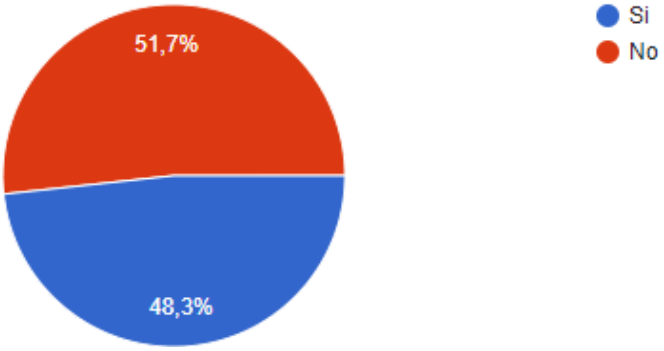
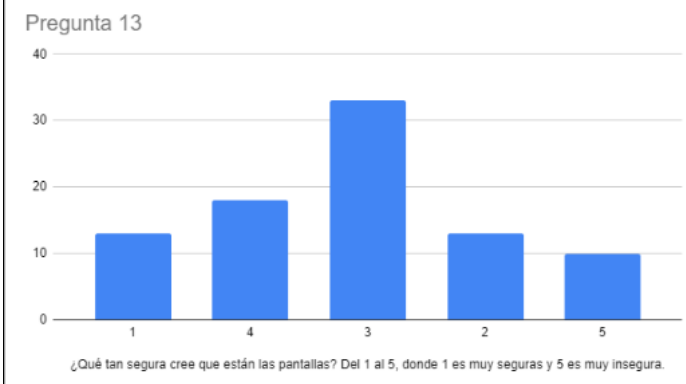
Pregunta	Grafico	Interpretación
¿Ha tenido que mover las pantallas a otro lugar fuera de su respectiva aula?		Más de la mitad de los encuestados supieron decir que no han movido las pantallas fuera del aula.
¿Existe un regulador de voltaje para las pantallas que las proteja de las variaciones de voltaje?		Un poco más de la mitad de las respuestas dicen que no existe un regulador de voltaje.
¿Qué tan segura cree que están las pantallas? Del 1 al 5, donde 1 es muy seguras y 5 es muy insegura.		El mayor porcentaje de las respuestas dicen que las pantallas están medianamente seguras, el menor porcentaje dice que están muy inseguras, siguiendo un pequeño porcentaje dice que son muy seguras.

Tabla 2 Tabulación y Análisis de Datos

- **Entrevista al director de carrera de TI y Software**

N°	Pregunta	Respuesta	Interpretación
1	¿Cómo se utilizan las pantallas electrónicas en las aulas como parte del proceso de enseñanza y aprendizaje en la institución?	Reemplazan a los proyectores, son táctiles, permiten anotaciones, guardar contenido y se usan para presentaciones.	Las pantallas facilitan el aprendizaje interactivo y mejoran la enseñanza respecto a los proyectores tradicionales.
2	¿Está al tanto de la existencia de algún manual o guía específica para el uso de las pantallas electrónicas? Si no, ¿cree que sería útil contar con uno?	Sí, existe un manual en la página de la universidad, pero muchos docentes no lo encuentran; la mayoría aprendió en capacitaciones.	Existe un recurso formal, pero su difusión es deficiente, lo que obliga a depender de capacitaciones previas.
3	¿Qué otros usos, además de los académicos, ha observado o considera que podrían darse a las pantallas electrónicas?	Se pueden usar con software especializado, actualmente solo se emplea software básico.	Existe potencial de uso más avanzado, pero se limita por falta de integración de herramientas específicas.
4	¿Qué conocimiento tiene sobre la vida útil de las pantallas electrónicas y cómo cree que esta información se gestiona dentro de la institución?	Vida útil estimada de 4 a 6 años; no hay información oficial ni sobre garantías.	Falta de gestión formal sobre la durabilidad y mantenimiento, lo que puede afectar su planificación.
5	¿Ha recibido o considera necesario recibir capacitación para optimizar el uso y manejo de las pantallas electrónicas?	Sí, los docentes recibieron capacitación en su momento.	Se ha dado formación inicial, aunque sería recomendable reforzarla para optimizar el uso.
6	¿Qué estrategias o recomendaciones se han compartido con los estudiantes sobre el uso responsable de las pantallas electrónicas?	Se recomienda cuidarlas, evitar golpes o líquidos, y usarlas solo para estudiar.	Existe concienciación básica de cuidado y uso responsable, aunque limitada a recomendaciones generales.
7	¿Ha habido situaciones o incidentes relacionados con el uso o funcionamiento de las pantallas? ¿Cómo se manejaron?	Contraseñas de fábrica bloqueaban funciones; también se reportó presencia de hormigas. TI se encargó del mantenimiento.	Los problemas han sido solucionados de manera reactiva, mostrando la necesidad de un protocolo preventivo.
8	¿Qué medidas se toman respecto a la seguridad de las aulas, incluyendo el cierre de puertas, al terminar las clases?	Solo se cierran las puertas; no hay cámaras en aulas.	La seguridad es mínima y depende del cierre físico de las aulas, lo que deja vulnerabilidades.

N°	Pregunta	Respuesta	Interpretación
9	¿Qué mecanismos existen para proteger las pantallas electrónicas y evitar su manipulación no autorizada?	No hay mecanismos específicos; se confía en el personal y conserjes para reportar.	Falta un control formal, lo que expone a las pantallas a posibles manipulaciones indebidas.
10	¿Ha habido ocasiones en que las pantallas han tenido que ser trasladadas fuera de las aulas? Si es así, ¿cuáles fueron las razones?	Sí, fueron movidas para una capacitación.	El traslado es poco frecuente y se hace solo en casos puntuales.
11	¿Qué precauciones se toman al mover las pantallas electrónicas para garantizar su integridad?	Se trasladan con cuidado, usando su base móvil y con apoyo de dos personas.	Existen medidas prácticas de transporte, lo que reduce riesgos de daños durante movimientos.
12	¿La institución cuenta con sistemas como reguladores de voltaje para proteger las pantallas de variaciones eléctricas? ¿Cómo se asegura su buen funcionamiento?	Sí, tienen reguladores que cortan la energía ante picos eléctricos, pero algunos están desgastados.	Se cuenta con protección eléctrica, aunque la falta de mantenimiento pone en riesgo su eficacia.
13	¿Qué medidas de seguridad, como sistemas de videovigilancia, están implementadas para prevenir el hurto o daño de las pantallas electrónicas?	Solo hay cámaras en pasillos, con poco tiempo de almacenamiento.	La videovigilancia es limitada y constituye una debilidad en la seguridad de los equipos.

Tabla 3 Interpretación entrevista

3.6.2 Presentación y descripción de los resultados obtenidos.

En cuanto a saber si existe un manual para usar las pantallas, más de la mitad dijo que sí lo sabe. Pero el director dijo que, aunque está en la web, muchos no lo hallan fácil y aprenden por otro lado. Esto muestra que, aunque exista el manual, no se encuentra, por lo que profes y alumnos batallan para encontrarlo.

En cuanto a las recomendaciones para un uso adecuado de las pantallas, más de la mitad dijo que nadie les ha dicho nada formal. Por otro lado, el director aseguró que se dan consejos para usar bien las cosas y que no se dañen. Esta diferencia en lo que piensan muestra que no se habla claro y que las reglas no le llegan bien a todos los que usan las pantallas.

Entonces, cuando se trata de mantener las pantallas a salvo de ser metido o robado, muchos estudiantes (como 60%) dijeron que no hay una manera fácil de hacerlo El director dijo que no están poniendo en su lugar ningún sistema específico, solo con la esperanza de que

los usuarios hagan lo correcto y confíen en la palabra del personal sobre él, esto muestra que nos faltan cosas sólidas para mantener nuestro equipo seguro y reduciendo las posibilidades de que se destrocen o pierdan.

3.6.3 Informe final del análisis de los datos (conclusiones para el marco investigativo)

Causa 1: Uso incorrecto de los equipos por desconocimiento

Los datos de la encuesta son claros: casi todos los estudiantes usan las pantallas electrónicas para sus estudios, lo que las convierte en una pieza fundamental de su aprendizaje. El problema es que más del 60% de ellos admite no haber recibido ninguna capacitación formal sobre cómo usarlas correctamente. Básicamente, las están utilizando a base de prueba y error, sin aprovechar todo su potencial.

Por si fuera poco, la entrevista con el director de carrera nos confirmó algo parecido desde el lado de los docentes. Aunque se les dio una formación inicial y existe un manual en la web de la institución, muchos profesores ni siquiera saben que está ahí o simplemente no lo consultan. Las recomendaciones para los estudiantes se dan de manera informal, sin un plan ni seguimiento. Esto deja un vacío enorme entre lo que la institución quiere lograr y lo que realmente pasa en las aulas.

En resumen, el problema no es que no haya guías o manuales, sino que nadie se ha encargado de que esa información llegue a quienes la necesitan, sea fácil de encontrar y se mantenga al día. Esta situación acorta la vida útil de las pantallas, aumenta los riesgos de que algo salga mal y hace que la inversión en tecnología no se aproveche como debería. Es urgente mejorar la forma en que se capacita, se supervisa y se controla el uso de estos equipos.

Causa 2: Falta de seguridad física y digital

Lo que muestra la encuesta es algo inquietante: casi el 60% de los chicos cree que no hay seguridad suficiente. Se siente que los equipos están solo 'más o menos' seguros, dando miedo a que los roben o los rompan."

Hablando con el director de la carrera, vi que esto era verdad. No hay sistemas que protejan de verdad y lo único que se hace es cerrar las clases, y las cámaras solo ven los pasillos y graban un rato. El director aceptó que esto es un problema serio que hay que arreglar ya.

Está claro que hay una falla grave en cómo se protegen las pantallas, tanto física como digitalmente. Esta vulnerabilidad las expone a robos, usos no autorizados y daños que podrían evitarse con mejor supervisión. Para solucionar esto, se sugiere instalar cámaras dentro de las aulas, crear reglas más estrictas sobre quién puede acceder a ellas, supervisar mejor al personal de limpieza y llevar un registro de quién usa qué y cuándo.

Causa 3: Carencia de mantenimiento y control

Un dato revelador de la encuesta es que una buena parte de los estudiantes no sabe si las pantallas tienen reguladores de voltaje o alguna protección eléctrica. Más de la mitad ni siquiera tiene idea de cuánto tiempo se supone que deben durar estos equipos. Esto demuestra una desconexión total con el lado técnico, poniendo en riesgo las pantallas por fallos de luz o por un desgaste que nadie está vigilando.

La entrevista con el director lo confirma: aunque las pantallas sí tienen reguladores, varios están dañados y no hay un control para asegurarse de que funcionen bien. Peor aún, no hay registros oficiales ni actualizados sobre la vida útil de cada pantalla o el estado de sus garantías.

En Conclusión

Queda claro que el problema no tiene una única raíz. Es una mezcla de tres cosas: la gente no sabe usar bien los equipos, no hay medidas de seguridad adecuadas y falta un mantenimiento planificado. Si se atacan estas tres áreas, se reducirán los riesgos, se protegerá la inversión tecnológica y se asegurará que las pantallas sigan siendo una herramienta útil para la educación. Por lo tanto, la necesidad de evaluar el nivel de riesgo existente es crucial para poder la implementación de las debidas correcciones y prevenir incidentes.

CAPÍTULO IV:

4 MARCO PROPOSITIVO

4.1 Introducción

El presente capítulo corresponde a un Sistema de Gestión de Seguridad de la Información a la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. La auditoría se llevó a cabo a las pantallas instaladas en las aulas de las carreras de Tecnologías de la Información y Software, aplicando la metodología ISO 27001.

4.2 Descripción de la propuesta.

Esta propuesta se centra en hacer una revisión para mirar cómo funcionan la seguridad y las normas al usar los aparatos de tecnología para estudiar. Nos fijaremos sobre todo en las pantallas que están en los salones donde se aprende sobre Tecnologías de la Información y Software. Estudiamos los peligros para saber qué tanto riesgo hay de que alguien use mal estas cosas. Para hacer este estudio, usamos la forma de trabajar de la norma ISO 27001, que nos ayuda a encontrar, estudiar y ver los riesgos de los aparatos tecnológicos que tocamos. Así, podemos ver qué fallas hay que puedan poner en peligro la seguridad y el uso de las pantallas.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recursos	Función	Actividad
1	Ing. Bladimir Mora	Coordinador de la carrera de TI y Software	Participó brindando información como coordinador de carrera mediante una entrevista.
1	Ing. Clara Pozo	Responsable de brindar asesoramiento de tesis.	Participó guiando con su conocimiento en el desarrollo de este trabajo de titulación.
1	Anthony Vélez	Investigador	Investigador encargado de desarrollar el trabajo de titulación.
128	Estudiantes de la carrera de TI y Software.	Usuarios de las pantallas de las aulas de la carrera de TI y Software.	Brindaron información relevante del uso de las pantallas en la fase de diagnóstico.

Tabla 4 Recursos Humanos

4.3.2 Tecnológicos

Cantidad	Recurso	Actividad
1	Portátil Lenovo AMD Ryzen 7 12 GB de RAM	Equipo informático utilizado para el desarrollo de la investigación.
1	Teléfono móvil Poco F3 5g con 256GB de almacenamiento y 8 GB de RAM.	Móvil usado para la toma de evidencias durante la realización de la investigación.
8 meses	Conexión a Internet	Usado para investigar sobre el tema del proyecto de titulación
1	Impresora HP	Equipo para las hojas de la encuesta, entrevista y tesis.
1	Paquete de Ofimática	Usado para la tabulación de datos, realización de tesis y presentación del proyecto final.

Tabla 5 Recursos tecnológicos

4.3.3 Económicos (presupuesto)

Cantidad	Descripción	Precio	Subtotal
1	Portátil Lenovo AMD Ryzen 7 12 GB de RAM	$860	$860
1	Teléfono móvil Poco F3 5g con 256GB de almacenamiento y 8 GB de RAM.	$199	$199
1	Paquete de Ofimática	$6	$6
1	Impresora	$300	$300
8	Conexión a Internet	$26	$208
1	Resma de hojas A4	$4	$4
		Total	$1577

Tabla 6 Recursos económicos

4.4 Etapas de acción para el desarrollo de la propuesta.

4.4.1 Fase 1 Planificar

4.4.1.1 Programa de Auditoría

Programa de auditoría informática de seguridad de la información a las pantallas de las carreras de TI y Software de la ULEAM Extensión el Carmen.

Objetivos:

1. Evaluar el nivel de madurez en la gestión de seguridad informática de las pantallas de las carreras de TI y Software según ISO 27001.
2. Identificar los riesgos de seguridad informática a los que están expuestas las pantallas.
3. Elaborar un plan de medidas de seguridad e implementar las más urgentes.

Técnicas y procedimiento	Ref.	Fecha
1.1. Revisar la norma ISO 27001	4.4.1.2	05/05/2025
1.2. Realizar una auditoría Inicial (fase 1 ISO 27001)	4.4.1.3	08/05/2025
2.2. Análisis de riesgos	4.4.1.4	09/06/2025
2.2.1. Elaborar cuestionarios para analizar riesgos	C1	21/05/2025
2.2.2. Tabulación de análisis de riesgos	4.4.1.4.2	11/06/2025
2.2.3. Impacto de análisis de riesgos	4.4.1.4.3	19/06/2025
2.2.4. Valoración de riesgos	4.4.1.4.4	30/06/2025
2.3. Elaborar Informe	5.1	05/07/2025

Realizado por: Anthony Vélez	**Observacion:**
Fecha:	**Revisado por:** **Fecha:**

Ilustración 8 Programa de Auditoría

4.4.1.2 Revisión de IS0 27001

La norma ISO/IEC 27001 establece un marco integral para la gestión de la seguridad de la información en las organizaciones. Su estructura se basa en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar) y comprende las siguientes cláusulas principales:

Según CONSULTORES ISO (2022), es una norma reconocida internacionalmente que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), está orientada a proteger la información sensible de los sistemas.

La ISO 27001 no es una norma enfocada a dar una solución detallada sobre las herramientas o técnicas que se van a utilizar, sino que nos permite identificar, evaluar, tratar y monitorear los riesgos relacionados con la seguridad de la información.

Las fases del método de la norma ISO 27001 son:

Ilustración 9 Método PHVA

En esta tabla listamos las cláusulas que la Norma ISO brinda, desde la 4 hasta la 1

Cláusulas de la Norma ISO 27001	
Cláusula 4: Contexto de la organización	Comprender la organización y su contexto: Identificar los factores internos y externos que afectan la capacidad de lograr los objetivos del SGSI. Comprender las necesidades y expectativas de las partes interesadas: Determinar los requisitos relevantes de las partes interesadas en relación con la seguridad de la información. Determinar el alcance del SGSI: Definir los límites y la aplicabilidad del SGSI. Sistema de gestión de seguridad de la información: Establecer, implementar, mantener y mejorar continuamente el SGSI.
Cláusula 5: Liderazgo	Liderazgo y compromiso: La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI. Política de seguridad de la información: Establecer una política adecuada a los propósitos de la organización. Roles, responsabilidades y autoridades organizacionales: Asignar responsabilidades y autoridades para así asegurar la eficacia del SGSI.
Cláusula 6: Planificación	Acciones para abordar riesgos y oportunidades: Determinar los riesgos y oportunidades que deben abordarse para asegurar que el SGSI pueda lograr sus resultados esperados. Objetivos de seguridad de la información y planificación para alcanzarlos: Establecer objetivos medibles y planificar como lograrlos.
Cláusula 7: Apoyo	Recursos: Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. Competencia: Asegurar que las personas sean competentes en función de la educación, formación o experiencia apropiadas. Concienciación: Asegurar que las personas sean conscientes de la política de seguridad de la información. Comunicación: Determinar las comunicaciones internas y externas pertinentes al SGSI. Información documentada: Establecer y controlar la información documentada requerida por la norma y por la organización.

