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

AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DEL ÁREA ADMINISTRATIVA ULEAM EXTENSIÓN EL CARMEN

FUERES MADERA ARIEL ALEXANDER
AUTOR

MINAYA MACIAS RENELMO WLADIMIR
TUTOR

EL CARMEN, FEBRERO 2026

CERTIFICACIÓN DEL TUTOR

Uleam	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 de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabi, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría del estudiante **FUERES MADERA ARIEL ALEXANDER**, legalmente matriculado/a en la carrera de Ingeniería en Tecnología de la Información, periodo académico 2025(1)-2025(2), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es "**AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DEL ÁREA ADMINISTRATIVA ULEAM EXTENSIÓN EL CARMEN**".

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, 02 de Enero de 2026.

Lo certifico,

Wladimir Minaya Macías, Mg.Sc.
Docente Tutor
Área: Tecnología de la Información

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: Auditoría Informática a la Seguridad de los equipos del Área Administrativa ULEAM Extensión El Carmen.

Modalidad: Proyector Integrador

Autor: Fueres Madera Ariel Alexander

Tutor: Ing. Minaya Macías Renelmo Wladimir, Mg

Tribunal de Sustentación:

Presidente:

Ing. Reascos Pinchao Raul Saed, Mg.

Miembro:

Ing. Pozo Hernández Clara Guadalupe, Mg.

Miembro:

Ing. Mendoza Villamar Rocio Alexandra, Mg.

Fecha de Sustentación:
23 de Febrero de 2026

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: Auditoría informática a la seguridad de los equipos del área administrativa Uleam Extensión El Carmen, corresponde exclusivamente a: Fueres Madera Ariel Alexander con CI. 2300702871 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Fueres Madera Ariel Alexander

C.I. 2300702871

DEDICATORIA

A mi familia por darme ese apoyo en todo momento a lo largo de este camino.

A cada uno de los profesores que me impartieron su conocimiento, sabiduría y enseñanzas que les dejo la vida en su largo camino como docentes.

Y con más orgullo me lo dedico a mí mismo, por haber logrado un objetivo que parecía imposible, pero paso a paso lo fui logrando.

ARIEL ALEXANDER FUERES MADERA

AGRADECIMIENTO

Agradezco a Dios, por darme las fuerzas y el enfoque que me mantuvo en todo momento atento a todo.

A la ULEAM, por ser ese lugar donde me fui formando como profesional.

A cada persona que conocí en este tiempo los cuales fueron momentos de ayuda y aprendizaje.

A mis compañeros de carrera con los que fueron muchos momentos de alegría.

ARIEL ALEXANDER FUERES MADERA

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

En la actualidad las Instituciones de Educación Superior dependen de gran parte de su infraestructura tecnológica para llevar a cabo sus procesos administrativos. La Universidad Laica "Eloy Alfaro" de Manabí Extensión El Carmen, no se queda lejos ante esta realidad, en la que se les presentan desafíos para la protección de su información.

El objetivo general es Desarrollar una Auditoria Informática para la seguridad de los equipos del área administrativa Uleam Extensión El Carmen, con el objetivo de identificar vulnerabilidades y amenazas, se propone realizar una Auditoria de Seguridad previo a eso la implementación de un Plan de Contingencia.

La metodología que se aplico fue descriptiva, evaluando al 100% de la población conformada por 7 personas, se emplearon cuestionarios y guías de observación basadas en los marcos de trabajo COBIT e ISO/IEC 27001:2022, los resultados que se obtuvieron revelaron un nivel de madurez de 1.4(Marginal) en donde se identificaron riesgos críticos como la falta de UPS y la ausencia de respaldos de información.

Finalmente se detallan los hallazgos que se encontraron y se proponen acciones correctivas para que deesa forma la Universidad tenga un ambiente seguro de su información.

ABSTRACT

Currently, Higher Education Institutions rely heavily on their technological infrastructure to carry out their administrative processes. The Laica "Eloy Alfaro" University of Manabí, El Carmen Extension, is no exception to this reality, as it faces challenges related to the protection of its information.

The general objective is to develop an Information Technology Audit for the security of the equipment in the administrative area of ULEAM El Carmen Extension, in order to identify vulnerabilities and threats. The proposal consists of conducting a Security Audit, preceded by the implementation of a Contingency Plan.

The methodology applied was descriptive, evaluating 100% of the population consisting of 7 people; questionnaires and observation guides based on the COBIT and ISO/IEC 27001:2022 frameworks were used. The results obtained revealed a maturity level of **1.4 (Marginal)**, where critical risks were identified, such as the lack of UPS.

Finally, this chapter details the findings identified and proposes corrective actions so that the University can ensure a secure information environment.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

En la era digital actual que nos encontramos las Instituciones de Educación Superior dependen en gran parte de la infraestructura que manejan para garantizar la seguridad de su información y garantizar la continuidad de sus procesos. Los equipos informáticos con los que cuentan no solo sirven como herramientas de apoyo, sino que son activos tecnológicos los cuales requieren protección ante amenazas o fallos técnicos.

El presente trabajo de titulación surge ante la necesidad de realizar un Plan de Contingencia para estar prevenidos ante algún incidente. La investigación partió mediante la realización de encuestas al personal del Area Administrativa, con esto se logró identificar la vulnerabilidad que enfrentan en las cuales destacan la falta de protección eléctrica (UPS), falta de respaldos automáticos.

Ante esta problemática se integró una Auditoria basada en la normativa ISO/IEC:27001:2022, esta revelo que aun cuentan con controles básicos. El proyecto está estructurado en seis capítulos, iniciando en el planteamiento del problema y fundamento de estándares globales, luego detalla una metodología que valida la información que fue recolectada, se propone una estrategia basada en el análisis de riesgo terminado con una revisión de los resultados para de tal forma fortalecer la infraestructura tecnológica.

Esta propuesta busca transcender la protección del hardware, promoviendo un ambiente seguro para los futuros estudiantes. Con esta implementación la ULEAM Extensión El Carmen busca asegurar un entorno educativo confiable y seguro.

1.2 Presentación del tema

Auditoría informática a la seguridad de los equipos del área administrativa ULEAM Extensión El Carmen.

1.3 Ubicación y contextualización de la problemática

La Universidad Laica Eloy Alfaro de Manabí (Uleam), Extensión El Carmen ubicada en Ecuador tiene una misión importante en el desarrollo profesional de cada estudiante matriculado en dicha Institución, siendo un pilar fuerte para el desarrollo educativo de la región, el área administrativa de la Universidad es el corazón de la gestión administrativa de la Universidad ya que se encarga del control académico, finanzas, recursos humanos y la atención estudiantil, todas estas actividades dependen en gran medida del uso de equipos informáticos es importante recalcar que estos sistemas manejan información sensible los cuales manejan datos importantes y personales de cada estudiante.

No obstante, en la Universidad no siempre se cuenta con políticas de seguridad informática ni con procedimientos que evalúen los riesgos, esto genera una amenaza dentro del área administrativa tanto interna como externa los cuales pueden ser accesos no autorizados, perdida de la información, malware o algún tipo de falla técnica.

No realizar una Auditoría Informática al área administrativa, no permite conocer el estado real de la seguridad en sus equipos, por tal motivo pueden afectar la continuidad operativa de sus servicios afectante tanto como al personal administrativo docentes y estudiantes, por tal razón resulta ser muy necesario realizar una Auditoría para poder evaluar los niveles de seguridad actual y proponer mejoras concretas, este trabajo contribuirá de gran manera para fortalecer la seguridad y garantizar una protección de los equipos y la información de la Uleam Extensión el Carmen.

1.4 Planteamiento del problema

1.4.1 Problematización

En la era digital actual que nos encontramos hoy en día, las instituciones dependen cada vez mas de su uso para el desarrollo de sus actividades, esto facilita la mejora en la eficiencia operativa y además una mayor exposición a amenazas relacionadas con la seguridad informática. En este sentido garantizar la protección de los datos y los equipos pasa a convertirse en una necesidad prioritaria.

La Universidad Laica Eloy Alfaro de Manabí (Uleam), Extensión el Carmen, no pasa por alto ante esta realidad, su área administrativa realiza el uso constante de equipos tecnológicos para gestionar la información de cada estudiante, personal y docentes, por tal motivo se realiza una auditoría que permita conocer el estado actual de la seguridad de los equipos para de esa manera identificar las vulnerabilidades y amenazas para sentar bases y tener definido estrategias efectivas para favorecer la protección de tan sensible información y prevenir fallos en su sistemas educativo.

1.4.2 Génesis del problema

Debido al crecimiento acelerado de las tecnologías en el ámbito institucional el proceso administrativo que se realizaba de forma tradicional se realiza digitalmente, esto permite más eficiencia y agilidad en sus procesos datos y servicios, debido a este cambio han surgido nuevos desafíos principalmente en el área informática.

En muchas Instituciones de educación superior, en este caso la Uleam Extensión el Carmen sus equipos tecnológicos han crecido significativamente pero no siempre conto con una excelente seguridad informática, como consecuencia los equipos pueden quedar expuestos a varias amenazas como son, virus, accesos no autorizados, perdida de información, e incluso fallas en sus equipos lo que compromete en la integridad de sus funciones.

Estas debilidades son aún más fuertes en instituciones Universitarias, donde no se cuente con personal especializado en Auditoria Informática. Dicha situación lleva a la necesidad de realizar una Auditoría Informática para de esa manera diagnosticar las debilidades de sus equipos y proponer soluciones para sus equipos tecnológicos.

Al tener falta de una Auditoría periódicamente ciega a la Universidad a tener conocimiento del estado actual que se encuentran sus activos tecnológicos. Sin la Auditoria resulta casi imposible identificar de donde provienen las brechas de seguridad, cuáles son los riesgos más fuertes o qué medidas se podría implementar, esto no solo pone en riesgo gran cantidad de información de estudiantes, docentes y personal administrativo, sino que esto podría generar un gran impacto negativo a la Universidad ya que un incidente de estos por más pequeño que sea puede generar

interrupciones operativas o incluso costos económicos significativos, ya lo peor que podría suceder seria la pérdida de confianza de gran parte de la comunidad Universitaria.

1.4.3 Estado actual del problema

La Universidad Laica Eloy Alfaro de Manabí (Uleam), Extensión el Carmen, ha mejorado en sus procesos administrativos con equipos informáticos para mejorar su funcionamiento, dichos equipos son muy importantes para la Universidad ya que permiten gestionar varias actividades de estudiantes y docentes.

A pesar de haber logrado un gran avance tecnológico, se nota la ausencia de una Auditoría Informática a los equipos usados, no existen registros de una Auditoria o políticas sobre el monitoreo de amenazas o vulnerabilidades, también los equipos no cuentan con medidas de seguridad que los proteja ante cualquier amenaza. Toda el área administrativa al estar constantemente operando con conectividad a internet aumenta más las posibilidades a ataques,

En este caso al no contar con una Auditora impide que se reconozca los riesgos a los que están expuestos limitando su operatividad continua, todos estos problemas a los que pueden quedar expuestos pone en una necesidad urgente de evaluar sus equipos con el objetivo de identificar las vulnerabilidades y amenazas para establecer políticas para mejorar la seguridad.

Esto también implica que la capacidad de respuesta ante un ataque de seguridad sea limitada, porque al no tener conocimiento claro de las debilidades cualquier problema que se presente generaría un alto a sus actividades operativas lo que también llevaría a generar mayores gastos de lo normal. Hoy en día en la actualidad en Ecuador donde la protección de datos personales es un tema muy delicado, al no contar con una seguridad informática podría generar sanciones, por eso esta Auditoria no solo tiene como objetivo la seguridad de la información sino también la responsabilidad de la Universidad de proteger los activos de información más valiosos y asegurar de siempre mantener un ambiente digital confiable para el desarrollo de sus funciones.

1.4.4 Diagrama causa – efecto del problema

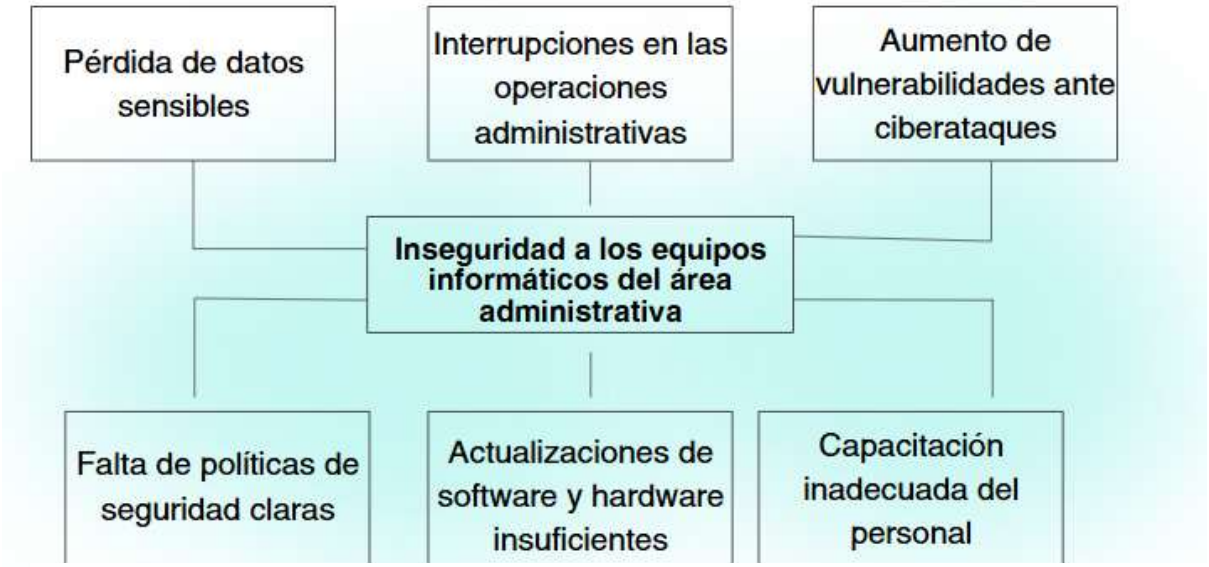


Ilustración 1 Diagrama Causa-Efecto del problema

1.5 Objetivos

1.5.1 Objetivo general

Desarrollar una Auditoría Informática para la seguridad de los equipos del área administrativa Uleam Extensión El Carmen, con el objetivo de identificar vulnerabilidades y amenazas, y proponer un Plan de Contingencia que garantice integridad y disponibilidad de la información.

1.5.2 Objetivos específicos

- Describir la problemática que se presenta en la Auditoría Informática de los equipos del área administrativa Uleam Extensión El Carmen, estableciendo la importancia de realizar una Auditoria Informática en el entorno Universitario.

- Establecer un fundamento teórico sólido sobre Auditoria Informática que sirva como base para diagnosticar o lo que está expuesto.

- Diagnosticar el estado actual de seguridad de los equipos del área administrativa Uleam Extensión El Carmen, logrando identificar vulnerabilidades y amenazas a través de la recolección y análisis de datos.

- Diseñar y proponer un conjunto de medidas y recomendaciones para aumentar la seguridad informática de los equipos, basándose en los hallazgos diagnosticados.

- Evaluar la viabilidad del impacto potencial de las propuestas que se presenten para aumentar la seguridad informática, a través de la realización de un análisis comparativo, para de esa manera demostrar como mejorarían la seguridad.

- Formular conclusiones claras y recomendaciones que orienten a la Universidad en la mejora continua de la seguridad de sus equipos.

1.6 Justificación

Contar con una seguridad informática hoy en día es una parte muy fundamental para de esa forma garantizar su continuidad operativa y la seguridad de sus datos de cualquier institución, en este caso la Universidad Laica Eloy Alfaro de Manabí (Uleam) extensión El Carmen, depende en gran parte de equipos informáticos el área administrativa para ejecutar sus actividades.

Al tener una ausencia de una auditoría pone en riesgo la información que podrían afectarla la eficiencia estudiantil, filtración de datos personales, con eso quedaría manchada la imagen de la Universidad ante los estudiantes.

La presenta investigación se enfoca en realizar la auditoría para diagnosticar el estado y la seguridad actual de sus equipos, servirá para identificar las amenazas y vulnerabilidades para proponer soluciones para fortalecer la infraestructura tecnológica, por otra parte, el objetivo de esta tesis no solo es el aporte técnico, sino que aplicar una mejora en sus actividades.