Cláusula 8: Operación	Planificación y control operacional: Implementar los procesos necesarios para cumplir con los requisitos del SGSI. Evaluación de riesgos de seguridad de la información: Realizar evaluaciones periódicas de riesgos. Tratamiento de riesgos de seguridad de la información: Implementar planes de tratamiento de riesgos.
Cláusula 9: Evaluación del desempeño	Seguimiento, medición, análisis y evaluación: Determinar qué necesita ser monitoreado y medido. Auditoría interna: Realizar auditorías internas en intervalos planificados. Revisión por la dirección: La dirección debe revisar el SGSI en intervalos planificados.
Cláusula 10: Mejora	No conformidad y acción correctiva: Reaccionar ante las no conformidades, tomar acciones para controlarlas y corregirlas. Mejora continua: Mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.

Tabla 7 Clausulas Norma ISO 27001

4.4.1.3 Auditoría Inicial

El análisis de brechas es una herramienta fundamental para evaluar el estado actual del SGSI frente a los requisitos de la norma ISO 27001. Este proceso permite identificar las diferencias entre la situación actual y la deseada, facilitando la planificación de acciones correctivas.

Esta tabla determina el nivel de madurez de un SGSI, desde la no existencia, hasta la presencia total de uno.

Nivel de Madurez	
Nivel 0 - No existencia	El control no está implementado ni documentado.
Nivel 1 - Ad- hoc	El control se aplica de manera informal y reactiva.
Nivel 2 - Ejecutado	El control está implementado, pero no documentado formalmente.
Nivel 3 - Definido	El control está implementado y documentado.
Nivel 4 - Manipulable y mediable	El control es monitoreado y medido regularmente.
Nivel 5 - Optimizado	El control es continuamente mejorado mediante procesos definidos.

Tabla 8 Nivel de Madurez

Tabla donde después de realizar la prueba de cumplimiento de requisitos, sacamos un puntaje, que, según la cantidad obtenida, se determina si existe o no existe el control.

Nivel Medio Cumplimiento = Puntuación total de cada Control /Número de controles	
Puntaje < 1.65	El control no cumple con los requisitos.
Puntaje entre 1.66 y 3.25	El control cumple parcialmente con los requisitos.
Puntaje > 3.26	El control cumple con los requisitos de la norma.

Tabla 9 Cumplimiento de requisitos

4.4.1.3.1 Cumplimiento de requisitos de la Norma ISO 27001

En la siguiente tabla se muestran el cumplimiento de requisitos y los criterios a evaluar según lo requerido en el programa de auditoría, los ítems que contiene cada requisito, los criterios que tiene y los que se van a evaluar.

Requisitos	**Ítems**	**Criterios**	**Criterios a evaluar**
4. La Organización y su Contexto	4	8	7
5. Liderazgo	3	9	8
6. Planificación	2	8	7
7. Soporte	5	10	10
8. Operación	3	8	8
9. Evaluación del desempeño	4	7	7
10. Mejora	2	3	3

Tabla 10 Cumplimiento de requisitos

4.4.1.3.2 Cumplimiento de los controles de la Norma ISO 27001

En esta tabla se muestran controles de seguridad que, según nuestro análisis, son aplicables en la auditoría, cada ítem contiene los criterios a evaluar de acuerdo con lo requerido en la auditoría.

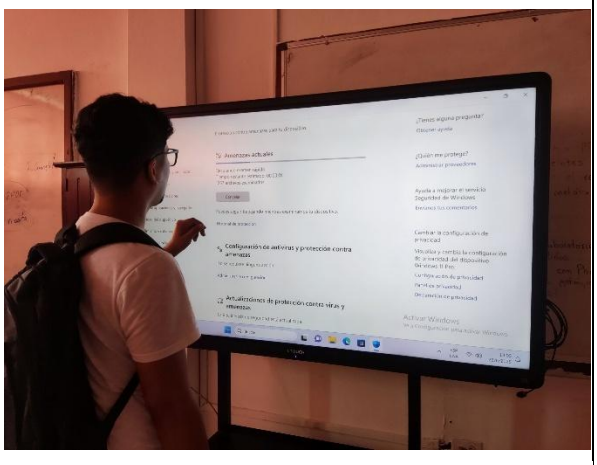
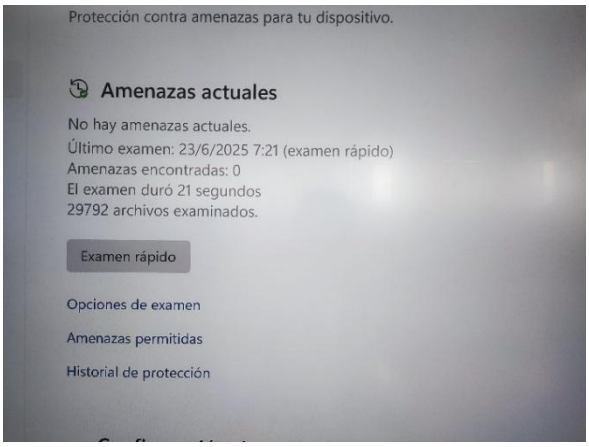
N°	Clausula	Descripción	Ítems	Criterios aplicables
A5	Políticas de Seguridad de la Información	Requiere que se definan políticas de la seguridad de la información para que sean aprobadas por la dirección, deben publicarse y comunicarse a los empleados y partes externas pertinentes	2	2
A6	Organización de la seguridad de la información.	Este dominio se enfoca en establecer una estructura organizativa para la gestión de la seguridad de la información.	7	2
A8	Gestión de activos	Proteger los activos de información (hardware, software, datos, personas, etc.) mediante su adecuada identificación, clasificación, uso y eliminación.	10	3
A11	Seguridad física y del entorno	Proteger los activos físicos y las instalaciones frente al acceso no autorizado, daños o interferencias físicas.	14	6

Tabla 11 Cumplimiento de controles

4.4.1.3.3 Aplicación de Instrumentos

Se llevó a cabo la realización de la entrevista para la recolección de información al director de carrera de TI y Software, además de la revisión de cada una de las aulas y pantallas.

Pasos de aplicación de auditoria	
• Para iniciar con la aplicación se realizó la ejecución de la auditoria inicial, la cual consta del cumplimiento de requisitos y el cumplimiento de controles, para realizar el análisis de la brecha GAP.	 *Ilustración 10 Entrevista con el director de carrera del área de TI y Software.*

Pasos de aplicación de auditoria	
• Para responder las preguntas relacionadas con configuraciones y software antivirus se procedió a la inspección detallada de cada uno de los sistemas operáticos de cada una de las pantallas.	 *Ilustración 11 Revisión del antivirus instalado en las pantallas.*
• Para constatar la existencia del nivel de riesgo a virus en las pantallas se procedió a la revisión de el ultimo análisis de antivirus de cada pantalla, donde se muestra que es automático y se realiza constantemente.	 *Ilustración 12 Ultimo análisis de antivirus.*

Pasos de aplicación de auditoria	
• En el siguiente paso se procedió a realizar el análisis de las áreas de protección activas dentro de Windows Defender.	 *Ilustración 13 Revisión de la protección de Windows Defender.*
• Luego de la aplicación del instrumento del cumplimiento de controles, el cual se realizó al director de carrera de TI y Software, este será usado para el posterior análisis de la Brecha GAP.	➔ Véase en Anexo F Cuestionarios, cuestionario de cumplimiento de controles.
• Aplicación de instrumento del cumplimiento de requisitos, para realizar también el análisis de la Brecha GAP.	➔ Véase en Anexo F Cuestionarios, cuestionario cumplimiento de requisitos
• Aplicación de instrumento para la recolección de datos para el posterior análisis e identificación de los riesgos a los que pueden estar expuestas las pantallas.	• Véase en Anexo F Cuestionarios, cuestionario de riesgos aplicado.

Tabla 12 Pasos de Auditoria.

4.4.1.3.4 Instrumento de recolección de requisitos

Tabla correspondiente a los cumplimientos de requisitos, el cual ayuda a determinar el nivel de madurez de los requisitos enmarcado en la ISO 27001.

CUESTIONARIO DE CUMPLIMIENTO DE REQUISITOS			C1 Pag. 1 - 3					
		Preguntas	**1**	**2**	**3**	**4**	**5**	**Observaciones**
1	La Organización y su Contexto	¿Están identificados los objetivos del SGSI Sistema de Gestión de la Seguridad de la Información?						
2		¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?						
3		¿Se han identificado las partes interesadas?						
4		¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?						
5		¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?						
6		¿Se ha determinado el alcance del SGS y se conserva información documentada?						
7		¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?						
8	Liderazgo	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?						
9		¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?						
10		¿Se ha definido una Política de la Seguridad de la Información?						
11		¿Se ha establecido un marco que permita el establecimiento de objetivos?						
12		¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?						
13		¿Se mantiene información documentada de la política del SGSI y de sus objetivos?						
14		¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?						
15		¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?						
16	Planificación	expectativas de las partes interesadas en relación a la Seguridad de la Información?						
17		¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?						
18		¿Se ha definido un proceso de tratamiento de riesgos?						
19		¿Se han establecido criterios para elaborar una declaración de aplicabilidad?						
20		¿Se mantiene información documentada de los puntos anteriores?						
21		¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?						

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

Ilustración 14 Instrumento Cumplimiento de requisitos

4.4.1.3.5 Tabulación de los datos correspondientes a requisitos

Una vez recolectada información necesaria se ingresaron los datos del cumplimiento de requisitos, tomados luego de aplicada la herramienta que brinda la Norma ISO 27001, evaluando en una escala del 1 al 5, donde 1 significa que no existe y 5 que está optimizado.

REQUISITOS		PREGUNTA	CUMPLIMIENT
4 La Organización y su Contexto	4.1 Entendiendo la Organización y su contexto	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	3
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	3
			4
	4.2 Expectativas de las partes interesadas	1.- ¿Se han identificado las partes interesadas?	3
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	4
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	4
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	3
	4.4 SGS Sistema de Gestión de la Seguridad de la información	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	4

Ilustración 15 Tabulación de requisitos

Luego tabulamos los datos para determinar el nivel cumplimiento de requisitos, obteniendo una brecha significativa del 31%, pero un nivel de cumplimiento del 69%, siendo muy favorable.

REQUISITO DE ISO 27001	Cumple la Norma	BRECHA
4. Organización y Contexto	70%	30%
5. Liderazgo	80%	20%
6. Planificación	71%	29%
7. Soporte	66%	34%
8. Operación	70%	30%
9. Evaluación y desempeño	66%	34%
10. Mejora	60%	40%
Promedio Requisitos	**69%**	**31%**

Tabla 13 Análisis de requisitos

4.4.1.3.6 Instrumento de recolección de controles

Controles con los ítems seleccionados, el cual se aplicó al director de carrera de TI y Software, el Ing., Bladimir Mora.

CUESTIONARIO DE CUMPLIMIENTO DE CONTROLES			C1		
			Cumple		Pag. 1 - 2
Preguntas			SI	NO	Observaciones
1	A5	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?			
2		¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?			
3	A6	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?			
4		¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?			
5		¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?			
6		¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?			
7		¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?			
8	A8	¿Se ha realizado un inventarios de activos que dan soporte al negocio y de Información?			
9		¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?			
10		¿Se han establecido normas para el uso de activos en relación a su seguridad?			
11		¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?			
12		¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?			
14		¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado			
15		¿Existen procedimientos establecidos para la eliminación de soportes?			
16		¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado etc.			
17	A11	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?			

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

Ilustración 16 Instrumento Cumplimiento de Controles

4.4.1.3.7 Tabulación de datos de controles obtenidos

Una vez registrados los datos, para verificar el cumplimiento de controles se usó 0, 1 y 2, donde 0 significa que no cumple, 1 que si cumple y 2 que no aplica.

				SI	*1*
				NO	*0*
				No Aplica	*2*
Numeral	Clausula		Requisito	CUMPLE	
A5	Políticas de Seguridad de la Información	A5.1 Dirección de gestión para la seguridad de la información	1.- ¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?	1	*1*
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	0	*2*
A6	Organización de la Seguridad de la Información	A6.1	1.- ¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	1	*3*
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	0	*4*
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	0	*5*
			4.- ¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	0	*6*
			5.- ¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?	0	*7*

Ilustración 17 Tabulación de controles

En la siguiente tabla se muestran todas las cláusulas que luego de un análisis se tomaron para la evaluación, además de los controles evaluados, contando cuales se cumplen y cuales no, arrojando un porcentaje de cumplimiento y no cumplimiento, para el posterior análisis.

CLAUSULAS	Total controles	Controles excluidos	Controles evaluados	Controles que cumplen	%Cumplimiento	% no Cumple
A5 Políticas de Información	2	0	2	1	50%	50%
A6 organización de Seguridad de la Información	7	0	7	1	14%	86%
A8 gestión de activos	10	0	10	5	50%	50%
A11 Seguridad Física y del entono	14	0	14	6	43%	57%

Tabla 14 Conteo de controles evaluados.

Luego tabulamos los datos obtenidos, dando como resultado el nivel de cumplimiento de los controles, el cual arrojó un resultado de que el 61% de los controles no se cumplen.

CLAUSULAS	%Cumplimiento	% no Cumple
A5 Políticas de Información	50%	50%
A6 organización de Seguridad de la Información	14%	86%
A8 gestión de activos	50%	50%
A11 Seguridad Física y del entono	43%	57%
PROMEDIO	***39%***	***61%***

Tabla 15 Análisis de resultados del cumplimiento de controles

4.4.1.4 Análisis de riesgos

4.4.1.4.1 Elaborar cuestionarios para analizar riesgos.

Para la elaboración de los cuestionarios se tomaron en consideración los riesgos a los cuales están más propensas las pantallas, usando preguntas para evaluar la existencia o ausencia de controles, son 4 cuestionarios los cuales cuentan con 25 preguntas cada uno, tienen una estructura checklists, de respuesta Si o No, correspondiente a los controles de Robo, Malware, Incendio y Daños.

Aula N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 1 - 4
	Preguntas: Robo	**SI**	**NO**	**Observaciones**
1	¿El aula donde está la pantalla cuentan con cerraduras de seguridad en puertas y ventanas?			
2	¿Se utiliza un sistema de control de acceso físico para ingresar al aula con pantalla?			
3	¿Hay cámaras de videovigilancia instaladas en el aula donde está la pantalla?			
4	¿Las cámaras están en funcionamiento y grabando continuamente?			
5	¿Existe monitoreo en tiempo real de las cámaras ubicada en el aula con pantalla?			
6	¿Las pantallas están fijadas o ancladas para evitar su sustracción?			
7	¿Se mantiene un registro de las personas que ingresan al aula donde se encuentra la pantalla?			
8	¿El acceso al aula con pantalla está restringido únicamente al personal autorizado?			
9	¿Se han reportado anteriormente robos o intentos de robo en aula con pantalla?			
10	¿El acceso a las aula fuera del horario regular está controlado?			
11	¿Se revisan periódicamente las condiciones de las cerraduras y accesos en el aula con pantallas?			
12	¿La pantalla está etiquetada con código de inventario?			
13	¿Existe un protocolo para el traslado de las pantallas?			
14	¿Los accesos al aula de la pantalla está bien iluminado por la noche?			
15	¿Se han instalado sensores de movimiento en el aula donde está las pantalla?			
16	¿Se realiza un inventario físico periódico de las pantallas instaladas en el aula?			
17	¿Se controlan el número de llaves que dan acceso al aula de la pantalla?			
18	¿Se capacita al personal en prevención de robos?			
19	¿Se ha realizado un análisis de riesgos por robo?			
20	¿El personal sabe cómo actuar ante un robo?			
21	¿Se revisan periódicamente las grabaciones de videovigilancia en dichas aulas?			
22	¿Existe guardias de seguridad que supervise las aulas donde estan las pantallas?			
23	¿Se hacen rondas de seguridad constantes?			
24	¿El sistema de videovigilancia está protegido contra manipulaciones?			
25	¿El aula con pantalla permanece cerrada cuando no está en uso?			

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

Ilustración 18 Identificación de riesgos – Robo

Ver en anexo los demás cuestionarios

4.4.1.4.2 Tabulación de análisis de riesgos

Luego de haber aplicado el cuestionario, se realizó el correspondiente ingreso a un archivo en Excel, organizada en 5 columnas correspondiente a cada aula auditada con la respuesta obtenida de los cuestionarios, donde 0 significa que no cumple y 1 que si cumple:

Cuestionario para Alizar Riesgos Robo	**Aula 204**	**Aula 205**	**Aula 206**	**Aula 208**	**Aula 210**
1. ¿El aula donde está la pantalla cuentan con cerraduras de seguridad en puertas y ventanas?	1	1	1	1	1
2. ¿Se utiliza un sistema de control de acceso físico para ingresar al aula con pantalla?	0	0	0	0	0
3. ¿Hay cámaras de videovigilancia instaladas en el aula donde está la pantalla?	0	0	0	0	0
4. ¿Las cámaras están en funcionamiento y grabando continuamente?	0	0	0	0	0
5. ¿Existe monitoreo en tiempo real de las cámaras ubicada en el aula con pantalla?	0	0	0	0	0
6. ¿Las pantallas están fijadas o ancladas para evitar su sustracción?	0	0	0	0	0
7. ¿Se mantiene un registro de las personas que ingresan al aula donde se encuentra la pantalla?	0	0	0	0	0
8. ¿El acceso al aula con pantalla está restringido únicamente al personal autorizado?	1	1	1	1	1
9. ¿Se han reportado anteriormente robos o intentos de robo en aula con pantalla?	0	0	0	0	0
10. ¿El acceso a las aula fuera del horario regular está controlado?	1	1	1	1	1
11. ¿Se revisan periódicamente las condiciones de las cerraduras y accesos en el aula con pantallas?	1	1	1	1	1
12. ¿La pantalla está etiquetada con código de inventario?	1	1	1	1	1
13. ¿Existe un protocolo para el traslado de las pantallas?	1	1	1	1	1
14. ¿Los accesos al aula de la pantalla está bien iluminado por la noche?	1	1	1	1	1
15. ¿Se han instalado sensores de movimiento en el aula donde está las pantalla?	0	0	0	0	0
16. ¿Se realiza un inventario físico periódico de las pantallas instaladas en el aula?	1	1	1	1	1
17. ¿Se controlan el número de llaves que dan acceso al aula de la pantalla?	1	1	1	1	1
18. ¿Se capacita al personal en prevención de robos?	0	0	0	0	0
19. ¿Se ha realizado un análisis de riesgos por robo?	0	0	0	0	0
20. ¿El personal sabe cómo actuar ante un robo?	1	1	1	1	1
21. ¿Se revisan periódicamente las grabaciones de videovigilancia en dichas aulas?	0	0	0	0	0
22. ¿Existe guardias de seguridad que supervise las aulas donde estan las pantallas?	0	0	0	0	0
23. ¿Se hacen rondas de seguridad constantes?	0	0	0	0	0
24. ¿El sistema de videovigilancia está protegido contra manipulaciones?	0	0	0	0	0
25. ¿El aula con pantalla permanece cerrada cuando no está en uso?	0	0	0	0	0

Tabla 16 Ingreso de datos obtenidos del cuestionario riesgo de robo.

Obtenemos el resultado de cada aula auditada, aplicando una suma del total de los riesgos evaluados, luego se dividen entre controles que significan seguridad y riesgo, dividiendo cada uno por el total de controles evaluados, dando un porcentaje, los cuales dicen el nivel de riesgo que existe y el porcentaje de seguridad.

Total Controles No Aplica:	0	0	0	0	0	**Total Controles No Aplica:**	0
Total Controles Evaluados:	25	25	25	25	25	**Total Controles Evaluados:**	125
Total Seguridad	10	10	10	10	10	**Total Seguridad**	50
Total Riesgo:	15	15	15	15	15	**Total Riesgo:**	75
Porcentaje Seguridad	40%	40%	40%	40%	40%	**Porcentaje Seguridad**	40%
Porcentaje Riesgo:	60%	60%	60%	60%	60%	**Porcentaje Riesgo:**	60%

Tabla 17 Análisis de datos de la aplicación del cuestionario de robo.

4.4.1.4.3 Impacto de análisis de riesgos

El análisis de riesgos permite identificar y evaluar los posibles eventos que pueden afectar la seguridad de la información y la operatividad de los activos críticos de una organización. Mediante la determinación del impacto, se establece el nivel de daño potencial que cada riesgo identificado (como daños a equipos, incendios, robos o malware) podría ocasionar sobre la confidencialidad, integridad y disponibilidad de los recursos tecnológicos. Este método sienta unas bases firmes para jerarquizar las estrategias de seguridad y para establecer las medidas correctivas o preventivas necesarias, garantizando de este modo la operatividad continua y el resguardo de los bienes más valiosos.

Para la realización de este cálculo se usaron valores dados por la norma ISO 27001, los cuales están identificados en niveles, desde el nivel 1, hasta el nivel 5, donde 1 es muy bajo y 5 muy alto.

ESCALA DE IMPACTO		CONSIDERACIONES POR NIVEL
NIVEL 1	MUY BAJO	Cierre temporal de las instalaciones o afectación menor que no impide continuar las actividades. La interrupción no supera las 8 horas y los daños a los activos son limitados, sin mayor repercusión en la mayoría de las instalaciones.
NIVEL 2	BAJO	Interrupciones o daños que requieren atención, pero no afectan de forma significativa la operación general.
NIVEL 3	MEDIO	Afectaciones que demandan intervenciones importantes para restablecer la normalidad operativa.
NIVEL 4	ALTO	Daños graves con interrupciones relevantes, que exigen respuestas inmediatas y podrían comprometer la continuidad operativa.
NIVEL 5	MUY ALTO	Daños irreversibles en las instalaciones, que las vuelven inhabitables. Pérdida o destrucción total de datos y activos, sin posibilidad de recuperación.

Tabla 18 Escala de Impacto.

Para calcular el impacto se usaron tres elementos fundamentales, la confidencialidad, integridad y disponibilidad de los equipos, los cuales ayudaron a calcular el valor del impacto.

IMPACTO

RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL IMPACTO
DAÑO DE EQUIPOS	2	4	4	3
INCENDIO	1	4	5	3
ROBO	4	3	5	4
MALWARE	3	4	4	4

Tabla 19 Calculo de Impacto.

4.4.1.4.4 Valoración de riesgos

Implica identificar posibles amenazas y vulnerabilidades, evaluar la probabilidad y el impacto de estos riesgos, y determinar las medidas apropiadas para mitigarlos. Se trata de averiguar qué probable es una amenaza y qué tan mala podría ser para nuestra información, mirar cosas como mantenerlo en secreto, asegurarse de que sea preciso y asegurarse de que siempre esté allí cuando la necesitemos. Esta evaluación nos brinda una forma sólida e imparcial de descubrir qué riesgos abordar primero, establecer lo que está bien y decidir sobre las medidas de seguridad correctas, asegurándonos de que seguimos funcionando sin problemas y apegarnos a nuestros objetivos.

Para poder calcular el nivel de aparición o probabilidad, se usó una tabla, la cual tiene una escala del 1 al 5, el cual se ubica según la consideración de ocurrencia del evento de riesgo.

ESCALA PARA DETERMINAR EL VALOR DE OCURRENCIA		
NIVEL DE OCURRENCIA (PROBABILIDAD)		
1	MAS BAJO	**1%-10%**
2		**11%-30%**
3		**31%-50%**
4		**51%-75%**
5	MÁS ALTO	**76%-100%**

Tabla 20 Nivel de ocurrencia.

Para valorar el nivel de riesgo se utilizó una tabla con una escala, la cual indica según el color el nivel de riesgo.

NIVEL DE RIESGO

COLOR	RANGO	NIVEL DE RIESGO	MEDIDAS
	DE15 A 25	MUY GRAVE	Implica un punto álgido que pide cuidado veloz antes de hacer cualquier cosa del plan. Se deben poner en marcha acciones de cuidado rápidas y vigilar muy de cerca el peligro señalado.
	DE 9 A 12	IMPORTANTE	Requiere acciones preventivas obligatorias y una supervisión constante de las variables relacionadas durante el desarrollo del proyecto.
	DE 3 A 8	APRECIABLE	Es posible mitigarlo mediante medidas preventivas, siempre que su aplicación sea económicamente factible. En caso contrario, se deben mantener bajo control los factores de riesgo.
	DE 1 A 2	MARGINAL	No demanda medidas inmediatas, pero debe ser objeto de observación continua para evitar su evolución a niveles superiores.

Tabla 21 Escala del nivel de riesgo.

Analizamos el nivel de riesgo al que están expuestas las pantallas, para lo cual tomamos varios valores y calculamos Aparición x Gravedad (el cual sacamos de valor del impacto) y así da el Valor de riesgo.

LEYENDA							
			GRAVEDAD (IMPACTO)				
			MUY BAJO **1**	BAJO **2**	MEDIO **3**	ALTO **4**	MUY ALTO **5**
APARICIÓN (probabilidad)	MUY ALTA	**5**	5	10	15	20	25
	ALTA	**4**	4	8	12	16	20
	MEDIA	**3**	3	6	9	12	15
	BAJA	**2**	2	4	6	8	10
	MUY BAJA	**1**	1	2	3	4	5

Tabla 22 Multiplicación de Aparición y Gravedad.

NIVEL DE RIESGO

COLOR	RANGO	NIVEL DE RIESGO	MEDIDAS
	DE15 A 25	MUY GRAVE	Implica un nivel crítico que exige atención inmediata antes de
	DE 9 A 12	IMPORTANTE	Requiere acciones preventivas obligatorias y una supervisión
	DE 3 A 8	APRECIABLE	Es posible mitigarlo mediante medidas preventivas, siempre que su
	DE 1 A 2	MARGINAL	No demanda medidas inmediatas, pero debe ser objeto de

Tabla 23 Rango de Nivel de riesgo

Tomando todos los datos de las tablas anteriores logramos calcular nuestro Valor de Riesgo.

MATRIZ DE RIESGOS				
Riesgo	**Aparición**	**Gravedad**	**Valor del Riesgo**	**Nivel de Riesgo**
DAÑO DE EQUIPOS	3	3	10	Importante
INCENDIO	2	3	7	Apreciable
ROBO	4	4	16	Muy grave
MALWARE	3	4	11	Importante

Tabla 24 Calculo del Valor de riesgo.

CAPÍTULO V:

5 EVALUACIÓN DE RESULTADOS

5.1 Elaboración Informe

Dirigido al: Dr. Temístocles Bravo Tuárez, decano de la ULEAM Extensión El Carmen.

Tipo de auditoría: Auditoría de Seguridad Informática

Motivo: Desarrollar un proyecto de Titulación.

Objetivos:

- Evaluar el nivel de madurez en la gestión de seguridad informática de las pantallas de las carreras de TI y Software según ISO 27001.
- Identificar los riesgos de seguridad informática a los que están expuestas las pantallas.
- Elaborar un plan de medidas de seguridad e implementar las más urgentes.

Alcance

- Revisar la norma ISO 27001
- Realizar una auditoría Inicial (fase 1 ISO 27001)
- Análisis de riesgos
- Elaborar cuestionarios para analizar riesgos
- Tabulación de análisis de riesgos
- Impacto de análisis de riesgos
- Valoración de riesgos
- Elaborar Informe

Personal relacionado

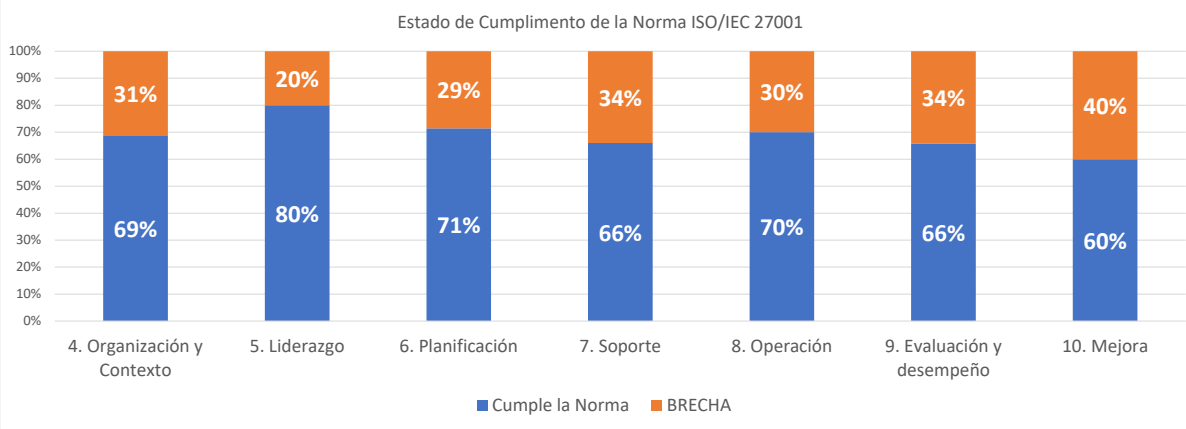
- Director de carrera de las áreas de TI y Software.
- Estudiantes de TI y Software.

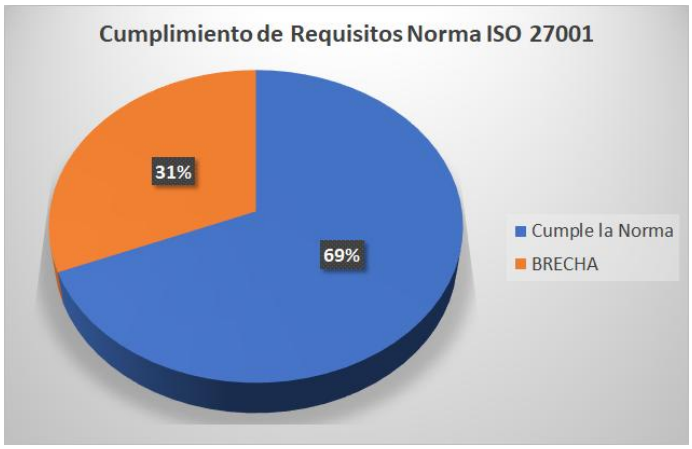
5.1.1 Hallazgos:

Luego de aplicada la auditoría y tomados todos datos necesarios de cada cuestionario, tabulados y graficados, se procede a analizar cada uno los gráficos para evidenciar los hallazgos encontrados con relación a la auditoria según la Norma ISO 27001.

5.1.1.1 Hallazgos correspondientes a los requisitos

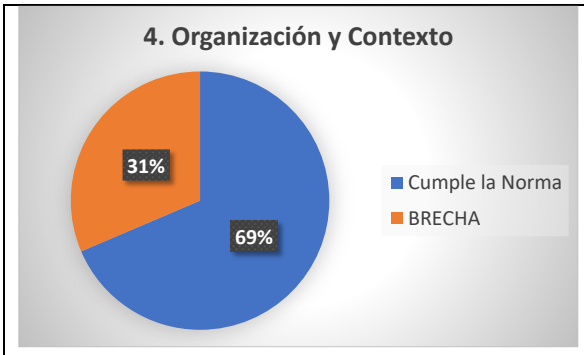
Al ejecutar el instrumento de verificación de la norma ISO 27001 el nivel de madurez que se encontró y la brecha con relación al cumplimiento es el siguiente.





Interpretación: El estado de cumplimiento requisitos de la Norma ISO/IEC 27001 de las pantallas electrónicas es de nivel medio, con un 69%, el requisito que más se cumple es el de los controles Liderazgo con el 80% y mientras que el que tiene menos es el control Mejora con el 60%, los demás se encuentran en un promedio de entre el 66% y el 71%.

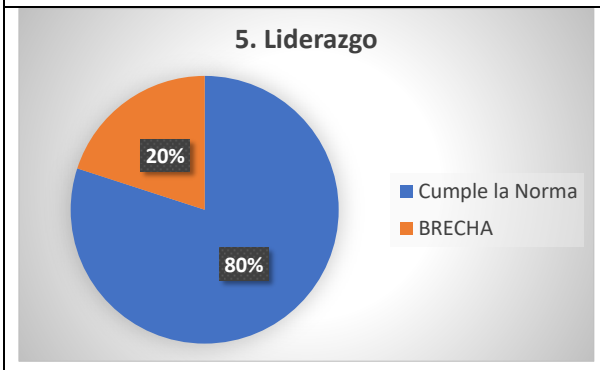
Véase la tabla de Nivel de madurez en la Tabla 5 de la página 46.



Interpretación: La ULEAM ha implementado el requisito de Organización y contexto más de la mitad por lo que su nivel de madurez es **Medio.**

Causas:

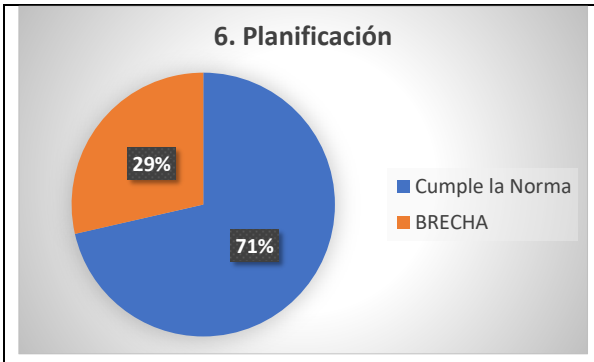
- No se ha identifican claramente los objetivos del SGSI.
- No se ha identificado las partes internas y externas lo que puede suponer una amenaza o riesgo para la seguridad de la información.
- El SGSI no está establecido, ni implementado, por lo que no se revisa de forma planificada considerando oportunidades de mejora.



Interpretación: La ULEAM cumple con un alto porcentaje de cumplimiento, con el ochenta por ciento, esto indica que el nivel de madurez es **alto**.

Causas:

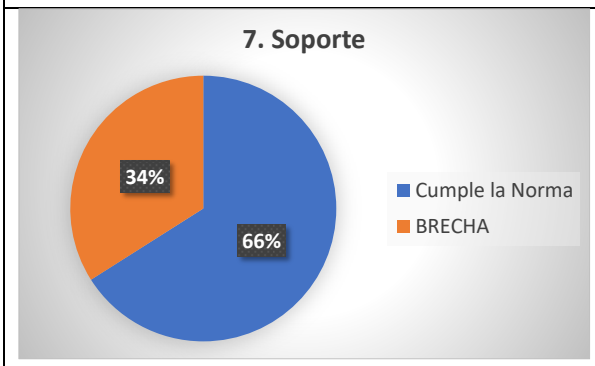
- No se revisa la eficacia del SGSI para que se garanticen que se cumplen los objetivos del SGSI.
- No se comunican las políticas de Seguridad de la Información a las partes interesadas y empresa.
- No se han asignado completamente las responsabilidades y autoridades sobre la Seguridad de la Información.