La única justificación de este trabajo no es la tecnología, sino que tiene varias más como por ejemplo socialmente, al tener la información de cada estudiante, docentes y personal

administrativo contribuye la privacidad y confianza de todos, si se generara una brecha de seguridad se generaría desconfianza dentro del campo Universitario, la otra justificación seria económicamente, al realizar una auditoria preventiva los gastos que se generarían serian mucho más rentable que enfrentarse a los costos que generaría un incidente de seguridad, incluirían por ejemplo recuperar datos o enfrentarse a posibles multas por incumplimiento en proteger la información.

Desde el punto de vista Universitario, la realización de esta tesis proporcionara a la Uleam Extensión El Carmen un conocimiento claro de las debilidades que presentan, logrando que puedan tomar decisiones sobre la implementación de controles de seguridad.

Se presentará una documentación clara con el objetivo de lograr un nivel de seguridad alto, este aporte no solo beneficiaría al área evaluada, sino que mejoraría a toda la comunidad Universitaria, en definitiva, esta auditoria es un paso crucial hacia el camino de una Universiada más segura, más confiable y lista para enfrentarse al futuro digital.

1.7 Impactos esperados

1.7.1 Impacto tecnológico

El impacto tecnológico en las Auditorías ha sido transformador debido a las incorporaciones de las tecnologías avanzadas, se han vuelto más eficientes y precisas facilitando la revisión y el análisis de grandes cantidades de datos, permite también que las personas que se encuentran realizando la Auditoría puedan identificar anomalías o posibles áreas de trabajo que puedan estar en riesgo. (Legalnet, 2023).

Esta auditoría genero un impacto significativo, ya que permitió detectar las debilidades de sus equipos, esto brindaro información real del estado actual de la infraestructura, así como sus vulnerabilidades y con el nivel de protección que cuentan. Una de las mejoras que se lograría es en la gestión de sus actividades ya que se contaría con configuraciones actuales en sus equipos, además permitirá reforzar sus niveles de seguridad como software, antivirus y sistemas de respaldos ya que con esto se reducirá en gran parte los riesgos a los están expuestos.

Detectar las debilidades y tener información precisa sobre la infraestructura actual son pasos importantes, no solo es necesario realizar actualizaciones o implementar nuevos sistemas de seguridad como software, antivirus o respaldos, al tener conocimiento exactamente de las brechas de seguridad la Universidad puede asignar recursos tecnológicos de una manera más eficiente priorizando inversiones menores.

Además, el impacto generara la optimización del rendimiento de sus equipos, las debilidades no solo representan riesgos de seguridad, sino que pueden afectar al sistema y afectar la continuidad operativa, al lograr corregir estas fallas la auditoria contribuiría a que dichos equipos funcionen de manera fluida, lo que generaría in grande impacto en la realización de procesos administrativos .

1.7.2 Impacto social

El valor de una Auditoria no solo radica en la prevención ante ataques internos o externos, sino que también tiene capacidad para ofrecer recomendaciones que permitan mejorar la eficiencia operativa. Varias investigaciones han detectado que la realización de una Auditoría genera descensos significativos reduciendo los incidentes y aumentando la conformidad regulatoria, con ellos trae ventajas competitivas y confianza ante clientes (Bonifaz, 2025).

Contar con una adecuada auditoría informática garantiza que los datos de sus estudiantes, docentes y personal administrativo estén protegidos antes algún tipo de amenaza generando un ambiente seguro en donde la información sea manipulada solo por el personal administrativo.

Detectar las amenazas ayuda a que el sistema administrativo tenga mejoras en su operatividad, ya que se evitan interrupciones por alguna falla o algún otro accidente, ayudando positivamente en la atención de los tramites de los estudiantes.

Mas allá de lograr una protección de datos una auditoría fomenta la confianza dentro de toda la comunidad Universitaria, si un estudiante tiene certeza de que su información personal está bien protegida se siente más tranquilo y con más seguridad al tener interacción con los sistemas que ofrece la Universidad, lograr este nivel de confianza de sus usuarios es algo intangible para cualquier institución educativa.

Además, al generar la operatividad y reducir interrupciones la auditoría aporta una experiencia más eficiente, al poder realizar los trámites sin mucha demora las consultas que se realizan se resuelven de una manera muy rápida, no solo optimiza el tiempo en realizar alguna acción de estudiantes o profesores, la Universidad al tener una seguridad informática solida demuestran el compromiso que tienen con sus estudiantes.

1.7.3 Impacto ecológico

La informática ecológica, conocida también como (TI ecológica), o (TI sostenible), son el diseño, fabricación, uso, y otros componentes de forma que se limite el impacto perjudicial sobre el medio ambiente, esto implica la eliminación de carbono y el consumo excesivo de energía. También abarca la selección de materias de origen renovable y la reducción de residuos electrónicos. (IBM, 2022)

El objetivo principal de una auditoria informática es detectar las amenazas y vulnerabilidades para llegar a soluciones, pero también pueden generar acciones positivas en lo ecológico, si de alguna manera se establecen normas y políticas en el uso de sus equipos informáticos para reducir el consumo innecesario de energía, identificando los equipos que presenten alguna falla lo cual aumenta su consumo energético. También logrando la reducción de hojas de papel al mejorar su sistema pasaría gran parte de sus actividades a ser de forma digital disminuyendo la impresión de documentos físicos, logrando también un aporte al ámbito ecológico.

Mas allá de diagnosticar las fallas en los equipos que aumentar el consumo de energía, una auditora informática puede establecer políticas de eficiencia energética para el uso de sus equipos, incluyendo la realización de una configuración de modos de ahorro de energía, implementar el apagado programado de todos sus equipos cuando ya se encuentren fuera del horario laboral.

Al realizar la migración de datos de físico a digital fomenta la confianza en su sistema, no solo legra la reducción de hojas de papel, sino que también se reduce los costos al realizar impresiones de documentos, estas acciones se traducen a que se desea lograr tener una sostenibilidad ambiental.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

2.1.1 Antecedentes de investigaciones relacionadas al tema presentado

Según la Auditoría realizada en la Dirección Distrital 02D03 Chimbo-San Miguel-Educación, Aplicando Cobit 5 entre los año 2014-2018 dice que existen varios trabajos de auditoría de sistemas que han ayudado en el desarrollo del presente trabajo investigativo, entre los cuales se puede mencionar: a nivel de postgrado se ha realizado los trabajos titulados: "Auditoría de Sistemas basada en riesgos a los procesos del Sistema Nacional de Nivelación y Admisión de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, Aplicando COBIT 4.1 y COSO ERM", realizado por (Vaca Benalcázar & Casanova, 2014); donde se ha evaluado el riesgo, contemplando el marco de referencia COBIT 4.1; en el repositorio digital de la Universidad Regional Autónoma de los Andes (UNIANDES), consta el trabajo titulado: "Auditoría informática y la calidad del servicio de las tecnologías de la información en el distrito de educación 06D04 Colta – Guamote", realizado por: (Pulgar Haro, 2018), donde se concluye que el marco de referencia COBIT, ayuda a entender los sistemas de Tecnologías de la Información (TI), permite decidir el nivel de seguridad y aplicar controles a fin de proteger los activos (información, hardware, software…) de la entidad auditada, basándose en un modelo de desarrollo de gobernación de TI. (Bayas, 2020)

La auditoría informática es esencial en las organizaciones debido al creciente uso de computadoras y centros de procesamiento de datos. Su implementación permite identificar riesgos y establecer controles que protegen la información y los recursos tecnológicos. En el caso del Hospital General Docente de Riobamba, este trabajo de titulación tiene como objetivo evaluar la importancia de la auditoría informática como herramienta de control, especialmente en relación con el cumplimiento de la normativa de control interno 410 sobre Tecnología de la Información. (Samaniego, 2022)

2.2 Definiciones conceptuales

2.3 Definición de Auditoría Informática

Según la RAE, auditor o auditora es aquella persona que realiza una «revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse». (Diccionario de la Lengua Española, 2024)

En otras palabras, es una persona especializada en examinar y evaluar las actividades de un profesional u organización, con el fin de proporcionar una opinión independiente sobre el cumplimiento de las regulaciones y estándares aplicables a la actividad que desempeña. (Auditoría De Seguridad Informática, 2024)

2.3.1 Evolución de Auditoría Informática

La auditoría informática surge como respuesta a la creciente dependencia de las organizaciones en los sistemas de información. Inicialmente, se enfocaba en verificar la correcta operación de los equipos y programas, pero con el tiempo evolucionó hacia la evaluación integral de riesgos, controles y cumplimiento normativo. Hoy en día, es una disciplina estratégica que asegura la confiabilidad, integridad y disponibilidad de la información.

La evolución también refleja la transición de auditorías manuales hacia auditorías automatizadas y basadas en riesgos. Esto ha permitido que las instituciones educativas y empresariales adapten sus procesos de control a entornos digitales, garantizando que los sistemas cumplan con estándares internacionales y respondan a amenazas emergentes (Espinoza, 2021)

2.3.2 Principales pruebas y herramientas para efectuar una Auditoría Informática

Pruebas Sustantivas

Se verifica la confiabilidad de los sistemas, esto se obtiene mediante la observación, cálculos, muestreos, entrevistas, técnicas de examen, todo esto es necesario para saber la exactitud de la información. (Siegal S. , 2024)

Pruebas de cumplimiento

Se verifica el grado de cumplimiento que se maneja mediante la realización de muestreo, para que tal manera pueda ser proporcionado la evidencia de que los controles si existen y que se apliquen efectivamente (Metric, 2022)

2.3.3 Metodologías para la Auditoria Informática

Como ya es de conocimiento existen varias metodologías para la realización de una Auditoría Informática, de los cuales los más usados son:

2.3.4 Octave

Es una evaluación que se basa en riesgos y la planeación técnica de seguridad, ya pasa a ser un proceso interno de la organización, lo que significa que las personas que se encuentren dentro tienen la obligación de la realización de la estrategia de seguridad, por eso esta metodología es interesante porque se basa en el conocimiento del personal que se encuentra dentro de la organización . (Auditoría Informatica , 2024).

2.3.5 Magerit

El objetivo de esta metodología es hacerles frente a los diversos riesgos que se presentan con la seguridad informática, además en Consejo Superior de Administración Electrónica(CSAE), promueve la utilización de esta como respuesta a la gran cantidad de empresas que se basan de esta para lograr sus objetivos (Megerit, 2025)

2.3.6 Objetivos de una Auditoria Informática

Identificación de riesgos: Detectar vulnerabilidades en equipos, redes y software.

Evaluación de controles: Verificar si las medidas de seguridad implementadas son efectivas.

Cumplimiento normativo: Asegurar que se cumplen estándares como ISO/IEC 27001.

Mejora continua: Proponer acciones correctivas para fortalecer la seguridad informática. (Ortega, 2024)

2.3.7 Importancia de Auditoria Informatica en Instituciones Educativas

En universidades, la auditoría informática es vital porque:

- Protege información sensible de estudiantes y docentes.
- Garantiza la continuidad de procesos administrativos.
- Refuerza la confianza en los sistemas digitales.
- Previene sanciones legales relacionadas con la protección de datos. (Contabilidad y Finanzas, 2022)

2.3.8 Tipos de Auditoria Informática

Auditoría de seguridad: centrada en la protección de datos y sistemas frente a amenazas.

Auditoría de cumplimiento: verifica la adhesión a políticas internas y normativas externas.

Auditoría operativa: analiza la eficiencia y eficacia de los procesos tecnológicos.

Auditoría forense: investiga incidentes de seguridad y recopila evidencias digitales.

2.3.9 Integridad

Se trata de dar la autorización a algunos usuarios para que puedan acceder y hacer uso de la información siempre y cuando sea necesario (Polanco, 2025).

2.3.10 Confidencialidad

Solo los usuarios que son autorizados tienen acceso a la variedad de recursos como datos e información (Ciencias, 2025).

2.3.11 Disponibilidad

Siempre tienen que estar disponible la información cuando se acceda al momento de ser utilizada por los usuarios. (Zeltzin, 2024).

2.3.12 Autenticación

Se caracteriza por presentar información real al momento de acceder (Sede Electronica, 2023)

2.3.13 Principios de la Auditoría

Contar con una Auditoria informática es muy crucial en toda organización en donde la información se manipulada por sistemas informáticos, los siguientes principios proporcionan un paso crucial para proteger la información de amenazas. (Auditol, 2024)

2.3.14 Planificación y Alcance de la Auditoría

La planificación y alcance de Auditoría es el proceso mediante el cual el auditor establece una estrategia general y un enfoque detallado de los estados financieros, esta planificación incluye:

- Comprender el entorno del cliente y su control interno.
- Evaluar los riesgos de incorrección material, prestando atención sobre las áreas importantes.
- Determinar los procedimientos de auditoría adecuados.
- Seleccionar a los miembros del equipo de trabajo con capacidad y competencia.
- Coordinar el trabajo de equipo. (Audágora, 2025)

2.3.15 Ciclo PHVA aplicado a Auditoría Informática

El uso de ciclo de mejora continua PHVA se aplica en el proceso de Auditoría para asegurar la adecuada ejecución y funcionamiento.

Planificar: El auditor debe planear y disponer de todos los recursos que sean necesarios para la ejecución de la Auditoría.

Hacer: Se debe tener dispuesto todo lo necesario en cuanto se refiere a recursos, una vez hecho eso se procede a su ejecución de acuerdo lo planeado.

Verificar: El Auditor procede a hacer un seguimiento y revisión al proceso y desempeño del programa de Auditoría con el propósito de observar su comportamiento, y así mismo realizar las mejoras si son necesarias.

Actuar: Una vez que se identifiquen las debilidades y teniendo el Plan de Contingencia Elaborado, se debe implementar las correcciones correspondientes. (Universidad Militar Nueva Granada, 2023)

2.3.16 Auditoria Continua

La auditoría permite revisar que los hechos, actividades y operaciones, se den en la forma planteada en base a políticas y procedimientos, además, permite administrar y aprovechar los recursos y poder aprovechar las oportunidades para reforzar los controles existentes. La auditoría interna al ser considerada como una práctica, es un instrumento basado de la propia administración que, se encarga de la valoración independiente de cada una de sus actividades. (Daniel, 2022).

2.3.17 Auditoria basada en riesgos

La Auditoría basada en riesgos se centra en identificar y evaluar los riesgos que afectan la seguridad de la información. En lugar de revisar todos los procesos de manera uniforme, este enfoque prioriza aquellos que representan mayor impacto para la organización. Esto permite optimizar recursos y focalizar la auditoría en áreas críticas.

En el ámbito académico y administrativo, este tipo de auditoría es esencial para proteger datos sensibles, como información de estudiantes y personal (Cárdenas, 2023).

2.3.18 Auditoria de seguridad en la nube

La auditoría de seguridad en la nube se centra en evaluar los controles de seguridad implementados en servicios cloud como AWS, Azure o Google Cloud. Este tipo de auditoría revisa aspectos como la gestión de accesos, cifrado de datos, cumplimiento normativo y continuidad del servicio. Es fundamental porque las instituciones educativas y empresas cada vez más migran sus datos y aplicaciones a entornos virtualizados.

Además, la auditoría en la nube permite identificar riesgos asociados a la externalización de servicios, como la dependencia de terceros y la exposición a ciberataques. Su objetivo es garantizar que la información alojada en la nube mantenga los mismos niveles de seguridad que en infraestructuras locales, asegurando la integridad y disponibilidad de los datos. (Calder, 2020)

2.3.19 Auditoria de cumplimiento normativo

La auditoría de cumplimiento normativo verifica que los sistemas de información y procesos tecnológicos cumplan con leyes, regulaciones y estándares aplicables. Esto incluye normativas de protección de datos, propiedad intelectual y seguridad informática.

En el ámbito universitario, este tipo de auditoría asegura que las instituciones respeten la legislación vigente sobre privacidad y gestión de información, evitando sanciones legales y fortaleciendo la confianza institucional. (Isaca, 2020)

2.3.20 Auditoria de incidentes y gestión de riesgos

Este subtema se enfoca en la revisión de los procesos de detección, respuesta y mitigación de incidentes de seguridad informática. La auditoría evalúa si las instituciones cuentan con protocolos claros para manejar ataques, fallas o accesos no autorizados.