Interpretación: Mas del 70% del control se cumple, lo que muestra un porcentaje de aplicación de nivel moderado lo cual indica un nivel de madurez **Medio.**

Causas:

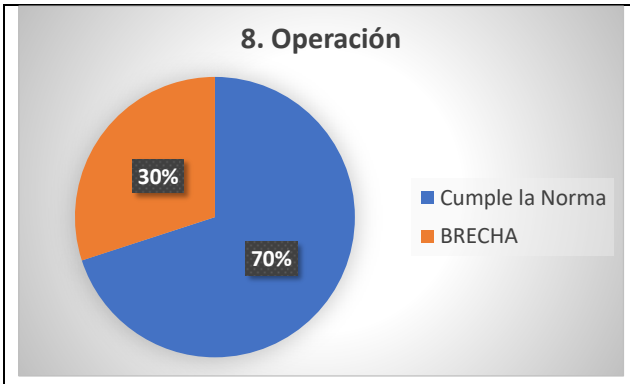
- Falta un entendimiento claro de los procesos para la seguridad de la información y la interacción entre ellos.
- No se ha realizado una evaluación o tratamiento de riesgos de la seguridad de la información con el detalle requerido.
- A pesar de la implementación de algunos planes, no se revisan de forma continua o planificada.



Interpretación: El requisito de Soporte se ha implementado en un 66%, por lo que su nivel de madurez es **Medio**.

Causas:

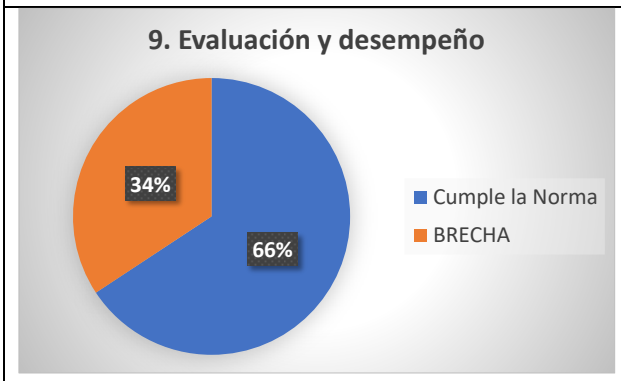
- La concienciación del personal sobre la seguridad de la información es insuficiente.
- Falta establecer un proceso formal y eficaz para la comunicación interna y externa.
- No se ha definido claramente el nivel de competencia necesario para la seguridad de la información.



Interpretación: El requisito de Operación ha sido implementado en un 70%, por lo que el nivel de madurez es **Medio**.

Causas:

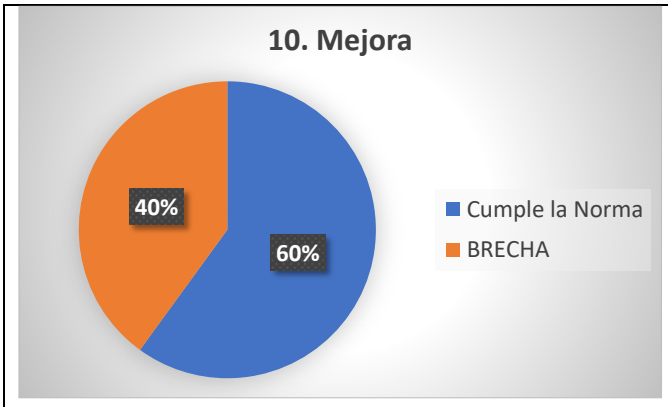
- No se ha documentado y evaluado adecuadamente el riesgo de los activos de la información, esto dificulta el control operacional.
- Falta establecer y aplicar procesos para el tratamiento de los riesgos identificados.
- Los procesos para el control operacional no están definidos y no se están midiendo.



Interpretación: El requisito de ha sido implementado en un poco más del 66%, por lo que su nivel de madurez es **Medio**.

Causas:

- Falta establecer un programa de auditoría interna de forma regular.
- No se ha definido un proceso claro para el seguimiento y medición de los resultados del SGSI.
- La revisión por la dirección no se ha realizado o no se ha documentado de forma que considere los resultados de las auditorías y las no conformidades.

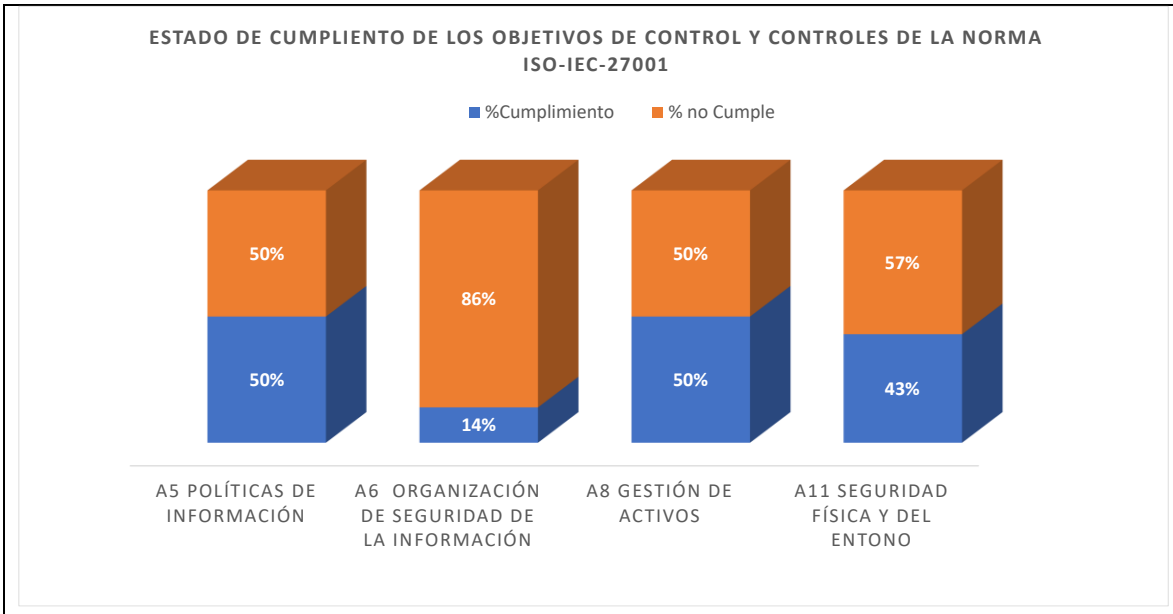
<table>
<tr>
<td> 
</td>
<td>Interpretación: El requisito ha sido implementado en un 60%, por lo que su nivel de madurez es Medio, pero el informe lo califica como "Cumple parcialmente" debido a su nivel de implementación de 3 en todas las preguntas.</td>
</tr>
<tr>
<td colspan="2">Causas:

• Los procesos para la gestión de no conformidades y acciones correctivas no se han definido o no se están aplicando correctamente.
• Falta un proceso estructurado para la mejora continua del SGSI que considere todos los resultados y acciones preventivas.</td>
</tr>
</table>

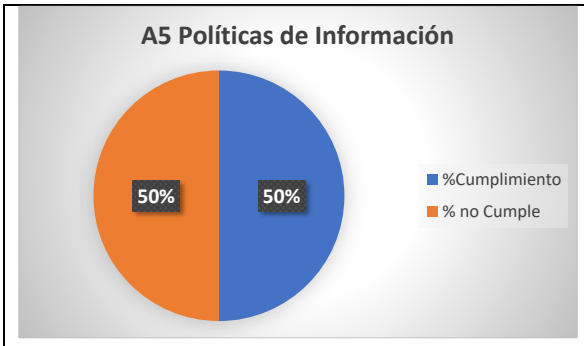
Tabla 25 Hallazgos de Requisitos

5.1.1.2 Hallazgos correspondientes a los controles

Una vez aplicada la auditoría de seguridad a las pantallas de cada una las aulas de las carreras de TI y Software se encontró lo siguiente en relación con la gestión de seguridad en el cumplimiento de controles según la ISO 27001.



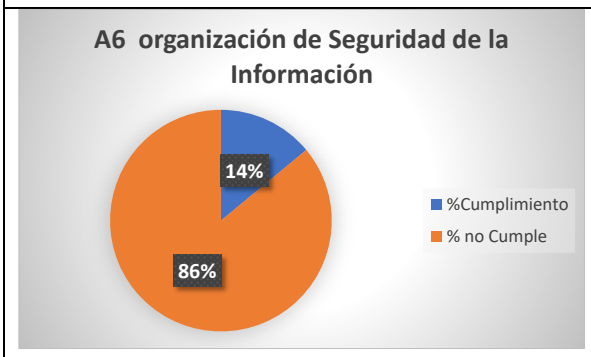
Interpretación: El estado de cumplimiento controles de la Norma ISO/IEC 27001 de la ULEAM Extensión El Carmen, es de nivel bajo, los únicos que alcanzan un 50% de cumplimiento son las políticas de la información y gestión de activos, mientras que organización de seguridad de la información da un valor muy bajo, del 14%, lo cual evidencia un bajo cumplimiento de controles y vulnerabilidad elevada.



Interpretación: La institución cumple con la mitad de sus políticas de seguridad de la información, por lo que su nivel de cumplimiento de controles es **Medio**.

Causas:

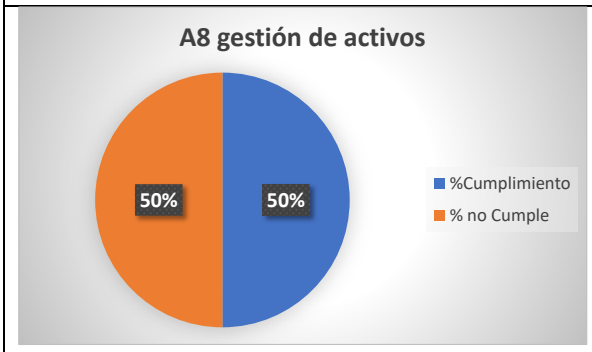
- No existe un proceso planificado y documentado para la revisión de la política de seguridad de la información.



Interpretación: La institución cumple menos de la mitad de los controles relacionados con la organización de la seguridad de la información, por lo que su nivel es **Bajo**.

Causas:

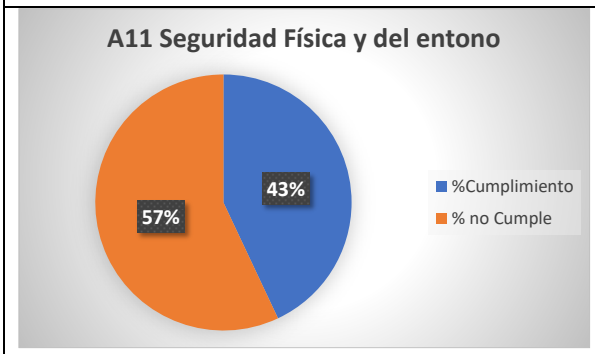
- No existen medios y se han prohibido las relaciones de grupos de interés.
- No existen requisitos para afrontar la seguridad de la información fuera de la organización.
- No existe un proceso de gestión de la información relacionado con los proyectos de la organización.
- No se ha realizado un inventario de activos de información del negocio de la institución.



Interpretación: La institución cumple con la mitad de los controles sobre la gestión de activos, por lo que su nivel es **Medio**.

Causas:

- No se han definido procedimientos documentados para la manipulación, traslado y salida de soportes.
- Los activos de información no tienen un responsable definido para su grado de confidencialidad o para su clasificación.
- No se han documentado las medidas de seguridad para los soportes extraíbles.



Interpretación: La institución cumple con menos de la mitad de los controles sobre la seguridad física y del entorno, siendo su nivel **Bajo**.

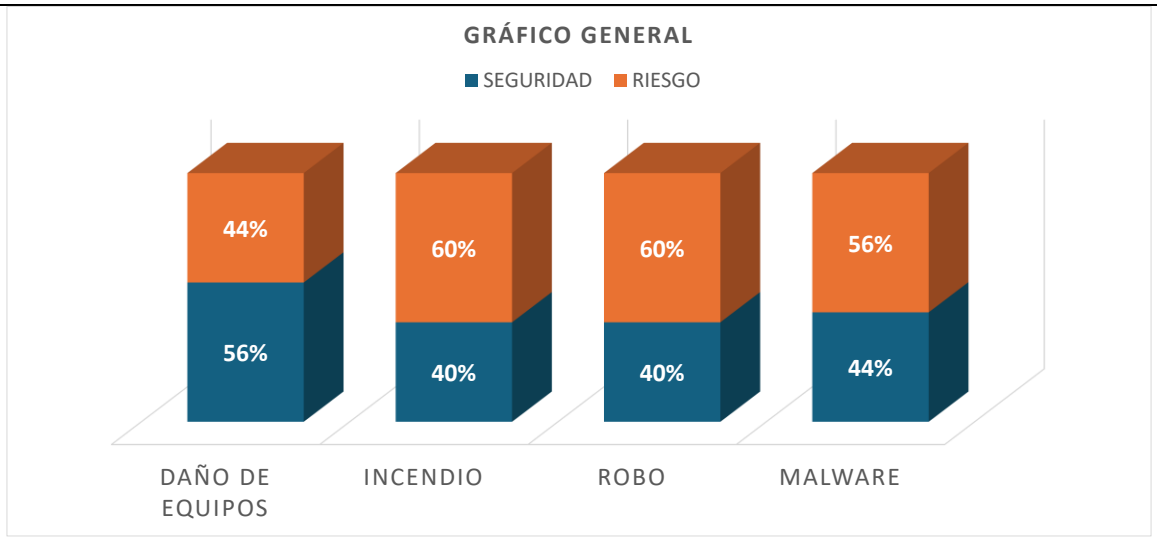
Causas:

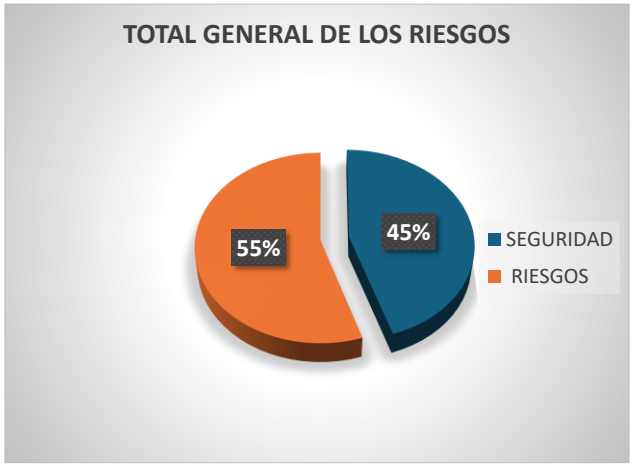
- No se han establecido medidas de protección para el acceso a las áreas restringidas o para proteger la información en dichas áreas.
- No se protege a los equipos contra fallos en el suministro de energía.
- No se controlan y autorizan la salida de equipos.
- No se han establecido protocolos para el mantenimiento y la eliminación o reutilización de los equipos.

Tabla 26 Hallazgos de Controles

5.1.1.3 Análisis de Riesgos

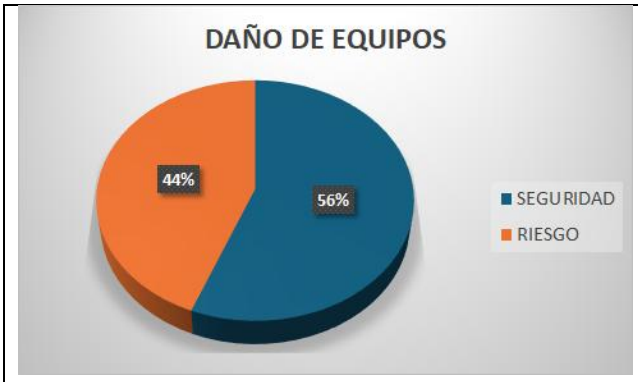
Una vez terminada la recolección de los datos sobre los riesgos a los cuales están expuestas las pantallas, se realizó la respectiva tabulación y análisis de los resultados obtenidos dando la siguiente información:



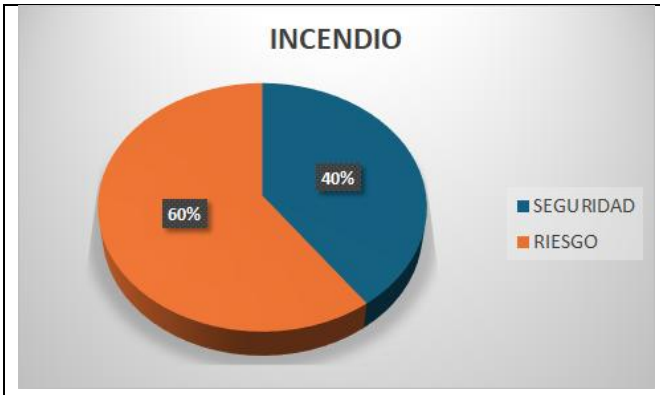


Interpretación:

Aunque la situación general de riesgos es alta, la organización ha logrado una buena gestión en áreas críticas como la protección contra incendios, robos y ataques de malware. Sin embargo, la vulnerabilidad más significativa se encuentra en el **daño de equipos** con un 56% de riesgo, mientras que los demás rondan el 40%, lo que nos da un riesgo **alto** total del 55%.

<table>
<tr>
<td> 
</td>
<td>Interpretación: La institución cumple con más de la mitad lo que nos da un nivel de riesgo Importante. Esto nos indica una vulnerabilidad baja.</td>
</tr>
<tr>
<td colspan="2">Causas:

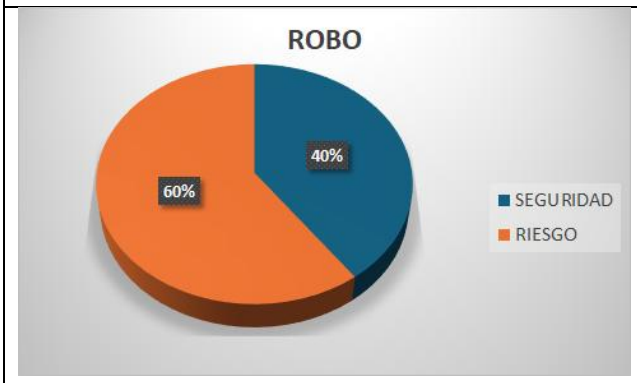
• No se han establecido medidas de protección para el acceso a las áreas restringidas o para proteger la información en dichas áreas.
• No se protege a los equipos contra fallos en el suministro de energía.
• No se controlan y autorizan la salida de equipos.
• No se han establecido protocolos para el mantenimiento y la eliminación o reutilización de los equipos.</td>
</tr>
</table>



Interpretación: La institución cumple con menos de la mitad de las medidas de seguridad para prevenir incendios, siendo su nivel de riesgo es **Apreciable**. Esto representa una vulnerabilidad crítica para la seguridad del personal y los bienes.

Causas:

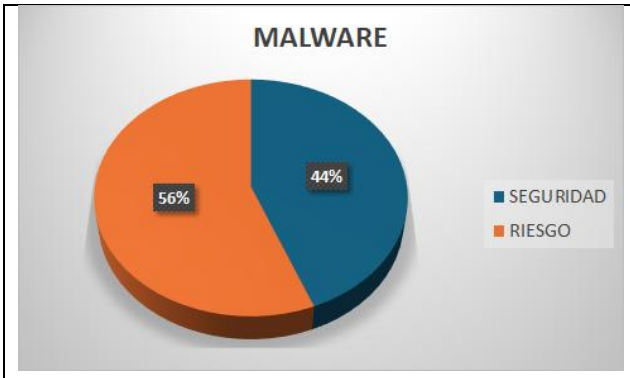
- No existen equipos básicos de seguridad como detectores de humo, extintores o alarmas de emergencia.
- No se han realizado simulacros de evacuación.
- El personal no conoce el plan de evacuación.
- Las instalaciones eléctricas no están certificadas y no se les da mantenimiento periódico.
- El personal no ha sido capacitado en el uso de extintores.



Interpretación: Se tiene un nivel de riesgo **Muy grave** en robo, ya que las medidas de seguridad implementadas son menores a los riesgos existentes.

Causas:

- No existen sistemas de control de acceso ni de videovigilancia en funcionamiento.
- No se realiza un inventario físico periódico de los equipos ni se tienen etiquetados.
- No existen procedimientos para la gestión de llaves y el registro de las personas que ingresan a las aulas.
- No se han realizado análisis de riesgos de robo y el personal no ha sido capacitado sobre cómo actuar ante un incidente.
- No se realizan rondas de seguridad ni se cuenta con guardias.

<table>
<tr>
<td> 
</td>
<td>Interpretación: La institución tiene un nivel de riesgo Importante en malware, ya que las medidas de seguridad implementadas son insuficientes frente a los riesgos existentes.</td>
</tr>
<tr>
<td colspan="2">Causas:

• No se tiene control sobre la instalación de software.
• No se supervisa el tráfico de red para detectar posibles ataques.
• No se limita el acceso a cuentas con privilegios de administrador.
• No existe una política formal de respuesta ante incidentes de malware.</td>
</tr>
</table>

Tabla 27 Hallazgos de Riesgos

5.1.2 Opinión

1) **Evaluar el nivel de madurez en la gestión de seguridad informática de las pantallas de las carreras de TI y Software según ISO 27001**

Tras analizar la situación, hemos concluido que la gestión de la seguridad informática para las pantallas se encuentra en un nivel intermedio.

Si bien la organización dispone de ciertas salvaguardas elementales (como una guía en línea, una formación introductoria y sistemas de seguridad), carece de la supervisión continua y los controles que la norma ISO/IEC 27001 considera esenciales. No se efectúan revisiones internas de manera oficial, ni se lleva un seguimiento al día del mantenimiento de los equipos.

2) **Identificar los riesgos de seguridad informática a los que están expuestas las pantallas**

Los riesgos identificados a los que están expuestos son:

Riesgo	Nivel de Riesgo
DAÑO DE EQUIPOS	Importante
INCENDIO	Apreciable
ROBO	Muy grave
MALWARE	Importante

Ilustración 19 Riesgos Identificados

3) Elaborar un plan de medidas de seguridad e implementar las más urgentes

A partir de los resultados de la evaluación, hemos desarrollado un plan de acción para mejorar la seguridad, guiándonos por la norma ISO/IEC 27001 y enfocándonos en lo más urgente.

Ver en el anexo G Manual de políticas de seguridad

5.1.3 Conclusiones y recomendaciones de la auditoria

De la auditoría realizada se concluye que la institución no cuenta con procedimientos claros ni registros adecuados para gestionar los riesgos que afectan a las pantallas electrónicas, lo que incrementa su vulnerabilidad frente a daños, robos, incendios y ataques de malware. Esta falta de controles, roles definidos y mantenimiento planificado limita la respuesta oportuna, genera costos innecesarios y pone en riesgo la continuidad de las actividades académicas.

Ver en el anexo G Manual de políticas de seguridad

5.1.4 Implementación de medidas de seguridad

Como medida de prevención se procedió a la compra e instalación de cámaras de seguridad, con el fin de precautelar la seguridad de las pantallas, las cuales están instaladas en el segundo piso, en las carreras de TI y Software.

Opciones de cámaras	
Cámaras	**Características**
DS-2CD1623G0-I.  	➢ Cámara de red tipo bullet vari focal de 2 MP ➢ Imágenes de alta calidad con resolución de 2 MP ➢ Tecnología de compresión eficiente H.265+ ➢ Imágenes nítidas incluso con fuerte luz de fondo gracias a la tecnología DWDR ➢ Ranura para tarjeta SD de hasta 256 GB para almacenamiento ➢ Lente vari focal motorizada de 2,8 a 12 mm para una fácil instalación y monitoreo ➢ Resistente al agua y al polvo (IP67) ➢ EXIR 2.0: tecnología infrarroja avanzada con gran alcance IR
DS-2CD1023G2-LIU  	➢ Cámara de red tipo bullet fija de 2 MP con luz híbrida inteligente ➢ Imágenes de alta calidad con una resolución de 2 MP ➢ Soporte para detección de humanos y vehículos ➢ Luz híbrida inteligente: tecnología avanzada con largo alcance ➢ Micrófono incorporado para seguridad de audio en tiempo real ➢ Resistente al agua y al polvo (IP67) ➢ Tecnología de compresión eficiente H.265+ ➢ Soporta almacenamiento integrado de hasta 512 GB (ranura para tarjeta SD) (Opcional)

DS-2CD1027G2H-LIU	
	➢ Cámara de red tipo bullet fija de 2 MP ColorVu con luz híbrida inteligente ➢ Imágenes de alta calidad con resolución de 2 M ➢ Soporte para detección de humanos y vehículos ➢ Luz híbrida inteligente: tecnología avanzada con gran alcance ➢ Tecnología de compresión eficiente H.265+ ➢ Soporta almacenamiento integrado de hasta 512 GB (ranura para tarjeta SD) (Opcional) ➢ Micrófono incorporado para seguridad de audio en tiempo real ➢ Resistente al agua y al polvo (IP67)

5.1.4.1 Elección de las cámaras.

Al momento de elegir de las cámaras a usar, se tomó en cuenta el modelo y marca del NVR, para que sean compatibles al momento de la instalación y configuración de las cámaras, además de tener en cuenta el precio y las necesidades de monitorear, la que se eligió fue el modelo DS-2CD1023G2-LIU, de la marca HIKVISION, la cual es de 2 Megapíxeles y nos brindan visión nocturna, las demás características se mencionan en la tabla anterior.

5.1.4.2 Materiales usados

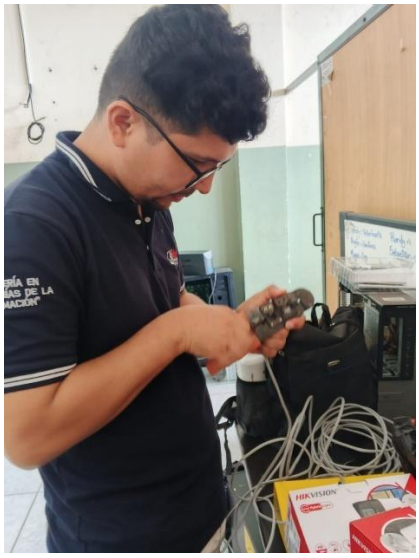
- Cámara Hikvision DS-2CD1023G2-LIU
- Cable UTP
- Laptop
- Conectores RJ45
- Tornillos
- Ponchadora

5.1.4.3 Instalación

Para la instalación se tomó en cuenta que cubriera la mayor cantidad de aulas, las cuales deben estar dentro del rango son: 204, 205, 206, 208 y 210.

<table>
<tr><th colspan="2">Pasos de instalación de cámaras</th></tr>
<tr><td>

- Ponchar los cables UTP



</td><td>

- Desplegar los cables UTP

</td></tr>
<tr><td>

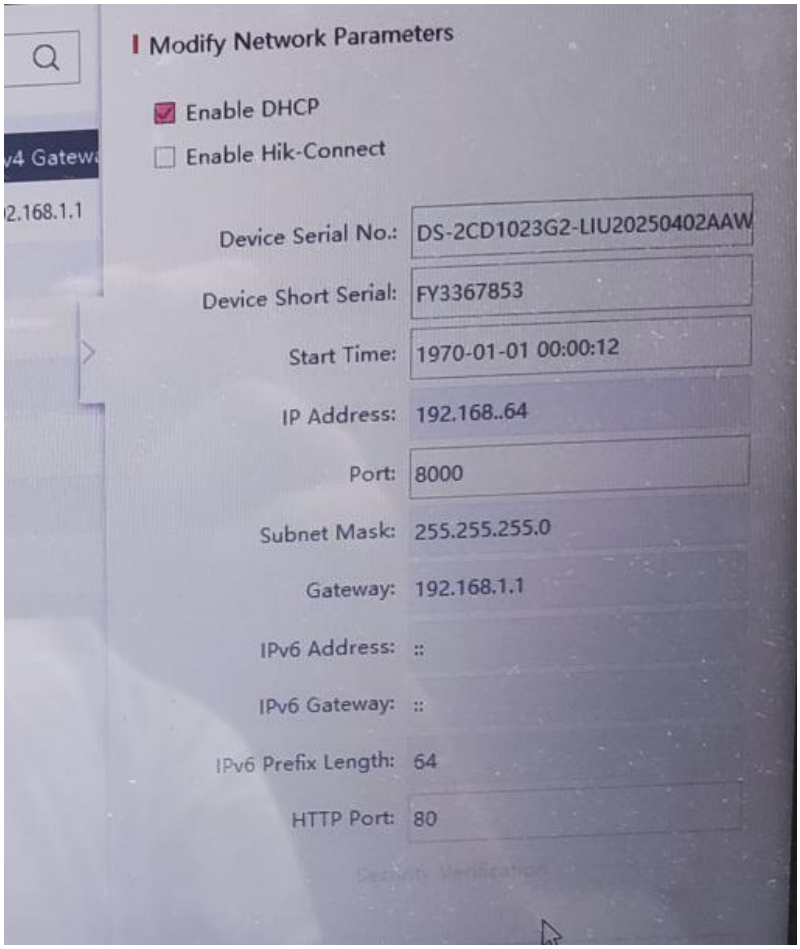
- Colocar las cámaras en el lugar correspondiente.

</td><td>

- Mover las cámaras para que queden estables y enfocando correctamente.

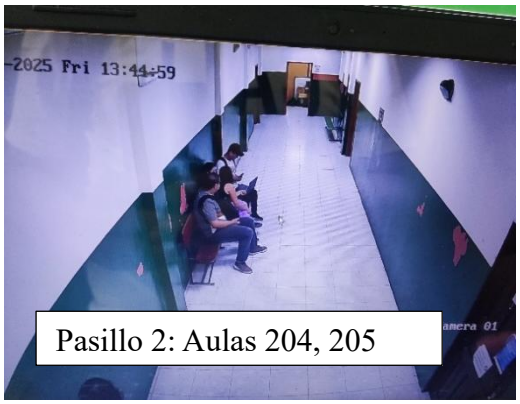
</td></tr>
</table>

- Una vez conectadas las cámaras en el NVR, se habilito el DHCP, para que a la cámara se le asigne la IP.



- Comprobación de funcionamiento de las cámaras.

- Luego de instalada y configuradas las cámaras se comprobó que cubran las aulas a monitorear, las 204, 205, 206, 208 y 210.



Pasillo 2: Aulas 204, 205

Pasillo 1: 206, 208 y 210

Tabla 28 Instalación de cámaras

CAPÍTULO VI:

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Se alcanzó la meta de detectar los problemas y los puntos débiles en la seguridad. Gracias a las encuestas y entrevista, dando como resultado que no sabían cómo usar bien las pantallas, que faltaban controles para entrar y que no había reglas claras. Esto confirmó que hacía falta un SGSI.
- Se logró respaldar la investigación con información de confianza. Revisando normas internacionales como la ISO 27001 y mirando casos anteriores importantes. Así se pudo crear una buena base teórica para llevar a cabo la auditoría.
- Se llevó a cabo las encuestas y entrevistas para conseguir datos reales. Esto ayudó a ver los puntos débiles concretos, las malas costumbres y lo poco que se hacía para mantener las pantallas. Obteniendo información directa de alumnos y director de carrera.
- Se revisó la seguridad de las pantallas con la auditoría informática. Usando herramientas para ver los riesgos y los controles de seguridad. Mostrando que había fallos tanto en lo físico como en lo lógico, midiendo cuánto peligro corrían las pantallas.
- Se cumplió el objetivo de proponer correcciones mediante un manual de uso y políticas de seguridad, entregando una propuesta concreta de procedimientos, roles, flujogramas, formatos y checklists para mitigar riesgos, prolongar la vida útil de las pantallas y proteger la información.

6.2 Recomendaciones

- **A la Dirección de la Carrera de TI y Software:** Actualizar y difundir ampliamente el manual de respuesta a incidentes y políticas de uso, asegurando que todos los docentes y estudiantes conozcan las normas de manejo de las pantallas.
- **Al Departamento de TI:** Implementar un plan de mantenimiento preventivo documentado, con los cronogramas claros y registros auditables, que garanticen una revisión periódica del estado físico y lógico de los equipos.
- **A la Coordinación de Seguridad y Administración:** Es necesario reforzar los controles físicos y la vigilancia de las aulas, optimizar accesos como cerraduras, la videovigilancia y cada mecanismo antirrobo para reducir el riesgo de sustracción o daño.
- **A la Coordinación Académica y Docente:** Realizar capacitaciones periódicas para docentes y estudiantes sobre cómo usar las pantallas, darles conceptos de seguridad informática básica y responsabilidad compartida para la conservación de los recursos.
- **A la Alta Dirección:** Que se replique este trabajo en la evaluación de las pantallas de las otras carreras para así mejorar el nivel de seguridad de la universidad y evitar pérdidas de equipos informáticos.

BIBLIOGRAFÍA

Bernal Torres, C. A. (2010). *Metodología de la investigación.* PEARSON EDUCACIÓN.

Carneiro, R., Toscano, J. C., & Díaz, T. (2021). *Los desafíos de las TIC para el cambio educativo.* Fundación Santillana.

Albornoz Zamora, E. J., & Guzmán, M. d. (2023). Fases de la investigación. Marco metodológico. En E. J. Albornoz Zamora, M. d. Guzmán, K. G. Sidel Almache, J. G. Chuga Guamán, J. L. González Villanueva, J. P. Herrera Miranda, . . . R. Arteaga Delgado, *Metodología de la investigación aplicada a las ciencias de la salud y la educación* (págs. 146-159). Quito: Mawil Publicaciones de Ecuador.

Allen, W. (1968). *Readings in educational media theory and research (Vol. 1).* U.S. Department of Health, Education, and Welfare.

Araujo Bedoya, G. J., Guerra Delgado, L. R., Bastidas Santana, V. G., Diaz Berruz, C. F., & Planta Ulloa, J. P. (2024). *Educación y tecnología digital.* CID - Centro de Investigación y Desarrollo.

Atómica Organismo Internacional de Energía. (2018). *Planificación de la respuesta a incidentes de seguridad física informática en las instalaciones nucleares.* Viena: OIEA.

Avenía Delgado, C. A. (2017). *Fundamentos de seguridad informática.* Fundación Universitaria del Área Andina.

Babativa Novoa, C. A. (2017). *Investigación cuantitativa.* Bogotá D.C.: Fundación Universitaria del Área Andina.