La gestión de riesgos complementa este proceso, identificando amenazas potenciales y estableciendo controles preventivos. En el contexto académico, permite proteger datos sensibles de estudiantes y personal, garantizando la continuidad de las operaciones. (Casey, 2020)

2.3.21 Auditoria de base de datos

La auditoría de bases de datos consiste en evaluar los mecanismos de seguridad, integridad y disponibilidad de la información almacenada en sistemas de gestión de datos. Se revisan aspectos como el control de accesos, trazabilidad de transacciones, respaldo y recuperación de datos, así como la protección contra ataques internos y externos.

Este tipo de auditoría es esencial en instituciones educativas y organizaciones que manejan grandes volúmenes de información sensible. Garantiza que los datos académicos, administrativos y financieros estén protegidos contra alteraciones no autorizadas y que se cumplan las normativas de confidencialidad y privacidad. (Gomez, 2021)

2.3.22 Auditoria de redes y comunicaciones

La auditoría de redes se centra en evaluar la seguridad de la infraestructura de comunicación, incluyendo routers, switches, firewalls y protocolos de transmisión. Se busca identificar vulnerabilidades que puedan ser explotadas por atacantes para interceptar o manipular datos en tránsito.

En el ámbito académico, esta auditoría asegura que las redes institucionales utilizadas por estudiantes y personal sean confiables y estén protegidas contra accesos no autorizados. Además, permite verificar la correcta implementación de políticas de seguridad y el cumplimiento de estándares internacionales.

La auditoría de redes y comunicaciones evalúa la seguridad, eficiencia y cumplimiento normativo de las redes y sistemas de comunicación de una organización. Incluye análisis de vulnerabilidades, pruebas de penetración, auditorías de gestión de comunicaciones y evaluaciones de continuidad del negocio. El objetivo es determinar si la infraestructura salvaguarda los activos, mantiene la integridad de datos y utiliza recursos de manera eficiente. (Torca, 2023)

2.4 Definición de Seguridad de Equipos

La seguridad de equipos es la protección de la información que se manipule dentro de la organización teniendo como objetivo evitar que sus datos sean filtrados y manipulados por personas que son autorizadas, también es el conjunto de prácticas, estratégicas o métodos para garantizar la integridad de los equipos informáticos. (IBM, ¿Que es la seguridad de equipos?, 2022)

2.4.1 Cuál es la importancia de tener los equipos seguros

Esto ha surgido como una necesidad debido al gran cambio que ha surgido en la tecnología actual, por tal motivo el activo más importante de una organización la información y para mantener todo bien seguro se debe invertir en seguridad, esta se encarga de prevenir y detectar si el sistema está siendo manipulado por personas no autorizadas. (García, 2023).

2.4.2 Cuáles son los tipos de seguridad informática

2.4.3 Seguridad de Hardware

Esta se relaciona con la protección de dispositivos que son usados para proteger su sistema, redes o incluso aplicaciones frente a los riesgos actuales, lo que más se utiliza es el método de manejo de sistemas de alimentación interrumpida (Enrique Villa, Ismael Morales, 2023).

2.4.4 Seguridad de Software

Este tipo se seguridad es usado para salvaguardar los sistemas ante ataques malintencionados que puedan estar expuestos, a causa de estos defectos los atacantes pueden ingresar a los sistemas. (Thales, 2023).

2.4.5 Seguridad de red

Está relacionada con el diseño de actividades para tener bajo seguridad los datos que son accedidos por medio de la red y que pueden ser expuestos y modificados o incluso robados, pero el problema

más frecuente que está expuesto son los virus, robo de información y suplantación de identidad. (UCSP, 2020).

2.4.6 Seguridad lógica de equipos

La seguridad lógica se centra en la protección mediante software y configuraciones. Incluye el uso de antivirus, firewalls, sistemas de respaldo, actualizaciones periódicas y políticas de contraseñas seguras. Su finalidad es evitar accesos no autorizados y reducir la exposición a malware o ataques cibernéticos. (Siegal, 2024)

2.4.7 Seguridad física de los equipos

La seguridad física se refiere a las acciones destinadas a proteger los equipos contra daños materiales, robos o desastres naturales. Incluye el control de acceso a salas de servidores, uso de sistemas de energía ininterrumpida (UPS), instalación de cámaras de vigilancia y medidas contra incendios. (ServeNet, 2023)

2.4.8 Resguardar la información

Esto implica identificar posibles brechas de vulnerabilidad que podrían poner en riesgo la información, para comprobar si la seguridad es excelente se examinan la forma en que realizan la autenticación o autorización .

2.4.9 Almacenar datos

Al realizar una Auditoría Informática se tiene como objetivo garantizar que la información sea tal cual se la guardo y no sea alterada

2.4.10 Cumplimiento regulatorio

Muchas empresas hoy en día están sujetas a regulaciones relacionadas con el tema de seguridad de la información, busca asegurar que dentro de la organización se esté cumpliendo las normativas de seguridad con normalidad. (Ucatalunya, 2023)

2.4.11 Confidencialidad

La confidencialidad se refiere a proteger la información y solo permitir el acceso a personas autorizadas, en este contexto mantener la confidencialidad significa que tienen que implementar medidas para que de esa forma toda la información este protegida contra vulnerabilidades (Ciencias, 2023)

2.4.12 Ciberataques

Al depender de la tecnología para almacenar la información se convierte en un blanco para los atacantes que por medios de virus buscan alterar el funcionamiento de los equipos para aprovecharse y hacer uso de la información (Fornited, 2024)

Las formas para protegerse de los ciberatacantes son:

1. No dar clic en mensajes de redes sociales de personas que no se conoce
2. No abrir correos sino se conoce al remitente
3. No ingresar en sitios web sospechosos
4. No descargar cualquier archivo de interner de fuentes no confiables
5. No dar clic en anuncios de publicidad
6. No usar cualquier USB en nuestros equipos

2.4.13 Control de acceso

Se recomienda utilizar sistemas para gestionar la autenticación y autorización y permitir que solo las personas autorizadas tengan acceso. (ISO, 2022)

2.4.14 Cifrado de datos

Realizar un cifrado de datos en la información almacenada y en la transmisión de datos para que de tal forma puedan evitar que personas no autorizadas puedan acceder. (Kaspersky, 2023)

2.4.15 Políticas de privacidad

Se tiene que desarrollar políticas y mantenerlas vigentes para que puedan regular el acceso y la manipulación de datos para proteger los datos que tengan un nivel de vulnerabilidad mayor a los demás (Komnenic, 2025).

2.4.16 Integridad

Implica mantener la información sin modificaciones para garantizar que no sea alterada sin la autorización durante el proceso de almacenar, contar con integridad de la información es crucial para asegurar que sea real y no alterada.

2.4.17 Hashing y firmas digitales

Se utilizan firmas digitales para verificar que la información no haya sido modificada al momento de ser almacenada (Mendible, 2021)

2.4.18 Control de Versiones

Siempre contar con un registro de todos los archivos para asegurar que al momento de realizar una modificación puedan ser rastreables y controladas (Atlassian, 2023).

2.4.19 Respaldo de datos

Realizar copias de seguridad regular y mantener planes para poder recuperar la información si se presente algún ataque pueden garantizar que puedan ser rastreados ante un caso de robo de información (David Giménez Muñoz, Antonio J, Manero Cantín, 2025).

2.4.20 Redundancia de sistemas

Implementar sistemas de conexión de red duplicada para que puedan asegurar la continuidad operativa incluso si se llega a presentar alguna falla (Ionos, 2023).

2.4.21 Mantenimiento preventivo

Realizar mantenimiento regular del hardware y software para que puedan prevenir si se llegase a presentar alguna interrupción del servicio (Fractial, 2021).

2.4.22 Mantenimiento preventivo

El mantenimiento preventivo consiste en realizar acciones periódicas para garantizar el correcto funcionamiento de los equipos informáticos. Incluye limpieza física, revisión de componentes, actualización de software y verificación de respaldos.

Este subtema es esencial porque prolonga la vida útil de los equipos y reduce la probabilidad de fallas inesperadas. En el ámbito académico, asegura que los sistemas estén disponibles para estudiantes y personal en todo momento. (Pressman, 2020)

2.4.23 Redundancia de sistemas

La redundancia de sistemas consiste en duplicar componentes críticos (servidores, discos, enlaces de red) para garantizar la disponibilidad continua de los servicios. Si un equipo falla, otro entra en funcionamiento automáticamente, evitando interrupciones.

En universidades y organizaciones, la redundancia es vital para mantener plataformas educativas y administrativas siempre disponibles. Esto asegura que los estudiantes y el personal puedan acceder a la información sin interrupciones, incluso en caso de fallas técnicas. (Wallace, 2020)

2.4.24 Vulnerabilidad de equipos

La gestión de vulnerabilidades consiste en identificar, evaluar y corregir debilidades en los equipos informáticos que puedan ser explotadas por atacantes. Incluye escaneos periódicos, aplicación de parches y monitoreo continuo de amenazas.

En instituciones educativas, esta práctica asegura que los equipos permanezcan actualizados y protegidos contra ataques. Una gestión proactiva de vulnerabilidades fortalece la resiliencia tecnológica y reduce el riesgo de incidentes de seguridad. (Isaca, 2020)

2.4.25 Seguridad de almacenamiento de datos

La seguridad en almacenamiento de datos se refiere a las medidas implementadas para proteger la información guardada en discos duros, servidores y servicios en la nube. Incluye cifrado, control de accesos y políticas de respaldo.

En universidades, el almacenamiento seguro es vital para preservar registros académicos y administrativos. Una gestión adecuada garantiza que los datos estén disponibles y protegidos contra pérdidas o accesos indebidos. (Schneir, 2021).

2.4.26 Seguridad de infraestructura

La seguridad en infraestructura crítica se centra en proteger los sistemas esenciales para el funcionamiento institucional, como servidores, redes eléctricas y sistemas de comunicación. Su objetivo es garantizar la continuidad de los servicios ante incidentes o ataques.

En el ámbito académico, la infraestructura crítica incluye servidores de gestión académica y plataformas de aprendizaje. Su protección asegura que los procesos educativos y administrativos no se vean interrumpidos por fallas técnicas o ataques externos. (ISO, 2024)

2.4.27 Seguridad en servidores

La seguridad en servidores se refiere a las prácticas y controles aplicados para proteger los equipos que almacenan y procesan información crítica. Incluye medidas como configuraciones seguras de

sistemas operativos, monitoreo de accesos, instalación de parches y protección contra ataques externos. Los servidores son el núcleo de la infraestructura tecnológica, por lo que su protección es esencial para garantizar la continuidad de los servicios.

En instituciones educativas, los servidores alojan plataformas de gestión académica, bibliotecas digitales y sistemas administrativos. Una falla en la seguridad de estos equipos puede comprometer datos sensibles de estudiantes y personal, afectando la confianza institucional. Por ello, se requiere una gestión proactiva que combine seguridad física y lógica. (Cobit, 2020)

2.4.28 Seguridad de dispositivos periféricos

La seguridad en dispositivos periféricos abarca la protección de impresoras, escáneres, cámaras y otros equipos conectados a la red institucional. Estos dispositivos, aunque suelen considerarse secundarios, pueden convertirse en puntos de entrada para ataques si no cuentan con configuraciones seguras.

En universidades, los periféricos son ampliamente utilizados para procesos administrativos y académicos. Una impresora conectada a la red, por ejemplo, puede ser explotada para acceder a documentos confidenciales. Por ello, es necesario implementar políticas de uso seguro y restringir accesos no autorizados.

La gestión de seguridad en periféricos también implica monitoreo constante y actualización de firmware. Al integrarlos dentro de la estrategia global de seguridad de equipos, se asegura que no representen vulnerabilidades y que contribuyan a la protección integral de la infraestructura tecnológica. (Withman, 2024).

2.5 Conclusiones del marco teórico

La exhaustiva revisión de libros, páginas web y artículos, permitieron realizar un planteamiento solido para la investigación sobre la Auditoria Informática a la seguridad de los equipos del área administrativa Uleam extensión El Carmen, se ha analizado la evolución de la informática y las crecientes amenazas a las que están expuestas hoy en día .

Se ha comprendido que la Auditoria Informática trasciende para convertirse en una herramienta estratégica para la gestión de riesgos, su metodología la posiciona como el mecanismo ideal para el diagnóstico de la seguridad de sus equipos , su función no solo es detectar las debilidades, sino que crear un plan de mejoras.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

En este capítulo se realiza una ruta metodológica empleada para la ejecución de la Auditoria Informática en el Area Administrativa ULEAM Extensión El Carmen, se basa en el fundamento de un enfoque científico para la recolección e interpretación de los datos recopilados sobre el estado en que se encuentra la seguridad de los equipos informáticos.

Para que los resultados tengan validez y sean confiables , se definieron métodos de investigación (inductivo y deductivo), tipo de estudio, técnica de recolección de datos, como fue la observación y aplicación de cuestionarios. Se delimito la población y muestra para asegurar que el proceso de investigación cumpla con los objetivos planteados y posteriormente elaborar el Plan de Contingencia.

3.2 Tipos de investigación

3.2.1 Investigación Descriptiva

Tiene como objetivo describir los comportamientos y situaciones, se lo puede llevar a cabo mediante la observación y las encuestas, ya que esta permite también a los investigadores recopilar información y datos mediante la elaboración de preguntas las cuales son abiertas o cerradas. Esta investigación también puede ser cualitativa o cuantitativa enfocándose con más fuerza en temas más específicos que se desarrollan dentro de la investigación.

La investigación Descriptiva destaca en que tiene integridad en los datos que fueron recopilados, evitando de tal manera la manipulación de los datos por personas externas a la investigación, otra de sus grandes ventajas de aplicar esta investigación es que se la puede aplicar tanto a individuos como ha grandez grupos. (Purdy, 2023)

Aplicar este tipo de investigación dentro de mi trabajo de titulación es un punto muy importante porque mediante la observación y la encuesta se recopilan datos para luego ser analizados y dar un

resultado del estado actual de los equipos, brindar ayuda en las áreas que más vulnerabilidad tiene y estar protegidos ante cualquier ataque o intento de manipulación de datos por personas externas

3.3 Métodos de investigación

3.3.1 Lógicos

3.3.2 Método Deductivo

Se conoce al Método Deductivo como el proceso para la obtención de información, utiliza un tipo de investigación que parte de lo general , basándose en leyes o principios hasta llegar a un hecho más real, esto quiere decir que este método permite extraer conclusiones a partir de cierta información (Aspasia, 2025).

Si las hipótesis que se tiene sobre el Método Deductivo llegan a ser verdaderas las conclusiones igual pasan a ser verdaderas , esto permite organizar las pruebas que se recopilaron para así llegar a una conclusión real y valida (Dávila Newman, 2020).

Este enfoque permitió organizar las soluciones de manera lógica , de tal forma que cada acción cuente con respaldo teórico sólido este orientada a resolver los problemas que se presenten de forma eficaz.

3.3.3 Método Inductivo

Se dice que el Método Inductivo está basado en el razonamiento, lo cual permite pasar de los hechos particulares a los principios generales, sin embargo, presenta un problema el cual es que este método solo se aplica a una cierta clase de objetos (Castellanos, 2017)

Este enfoque permitió garantizar que las propuestas sean realistas y aplicables al contexto del Area Administrativa de la ULEAM Extensión El Carmen.

3.4 Fuentes de información de datos

3.4.1 Encuestas

El uso d la encuesta es ampliamente usada como una herramienta de investigación, ya que permite tener el control de datos dentro de una población en especifico (J. Casas Anguitaa, 2021)

El uso de encuestas dentro de la investigación se la aplica a un grupo especifico de personas con una serie de preguntas las cuales pueden ser de diversos tipos como, por ejemplo: opción múltiple, matriz, escala. El tipo de preguntas que se elaboren será respondido dependiendo el objetivo de la encuesta y lo que se desea saber o tener conocimiento, un pequeño ejemplo seria encuestar a los trabajadores de una empresa con el objetivo de tener conocimiento sobre cómo se sienten desempeñando el rol que les fue asignado.

Los tipos de encuestas que se pueden aplicar son: las encuestas en línea, por correo, llamadas o entrevistas en persona, la más sencilla y fácil de aplicar es la encuesta en línea, además que el costo de aplicarlas puede ser muy mínimo y la gran cantidad de datos que se obtienen los hace en muy poco tiempo, esto la convierte en la opción más usada por las personas que se encuentran realizando una investigación. (Survey Monkey, 2020)

Mediante la utilización de la encuesta se logró obtener la recopilación de la información de una forma muy rápida y sencilla, al usar preguntas en línea al personal administrativo de la Uleam Extensión El Carmen se logró identificar en las áreas en la pueden ser más vulnerables ante algún tipo de amenaza o robo de información.

3.4.2 Población

Cuando la población es pequeña se realiza el estudio al 100% de las personas, es decir ninguna persona queda fuera. La Población es un conjunto de individuos u objetos los cuales comparten similitud dentro de sus características, muchas veces las personas que realizan este tipo de investigación dentro de una población no logran analizar a todos los individuos de la población, en ocasiones es necesario tomar los datos de una pequeña muestra, es decir, analizar solo una pequeña parte. (Escuela de Ivestigación, 2023)

Existen 2 tipos de población los cuales son:

población diana: Se refiere al grupo de individuos en los que los investigadores están interesados en investigar, la característica que presenta es que tiene características variables.

población accesible: Es la parte que los investigadores extraen para realizar la investigación, es un subconjunto de la población completa ya que no la pueden realizar a todos. (QuestionPro, 2025)

Al ser una población pequeña de siete personas que trabajan en el Área Administrativa Uleam Extensión El Carmen, la realización del estudio fue del 100%.

3.4.3 Muestra

La muestra es una fracción o parte representativa de una población, que se ha obtenido con la finalidad de investigar, por lo que se entiende que la muestra es una parte seleccionada de una población que reúne las características de la totalidad (Galindo, 2021).

Debido a que la población es muy pequeña (7 personas), se determinó trabajar con la totalidad de los elementos, al tener una muestra pequeña elimina el margen de error garantizando que los hallazgos sean exactos.

3.4.3.1 Estructura de los instrumentos de recolección de datos aplicados

La recolección de datos se la realizo con el propósito de recopilar información clara y precisa para tener un conocimiento actual del estado de los equipos informáticos en el área administrativa Uleam Extensión El Carmen, se diseñó como un instrumento cualitativo que fue dirigido especialmente al personal administrativo. Está compuesto por un total de 15 preguntas en donde todas son de opción cerradas.

3.4.1 Plan de recolección de datos

3.5 Análisis y presentación de resultados

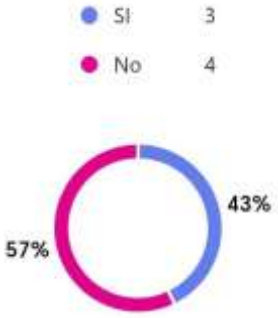
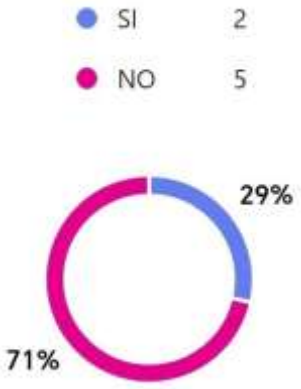
Día	Hora	Personal	Tipo de Instrumento
24/09/2025	11:00 horas	Personal Administrativo Uleam Extensión El Carmen	Encuesta

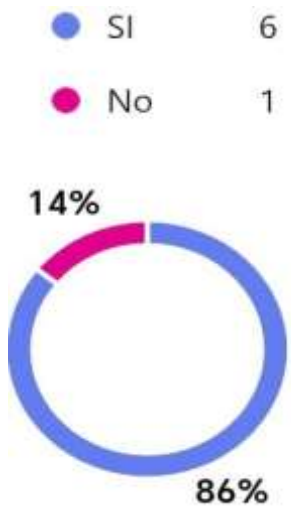
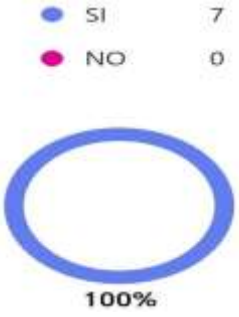
Tabla 1 Plan de Recolección de Datos

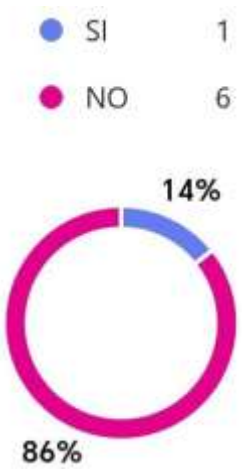
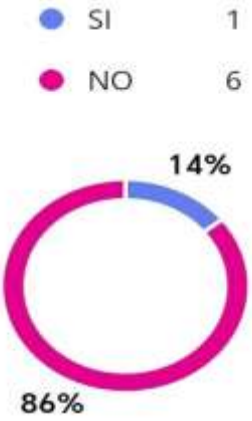
3.5.1 Presentación y descripción de los resultados obtenidos

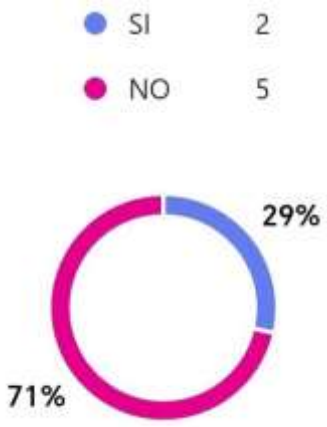
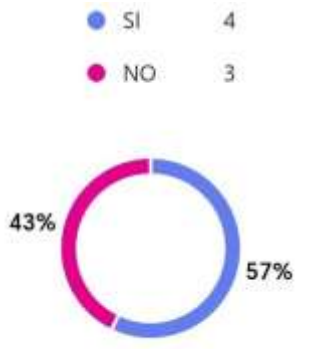
3.5.2 Encuesta aplicada al personal administrativo Uleam Extensión El Carmen

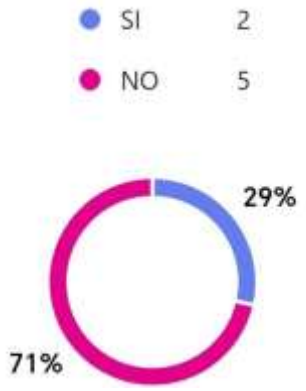
Preguntas	Respuestas	Interpretación
1. ¿Utiliza una contraseña diferente para cada equipo o sistema que usa en el área administrativa?		Mas de la mitad de las personas si utilizan una contraseña diferente por cada equipo utilizado, garantizando más seguridad a su información personal.
Preguntas	**Respuestas**	**Interpretación**

Preguntas	Respuestas	Interpretación
2. ¿Ha recibido capacitación formal sobre seguridad informática en los últimos 12 meses?		Como se puede observar solo 2 personas han recibido capacitación sobre seguridad informática, las cuales tendrán más precaución al realizar una acción en sus equipos.
3. ¿Sabe cómo identificar un correo electrónico de phishing (suplantación de identidad)?		Mas de la mitad de las personas que se encuentran en el área administrativa, no saben identificar un correo electrónico de phishing, de esa manera ponen en riesgo que algún hacker pueda acceder al sistema y manipularlo a su manera.
4. ¿Cuenta su equipo con un antivirus instalado y activo?		Mas de la mitad de las personas del área administrativa, no cuentan con un antivirus instalado en sus equipos, corriendo el riesgo de ser infectado por un virus y tener colapsos en su sistema.

Preguntas	Respuestas	Interpretación
5. ¿Realiza copias de seguridad de sus archivos de trabajo de manera periódica?		Mas de la mitad de las personas del área administrativa, no realizan copias de seguridad de manera periódicamente , teniendo en riesgo la información.
6. ¿Ha detectado alguna vez un comportamiento inusual en su equipo, como lentitud extrema o aparición de programas extraños?		Mas de la mitad de las personas del área administrativa , han pasado por este problema en sus equipos, lo cual interrumpe su correcto funcionamiento .
7. ¿Cierra su sesión o bloquea su equipo cuando se ausenta de su puesto de trabajo?		Todas las personas del área administrativa , si cierran sus sesiones al momento de salir de sus puestos de trabajo.

Preguntas	Respuestas	Interpretación
8. ¿Le han solicitado datos personales o de la universidad a través de un enlace web o un mensaje de texto no oficial?		Mas de la mitad de las personas del área administrativa han pasado por este problema que les piden información de la Universidad mediante un enlace web o mensaje.
9. ¿Considera que el nivel de seguridad de los equipos del área administrativa es el adecuado?		Mas de la mitad de las personas del área administrativa consideran que la seguridad de los equipos no es adecuada.
10. ¿Sabe si su equipo recibe actualizaciones de seguridad de manera automática?		Todas las personas del área administrativa desconocen si sus equipos reciben actualizaciones de manera automática.

Preguntas	Respuestas	Interpretación
11. ¿Reportaría a un superior cualquier problema de seguridad que detecte, por pequeño que sea?		Mas de la mitad de las personas del área administrativa si reportaran a un supervisor cualquier problema de seguridad que detecte.
12. ¿Utiliza las redes sociales personales en los equipos de la universidad?		Mas de la mitad de las personas del área administrativo no utilizan sus redes sociales personales en los equipos de trabajo.
13. ¿Ha compartido su contraseña de trabajo con algún compañero o superior?		Mas de la mitad de las personas del área administrativa si han compartido sus contraseñas entre compañeros de trabajo.

Preguntas	Respuestas	Interpretación
14. ¿Tiene acceso a toda la información digital del área administrativa, sin restricciones de roles?		Mas de la mitad de las personas del área administrativa no tienen acceso a toda la información digital.

3.5.3 Presentación y descripción de los resultados obtenidos

El diagnostico que se obtuvo mediante la encuesta aplicada a las personas dentro del área administrativa de la Uleam Extensión El Carmen dio como resultado la obtención de algunos datos los cuales pueden llegar a ser riesgoso.

3.5.4 Principales hallazgos cuantitativos

La mayor parte de las personas encuestadas del área administrativa reutilizan la misma contraseña para usar en otros sistemas (P1), lo cual no es tan seguro porque deja una puerta abierta para los atacantes. De igual manera también se tiene una usencia de capacitación sobre auditoria informática (P2) ya que la gran parte del personal tampoco sabe identificar un correo electrónico de phishing (P3) siendo este la principal vía de entrada del malware, pero la gran mayoría de los equipos si cuenta con software antivirus actualizado (P4), la efectividad de esta área también se ve afectada por la ausencia de la realización de respaldo de la información (P5) también puede afectar al sistema algún código malicioso no detectado (P6) o algún USB los cuales son la vía más común para afectar al sistema (P7) siendo más fácil de infiltrarse al dejar la sesión abierta en el

equipo (P8) o solicitando algún tipo de información como pueden ser datos personales de los estudiantes (P9), también la seguridad actual de los equipos no es adecuada (P10) y desconocen si el equipo recibe actualizaciones automáticas (P11), y no reportan a su superior algún problema que detecte dando paso a que se infiltren en el sistema (P12) al usar sus redes sociales en los equipos de trabajo pueden acceder a algún tipo de link e infectar de virus el equipo (P13) o a la persona que le presta su contraseña puede también acceder a algún link por error (P14) ya que tienen acceso a información que no necesitan para su trabajo aumentando más el riesgo de robo de información (P15).

3.5.5 Informe final del análisis de los datos

A continuación, se detalla de forma concisa y clara las principales fallas que comprometan la seguridad del área administrativa

- **Vulnerabilidad Humana :** La reutilización de contraseñas o compartición de contraseñas se convierte en la parte más vulnerable.
- **Falta de control de dispositivos:** No cuentas con políticas establecidas sobre el uso de dispositivos externos.
- **Perdida de información :** Según los resultados obtenidos el área administrativa no se encuentra preparada para recuperarse de algún tipo de incidente sin que genera pérdidas.
- **Vulnerabilidad Latente :** A pesar de si contar con antivirus, pero al no reportar algún comportamiento fuera de lo normal existe vulnerabilidad

En conclusión, los equipos del área administrativa de la Uleam Extensión El Carmen se encuentran en alto riesgo, los resultados obtenidos mediante la encuesta dieron a conocer los riesgos a los cuales están expuestos, obligando a tener la necesidad de implementar una propuesta de mejora para fortalecer los controles de seguridad y poder elevar su nivel.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

La presente propuesta de una Auditoría Informática surgió como una necesidad después de analizar los riesgos que se obtuvieron en la encuesta realizada al personal administrativo de la ULEAM, previo a eso se elaboró un Plan de Contingencia, este es un documento que tiene reglas a seguir, sino que se trata de un documento realizado para prevenir y recuperarse ante algún tipo de accidente en los que se puedan ver afectados los equipos. La propuesta de Plan de Contingencia es la parte final del proceso de Auditoría que se realizó en el área administrativa, tras la culminación del Capítulo III en donde se identificó puntos en los cuales tienen más vulnerabilidad.

La siguiente propuesta se fundamenta en la normativa ISO/IEC 27001:2022, la cual brinda un marco robusto para la seguridad de la información, además es una norma que establece mejoras para un sistema de gestión de seguridad de la Información (SGSI), estableciendo el alcance del sistema, se puede establecer para que el alcance sea eficaz y se adapte a las necesidades de la organización. (ISO, 2022).

También se aplicará el Ciclo de Mejora Continua PHVA(Planificar, Hacer, Verificar, Actuar), este se aplica a los planes de contingencia para la identificación de posibles riesgos, establecer respuestas, establecer estrategias y actuar de tal manera que sea favorable para la empresa u organización de que sean capaces de poder recuperarse ante algún tipo de emergencia, y así asegurando su continuidad operativa.

4.2 Descripción de la propuesta

La siguiente propuesta consiste en diseñar un plan de contingencia para los equipos informáticos de Área Administrativa Uleam Extensión El Carmen, surgió luego de identificar las respuestas de las preguntas en donde se identificaron problemas como lo son el uso de las contraseñas, la falta de capacitaciones para estar preparados ante algún problema, la usencia de copias de seguridad y tener acceso a toda la información digital.

Como objetivo principal de realizar este plan de contingencia es que los equipos del área administrativa siempre estén en funcionamiento correcto, y si llegase a presentar una falla se puedan recuperar de manera rápida, ya que este plan de contingencia está diseñado bajo los estándares de la normativa ISO 27001:2022, a diferencia de ser algún manual de usuario simple, esta propuesta se rige bajo el modelo de mejora continua PHVA(Planificar, Hacer, Verificar, Actual), esto además garantiza que las medidas de seguridad no sean fijas sino que evolucionen según vayan surgiendo nuevas amenazas.

En conclusión, este plan de contingencia elabora un conjunto de recomendación y buenas prácticas desarrolladas según los resultados obtenidos de la encuesta al personal administrativo, para ser usadas por el personal actual o futuras personas encargadas logrando evitar algún tipo de interrupción o fallas al sistema y su continuidad operativa siga siendo normal.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recursos	Función	Actividad
7	Secretaria de la carrera	Personal administrativo de la Uleam	Será la población participe de la de encuesta
1	Ariel Fueres	Investigador	Investigará todo para establecer la propuesta

Tabla 2 Recursos Humanos

4.3.2 Tecnológicos

Cantidad	Recursos	Actividad
1	Portátil Lenovo core i5 16 GB de RAM	Equipo utilizado para todo el desarrollo de la investigación.
1	Celular HONOR X8	Equipo usado en la investigación para alguna toma de evidencia.
1	Impresora EPSON	Equipos usados para la impresión de hojas.
1	Programa Microsoft Forms	Se uso para la tabulación de datos.
1	Programa Microsoft Word	Usado para realizar toda la redacción del proyecto de titulación .
10 meses	Conexión a Internet	Usado para acceder a la información y realizar el proyecto de titulación.

Tabla 3 Recursos Tecnológicos

4.3.3 Económicos

Cantidad	Descripción	Precio	Subtotal
1	Portátil Lenovo core i5 16 GB de RAM	765.00$	765.00$
1	Celular Honor X8	200.00$	200.00$
10	Conexión a Internet	28.00$	280.00$
330	Impresiones	0.20$	66.00$
80	Transporte	0.40$	32.00$
	TOTAL	1343.00$	

Tabla 4 Recursos Económicos

4.4 Desarrollo (Metodología PHVA (Planificar-Hacer-Verificar-Actuar) alineada con la norma ISO/IEC 27001:2022)

Para el desarrollo del plan de Contingencia, se estructuro bajo la metodología del ciclo de mejora continua PHVA (Planificar- Hacer- Verificar- Actuar), este es una base fundamental para la mejora de un Sistema de Gestión de Seguridad de la información (SGSI), esta metodología fue seleccionada por poseer una gran capacidad para transformar los respaldos de datos en protocolos más seguros y confiables.