Blandón Jaramillo, C. J., & Benavides Sepúlveda, A. M. (2018). *Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico.* Scientia et Technica.

Buitargo Giraldo, R. E. (2020). *SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA SGSI EN UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO – COLOMBIA.* UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.

Calder, A. (2020). *Implementing Information Security Based on ISO 27001/ISO 27002.* Van Haren Publishing.

Colás Bravo, M. P., & Lozano Martínez, J. (2011). *Escuelas Inclusivas y TIC. Buenas prácticas educativas en el tratamiento de la diversidad.* Revista Comunicación y Pedagogía, Nº 249.

CONSULTORES ISO. (2022). *Introducción a la Norma ISO 27001.* Sevilla: GDS & Consultores ISO, SL.

Dávila Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. *Laurus, 12*(Ext, 2006), 180-205.

Díaz Bravo, L., Torruco García, U., Martínez Hernández, M., & Varela Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en Educación Médica, 2*(7), 162-167.

Díaz Quezada, I. F. (2024). *Gestión de la seguridad y protección de la información de la UTMACH mediante estándares y buenas prácticas.* Universidad Técnica de Machala.

DTS Solution. (15 de Febrero de 2022). *Decoding the changes: An important update on ISO 27002:2022.* Obtenido de DTS Solution.: https://www.dts-solution.com/decoding-the-changes-an-important-update-on-iso-270022022/

Gómez Fernández, L., & Fernández Rivero, P. P. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* AENOR Internacional, S.A.U.

Guaña, J. (2023). *La importancia de la seguridad informática en la educación digital: retos y soluciones.* Editorial Saberes del Conocimiento. doi:10.26820/recimundo/7.(1).enero.2023.609-616

Guevara Alban, G. P., Verdesoto Arguello, A. E., & Castro Molina, N. E. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO*, 163-173.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación (6.ª ed.).* McGraw-Hill Education.

ISO. (2022). *ISO/IEC 27001. Information security, cybersecurity and privacy protection.* Geneva: International Organization for Standardization.

Johnson, A., & Smith, L. (2019). Interactive whiteboards in education: Engaging students in digital learning environments. *Educational Technology Journal*, 45-58.

López Roldán, P., & Fachelli, S. (2015). *METODOLOGÍA DE LA INVESTIGACIÓN SOCIAL CUANTITATIVA.* Universitat Autònoma de Barcelona. doi:http://ddd.uab.cat/record/129382

Maradi, A., Archenti, N., & Piovani , J. I. (2010). *Metodología de las Ciencias Sociales. 1º Edición.* Buenos Aires: Cengage Learning.

Ministerio de Educación de la Nación. (2008). *Estrategias pedagógicas para el uso de las computadoras portátiles en el aula.* Buenos Aires: Ministerio de Educación de la Nación.

Ochoa, C. (19 de febrero de 2015). *netquest*. Obtenido de netquest: https://www.netquest.com/blog/muestreo-que-es-porque-funciona

Oviedo Regueros, L. A. (21 de Marzo de 2023). *EQUIPO AUDEA*. Obtenido de AUDEA: https://audea.com/controles-de-seguridad-y-sus-tipos/

Prieto Castellanos , B. J. (2017). *El uso de los métodos deductivo e inductivo para aumentar la e□ciencia del procesamiento de adquisición de evidencias digitales.* Pontificia Universidad Javeriana. doi:https://doi.org/10.11144/Javeriana.cc18-46.umdi

Quecedo, R., & Castaño, C. (2002). Introducción a la metodología de investigación cualitativa. *Revista de Psicodidáctica*, 5-39.

Rodríguez Osuna, J. (2001). *Métodos de muestreo.* Madrid: SIGLO XXI DE ESPAÑA EDITORES, S.A.

Rosales, E. A. (2019). *Diseño de un sistema de gestión de seguridad de la información para el proceso de gestión de la infraestructura tecnológica del Colegio Salesiano basado en Magerit.* Universidad de Cartagena.

Sánchez Ruipérez, F. G. (2010). *Dedos: una experiencia educativa con la tableta digital.* Macotera, Salamanca: CEO Miguel Delibes.

Schellman Blog. (24 de Febrero de 2022). *ISO 27002:2022 – What you need to know. Schellman & Company, LLC.* Obtenido de Schellman.:

https://www.schellman.com/blog/iso-certifications/iso-27002-2022-what-you-need-to-know

Silva Coelho, F. E., Segadas de Araújo, L. G., & Kowask Bezerra, E. (2014). *Gestión de la seguridad de la información (Versión adaptada al Ecuador.* RENATA - Red Nacional Académica de Tecnología Avanzada.

Taylor, A., Alexander, D., Finch, A., & Sutton, D. (2020). Information Security Management Principles (3rd ed.). En A. Taylor, D. Alexander, A. Finch, & D. Sutton, *Information Security Management Principles (3rd ed.).* (pág. 19). BCS Learning & Development Ltd.

Toledo Morales, P., & Sánchez García, J. M. (2013). *Utilización de la pizarra digital interactiva como herramienta en las aulas universitarias.* Universidad de Guadalajara.

Vázquez Cano, E. (2021). *Medios, recursos didácticos y tecnología educativa.* UNED - Universidad Nacional de Educación a Distancia.

Watters, A. (2019). *Teaching machines: Learning from the intersection of education and technology.* MIT Press.

ANEXOS

Anexo A Aprobación de tema

Outlook

DPGA | Titulación | Periodo 2024-2025(2) - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Desde NOTIFICACIONES TITULACION <notificaciones.titulacion@uleam.edu.ec>
Fecha Mar 23/07/2024 9:57
Para POZO HERNANDEZ CLARA GUADALUPE <clara.pozo@uleam.edu.ec>
CC VELEZ VILLAVICENCIO ANTHONY BLADIMIR <e1313528398@live.uleam.edu.ec>; REASCOS PINCHAO RAUL SAED <raul.reascos@uleam.edu.ec>

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Universidad Laica Eloy Alfaro de Manabí

Periodo 2024-2025(2) - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Estimad@
Docente y Estudiante
Uleam

En cumplimiento de lo establecido en la Ley, el Reglamento de Régimen Académico y las disposiciones estatutarias de la Uleam, por medio de la presente se oficializa la dirección y tutoría en el desarrollo del Trabajo de Integración curricular / Trabajo de Titulación del siguiente estudiante:

Tema: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA TECNOLOGÍA EDUCATIVA DE LAS AULAS DE TI Y SOFTWARE EN LA ULEAM EXTENSIÓN EL CARMEN

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

Tipo de proyecto: Trabajo de Integración Curricular / Trabajo de titulación se articula con proyectos y programas de Investigación.

Apellidos y nombres del tutor asginado: POZO HERNANDEZ CLARA GUADALUPE

Apellidos y nombres del estudiante: VELEZ VILLAVICENCIO ANTHONY BLADIMIR

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2024-2025(2)

Sírvasen cumplir con lo dispuesto en el Manual de Procedimientos de TITULACIÓN DE ESTUDIANTES DE GRADO: TRABAJO DE INTEGRACIÓN CURRICULAR https://departamentos.uleam.edu.ec/gestion-aseguramiento-calidad/files/2023/04/Titulacion-de-Est.-Grado-Bajo-la-Unidad-Integr.-Curri.-V.2-1-1.pdf.

Particular que se informa para los fines consiguientes.

Atentamente,

Comisión Académica y Responsable de Titulación.

Borde superior de firma

NOTIFICACIONES TITULACION

emailnotificaciones.titulacion@uleam.edu.ec
mobileTeléfono:
officeTeléfono movíl:

Borde inferior firma

• • • EC

Anexo B Instrumento entrevista

1) ¿Cómo se utilizan las pantallas electrónicas en las aulas como parte del proceso de enseñanza y aprendizaje en la institución?
2) ¿Está al tanto de la existencia de algún manual o guía específica para el uso de las pantallas electrónicas? Si no, ¿cree que sería útil contar con uno?
3) ¿Qué otros usos, además de los académicos, ha observado o considera que podrían darse a las pantallas electrónicas?
4) ¿Qué conocimiento tiene sobre la vida útil de las pantallas electrónicas y cómo cree que esta información se gestiona dentro de la institución?
5) ¿Ha recibido o considera necesario recibir capacitación para optimizar el uso y manejo de las pantallas electrónicas?
6) ¿Qué estrategias o recomendaciones se han compartido con los estudiantes sobre el uso responsable de las pantallas electrónicas?
7) ¿Ha habido situaciones o incidentes relacionados con el uso o funcionamiento de las pantallas? ¿Cómo se manejaron?
8) ¿Qué medidas se toman respecto a la seguridad de las aulas, incluyendo el cierre de puertas, al terminar las clases?
9) ¿Qué mecanismos existen para proteger las pantallas electrónicas y evitar su manipulación no autorizada?
10) ¿Ha habido ocasiones en que las pantallas han tenido que ser trasladadas fuera de las aulas? Si es así, ¿cuáles fueron las razones?
11) ¿Qué precauciones se toman al mover las pantallas electrónicas para garantizar su integridad?
12) ¿La institución cuenta con sistemas como reguladores de voltaje para proteger las pantallas de variaciones eléctricas? ¿Cómo se asegura su buen funcionamiento?
13) ¿Qué medidas de seguridad, como sistemas de videovigilancia, están implementadas para prevenir el hurto o daño de las pantallas electrónicas?

Encuesta sobre el uso y función de las pantallas electrónicas de las aulas de TI y Software.

Objetivo: Aplicación de encuesta y entrevista para identificar los riesgos a los que están expuestas las pantallas.

* Indica que la pregunta es obligatoria

1. 1. ¿Usa regularmente las pantallas electrónicas de las aulas como método de enseñanza y/o aprendizaje? *

   Marca solo un óvalo.

   - Si
   - No

2. 2. ¿Conoce de la existencia de un manual de uso exclusivo de las pantallas electrónicas? *

   Marca solo un óvalo.

   - Si
   - No

3. 3. ¿Al momento de ingresar a las aulas, encuentra encendidas o apagadas las pantallas electrónicas? *

   Marca solo un óvalo.

   - Nunca
   - Aveces
   - Siempre

4. 4. ¿Ha usado las pantallas para otra actividad que no sea académica? *

Marca solo un óvalo.

- Si
- No

5. 5. ¿Conoce usted sobre el tiempo de vida útil de cada pantalla electrónica? *

Marca solo un óvalo.

- Si
- No

6. 6. ¿Ha recibido capacitaciones para el uso y manejo de las pantallas electrónicas? *

Marca solo un óvalo.

- Si
- No

7. 7. ¿Ha recibido alguna recomendación o directriz sobre el uso y manejo de las pantallas electrónicas? *

Marca solo un óvalo.

- Si
- No

8. 8. ¿Se han registrado incidentes en cuanto al uso y funcionamiento de las pantallas electrónicas? *

Marca solo un óvalo.

- Si
- No

Anexo D Fotografías

(Cada fotografía debe incluir una descripción detallada de los elementos que se deben observar. No es necesario añadir un título a la ilustración, ya que se encuentra fuera del cuerpo principal del texto)

Lugares donde quedaron instaladas las cámaras, las cuales vigilan los pasillos del segundo piso, las cuales corresponden a las aulas de TI y Software.

CERTIFICADO DE ANÁLISIS

ANTHONY BLADMIR VÉLEZ VILLAVICENCIO(4)

8% Textos sospechosos

5% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos
3% Textos potencialmente generados por la IA

Nombre del documento: ANTHONY BLADMIR VÉLEZ VILLAVICENCIO(4).pdf
ID del documento: f37cf085eff8c5abc210ba6e827a61b6480b02f7
Tamaño del documento original: 2,28 MB

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 18/8/2025
Tipo de carga: interface
fecha de fin de análisis: 18/8/2025

Número de palabras: 18.321
Número de caracteres: 116.640

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

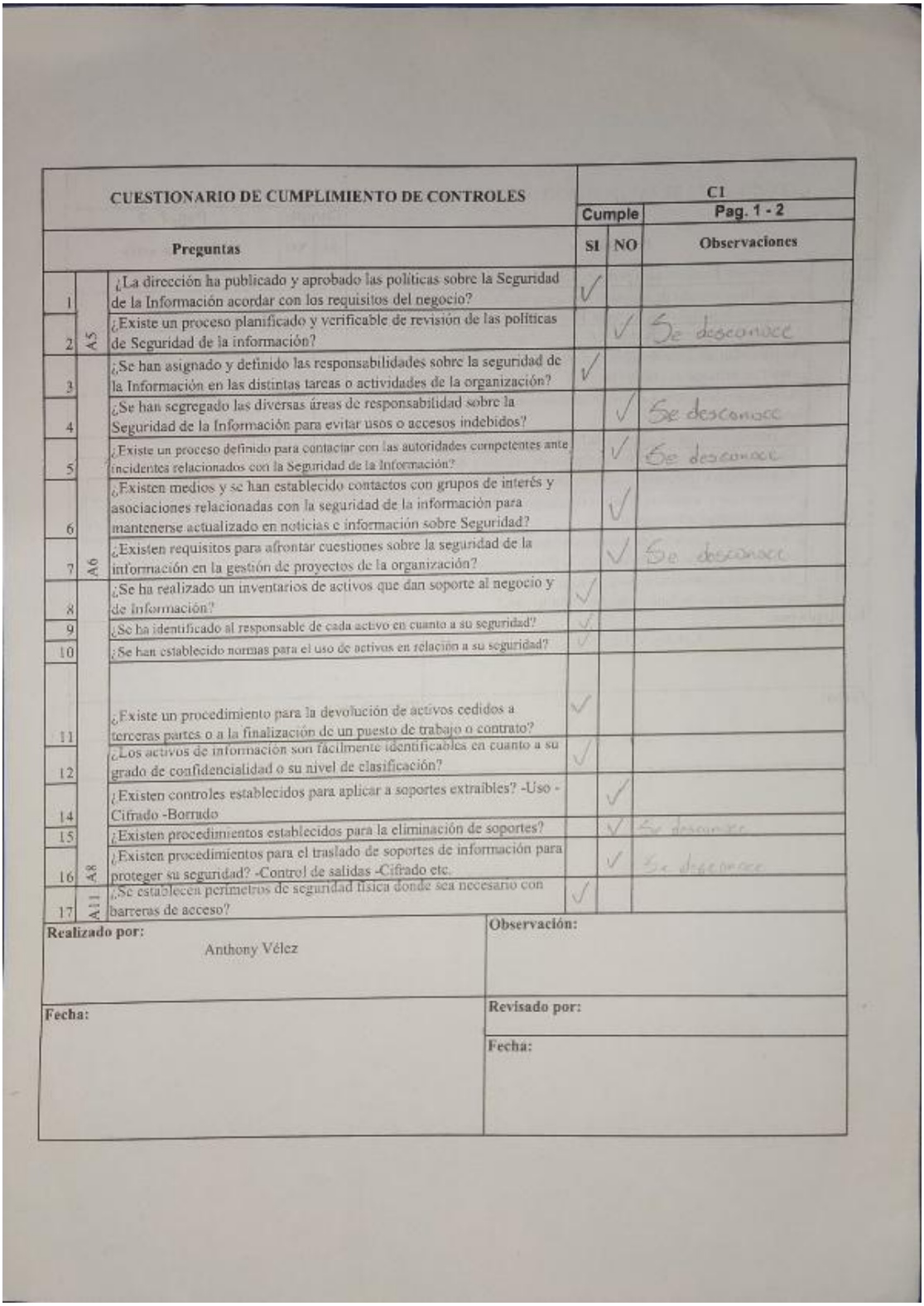
N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**David Anddrade Final compilatio.docx** | David Anddrade Final compilatio #600654 Viene de de mi grupo 1 fuente similar	3%		Palabras idénticas: 3% (508 palabras)
2	normalso27001.es https://normalso27001.es/wp-content/uploads/2019/02/Test_cumplimiento_ISO_27001.pdf	2%		Palabras idénticas: 2% (266 palabras)
3	**repositorio.pucesa.edu.ec** | Modelo de gestión de seguridad de la información e... http://repositorio.pucesa.edu.ec/bitstream/123456789/3712/1/77995.pdf	1%		Palabras idénticas: 1% (212 palabras)
4	hdl.handle.net | Diseño de un sistema de gestión de seguridad de la información... http://hdl.handle.net/20.500.12918/10221 8 fuentes similares	< 1%		Palabras idénticas: < 1% (68 palabras)
5	Documento de otro usuario #64a60f Viene de de otro grupo 7 fuentes similares	< 1%		Palabras idénticas: < 1% (57 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**reunir.unir.net** | (Metodología para la implementación de un SGSI en la fundació... https://reunir.unir.net/bitstream/123456789/3129/1/HelenaClaralsabel_Aleman_Novoa.pdf	< 1%		Palabras idénticas: < 1% (40 palabras)
2	**dialnet.unirioja.es** | Modelo sistema de gestión de seguridad de la información p... https://dialnet.unirioja.es/servlet/articulo?codigo=6413736	< 1%		Palabras idénticas: < 1% (36 palabras)
3	**Documento de otro usuario** #233439 Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (28 palabras)
4	**uvadoc.uva.es** | Cómo gestionar la seguridad de la información (según ISO 27001... http://uvadoc.uva.es/handle/10324/16838	< 1%		Palabras idénticas: < 1% (20 palabras)
5	**localhost** | Investigación para el desarrollo de un sistema de gestión de seguridad... http://localhost:8080/xmlui/bitstream/redug/20222/4/TESIS ING. ROSANA CHERREZ.pdf.txt	< 1%		Palabras idénticas: < 1% (23 palabras)

18-08-2025

- **Cuestionario cumplimiento de controles.**



CUESTIONARIO DE CUMPLIMIENTO DE CONTROLES			C1		
			Cumple		Pag. 1 - 2
Preguntas			SI	NO	Observaciones
1	A5	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?	✓		
2		¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?		✓	Se desconoce
3	A6	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	✓		
4		¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?		✓	Se desconoce
5		¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?		✓	Se desconoce
6		¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?		✓	
7		¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?		✓	Se desconoce
8	A8	¿Se ha realizado un inventarios de activos que dan soporte al negocio y de Información?	✓		
9		¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	✓		
10		¿Se han establecido normas para el uso de activos en relación a su seguridad?	✓		
11		¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?	✓		
12		¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?	✓		
14		¿Existen controles establecidos para aplicar a soportes extraíbles? -Uso -Cifrado -Borrado		✓	
15		¿Existen procedimientos establecidos para la eliminación de soportes?		✓	Se desconoce
16		¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? -Control de salidas -Cifrado etc.		✓	Se desconoce
17	A11	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?	✓		

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

- **Cuestionario cumplimiento de requisitos**

CUESTIONARIO DE CUMPLIMIENTO DE REQUISITOS			C1					
								Pag. 1 - 3
		Preguntas	1	2	3	4	5	Observaciones
1	La Organización y su Contexto	¿Están identificados los objetivos del SGSI Sistema de Gestión de la Seguridad de la Información?			X			No se especifica
2		¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?			X			Se da poco detalle
3		¿Se han identificado las partes interesadas?				X		
4		¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?			X			
5		¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?				X		
6		¿Se ha determinado el alcance del SGS y se conserva información documentada?				X		
7		¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?			X			
8	Liderazgo	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?				X		
9		¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?			X			
10		¿Se ha definido una Política de la Seguridad de la Información?					X	
11		¿Se ha establecido un marco que permita el establecimiento de objetivos?				X		
12		¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?				X		
13		¿Se mantiene información documentada de la política del SGSI y de sus objetivos?				X		
14		¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?				X		
15		¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?				X		
16	Planificación	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?			X			
17		¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?				X		
18		¿Se ha definido un proceso de tratamiento de riesgos?				X		
19		¿Se han establecido criterios para elaborar una declaración de aplicabilidad?			X			
20		¿Se mantiene información documentada de los puntos anteriores?				X		
21		¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?				X		

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

CUESTIONARIO DE CUMPLIMIENTO DE REQUISITOS			CI					
								Pag. 2 - 3
		Preguntas	1	2	3	4	5	Observaciones
22	Planifica	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?			X			
23		¿Se identifican y asignan los recursos necesarios para el SGSI?				X		
24		¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?			X			
25		¿Se mantiene información actualizada sobre la competencia del personal?			X			
26		¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?			X			
27		¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?			X			
28		¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?				X		
29		¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?			X			
30	Soporte	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)				X		
31		¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección			X			
32		¿Se controlan los documentos de origen externo?			X			
33	Operación	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?				X		
34		¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?				X		
35		¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?				X		
36		¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?			X			
37		¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia				X		

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

CUESTIONARIO DE CUMPLIMIENTO DE REQUISITOS			C1 Pag. 3 - 3					
		Preguntas	1	2	3	4	5	Observaciones
38	Operación	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados				X		
39		¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?			X			
40		¿Se documenta el nivel de aplicación de todos los controles a aplicar?		X				
41	Evaluación del desempeño	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?			X			
42		¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?				X		
43		¿Se ha establecido un proceso documentado para evaluar los resultados			X			
44		¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?				X		
45		¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?		X				
46		¿Se ha establecido una programación de Auditorías Internas y asignado responsables?				X		
47		¿Se ha definido el alcance y los requisitos para el informe de auditoría?			X			
48		¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?			X			
49		¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?			X			
50		¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?			X			
51	Mejora	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?			X			
52		¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?			X			
53		¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?			X			

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

- **Cuestionario de Daños**

Aula N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 2 - 4		
	Preguntas: Control de daños	**SI**	**NO**	**Observaciones**
1	¿Las pantallas están protegidas contra caídas o golpes accidentales dentro del aula?			
2	¿Se han instalado soportes adecuados para evitar que las pantallas se desplacen o se caigan?			
3	¿Las aulas tienen protección contra variaciones eléctricas (reguladores o UPS)?			
4	¿Se realiza mantenimiento preventivo regular a las pantallas?			
5	¿Se inspeccionan periódicamente los cables y conexiones de las pantallas?			
6	¿Las pantallas están alejadas de fuentes de humedad dentro del aula?			
7	¿Existen normas para evitar el uso indebido de las pantallas?			
8	¿Se ha capacitado al personal sobre el uso correcto de las pantallas?			
9	¿Se supervisa adecuadamente la manipulación de las pantallas por parte de los estudiantes dentro del aula?			
10	¿Existen protecciones físicas (acrílicos o fundas) sobre las pantallas?			
11	¿Se limita el acceso a los puertos físicos de las pantallas (HDMI, USB, etc.)?			
12	¿Hay supervisión del uso de las pantallas durante el horario de clases?			
13	¿Se desconectan correctamente las pantallas al finalizar la jornada?			
14	¿Las aulas cuentan con ventilación adecuada para evitar sobrecalentamiento de las pantallas?			
15	¿Las pantallas han presentado daños físicos en los últimos seis meses?			
16	¿Se dispone de un protocolo de reporte ante daño o mal funcionamiento de las pantallas?			
17	¿Las pantallas tienen garantía activa por parte del proveedor?			
18	¿Se cuenta con repuestos o equipo de reemplazo ante fallas críticas?			
19	¿Se han presentado errores en la pantalla durante el uso regular durante clases?			
20	¿Se hace revisión de voltajes antes de conectar nuevos equipos a las pantallas?			
21	¿Se cuenta con un inventario actualizado de las pantallas con su estado operativo?			
22	¿Las aulas están protegidas contra ingreso de animales o plagas que puedan dañar los equipos?			
23	¿Existe algún sistema de monitoreo de temperatura en las aulas para proteger los dispositivos?			
24	¿Se hacen pruebas de funcionamiento de las pantallas antes del inicio del periodo académico?			
25	¿El personal responsable informa oportunamente sobre cualquier señal de daño en las pantallas?			

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

- **Cuestionario Malware**

Aula N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 3 - 4		
	Preguntas: Malware	**SI**	**NO**	**Observaciones**
1	¿Las pantallas están conectadas a una red segura?			
2	¿Cuentan con antivirus instalados?			
3	¿Se actualiza regularmente el software antivirus?			
4	¿Se realizan escaneos periódicos de virus a las pantallas?			
5	¿Se controla la instalación de software no autorizado en las pantallas?			
6	¿El sistema operativo está actualizado?			
7	¿Existe un firewall activo?			
8	¿Se restringe el acceso remoto no autorizado a las pantallas dentro del aula?			
9	¿Se capacita al personal sobre amenazas informáticas?			
10	¿Se han detectado infecciones por malware en el pasado?			
11	¿Se hace copia de seguridad de la configuración de las pantallas?			
12	¿Se cuenta con medidas de protección para evitar la ejecución de software malicioso en las pantallas?			
13	¿Las redes inalámbricas tienen cifrado WPA2 o superior?			
14	¿Se realiza monitoreo periódico del estado del software instalado en las pantallas?			
15	¿Se han detectado comportamientos anómalos en las pantallas recientemente?			
16	¿Se restringe el acceso a páginas web peligrosas?			
17	¿Los puertos USB están controlados?			
18	¿Se notifica a TI cuando se detecta un comportamiento anómalo?			
19	¿Se monitorean los logs del sistema?			
20	¿Se limita el acceso a cuentas con privilegios de administrador?			
21	¿Los usuarios tienen sesiones con tiempo de expiración?			
22	¿Se bloquea el acceso a sitios web sospechosos en la pantalla?			
23	¿Se controlan las aplicaciones que pueden instalarse en las pantallas?			
24	¿Se supervisa el tráfico de red de las pantallas para detectar posibles ataques o infecciones?			
25	¿Existe una política de respuesta ante incidentes por malware?			

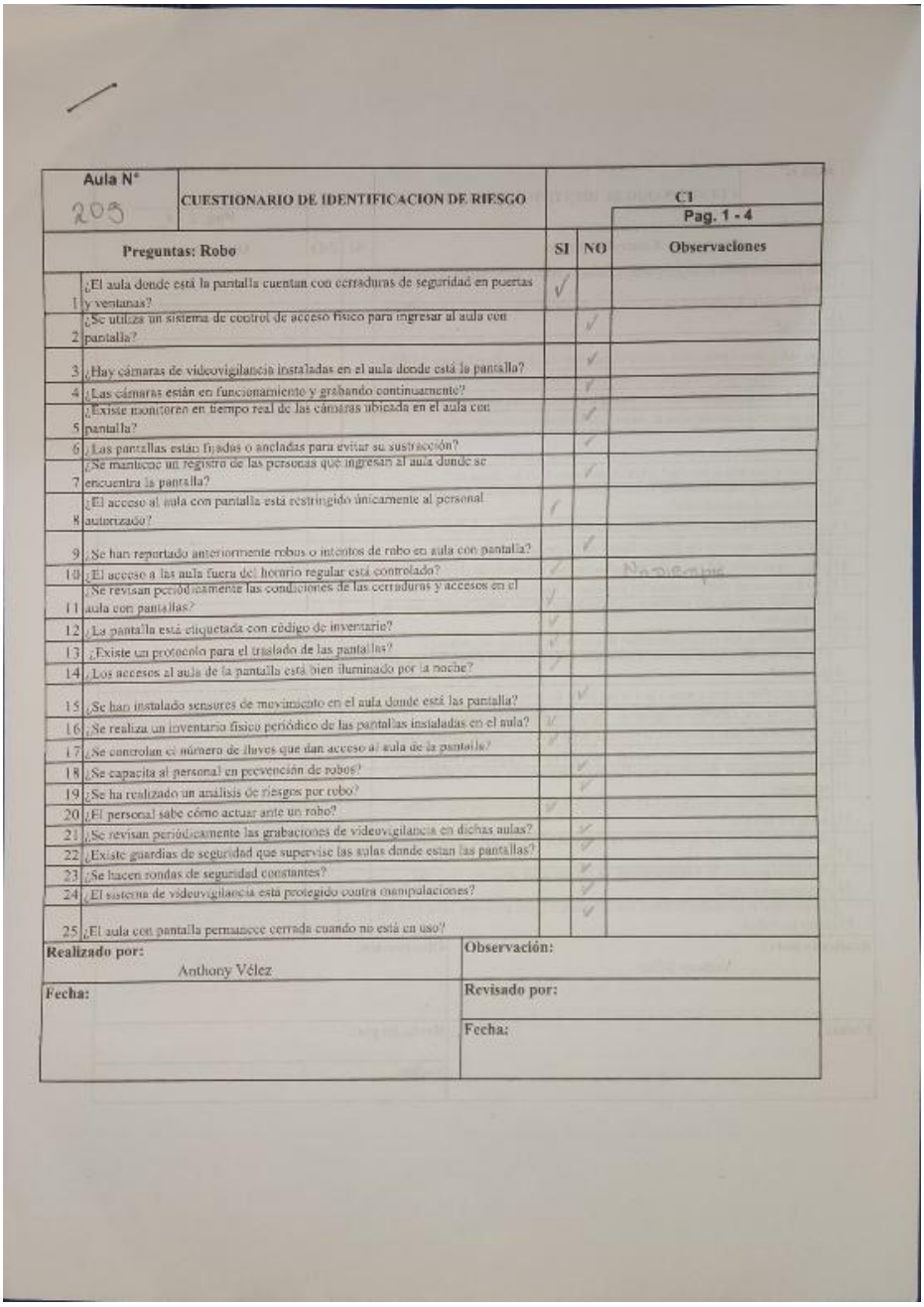
Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

- **Cuestionario Incendio**

Aula N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1		
				Pag. 4 - 4
	Preguntas: Incendio	**SI**	**NO**	**Observaciones**
1	¿Las aulas cuentan con detectores de humo?			
2	¿Existen extintores disponibles y visibles?			
3	¿Están los extintores dentro de su periodo de vigencia?			
4	¿Se han hecho simulacros de evacuación?			
5	¿Hay salidas de emergencia claramente señalizadas?			
6	¿El personal conoce el plan de evacuación?			
7	¿Las instalaciones eléctricas están certificadas?			
8	¿Se realiza mantenimiento a los detectores de humo?			
9	¿Hay sensores de calor o sistemas automáticos contra incendio?			
10	¿Las pantallas están alejadas de fuentes inflamables?			
11	¿Se hace revisión periódica de cables y enchufes?			
12	¿Los enchufes múltiples están controlados?			
13	¿El sistema eléctrico tiene protección contra sobrecarga?			
14	¿Se revisa periódicamente la instalación eléctrica?			
15	¿Existen mapas de rutas de evacuación?			
16	¿Se cuenta con un comité de seguridad?			
17	¿Se documentan los incidentes relacionados con fuego?			
18	¿Se han presentado conatos de incendio anteriormente?			
19	¿Hay iluminación de emergencia?			
20	¿Las puertas de emergencia están desbloqueadas?			
21	¿Los equipos están apagados al finalizar la jornada?			
22	¿Hay señalización de no fumar?			
23	¿Se dispone de alarmas sonoras para emergencias?			
24	¿Se ha capacitado al personal en uso de extintores?			
25	¿Existe un sistema de detección centralizado?			

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

- **Cuestionario de riesgos aplicado**



Aula N° 203	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 1 - 4		
	Preguntas: Robo	**SI**	**NO**	**Observaciones**
1	¿El aula donde está la pantalla cuentan con cerraduras de seguridad en puertas y ventanas?	✓		
2	¿Se utiliza un sistema de control de acceso físico para ingresar al aula con pantalla?		✓	
3	¿Hay cámaras de videovigilancia instaladas en el aula donde está la pantalla?		✓	
4	¿Las cámaras están en funcionamiento y grabando continuamente?		✓	
5	¿Existe monitoreo en tiempo real de las cámaras ubicada en el aula con pantalla?		✓	
6	¿Las pantallas están fijadas o ancladas para evitar su sustracción?		✓	
7	¿Se mantiene un registro de las personas que ingresan al aula donde se encuentra la pantalla?		✓	
8	¿El acceso al aula con pantalla está restringido únicamente al personal autorizado?	✓		
9	¿Se han reportado anteriormente robos o intentos de robo en aula con pantalla?		✓	
10	¿El acceso a las aula fuera del horario regular está controlado?	✓		Nadie ingresa
11	¿Se revisan periódicamente las condiciones de las cerraduras y accesos en el aula con pantallas?	✓		
12	¿La pantalla está etiquetada con código de inventario?	✓		
13	¿Existe un protocolo para el traslado de las pantallas?	✓		
14	¿Los accesos al aula de la pantalla está bien iluminado por la noche?	✓		
15	¿Se han instalado sensores de movimiento en el aula donde está las pantalla?		✓	
16	¿Se realiza un inventario físico periódico de las pantallas instaladas en el aula?	✓		
17	¿Se controlan el número de llaves que dan acceso al aula de la pantalla?	✓		
18	¿Se capacita al personal en prevención de robos?		✓	
19	¿Se ha realizado un análisis de riesgos por robo?		✓	
20	¿El personal sabe cómo actuar ante un robo?	✓		
21	¿Se revisan periódicamente las grabaciones de videovigilancia en dichas aulas?		✓	
22	¿Existe guardias de seguridad que supervise las aulas donde estan las pantallas?		✓	
23	¿Se hacen rondas de seguridad constantes?		✓	
24	¿El sistema de videovigilancia está protegido contra manipulaciones?		✓	
25	¿El aula con pantalla permanece cerrada cuando no está en uso?		✓	

Realizado por: Anthony Vélez	**Observación:**
Fecha:	**Revisado por:**
	Fecha:

VERSIÓN 1.0

23 DE JULIO 2025

UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

MANUAL DE POLÍTICAS DE SEGURIDAD

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

AUTOR: ANTHONY BLADIMIR VÉLEZ VILLAVICENCIO

EL CARMEN - MANABÍ

CONTENIDO

MANUAL DE POLÍTICAS DE SEGURIDAD

El presente manual establece procedimientos y medidas específicas de respuesta ante incidentes que puedan afectar las pantallas electrónicas utilizadas como herramienta de apoyo en las aulas. Basado exclusivamente en los riesgos identificados mediante el análisis de riesgos realizado —Daño de Equipos, Incendio, Robo y Malware— este documento tiene como propósito minimizar las interrupciones del servicio, proteger la integridad de la información proyectada y asegurar la continuidad operativa de los recursos tecnológicos.

La implementación de este manual permitirá a los responsables tomar decisiones oportunas y documentar cada evento, reforzando la cultura de seguridad y mantenimiento preventivo dentro de la institución.

1. CONCEPTOS BÁSICOS

1.1 VALORACIÓN DE RIESGOS

De acuerdo con la ISO/IEC 27005, la valoración de riesgos combina la probabilidad de ocurrencia de un evento no deseado con el impacto que este puede generar sobre los activos de información. La matriz de riesgos levantada identifica cuatro riesgos principales: Daño de Equipos, Incendio, Robo y Malware, los cuales fueron evaluados según su impacto en la Confidencialidad, Integridad y Disponibilidad de la información (Modelo CIA).