Llevar una alineación con la normativa ISO/27001:2022, garantiza que cuando se realiza el plan de contingencia no solo sea una respuesta temporal, sino un marco establecido ya que el personal carece de algún tipo de instrucción a tipo de robo o infiltración al sistema

Integrar el modelo de ciclo de mejora continua dentro del plan de contingencia permite abordar la seguridad desde cuatro puntos distintos.

Planificar: Establecer objetivos y procesos que sean necesarios para obtener resultados de acuerdo con las políticas establecidas dentro del plan de contingencia.

Hacer: Implementar los controles que fueron establecidos y la capacitación del personal.

Verificar: Llevar un seguimiento de los procesos respecto a las políticas y objetivos establecidos.

Actuar: Tomar acciones si se llegase a presentar fallas para continuar el funcionamiento de los equipos informáticos .

4.4.1 Fase 1 Planificar

4.4.2 Programa de Auditoría

Programa de Auditoría Informática: Seguridad de los Equipos (ISO/IEC 27001:2022)		
Objetivo: • Identificar riesgos y vulnerabilidades críticas en la protección de activos tecnológicos y la información de toda la ULEAM • Evaluar la implementación y eficacia del Plan de Contingencia basado en el ciclo PHVA para asegurar la continuidad operativa del área administrativa		
Técnicas y procedimientos		
Actividad	**Ref. a Papel**	**Fecha**
1.1. Revisión de la norma ISO/IEC 27001:2022 (Anexo a)	4.4.1.2	28/04/2025
1.2. Ejecución de Auditoria Inicial: Diagnostico de hardware y prácticas del personal	4.4.1.3	04/05/2025
1.3. Análisis de contexto: Evaluación de vulnerabilidades y controles de acceso	4.4.2	30/05/2025
2.3 Tabulación de resultados matriz de riesgo	4.4.3.3	10/06/2025
2.4 Evaluación de impacto medición de efectividad de respaldo	4.4.3.5	16/06/2025
2.5 Valoración final de riesgo priorización	4.4.3.5	17/06/2025
2.6 Elaboración del Informe de Auditoría hallazgos finales y recomendaciones	5.1	17/06/2025

Tabla 5 Programa de Auditoría

4.5 Revisión ISO/IEC 27001

El estándar internacional ISO/IEC 27001:2022, es un protocolo que está diseñado para brindar un soporte más seguro a la Confidencialidad, Integridad y Disponibilidad (CIA), sobre los recursos tecnológicos de la ULEAM. Su arquitectura permite a las organizaciones tener una protección a sus activos tecnológicos mediante la aplicación del modelo de mejora continua, Planificar, Hacer, Verificar, Actuar (PHVA), la cual garantiza que las estrategias que se establezcan no sean estáticas, sino que evolucionen ante las nuevas amenazas emergentes.

Los requisitos de la norma ISO/27001:2022 consta de 10 clausulas las cuales establecen un marco más robusto que integra la seguridad de la información mediante el análisis contextual, la responsabilidad, planificación, apoyo, controles, evaluación, y mejora continua. Este conjunto de cláusulas de garantía que la seguridad del sistema sea medible y que de confianza a largo plazo (Edwars, 2025)

4.5.1 Auditoria Inicial

La Auditoria Inicial es el diagnostico fundamental donde se evalúa el estado de madurez de los controles de seguridad de los equipos informáticos del Area administrativa Uleam Extensión El Carmen, este proceso se ejecuta a través de un análisis de brechas GAP (GAP Analysis) con el objetivo de cuantificar entre procesos actuales y estándares exigidos por la normativa ISO/IEC 27001:2022. (Velázquez, 2022)

El análisis de Brechas GAP consiste en el desarrollo del desempeño que está teniendo la empresa, con el que se busca contrastar el punto en el que esta y en el que se desea llegar en crecimiento y desarrollo de la empresa.

También logra mostrar las diferencias que presenta la organización entre sus objetivos y el rendimiento que están prestando, permitiendo que se identifiquen de manera rápida algún error con la finalidad de crear acciones correctivas ante alguna falla permitiendo disminuir brechas entre el estado anterior y el estado actual de la empresa.

El análisis de brechas GAP permite a las empresas lo siguiente

- Identificar puntos débiles
- Evaluar y cuantificar los recursos actuales
- Buscar soluciones en equipo
- Optimizar los procesos de negocio

Al momento de realizar un análisis de brechas GAP hay que ser muy sincero para tener bien en claro las debilidades y fortalezas de la empresa, ya que esta es la única manera de conseguir mejores prácticas, este proceso puede variar según las necesidades de cada empresa. (Martinez, Delta Protect, 2023)

A continuación se utilizara una escala de niveles de madurez, con el objetivo de evaluar los controles de seguridad, la documentacion y ejecucion efectiva para la mejora continua permitiendo identificar las debilidades y fortalezas de la empresa.

Nivel de Madurez	**Descripción**
Nivel 0 – No existencia	No cuenta con implementación de ningún control.
Nivel 1 – Ad hoc	Existe una operación táctica de los riesgos operativos.
Nivel 2 - Ejecutado	Existen los controles, pero no formalmente.
Nivel 3 - Definido	Se implementaron los controles.
Nivel 4 – Manipulable y Medible	Se lleva un control interno para verificar los controles.

Nivel de Madurez	Descripción
Nivel 5 - Optimizado	Los controles están integrados y optimizados.

Tabla 6 Nivel de Madurez

Nivel Medio Cumplimiento = Puntuación total de cada Control/Numero de controles	
Por debajo de 1.65	El control no cumple con los requisitos de la norma.
Entre 1.66 y 3.25	El control cumple parcialmente.
Por encima de 3.26	El control cumple adecuadamente con los requisitos normativos.

Tabla 7 Nivel de Cumplimiento

La fase de diagnóstico fue estructurada bajo el marco analítico de los siete dominios principales de la normativa ISO/IEC 27001:2022, permitieron una evaluación completa de la seguridad de los equipos informáticos del Area Administrativa Uleam Extensión El Carmen, este análisis comprendió el compromiso del liderazgo, la gestión de riesgos, la infraestructura de soporte y la continuidad operativa.

Este análisis fue complementado bajo un instrumento de evaluación técnica centrado en los indicadores siguientes .

- **Definición de objetivos de seguridad:** Protección de datos operativos de la empresa.
- **Determinación del alcance:** Identificación de equipos informáticos y activos.
- **Estandarización de protocolos:** Verificación de existencia de políticas de respaldo y recuperación.
- **Estructura de gobernanza:** Asignación de roles y responsabilidades en la protección de información.
- **Controles de verificación :** Medición de los procesos y respuesta ante incidentes.

La aplicación de este instrumento permitió consolidar las bases de seguridad de la Uleam Extensión El Carmen, fue importante este diagnóstico para determinar e identificar la gestión actual.

N.º	**Capítulo**	**Descripción breve**
1	Alcance	Define los límites del Area Administrativa.
2	Referencias normativas	Enlista los estándares requeridos.
3	Términos y definiciones	Proporciona el vocabulario técnico usado en la norma.
4	Contexto de la organización	Identifica factores internos y externos que impactan la seguridad del área.

N.º	Capítulo	Descripción breve
5	Liderazgo	Determina responsabilidad con la seguridad de la información.
6	Planificación	Reconoce objetivos de seguridad para tratar riesgos.
7	Apoyo	Gestiona presupuesto y herramientas a la formación personal.
8	Operación	Ejecuta planes antes incidentes.
9	Evaluación del desempeño	Supervisa los controles implementados.
10	Mejora	Corrige las fallas que se presenten para la protección de la información.

Tabla 8 Capítulos Principales de la norma ISO/IEC 27001:2022

4.5.2 Diseño de instrumento de evaluación del cumplimiento de requisitos según ISO/IEC 27001:2022

Requisito ISO 27001	Preguntas para Evaluación	Cumplimiento
Contexto de la Organización	1. ¿Están identificados los objetivos del plan de contingencia para los equipos informáticos de los laboratorios?	
	2. ¿ Se han identificado cuestiones internas y externas que podrían afectar el servicio ¿	
	3. ¿Se han identificado posibles amenazas para los equipos?	
Requisitos ISO 27001	**Preguntas para Evaluación**	**Cumplimiento**
Liderazgo	1. ¿Controla los procesos a cumplir según los requisitos ¿	
	1. ¿Se evalúa la eficacia del sistema?	
	2. ¿Se aplican acciones para optimizar el sistema?	

Tabla 9 Diseño del instrumento de evaluación del cumplimiento de requisitos según ISO/IEC 27001:2022

4.5 Ejecución

4.5.1Tabulación de datos del cumplimiento de requisitos de la Norma ISO 27001

Los datos recopilados fueron trabajados en Microsoft Excel para ver el cumplimiento de los requisitos, se usó la evaluación de brechas basadas en el modelo de madurez por niveles, equivalentes del 0 al 5.

Se desarrollo de la siguiente manera:

- Se calculo el promedio de cada requisito
- Después se cuantifico la brecha (GAP), se divide el promedio entre 5 y el resultado como un porcentaje de déficit.

Requisitos	Pregunta	Cumplimiento	Observación	Promedio	Estado GAP	Brecha	Estado de Madurez
4.Contexto De la Organización	1.¿Estan identificados los objetivos del plan de contingencia para los equipos informáticos del Area Administrativa?	0		3,333333	66%	34%	No Cumple
	2.¿Se han identificado cuestiones internas que afecten a la disponibilidad de su servicio?	5					
	3.¿Se han identificado posibles amenazas para los equipos?	5					
5.Liderazgo	1.¿Cuenta el Area Administrativa con un protocolo que regule la cooperación y préstamo de equipos con otras áreas?	0		1,333333	27%	73%	Parcialmente
	2.¿Se encuentras automatizados los respaldos de la documentación para evitar pérdidas?	4					
	3.¿Dispone cada puesto de trabajo con protección eléctrica (Reguladores), o un registro de mantenimiento preventivo para evitar fallas?	0					

Tabla 10 Tabulación de los requisitos de la norma ISO 27001:2022

4.5.2 Cumplimiento de controles

Este ecosistema normativo, que se basa en los estándares ISO brinda un catálogo de salvaguardas que están orientadas a brindar más seguridad a los equipos del Area Administrativa Uleam Extensión El Carmen, su arquitectura desglosa en varios dominios de control que brindan seguridad y dan prevención a la infraestructura digital.

A continuación, se describen las métricas de cumplimiento y los controles específicos de las necesidades operativas, bajo los lineamientos de la normativa ISO/IEC 27001:2022

Numeral	**Clausulas**	**Descripción**
A5	Políticas de contingencia	Protocolo usado para responder a las a emergencias y reducir impactos.
A6	Organización	Establece una estructura de técnicos responsables para brindar soporte.
A7	Recursos Humanos	Gestiona capacitaciones al personal administrativo.
A8	Gestión de Activos	Asegura el inventario y protege la información.
A9	Control de Acceso	Restringe el acceso a sistemas vulnerables mediante la aplicación de políticas de uso de contraseñas.
A10	Seguridad Física	Implementación de protección eléctrica.
A11	Operaciones	Lleva un control de los procedimientos de mantenimientos preventivos.

Numeral	Clausulas	Descripción
A12	Copias de seguridad	Respaldos automáticos en la nube, para poder ser recuperados
A13	Incidentes	Reporte ante fallas o brechas de seguridad.
A14	Continuidad	Estrategias para mantenerse activos los servicios ante alguna falla
A15	Cumplimiento	Respetar las normativas establecidas.

Tabla 11Descripción de Clausulas según la norma ISO

4.5.2 Diseño del instrumento de cumplimiento de controles de la Norma ISO 27001

Numeral	Clausula	Requisito	Cumple
A5	Políticas de Contingencia	1. ¿Existe un plan de contingencia de equipos?	
		2. ¿Se revisa seguido el plan de contingencia?	
A6	Organización	1. ¿Hay responsables encargados del Area Administrativa?	
		2. ¿Existen procedimientos para coordinar apoyo entre otras áreas?	
A7	Recursos Humanos	1. ¿El personal conoce su rol dentro en el plan?	
		2. ¿Se capacita al personal administrativo sobre el uso correcto de los equipos?	
A8	Gestión de Activos	1. ¿Hay un inventario detallado de los equipos?	
		2. ¿Se clasifican los equipos por necesidad de cada persona?	

Tabla 12 Diseño de instrumentos de controles

4.6 Ejecución

Se realizo una entrevista al Ing. Jean Carlos Cedeño ya que él es el responsable de dar mantenimiento al Área Administrativa de la Uleam extensión El Carmen, con el objetivo de recopilar datos para la implementación de controles de seguridad requeridos por la normativa ISO 27001.

4.6.1 Tabulación de datos del cumplimiento de controles de la Norma IO 27001

El procesamiento de los datos se desarrolló en Microsoft Excel para determinar el cumplimiento de los controles de la normativa ISO 27001, en el Area Administrativa Uleam Extensión El Carmen. Se utilizo el código 0, 1, 2 en donde Si (1), No (0) y No Aplica (2) por cada control evaluado.

Metodología aplicada:

1. Conteo de todos los controles evaluados incluyendo los excluidos.
2. Cálculo de controles totales, restando los excluidos de la suma total.
3. Determinar el porcentaje de cumplimiento y no cumplimiento .

Numeral	Clausula	Requisito	Cumple
A5	Politicas de Contingencia	1.¿Existe un plan de contingencia de equipos?	0
		2. ¿Se revisa periódicamente la política de contingencia?	0
A6	Organización	1. ¿Hay responsables encargados del Area Administrativa?	1
		2. ¿Existen procedimientos para coordinar apoyo entre otras áreas?	0
A7	Recursos Humanos	1. ¿El personal conoce su rol dentro en el plan?	1
		2. ¿Se capacita al personal administrativo sobre el uso correcto de los equipos?	1
A8	Gestión de Activos	1. ¿Hay un inventario detallado de los equipos?	0
		2. ¿Se clasifican los equipos por necesidad de cada persona?	1
A9	Control de Acceso	1. ¿Existen controles para evitar daños intencionales a los equipos?	0
		2. ¿Se registra el uso de los equipos?	0

Tabla 13 Datos de la Institución

Nivel de Madurez

Luego de evaluar los controles se obtuvo el porcentaje de los requisitos que se cumplen y los que no se cumplen.

Requisito de ISO 27001	**Cumple la Norma**	**Brecha**
4. Organización y su contexto	66%	34%
5. Liderazgo	40%	60%
6. Planificación	27%	73%
7. Soporte	33%	67%
8. Operación	47%	53%
9. Evaluación y desempeño	60%	40%
10. Mejora	100%	0%
Promedio Requisitos	54%	46%

Tabla 14 Nivel de Madurez de Requisito

2.Identificar las brechas de cumplimiento de los porcentajes que se obtuvieron

Cláusulas	Cumple	No Cumple
A5. Políticas de Contingencia	0%	0%
A6. Organización	50%	50%
A7. Recursos Humanos	100%	0%
A8. Gestión de Activos	50%	50%
A9. Control de Acceso	0%	0%

Tabla 15 Nivel de Madurez de Controles

4.6.2 Conclusión

Luego de terminar la evaluación de madurez bajo el estándar ISO/IEC 27001:2022, se llega a la conclusión que el Area Administrativa Uleam Extensión El Carmen tiene un promedio de 1.26/5, los resultados obtenidos evidencian una brecha de 73.4% por la ausencia de objetivos de seguridad, ausencia de recursos técnicos, ausencia de respaldos de información y falta de protección eléctrica hacia los equipos.

Esto confirma que la información de los equipos esta vulnerable y justifica que de manera inmediata se realice un Plan de Contingencia para garantizar la continuidad del área administrativa.

4.6.3 Análisis del Contexto

Se realizo un análisis del contexto externo e interno del área Administrativa Uleam Extensión El Carmen conforme lo establece los lineamientos de la normativa ISO/IEC 27001:2022, tuvo como objetivo identificar los factores que puedan afectar la seguridad de la información e interrumpir la continuidad operativa de los equipos informáticos .