1.2 IMPORTANCIA DE LA RESPUESTA A INCIDENTES

La respuesta efectiva ante incidentes permite mitigar pérdidas, garantizar la continuidad de los procesos académicos y proteger los activos tecnológicos de la institución. Cada riesgo identificado requiere procedimientos diferenciados, responsables asignados y registros que respalden las acciones realizadas.

1.3 CONTEXTO DE LAS PANTALLAS ELECTRÓNICAS

Las pantallas electrónicas son herramientas clave en entornos educativos, pues facilitan la presentación de información visual, clases interactivas y procesos de enseñanza-aprendizaje dinámicos. Su falla, daño o vulneración puede afectar gravemente la calidad educativa.

2. PROCEDIMIENTOS DE RESPUESTA

2.1 RIESGO: DAÑO DE EQUIPOS

2.1.1. DESCRIPCIÓN DEL RIESGO

El daño de equipos se refiere a la posibilidad de fallos físicos, averías mecánicas o deterioros imprevistos que afecten el funcionamiento normal de las pantallas electrónicas instaladas en las aulas. Este riesgo puede originarse por desgaste natural, mal uso, falta de mantenimiento preventivo o factores ambientales (humedad, polvo, sobrecargas eléctricas).

2.1.2. MEDIDAS PREVENTIVAS

Para reducir la probabilidad y severidad del daño de equipos, se recomienda:

- Realizar mantenimientos preventivos periódicos de limpieza y revisión técnica.
- Proteger las pantallas con reguladores de voltaje o sistemas de protección eléctrica.
- Capacitar al personal y usuarios sobre el uso correcto de los equipos.
- Documentar el estado físico de las pantallas mediante inspecciones regulares.

2.1.3. PROCEDIMIENTOS DE RESPUESTA INMEDIATA

En caso de presentarse un daño:

- Identificar y aislar la pantalla afectada para evitar daños mayores.
- Notificar al área técnica o responsable de infraestructura.
- Registrar la incidencia en el formato de reporte de incidentes físicos.
- Revisar si el daño es reparable en sitio o requiere reemplazo.

2.1.4. PROCEDIMIENTOS DE RECUPERACIÓN

- Ejecutar la reparación o sustitución del componente afectado en el menor tiempo posible.
- Validar el correcto funcionamiento de la pantalla después de la intervención.
- Actualizar el inventario de equipos y registrar las acciones correctivas realizadas.
- Analizar la causa raíz para evitar reincidencias.

2.1.5. RESPONSABLES

- Departamento de TI: coordinar mantenimiento y soporte técnico.
- Personal de aula: reportar daños inmediatamente.
- Departamento de TI: validar reparaciones mayores o compras de reemplazo.

2.1.6. REGISTROS Y EVIDENCIAS

- Formatos de reporte de daños.
- Bitácoras de mantenimiento preventivo y correctivo.
- Evidencias fotográficas de daños y reparaciones.

2.1.7. FORMATO DE REGISTRO SUGERIDO:

Código de incidente: **Fecha y hora:** **Aula/Ubicación:** **Descripción del daño.** **Acciones correctivas aplicadas.** **Responsable técnico.** **Firma de conformidad**

2.1.8. ROLES IMPLICADOS:

Docente: notifica el incidente.

Soporte Técnico: evalúa, repara o reemplaza.

Coordinador TI: aprueba reemplazos o compras.

2.1.9. FLUJOGRAMA DE RESPUESTA:

2.2 RIESGO: INCENDIO

2.2.1. DESCRIPCIÓN DEL RIESGO:

El riesgo de incendio comprende cualquier situación que pueda provocar fuego en las instalaciones donde se encuentran las pantallas electrónicas. Puede originarse por fallos eléctricos, cortocircuitos, sobrecalentamiento de equipos o condiciones ambientales.

2.2.2. MEDIDAS PREVENTIVAS:

- Realizar inspecciones eléctricas periódicas.
- Instalar extintores adecuados cerca de las áreas de pantallas.
- Capacitar a docentes y personal en uso de extintores.
- Evitar sobrecargas eléctricas y múltiples conexiones improvisadas.

Las medidas preventivas nos ayudan a mitigar el riesgo de sufrir algún daño causado por incendio, las cuales deben ser planificadas con anticipación.

2.2.3. RESPUESTA INMEDIATA:

- Activar alarmas de incendio.
- Evacuar la zona siguiendo el plan de emergencia.
- Usar extintores si el fuego es incipiente.
- Notificar a bomberos o personal de seguridad.

2.2.4. RECUPERACIÓN:

- Evaluar daños estructurales y de equipos.
- Reemplazar equipos dañados.
- Revisar instalaciones eléctricas antes de reinstalar pantallas.
- Actualizar inventarios y planes de contingencia.

2.2.5. FORMATO DE REGISTRO

En el siguiente apartado se muestra un formato de ejemplo para registrar un incidente:

Fecha y hora del incidente: **Descripción del evento** **Reporte de daños** **Acciones tomadas** **Lecciones aprendidas** **Firma de conformidad**

2.2.6. ROLES IMPLICADOS:

- Personal de seguridad.
- Área de mantenimiento.
- Responsable de infraestructura.

2.3 RIESGO: ROBO

2.3.1. DESCRIPCIÓN:

El robo comprende la sustracción deliberada de las pantallas electrónicas o de componentes críticos. Puede ocurrir durante horarios sin supervisión, en espacios vulnerables o por ausencia de medidas físicas de protección.

2.3.2. MEDIDAS PREVENTIVAS:

- Anclar físicamente las pantallas a la pared o mobiliario.
- Instalar cámaras de seguridad en aulas y pasillos.
- Controlar accesos y cerrar aulas fuera de horario.
- Registrar entradas y salidas de personal.

2.3.3. RESPUESTA INMEDIATA:

- Notificar a seguridad institucional.
- Levantar acta de robo.
- Revisar grabaciones de cámaras.
- Denunciar ante autoridades competentes si aplica.

2.3.4. RECUPERACIÓN:

- Sustituir la pantalla.
- Revisar protocolos de seguridad física.
- Reforzar cerraduras y sistemas de vigilancia.

2.3.5. FORMATO DE REGISTRO:

Fecha y hora:
Ubicación:
Descripción de lo sustraído.
Notificación a autoridades.
Seguimiento del caso
Firma de conformidad

2.3.6. ROLES IMPLICADOS:

Personal de seguridad.

Coordinación administrativa.

Autoridades locales.

2.4 RIESGO: MALWARE

2.4.1 DESCRIPCIÓN:

El malware es software malicioso que puede infectar sistemas operativos vinculados a las pantallas inteligentes, afectando su funcionamiento, integridad de datos y disponibilidad de los servicios.

2.4.2. MEDIDAS PREVENTIVAS:

- Instalar antivirus actualizado.
- Restringir conexiones USB no autorizadas.
- Capacitar usuarios sobre riesgos de descargas y sitios no seguros.
- Realizar escaneos periódicos.

2.4.3. RESPUESTA INMEDIATA:

- Desconectar la pantalla de la red.
- Ejecutar escaneo de malware.
- Eliminar archivos infectados.
- Restaurar configuraciones si es necesario.

2.4.4. RECUPERACIÓN:

- Actualizar el sistema operativo.
- Reinstalar software legítimo.
- Validar integridad de archivos.
- Documentar lecciones aprendidas.

2.4.5. FORMATO DE REGISTRO:

Fecha y hora:
Descripción de infección
Herramienta usada para limpieza
Evidencias de eliminación
Firma de conformidad

2.4.7. Roles implicados:

- Personal de soporte técnico.
- Responsable de ciberseguridad.
- Usuarios finales.

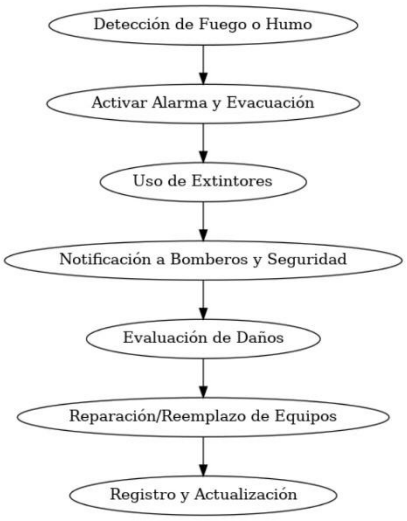
CONCLUSIONES

La implementación de procedimientos claros para responder ante incidentes de Daño de Equipos, Incendio, Robo y Malware permite a la institución educativa fortalecer la seguridad física y lógica de sus pantallas electrónicas, garantizando la continuidad de las clases y la protección de la información proyectada. La aplicación constante de medidas preventivas, la capacitación y la mejora continua de estos protocolos contribuirán a reducir la materialización de estos riesgos y a minimizar sus impactos.

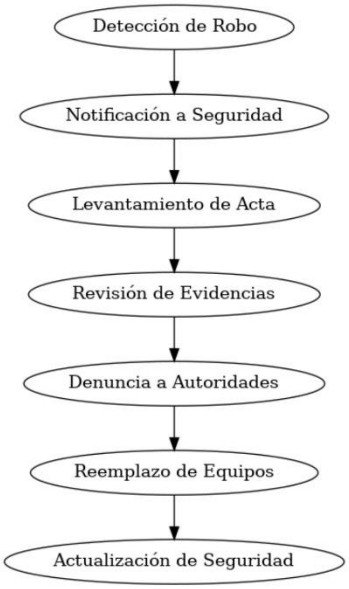
ANEXOS

1. **Flujogramas resumidos de respuesta.**
   - **Daños**

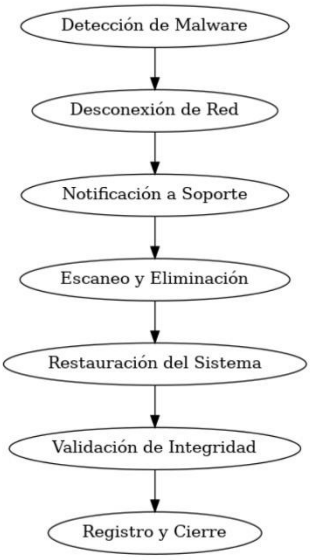
   - **Incendios**



- **Robo**



- **Malware**



2. **Modelos de formatos de registro.**

Ejemplo

Campo	Descripción
Código de Incidente	Identificador único del reporte.
Fecha y Hora	Fecha y hora de detección del daño.
Aula o Ubicación	Lugar exacto donde está instalada la pantalla.
Descripción del Daño	Detalles del problema físico identificado.
Persona que Reporta	Nombre y cargo de quien detecta el daño.
Responsable de Soporte	Técnico encargado de la revisión.
Acciones Correctivas Aplicadas	Reparación o sustitución realizada.
Observaciones	Comentarios adicionales.
Firma Responsable	Firma del técnico que realiza la acción.
Firma de Conformidad	Firma de quien valida la reparación.

3. **Checklists de mantenimiento y seguridad**

Ejemplo

Ítem	Verificación	Observaciones	Responsable	Firma
Estado físico de la pantalla (sin golpes, rayones)	☐ Sí ☐ No			
Funcionamiento de imagen y sonido	☐ Sí ☐ No			
Limpieza externa realizada	☐ Sí ☐ No			
Conexiones eléctricas revisadas	☐ Sí ☐ No			
Regulador de voltaje en funcionamiento	☐ Sí ☐ No			
Pruebas de encendido y apagado correctas	☐ Sí ☐ No			
Reporte de fallas menores levantado (si aplica)	☐ Sí ☐ No			

GLOSARIO

A

Activo (informático)

Recurso valioso para una organización, como hardware, software, datos o instalaciones, que debe ser protegido contra riesgos.

Amenaza

Evento o acción potencial que puede explotar una vulnerabilidad y afectar la seguridad de un activo.

Análisis de Riesgos

Identificación y evaluación de amenazas, vulnerabilidades y riesgos que afectan a los activos de información.

Auditoría de Seguridad Informática

Proceso de revisión sistemática para evaluar controles, identificar vulnerabilidades y verificar el cumplimiento de políticas de seguridad.

B

Backup (Copia de Seguridad)

Duplicado de información almacenado para restaurarla en caso de pérdida o daño.

C

Confidencialidad, Integridad y Disponibilidad (C-I-D)

Principios básicos de la seguridad de la información que buscan garantizar que los datos sean accesibles solo para quienes corresponda (confidencialidad), se mantengan correctos y completos (integridad) y estén disponibles cuando se necesiten (disponibilidad).

Control Compensatorio

Medida alternativa implementada cuando no es posible aplicar un control de seguridad principal, con el objetivo de mitigar riesgos.

Control Correctivo

Acción implementada después de un incidente para mitigar sus efectos y restaurar el funcionamiento normal.

Control Disuasivo

Medida que busca desalentar o disuadir a un atacante de intentar violar la seguridad.

Control Preventivo

Medida de seguridad diseñada para evitar que una amenaza se materialice y cause un incidente.

Control Señuelo (Honeypot)

Mecanismo que simula un objetivo vulnerable para atraer a atacantes y desviar ataques, facilitando su detección.

Controles de Seguridad

Medidas técnicas, organizativas o físicas diseñadas para proteger la información y reducir los riesgos asociados a amenazas y vulnerabilidades.

Controles Físicos y Lógicos

Medidas para proteger los activos de información; los controles físicos incluyen cerraduras y vigilancia, mientras que los lógicos se refieren a software y configuraciones de sistemas.

E

Encuesta Tipo Cuestionario

Herramienta de recolección de datos estructurada con preguntas cerradas para obtener información cuantitativa.

Entrevista Estructurada

Técnica de investigación cualitativa con preguntas definidas de antemano para obtener información específica y comparable.

Error de Muestreo

Diferencia entre los resultados obtenidos de la muestra y los que se obtendrían si se estudiara toda la población.

F

Firewall

Dispositivo o software que filtra y controla el tráfico de red para proteger sistemas de accesos no autorizados.

G

GDPR (General Data Protection Regulation)

Reglamento General de Protección de Datos de la Unión Europea que regula la protección de datos personales y la privacidad de los individuos.

H

Honeypot / Honeynet

Técnicas de seguridad que utilizan sistemas señuelo para atraer atacantes y analizar sus métodos sin comprometer sistemas reales.

I

Impacto (de seguridad)

Consecuencia o daño resultante de que una amenaza materialice una vulnerabilidad sobre un activo.

IPS (Intrusion Prevention System)

Sistema de prevención de intrusiones que detecta y bloquea actividades maliciosas en la red en tiempo real.

ISO/IEC 20000-1

Norma internacional que define los requisitos para un Sistema de Gestión de Servicios de TI, alineado a la calidad y mejora continua de los servicios tecnológicos.

ISO/IEC 27001

Norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO/IEC 27002

Norma complementaria a la ISO 27001 que proporciona directrices para la implementación de controles de seguridad de la información.

M

MAGERIT

Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información, desarrollada en España para evaluar y tratar riesgos informáticos.

Malware

Software malicioso diseñado para dañar, infiltrarse o robar información de sistemas informáticos.

Manual de Uso

Documento que establece instrucciones y recomendaciones para el uso correcto de equipos o sistemas tecnológicos.

Modelo PHVA (Planificar, Hacer, Verificar, Actuar)

Ciclo de mejora continua usado en sistemas de gestión para planificar, ejecutar, verificar resultados y actuar para optimizar procesos.

Muestreo Aleatorio Simple

Técnica estadística para seleccionar una muestra representativa de una población, donde todos los elementos tienen la misma probabilidad de ser elegidos.

N

Nivel de Confianza

Porcentaje que indica la certeza de que los resultados obtenidos de una muestra reflejan la realidad de la población.

P

Pizarra Digital Interactiva (PDI)

Dispositivo electrónico que combina proyector y superficie táctil para permitir interacción directa con contenidos digitales.

Plan de Respuesta a Incidentes

Procedimiento organizado para detectar, responder y recuperar ante incidentes de seguridad de la información.

Políticas de Seguridad

Normas y directrices internas que definen cómo se debe proteger la información dentro de una organización.

Población Marco

Conjunto definido de elementos o individuos que conforman el universo de estudio para una investigación.

Probabilidad (de riesgo)

Posibilidad de que ocurra un incidente de seguridad como resultado de una amenaza sobre una vulnerabilidad.

Procedimientos Estándar

Instrucciones detalladas y sistemáticas para realizar tareas de forma consistente y segura.

R

Regulador de Voltaje

Dispositivo que estabiliza la corriente eléctrica para proteger equipos sensibles de variaciones de voltaje.

Riesgo

Combinación de la probabilidad de que ocurra un evento de seguridad y el impacto que este podría generar.

S

Sistema de Gestión de Seguridad de la Información (SGSI)

Conjunto de procesos y políticas que permiten gestionar y mejorar de forma continua la seguridad de la información en una organización, protegiendo su confidencialidad, integridad y disponibilidad.

T

Tabulación de Datos

Organización y presentación de datos recolectados para facilitar su análisis e interpretación.

Tecnología Educativa

Uso planificado de dispositivos, recursos digitales y herramientas tecnológicas para apoyar, optimizar y mejorar los procesos de enseñanza y aprendizaje.

TIC (Tecnologías de la Información y la Comunicación)

Conjunto de tecnologías que facilitan el acceso, producción, almacenamiento y transmisión de información mediante herramientas como computadoras, internet, redes y software especializado.

V

Vulnerabilidad

Debilidad o falla en un sistema o activo que puede ser explotada por amenazas para causar daños o pérdidas.