Contexto externo	
Aspecto	**Detalle**
Político	Cumplir con las directrices emitida por el Ministerio de Telecomunicaciones (MINTEL) y las políticas internas de la Uleam.
Económico	Tener a disposición presupuesto para la adquisición de hardware y protección eléctrica a los equipos (UPS), también suscripciones para respaldar la información en la nube.
Social	Generar un ambiente de trabajo en donde el personal administrativo pueda hacer un manejo seguro de la información de la Universidad.
Tecnológico	Depender de la infraestructura de servidores o de red, y tener vulnerabilidad ante ataques malware o perdida de información por algún equipo que pueda fallar.
Ecológico	Los cambios climáticos de la zona pueden provocar cortes de energía o daños en los equipos.
Legal	Cumplir con la Ley Orgánica de Educación Superior (LOES), y las normativas internas de la Uleam.

Tabla 16 Contexto Externo ULEAM Extensión El Carmen

Contexto Interno	
Aspecto	**Detalle**
Gobernanza y liderazgo	Se encontró una ausencia de políticas formales de seguridad.
Infraestructura tecnológica	Los equipos están trabajando sin protección eléctrica(UPS), y no cuentan con mantenimientos preventivos.
Gestión de respaldos	Dependen solo de almacenamientos locales, sin contar con respaldos automáticos en la nube.
Recursos Humanos	El personal cuenta con conocimiento operativo, pero existe una brecha sobre riesgos.
Capacidad Financiera	La capacidad financiera es nula, lo que lo convierte en una zona de alto riesgo.

Tabla 17 Contexto Interno Uleam Extensión El Carmen

4.7 Justificación técnica del Plan de Contingencia

1. **Justificación técnica y operativa**

   El diagnostico que se realizó bajo la normativa ISO/IEC 27001:2022, nos dio como resultado una brecha del 73.4% según los estándares de seguridad, la falta de protección eléctrica (UPS) para los equipos y la carencia de procesos de respaldos de la información representan un riesgo alto ante alguna perdida de información.

El desarrollo de este Plan de Contingencia permitirá establecer normas para de esa manera garantizar que los equipos informáticos del Area Administrativa Uleam Extensión El Carmen trabajen con normalidad y no tengan interrupciones.

2. **Justificación Legal**

   La Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador exige que todas las Instituciones garanticen la integridad y disponibilidad de la información que poseen, la realización de este Plan de Contingencia establece normas para que el área Administrativa cumpla con las normas establecidas para evitar posibles sanciones legales por motivos de perdida de información.

3. **Justificación Institucional**

   El área administrativa transita una seguridad "Ad-hoc, quiere decir que la información es desorganizada y no documentada, ya que no existe manuales o políticas establecidas por eso si algún empleado quiere hacer por ejemplo un respaldo lo hace a su manera porque no existen normas establecidas.

4.8 Elaboración de Cuestionarios para Analizar Riesgos

El diseño del cuestionario para Analizar Riesgos fue dividido en cinco secciones para identificar los riesgos que podrían afectar a los equipos informáticos del Area Administrativa Uleam Extensión El Carmen.

- **15 ítems:** para daños de equipos
- **15 ítems:** para riesgos de incendios
- **15 ítems:** para riesgo de inundaciones
- **15 ítems:** para riesgos de robos y prevención
- **15 ítems:** para riesgos de malware y software malicioso

Cada punto evalúa puntos vulnerables, medidas preventivas y controles que podrían interrumpir la continuidad operativa de los equipos informáticos.

4.8.1 Ejecución de los cuestionarios para analizar riesgos

Se realizó la evaluación de todos los equipos informáticos del Area Administrativa Uleam Extensión El Carmen, con el fin de analizar los riesgos relacionados con robo, daños físicos, incendios, inundaciones y malware. El objetivo es determinar el nivel de seguridad y el riesgo de los equipos informáticos.

4.8.2 Aplicación de Análisis de Riesgo

Se realizo una inspección personalmente en el Area Administrativa con el fin de analizar el funcionamiento de todos los activos del lugar.

Fotografía	Descripción
	Aire acondicionado funcionando a la perfección , garantizando un ambiente fresco para los equipos informáticos y el personal que labora en el lugar

Fotografía	Descripción
	Extintor revisado y fecha de caducidad válido, listo por si se presenta algún incendio.
	Computadoras en buen estado , funcionado correctamente no presenta fallas en la pantalla y la claridad en buena .

Fotografía	Descripción
	Teclados en perfecto estado, no presentan fallas las teclas.
	Mouse en buen estado, no presentan fallas sus botones.

Fotografía	Descripción
	Equipos conectados directo a la energía eléctrica, ausencia de equipos de protección (UPS),poniendo en riesgo el equipo ante algún daño eléctrico.
	Impresora funcionando correctamente, no presenta ninguna falla de colores al imprimir.

Tabla 18 Aplicación de Análisis de Riesgo

4.8.2 Evaluación de Recursos Disponibles para Contingencia

Para la elaboración del Plan de Contingencia requirió evaluar personalmente los recursos del Area Administrativa Uleam Extensión El Carmen, esta acción permite identificar brechas y aplicar acciones correctivas dentro del Plan de Contingencia.

- Mediante la inspección que se realizó personalmente al Area Administrativa se realizó un inventario de los activos con los que cuentan para enfrentarse a una falla como cortes eléctricos, ataques al hardware o software, o desastres naturales como inundaciones .

- En la parte de respaldos de la información hay un problema ya que no todos realizan respaldos y contar únicamente con almacenamiento local es un problema ya que no cuentan con políticas establecidas.

- No cuentan con protección eléctrica (UPS) poniéndose en riesgo ante un daño eléctrico.

- Solo se cuenta con una persona encargada del soporte técnico y es el encargado de toda la extensión.

- No cuentan con protocolos de contingencia, si se presenta alguna falla se resuelve de manera improvisada.

En conclusión, el Plan de Contingencia deberá establecer normas y procedimientos claros para el fortalecimiento de los recursos, con esto se busca que los funcionamientos de los equipos no se interrumpan.

4.8.3 Tabulación de Análisis de Riesgos

La tabulación de Análisis de Riesgos se la realizo en Microsoft Excel a partir de los instrumentos aplicados en el Area Administrativa Uleam Extensión El Carmen, la escala que se utilizo fue la siguiente: 0 indica peligro, 1 indica seguridad y 2 no aplica.

Cuestionario para Analizar Riesgos	
	Area Administrativa
Daño de Equipos	
1. ¿Cuentan con protectores de energía (UPS) los puestos de trabajo	0
2. ¿Realizan mantenimientos preventivos?	0
3. ¿Están expuestos a humedad o calor los equipos?	1
4. ¿Utilizan adecuadamente los cables de alimentación o de transferencia de datos?	0
5. ¿Reportan alguna falla el mismo momento que ocurren?	1
6. ¿El personal Administrativo da uso correcto a los equipos?	1

Tabla 19 Tabulación de Análisis de Riesgos

4.8.4 Escala de Probabilidad de Ocurrencia

Esta escala que consta de cinco niveles nos permite transformar percepciones en valores numéricos, de esta forma nos facilita la priorización de las estrategias dentro del Plan de Contingencia.

Escala para determinar el valor de Ocurrencia		
Nivel de Ocurrencia		
1	Muy bajo	1% - 10%
2	Bajo	11% - 30%
3	Moderado	31% - 50%
4	Alto	51% - 75%
5	Muy alto	76% - 100%

Tabla 20 Escala de Valor de Ocurrencia

Nivel de Gravedad

Esta escala de cinco niveles ordenar las amenazas según su severidad, al categorizarlas el Plan de Contingencia puede priorizar los recursos para prevenir aquellos eventos que comprometan la resiliencia de los equipos tecnológicos.

Escala de Impacto		**Consideraciones por nivel**
Nivel 1	**Muy bajo**	Cierres temporales de la instalación , no puede ser superior a 8 horas, los daños son mínimos.

Escala de Impacto		Consideraciones por nivel
Nivel 2	**Bajo**	Las interrupciones ya requieren intervención, pero no afectan al Area Administrativa.
Nivel 3	**Medio**	Requieren intervención técnica para restablecerse con normalidad la continuidad operativa.
Nivel 4	**Alto**	Daños más graves con interrupciones relevantes, estas ya exigen respuesta de manera inmediata o podrían comprometer los servicios.
Nivel 5	**Muy alto**	Daños irreversibles, los servicios colapsan totalmente se pierden por completo los datos sin que exista forma de poder recuperarlos.

Tabla 21 Escala de Impacto

Clasificación del Nivel por Riesgo

Riesgo	Color	Rango	Medidas
Muy Grave		De 15 a 25	Nivel de riesgo crítico, requiere atención inmediata y la implementación de medidas preventivas de manera urgente.
Importante		De 9 a 12	Acciones preventivas obligatorias apoyadas de supervisión constante.

Riesgo	Color	Rango	Medidas
Apreciable		De 3 a 8	Puede disminuir con acciones preventivas.
Marginal		De 1 a 2	No requiere acciones inmediatas, pero requiere observación para evitar daños a futuro.

Tabla 22 Escala de Nivel de Riesgo

Nivel de Riesgo	Descripción	Medidas de Tratamiento
Bajo	Riesgo mínimo, no afectan el cumplimiento de sus objetivos.	Monitoreo anual sin la necesidad de controles seguidos.
Moderado	Riesgo que puede generar interrupciones más de 24 horas.	Asignar recursos o planes de Contingencia Detallados.
Alto	Riesgo que impide totalmente su continuidad operativa.	Requiere supervisión inmediata.
Critico	Riesgo muy alto, impedicion totalmente de la continuidad operativa.	Requiere atención inmediata, implementar controles de alta disponibilidad.

Tabla 23 Clasificación de Nivel de Riesgo

4.8.5 Evaluación del impacto en el análisis de riesgo

Para calcular el impacto de riesgo como daño de quipos, incendio, inundaciones, robo y malware, se utilizó la herramienta Microsoft Excel, se tomaron en cuenta tres puntos fundamentales; Confidencialidad, Integridad y Disponibilidad.

Resultados del impacto según categoría de riesgo				
Riesgo	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Impacto total**
Daños de equipo	1	4	4	3
Incendio	1	3	5	3
Inundaciones	1	1	1	1
Robo	4	2	5	4
Malware	4	5	4	4

Tabla 24 Impacto de Análisis de Riesgo

4.8.5.1 Evaluación de los riesgos

Se adopto un modelo basado en los pilares de seguridad de la información: Confidencialidad, Integridad y Disponibilidad (C,I,D), teniendo estos datos el cálculo se realizó de la siguiente manera, se caculo el porcentaje de seguridad dividiendo el número de controles seguros entre el control total de los controles evaluados., también se obtuvo el porcentaje de riesgo mediante la división total de los controles de riesgo cobre los controles evaluados.

Pregunta Daños de Equipos	Area administrativa
12. ¿El software que tiene instalado en el equipo presenta alguna falla?	1
13. ¿Realizan respaldos de la información antes de usar el sistema operativo?	0
14. ¿El área donde están los equipos es seguro?	1
15. ¿Se usan los equipos solo con fines de trabajo?	1
Total, controles No Aplica	0
Total, controles Evaluados	15
Total, Seguridad	10
Total, Riesgo	5
Porcentaje de seguridad	67%
Porcentaje Riesgo	33%

Tabla 25 Evaluación de Riesgos

4.8.5.2 Matriz de Riesgo

Se elaboro una matriz de Riesgo en Microsoft Excel, para en análisis de los eventos: daño de equipo, incendio, inundaciones, robo y malware, el cálculo se realizó de la siguiente manera, el valor de riesgo se obtuvo multiplicando la probabilidad de aparición por el nivel de impacto.

Obteniendo esos resultados se clasificaron según su gravedad asignándole un color.

Riesgo	Probabilidad	Impacto	Valor de Riesgo	Nivel
Daño de Equipos	4	4	16	Muy grave
Incendio	5	3	15	Muy grave
Inundaciones	2	4	8	Apreciable
Robo	1	3	3	Marginal
Malware	1	1	1	Marginal

Tabla 26 Matriz de Riesgo

CAPÍTULO V

5. EVALUACIÓN DE RESULTADOS

5.1 Informe de Auditoria

Dirigido al:

Dr. Temístocles Bravo Tuarez Administrador y Director de la Extensión.

Tipo de Auditoría:

Auditoría Informática a la Seguridad de los Equipos del Area Administrativa Uleam Extensión El Carmen.

Motivo:

Cumplir con los requisitos establecidos previo a obtener el Título de Ingeniero en Tecnologías de la información correspondientes a, diseñar la implementación de un Plan de Contingencia a los equipos informáticos del Area Administrativa Uleam Extensión EL Carmen. Aplicando los principios establecidos por la normativa ISO/ 27001:2022.

Objetivos:

- Evaluar los niveles de madurez de la gestión de Seguridad Informática del Área Administrativa Uleam Extensión El Carmen.

- Analizar e Identificar los principales riesgos que pueden enfrentar los activos tecnológicos en los que se puede afectar su disponibilidad, integridad y disponibilidad.

Alcance:

- Revisar los requisitos establecidos por la normativa ISO/IEC 27001:2022.

- Realizar una Auditoria Inicial en el Area Administrativa Uleam Extensión El Carmen
- Realizar la recopilación de datos.
- Analizar las posibles amenazas según su categoría.
- Evaluar los niveles de madurez.
- Elaboración de la matriz de riesgo
- Valoración de impacto y probabilidad.
- Propuestas de acciones correctivas y mejoras .

Personal involucrado:

Personal que labora en el Area Administrativa

5.2 Presentación y monitoreo de resultados

5.3 Planificación de la evaluación

No cumple: 0% — 39%

Parcialmente: 40% — 79%

Cumple: 80% — 100%

Requisito	Cumplimiento (%)	Nivel de madurez
4. Contexto de la Organización	66%	Parcialmente
5. Liderazgo	40%	Parcialmente
6. Planificación	27%	No cumple

Requisito	Cumplimiento (%)	Nivel de madurez
7. Soporte	33%	No cumple
8. Operación	47%	Parcialmente
9. Evaluación del desempeño	60%	Parcialmente
10. Mejora	100%	Cumple

Tabla 27 Requisito ISO/IEC 27001:2022

Promedio general:53.2% Nivel de Cumplimiento: Medio

5.4 Interpretación y causas por requisito

- **Contexto de la Organización (66% -- Parcialmente):** Se ha identificado en entorno interno y externo que afecten el sistema de gestión , no se evidencia un análisis de las partes interesadas.
  Causas: Documentación limitada

- **Liderazgo (40% -- Parcialmente):** Demuestra compromiso limitado, existiendo debilidades .
  Causas: Las políticas no han sido impartidas al personal administrativo.

- **Planificación (27% -- No Cumple):** No cuentan con una planificación ante riesgos, ni se han identificado los objetivos.
  Causas: Falta establecer políticas ante riesgos.

- **Soporte (33% -- No cumple):** Se desconocen los recursos que poseen.
  Causas : Ausencia de información técnica.

- **Operación (47% --Parcial):** Existen los procesos, pero son inconsistentes.
  Causas: No cuentan los procesos conseguimiento continuo.

- **Evaluación y desempeño (60 – Parcialmente):** Se la realiza de forma limitada.
  Causas: Es necesario que se establezcan métricas y se realice seguimiento continuo.

- **Mejora (100% -- Cumple):** Realizan acciones de mejora continua.
  Causas: Mejoras en el área administrativa.

5.5 Evaluación y controles

5.6 Principales controles evaluados

Control	Cumplimiento (%)	Nivel de Madurez
A5. Políticas de Contingencia	0%	Muy bajo
A6. Organización	50%	Bajo
A7. Recursos Humanos	100%	Alto
A8. Gestión de Activos	50%	Bajo
A9. Control de Acceso	0%	Muy bajo

Tabla 28 Principales Controles Evaluados

Promedio general de cumplimiento: 40% **--** Nivel de madurez: Bajo

5.7 Análisis de Riesgo

Riesgo	Nivel de seguridad	Nivel de riesgo	Causas identificadas
Daño de equipos	Bajo	Muy grave	No cuentan con protecciones eléctricas(UPS).
Incendio	Bajo	Muy grave	No cuentan con protecciones eléctricas(UPS).
Inundaciones	Bajo	Muy grave	No de evidencian sistemas de drenaje.
Robo	Medio	Importante	Acceso sin control.
Malware	Bajo	Muy grave	No todos cuentan con antivirus.

Tabla 29 Análisis de Riesgo

Evaluación general del riesgo: 45% -- Muy grave

5.8 Conclusiones y Recomendaciones

Una vez finalizada la Auditoría Informática a la Seguridad de los equipos del Area Administrativa Uleam Extensión El Carmen, se evidencio un nivel de madurez bajo el cual pone en riesgos los servicios que presta esta área y puede interrumpir su continuidad operativa.

Los riesgos más críticos que se encontraron fueron daños de equipos ya se por incendios o daños eléctricos por la falta de protecciones eléctricas (UPS), falta de un sistema de drenaje ante alguna inundación y falta de antivirus para evitar daños al malware.

Se recomienda:

La implementación del Plan de Contingencia (Anexo 1), para fortalecer las vulnerabilidades que presentan y estar aptos para enfrentarse a algún problema en el cual se vea afectado su continuidad operativa.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Se identifico una problemática muy clara en la seguridad de los equipos del Area Administrativa, la falta de auditorías periódicas más la ausencia de un Plan de Contingencia ponen en riesgo la información, esto resalta la importancia de contar con una Auditoria para proteger la información y garantizar una continuidad operativa.

- Se construyo un marco teórico robusto en donde se destaca la importancia de la Auditoria Informática como herramienta principal para la gestión de riesgos.

- El diagnóstico revelo las vulnerabilidades de los equipos informáticos, como la falta de protección eléctrica(UPS), ausencia de respaldos de información dando como resultado la necesidad de implementar medidas correctivas.

- La realización del Plan de Contingencia estuvo alineada bajo la normativa ISO/IEC 27001:2022, también estuvo basado bajo el ciclo de mejora continua (PHVA) proporcionado un conjunto de recomendaciones para fortalecer la seguridad de los equipos informáticos.

- El Plan de Contingencia demostró ser una medida de mejoramiento apara los equipos informáticos en donde se pretende reducir los riesgos y fortalecer el Area Administrativa ante posibles incidentes.

- Finalmente se elaboró el informe de la auditoria en donde se expuso lo hallazgos que pueden afectar su continuidad operativa y se diseñó un Plan de Contingencia (Anexo 1) que busca mejorar su seguridad de los equipos informáticos, esta investigación aporta normas y procedimientos para fortalecer el Area Administrativa.

6.2 Recomendaciones

- Se recomienda que adopten el Plan de Contingencia que está en el Anexo 1, esto brindara un aporte para evitar eventos que afecten todo el sistema del Area Administrativa.

- Establecer políticas y normas claras para que el uso de los equipos informáticos .

- Realizar Auditorías Informáticas de manera más seguido para ir evaluando el estado en que se encuentran los equipos para así detectar fallas tempranas que puedan afectar la continuidad operativa.

- Capacitar al personal administrativo sobre buenas prácticas digitales y el manejo adecuado de la información que poseen, usando software de protección (antivirus), para garantizar que no se interrumpa la continuidad operativa, mediante políticas desarrolladas (Anexo 1).

BIBLIOGRAFÍA

7. Bibliografía

(s.f.). https://ecuador.unir.net/actualidad-unir/sistema-deteccion-intrusos/

(2020). UCSP: https://postgrado.ucsp.edu.pe/articulos/que-es-seguridad-redes/

(2021). TIC: https://www.mintic.gov.co/portal/inicio/Glosario/C/18728:Ciberterrorismo

(2021). Fractial: https://www.fracttal.com/es/guias-mantenimiento/mantenimiento-preventivo

(2022). Metric: https://www.metricstream.com/learn/compliance-testing.html

(2022). ISO: https://www.iso.org/es/seguridad-informacion/control-de-acceso

(2022). Securiti: https://securiti.ai/glossary/availability/

(2022). Contabilidad y Finanzas: https://contabilidadfinanzas.com/auditoria/auditoria-informatica/?utm_source=copilot.com

(2023). Thales: https://cpl.thalesgroup.com/es/software-monetization/what-is-software-security

(2023). Sede Electronica: https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/-/asset_publisher/1RphW9IeUoAH/content/1032-que-significa-autenticacion-

(2023). Ciencias: https://minciencias.gov.co/glosario/confidencialidad

(2023). Kaspersky: https://latam.kaspersky.com/resource-center/definitions/encryption

(2023). Atlassian: https://www.atlassian.com/es/git/tutorials/what-is-version-control

(9 de Julio de 2023). Ionos: https://www.ionos.com/es-us/digitalguide/servidores/seguridad/redundancia/

(13 de Octubre de 2024). Auditoría Informatica : https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica?utm_source=chatgpt.com

(2024). Fornited: https://www.fortinet.com/lat/resources/cyberglossary/what-is-cyber-attack

(10 de Marzo de 2025). Megerit: https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa)?utm_source=chatgpt.com

(2025). Ciencias: https://minciencias.gov.co/glosario/confidencialidad

(17 de Julio de 2025). Unir: https://ecuador.unir.net/actualidad-unir/sistema-deteccion-intrusos/

Alzate, A. T. (2020). Auditoría De Sistemas Una Visión Práctica. En A. T. Alzate, *Auditoría De Sistemas Una Visión Práctica.* Centro de Publicaciones Universidad Nacional de Colombia Sede Manizales.

Arantes, S. C. (2023). Auditoría de Seguridad Informática. En S. C. Arantes. Ra-ma.

Arantes, S. C. (2023). *Auditoría de Seguridad Informtica.* Ra-ma .

Aspasia. (2025). https://grupoaspasia.com/es/glosario/metodo-de-investigacion-deductivo/

Atlas. (2025). https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/entrevistas

Audágora. (13 de Febrero de 2025). https://auditoria-auditores.com/articulos/articulo-auditoria-la-planificaci-n-en-auditor-a/

Auditol. (2024). Auditol: https://www.auditool.org/blog/auditoria-de-ti/principios-basicos-de-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad-cia

Auditoría De Seguridad Informática. (2024). Ediciones Nobel.

Bayas, A. P. (2020). *AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN, APLICANDO COBIT 5.*

Benítez Lázaro, E. S. (2023). *Energy efficiency and Latin America.* Springer.

Bonifaz, L. A. (1 de Julio de 2025). *InvestiGO*. https://www.revistainvestigo.com/EditorInvestigo/index.php/hm/article/view/316/A40H

Cárdenas, L. C. (2023). https://www.udea.edu.co/wps/portal/udea/web/generales/interna/unidades%20acad!c3!a9micas/ciencias%20econ!c3!b3micas/ascontenidos/aslistado/auditoria-basada-en-riesgos-la-organizacion-como-un-todo/!ut/p/z1/1VRLc9owEP4r4ZCjRrJkg310HA_FvEl52JfOIglQiyViG_L49R

Castellanos, B. J. (2017). El uso de los métodos deductivo e inductivo para aumentar la e□ciencia del. 27. https://doi.org/ https://doi.org/10.11144/Javeriana.cc18-46.umdi

Concepto. (2025). https://concepto.de/metodo-inductivo/

Cuzco, A. J. (4 de agosto de 2023). *Repositorio Digital Universidad Técnica del Norte* . Repositorio Digital Universidad Técnica del Norte : https://repositorio.utn.edu.ec/handle/123456789/14582

Daniel, B. (Abril de 2022). https://repositorio.puce.edu.ec/server/api/core/bitstreams/e9e31021-fe20-44cb-88b6-29f3f3888edd/content

David Giménez Muñoz, Antonio J, Manero Cantín. (2025). *Bastionado de Redes y Sistemas.* RA-MA S.A. Editorial y Publicaciones.

Dávila Newman, G. (2020). *El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y.*

Diccionario de la Lengua Española. (2024). Auditoría: https://dle.rae.es/auditor%C3%ADa

Edwars, M. (15 de Septiembre de 2025). *Requisitos y cláusulas de la norma ISO 27001:2022*. IO: https://es.isms.online/iso-27001/requirements-2022/#:~:text=Los%20requisitos%20de%20la%20norma,valor%20empresarial%20a%20largo%20plazo.

Enrique Villa, Ismael Morales. (2023). *Ciberseguridad.* Ediciones de la U.

Escuela de Ivestigación. (2023). Blog: https://escueladeinvestigacion.com/2024/09/05/cual-es-la-diferencia-entre-poblacion-muestra-y-unidad-de-analisis/

Espinoza. (2021).

Galindo, E. M. (14 de Noviembre de 2021). https://tesis-investigacion-cientifica.blogspot.com/2021/11/muestra.html#google_vignette

García, A. E. (2023). *Seguridad de Equipos Informáticos.* Ra-Ma S.A. Editorial y Publicaciones.

Google Libros. (2023). https://www.google.com.ec/books/edition/Auditor%C3%ADa_de_seguridad_inform%C3%A1tica/VcK_EAAAQBAJ?hl=es-419&gbpv=1&dq=auditoria+informatica+inicio&pg=PA214&printsec=frontcover

IBM. (2022). https://www.ibm.com/es-es/think/topics/green-computing

IBM. (2022). *¿Que es la seguridad de equipos?* IBM: https://www.ibm.com/mx-es/think/topics/it-security

ISO, C. (2022). *Introduccion a la Norma ISO 27001:2022.* GDS & Consultores ISO, SL.

J. Casas Anguitaa, J. R. (2021). *Elsevier*. https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion-elaboracion-cuestionarios-13047738

Jiménez., C. I. (Febrero de 2024). *Repositorio Institucional de la Universidad Politécnica Salesiana*. Repositorio Institucional de la Universidad Politécnica Salesiana: http://dspace.ups.edu.ec/handle/123456789/27049

Jonathan Stalin Villafuerte Solórzano. (2020). *Universidad Tecnica Estatal de Quevedo*. Universidad Tecnica Estatal de Quevedo: https://repositorio.uteq.edu.ec/handle/43000/5943

Komnenic, M. (7 de Noviembre de 2025). https://termly.io/es/recursos/articulos/que-es-una-politica-de-privacidad/

Legalnet. (1 de 12 de 2023). *Auditoría y Co*. https://auditoria-auditores.com/articulos/articulo-auditoria-el-uso-de-la-tecnolog-a-en-las-auditor-as/

Liu, C. (2024). *Curating Digital Lives.* Lexington Books.

Martinez, J. G. (4 de 01 de 2023). *Delta Protect*. Análisis GAP: ¿Qué es, cómo se hace y por qué es importante para las empresas?: https://www.deltaprotect.com/blog/analisis-gap-que-es#:~:text=nivel%20de%20ciberseguridad.-,%C2%BFQu%C3%A9%20es%20un%20an%C3%A1lisis%20GAP?,Optimizar%20los%20procesos%20de%20negocio

Martinez, J. G. (4 de 01 de 2023). *Delta Protect*. Análisis GAP: ¿Qué es, cómo se hace y por qué es importante para las empresas?: https://www.deltaprotect.com/blog/analisis-gap-que-es#:~:text=nivel%20de%20ciberseguridad.-,%C2%BFQu%C3%A9%20es%20un%20an%C3%A1lisis%20GAP?,Optimizar%20los%20procesos%20de%20negocio

Mendible, J. G. (6 de Mayo de 2021). https://web.uanataca.com/ec/blog/tecnologia/hash-y-firma-electronica

Ortega, K. (29 de Mayo de 2024). Saint Leo University: https://worldcampus.saintleo.edu/blog/fases-de-una-auditoria-informatica-y-en-que-consisten?utm_source=copilot.com

Polanco, M. (7 de Enero de 2025). *Instituto fe y Libertad*. https://feylibertad.org/la-integridad/

Purdy, E. R. (2023). *EBSCO*. https://www.ebsco.com/research-starters/social-sciences-and-humanities/descriptive-research

QuestionPro. (2025). https://www.questionpro.com/blog/es/que-es-una-poblacion/

Samaniego, V. (2022). Auditoría Informática al Departamento de Tecnología de la Información y Comunicación del Hospital Provincial General Docente Riobamba,.

Sánchez Cano, J. E. (2023). *Sector energético crecimiento económico y desarrollo sostenible frente al cambio climático.* Universidad Juárez del Estado de Durango.

ServeNet. (2023). https://aceproject.org/main/espanol/et/ete01a.htm

Siegal. (2024). https://www.uh.edu/infotech/policies/reference-guide/logical-security/index.php

Siegal, S. (3 de Octubre de 2024). *AuditBoard*. Pruebas Sustantivas Definición: https://auditboard.com/blog/substantive-testing-key-definitions-goals-and-best-practices

Steinbuch, K. (1957). *Wikipedia*. https://es.wikipedia.org/wiki/Inform%C3%A1tica

Survey Monkey. (2020). https://es.surveymonkey.com/learn/survey-best-practices/why-are-surveys-important-in-research/

Ucatalunya. (2023). U de Cataluña: https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber

UNEMI. (2021). *METODOLOGÍA DE LA INVESTIGACION EDUCATIVA.*

Universidad Militar Nueva Granada. (2023). http://virtual.umng.edu.co/distancia/ecosistema/ovas/diplomados/diplomado_gestion_de_procesos_y_sistemas_de_gestion_de_calidad/unidad_4/medios/interactividades/pat4_2/pat4_2.html

Universidad Veracruzana. (s.f.). https://www.uv.mx/apps/bdh/investigacion/unidad3/encuesta.html

Velázquez, A. (2022). *Que es el análisis de brechas o GAP*. QuestionPro: https://www.questionpro.com/blog/es/analisis-de-brechas/

Wikipedia . (s.f.). Wikipedia: https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

Zeltzin. (2024). *Tractian*. https://tractian.com/es/blog/que-es-disponibilidad-definicion-calculo-e-importancia-en-el-mantenimiento-industrial

ANEXOS

Anexo 1 : Plan de Contingencia

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

PLAN DE CONTINGENCIA PARA EQUIPOS INFORMÁTICOS

ÁREA ADMINISTRATIVA ULEAM EXTENSIÓN EL CARMEN

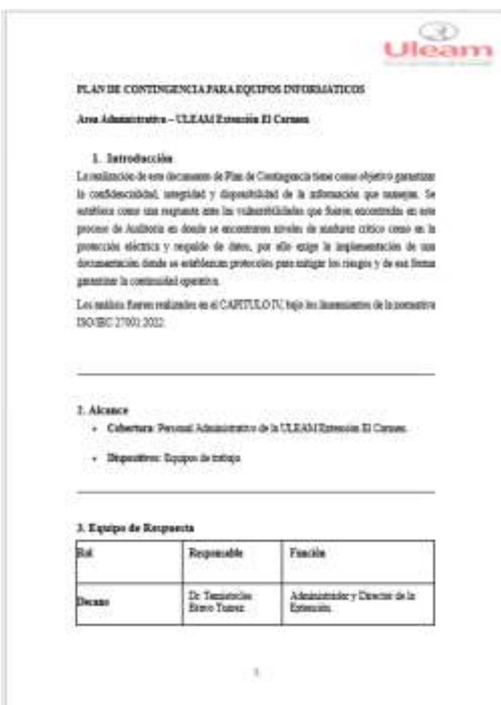
PRESENTADO POR:

FUERES MADERA ARIEL ALEXANDER

Uleam

Contenido

2



Uleam

PLAN DE CONTINGENCIA PARA EQUIPOS INFORMÁTICOS

Área Administrativa – ULEAM Extensión El Carmen

1. Introducción

La realización de este documento de Plan de Contingencia tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información que manejan. Se establece como una respuesta ante las vulnerabilidades que fueron encontradas en este proceso de Auditoría en donde se encontraron niveles de madurez crítico como en la protección eléctrica y respaldo de datos, por ello exige la implementación de una documentación donde se establezcan protocolos para mitigar los riesgos y de esa forma garantizar la continuidad operativa.

Los análisis fueron realizados en el CAPITULO IV, bajo los lineamientos de la normativa ISO/IEC 27001:2022.

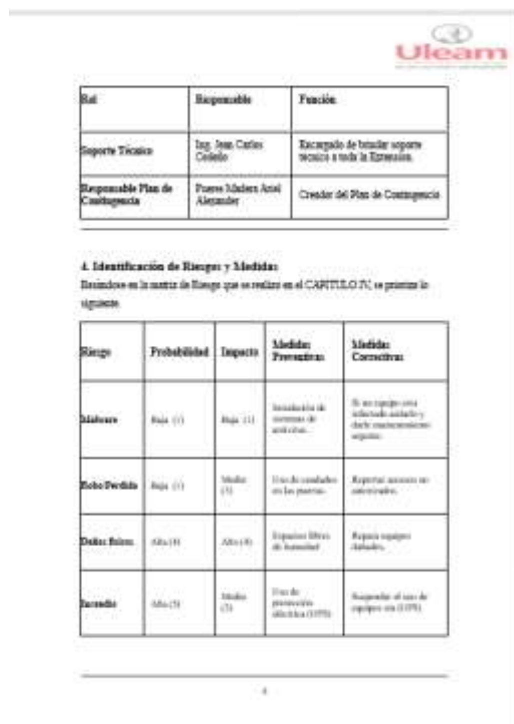
2. Alcance

- **Cobertura**: Personal Administrativo de la ULEAM Extensión El Carmen.
- **Dispositivos**: Equipos de trabajo.

3. Equipo de Respuesta

Rol	Responsable	Función
Decano	Dr. Temístocles Bravo Tuárez	Administrador y Director de la Extensión.

3



Uleam

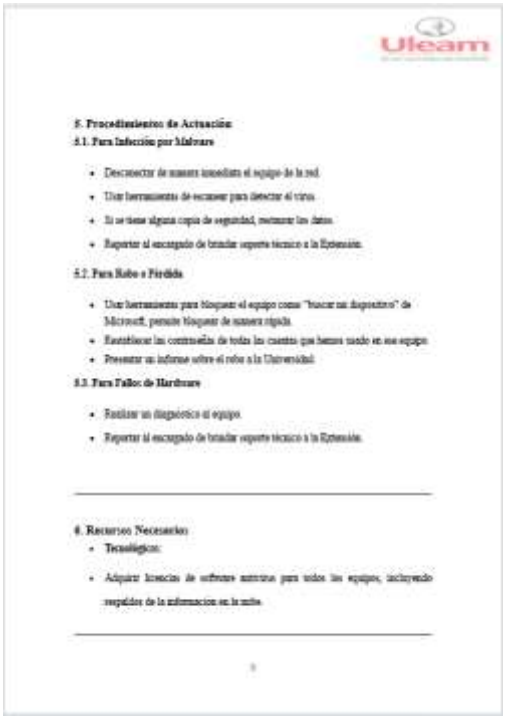
Rol	Responsable	Función
Soporte Técnico	Ing. Jean Carlos Cedeño	Encargado de brindar soporte técnico a toda la Extensión.
Responsable Plan de Contingencia	Fueres Madera Ariel Alexander	Creador del Plan de Contingencia

4. Identificación de Riesgos y Medidas

Basándose en la matriz de Riesgo que se realizó en el CAPITULO IV, se prioriza lo siguiente.

Riesgo	Probabilidad	Impacto	Medidas Preventivas	Medidas Correctivas
Malware	Baja (1)	Baja (1)	Instalación de sistemas de antivirus.	Si un equipo está infectado aislarlo y darle mantenimiento seguido.
Robo/Pérdida	Baja (1)	Media (3)	Uso de candados en las puertas.	Reportar accesos no autorizados.
Daños físicos	Alta (4)	Alta (4)	Espacios libres de humedad.	Reparar equipos dañados.
Incendio	Alta (5)	Media (3)	Uso de protección eléctrica (UPS)	Suspender el uso de equipos sin (UPS)

4



5. Procedimientos de Actuación

5.1. Para Infección por Malware

- Desconectar de manera inmediata el equipo de la red.
- Usar herramienta de escaneo para detectar el virus.
- Si se tiene alguna copia de seguridad, restaurar los datos.
- Reportar al encargado de brindar soporte técnico a la Extensión.

5.2. Para Robo o Pérdida

- Usar herramienta para bloquear el equipo como "buscar un dispositivo" de Microsoft, permite bloquear de manera rápida.
- Restablecer las contraseñas de todas las cuentas que hayan usado en ese equipo.
- Presentar un informe sobre el robo a la Universidad.

5.3. Para Fallo de Hardware

- Realizar un diagnóstico al equipo.
- Reportar al encargado de brindar soporte técnico a la Extensión.

---

6. Recursos Necesarios

- Tecnológicos:
- Adquirir licencias de software antivirus para todos los equipos, incluyendo respaldos de la información en la nube.

7. Comunicación

- La comunicación la pueden realizar mediante vía WhatsApp, o chats de Teams si se llegara a presentar alguna alerta.

---

8. Capacitación y Simulacros

- Realizar simulacros al personal administrativo sobre algún evento que podría afectar al sistema y ponerse la continuidad operativa.

---

9. Monitoreo Bajo el Ciclo Mejora Continua (PHVA)

- **Planificar**: Revisar los riesgos que puedan afectar al Área Administrativa una2 veces al año.
- **Hacer**: implementar actualizaciones de software antivirus y respaldos de la información en la nube.
- **Verificar**: realizar las Auditorías según los estándares establecidos por la normativa ISO/IEC 27001:2022
- **Actuar**: Realizar actualizaciones dentro del Plan de Contingencia según sea necesario.

Elaborado por: Franco Madera Ariel Alexander

Revisado por: Ing Lenin Zambrano

Fecha: 31-01-2026

Anexo 1Plan de Contingencia

Anexo2 Anti-plagio

CERTIFICADO DE ANÁLISIS

PROYECTO DE TITULACION ARIEL FUERES COMPILATIO

5% Textos sospechosos

4% Similitudes

< 1% Idiomas no reconocidos

2% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: PROYECTO DE TITULACION ARIEL FUERES COMPILATIO.docx
ID del documento: b55b6601ea09bdc13ba478d335fda56662a81164
Tamaño del documento original: 1,13 MB

Depositante: RENELMO MINAYA MACAS
Fecha de depósito: 7/2/2026
Tipo de carga: interface
Fecha de fin de análisis: 7/2/2026

Número de palabras: 13.749
Número de caracteres: 93.765

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Dentro de de otro grupo	2%		
2		2%		
3		1%		
4	Dentro de de mi grupo	< 1%		
5	Dentro de de otro grupo	< 1%		

Fuentes con similitudes fortuitas

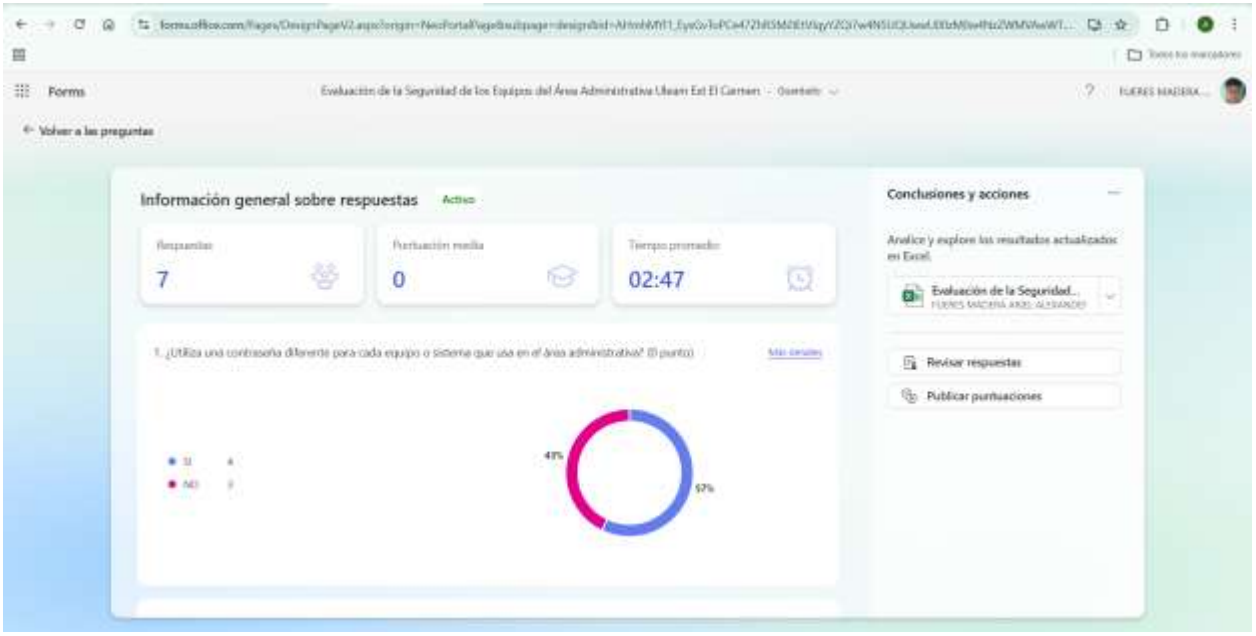
Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.unach.edu.ec	< 1%		
2	localhost	< 1%		
3	TESIS APQC 20_7_2023 correcion(1).docx	< 1%		
4	es.linkedin.com	< 1%		
5	repository.unad.edu.co	< 1%		

Fuentes mencionadas (sin similitudes detectadas)

1 https://www.mintic.gov.co/portal/inicio/Glosario/C/18728:Ciberterrorismo
2 https://www.metricstream.com/learn/ramp/iunca-testing.html
3 https://grupoasesa.com/es/glosario/metodo-de-investigacion-deductivo/
4 https://ariaki.com/es/guias/guia-investigacion-cualitativa-parte-1/entrevistas
5 https://www.auditool.org/blog/auditoria-de-sti/principios-basicos-de-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad-cia

Anexo 2 Certificado Anti-Plagio

Anexo 3: Encuesta al personal Administrativo Uleam Extensión El Carmen



Anexo 3Encuesta al personal Administrativo Uleam Extensión El Carmen

Anexo 4 : Cuestionario de Análisis de Riesgo

Cuestionario para Analizar Riesgos			C1
Daños de Equipos	**Respuestas**		**Observaciones**
	SI	**NO**	
1. ¿Cuentan con protectores de energia(UPS), los puestos de trabajo?			
2. ¿Realizan mantenimientos preventivos?			
3. ¿Están expuestos a humedad o calor los equipos?			
4. ¿Utlizan adecuadamente los cables de alimentación o de transferencia de datos?			
5. ¿Reportan alguna falla el ismo momento que ocurren?			
6. ¿El personal administrativo da uso correcto a los equipos?			
7. ¿Exsiten normas sobre el uso de equipos?			
8. ¿Una vez finalizado la hora de trabajo se apagan correctamente los equipos?			
9. ¿Existen fallas frecuentes a los equipos?			
10. ¿Dejan bebidas cerca de los equipos?			
11. ¿Presentan daños los perifericos(teclado, mouse)?			
12. ¿Preseta algun tipo de error el software instalado?			
13. ¿Realizan respaldos de la informació?			
14. ¿Es seguro el area de los equipos?			
15. ¿Se utilizan los equipos solo para motivos de trabajo?			
Realizado por:	**Revisado por:**	**Observaciones:**	
Fecha:	**Fecha:**		

Anexo 4 Cuestionario de Análisis de Riesgo

Encuesta

Dirigida al personal Administrativo Uleam Extensión El Carmen

Objetivo: El objetivo principal es diagnosticar el estado actual de la seguridad informática, identificando las vulnerabilidades, amenazas y deficiencias en las políticas o controles existentes que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información.

1. ¿Utiliza una contraseña diferente para cada equipo o sistema que usa en el área administrativa?

   SI ( ) NO ( )

2. ¿Ha recibido capacitación formal sobre seguridad informática en los últimos 12 meses?

   SI ( ) NO ( )

3. ¿Sabe cómo identificar un correo electrónico de phishing (suplantación de identidad)?

   SI ( ) NO ( )

4. ¿Cuenta su equipo con un antivirus instalado y activo?

   SI ( ) NO ( )

5. ¿Realiza copias de seguridad de sus archivos de trabajo de manera periódica?

   SI ( ) NO ( )

6. ¿Ha detectado alguna vez un comportamiento inusual en su equipo, como lentitud extrema o aparición de programas extraños?

   SI ( ) NO ( )

7. ¿Tiene políticas claras sobre el uso de dispositivos de almacenamiento externos (USB, discos duros) en los equipos de la oficina?

SI ( ) NO ( )

8. ¿Cierra su sesión o bloquea su equipo cuando se ausenta de su puesto de trabajo?

   SI ( ) NO ( )

9. ¿Le han solicitado datos personales o de la universidad a través de un enlace web o un mensaje de texto no oficial?

   SI ( ) NO ( )

10. ¿Considera que el nivel de seguridad de los equipos del área administrativa es el adecuado?

    SI ( ) NO ( )

11. ¿Sabe si su equipo recibe actualizaciones de seguridad de manera automática?

    SI ( ) NO ( )

12. ¿Reportaría a un superior cualquier problema de seguridad que detecte, por pequeño que sea?

    SI ( ) NO ( )

13. ¿Utiliza las redes sociales personales en los equipos de la universidad?

    SI ( ) NO ( )

14. ¿Ha compartido su contraseña de trabajo con algún compañero o superior?

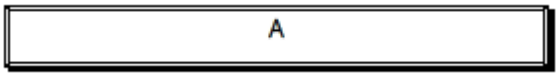
    SI ( ) NO ( )

15. ¿Tiene acceso a toda la información digital del área administrativa, sin restricciones de roles?

    SI ( ) NO ( )

Anexo 5 Encuesta Personal Administrativo

8. Glosario

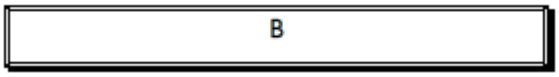


Auditoria :

Proceso de evaluar los controles y seguridad de los sistemas.

Antivirus :

Sistema para detectar y eliminar amenazas

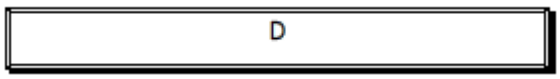


Backup :

Proceso de respaldo de la información para evitar pérdidas.

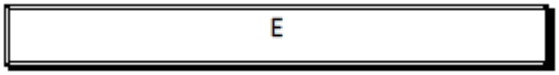
Cobit :

Usado para gestión de TI



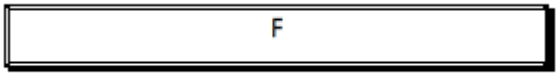
Disponibilidad :

Equipos siempre disponibles para el uso



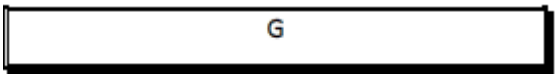
Equipos informáticos :

Dispositivos tecnológicos (Computadora)



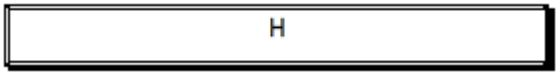
Fuente de poder :

Componente que da vida al equipo.



Gestión de riesgos :

Proceso para analizar amenazas de una infraestructura.

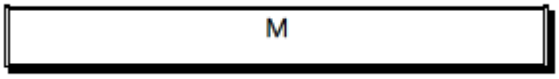


Hardware :

Elementos físicos de una computadora.

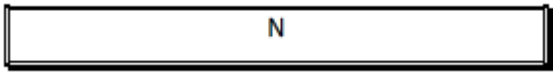
Impacto :

Perdida a causa de algún daño



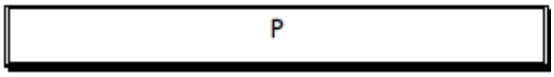
Madurez :

Grado de un proceso de organización



Normativa :

Conjunto de reglas para el uso de equipos.



PHVA :

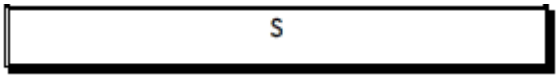
Planifica, Hacer, Verificar, Actuar

Probabilidad :

Posibilidad de que ocurra un riesgo

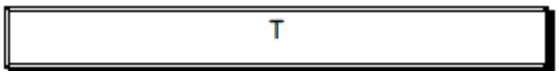
Recuperación de datos :

Proceso para recuperar información perdida.



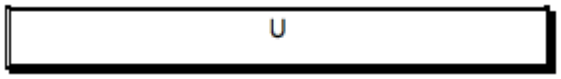
Software :

Sistemas internos de la computadora.



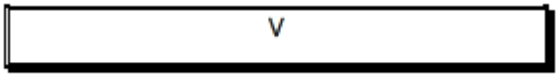
TI :

Tecnologías de la Información.



Uleam Extensión El Carmen :

Institución educativa universitaria El Carmen Manabí .



Vulnerabilidad :

Debilidad que presenta el sistema.