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

PLAN DE CONTINGENCIA PARA EQUIPOS INFORMÁTICOS DE LOS ESTUDIANTES DE TI DE ULEAM EXTENSIÓN EL CARMEN

ZAMBRANO VERA NEICER DANIEL

AUTOR

ING. RENELMO WLADIMIR MINAYA MACÍAS

TUTOR

EL CARMEN, AGOSTO 2024

CERTIFICACIÓN DEL TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CODIGO: 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 Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de investigación, bajo la autoría del estudiante **Zambrano Vera Neicer Daniel**, legalmente matriculada en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(2)-2025(1), cumpliendo el total de 384 horas, bajo la opción de titulación de proyecto integrador, cuyo tema del proyecto es "Plan de contingencia para equipos informáticos de los estudiantes de TI de 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, 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, 23 de Agosto del 2025.

Lo certifico,

Wladimir Mínaya Macías, Mg.
Docente Tutor
Área: Sistemas

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: Plan de Contingencia para Equipos Informáticos de los Estudiantes de TI de Uleam Extensión El Carmen

Modalidad: Proyector Integrador

Autor: Zambrano Vera Neicer Daniel

Tutor: Mg. Minaya Macias Renelmo Wladimir.

Tribunal de Sustentación:

Presidente:
Ing. Mora Marcillo Alex Bladimir, Mg.

Miembro:
Ing. Arévalo Hermida Rómulo Danilo, Mg.

Miembro:
Ing. Quiroz Valencia Arturo Patricio, Mg.

Fecha de Sustentación: 11 de septiembre de 2025

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: Plan de contingencia para equipos informáticos de los estudiantes de TI de ULEAM Extensión el Carmen, corresponde exclusivamente a: Zambrano Vera Neicer Daniel con CI. 1314773837, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Zambrano Vera Neicer Daniel

C.I. 1314773837

DEDICATORIA

A mi Abuela y Familia en general, por ser mi base y motivación en cada paso de este camino.

A mi novia, por tu paciencia infinita, por esos cafés a medianoche y por creer en mí incluso cuando yo dudaba.

A mis profesores, por compartir su sabiduría y guiarme con dedicación.

Y a mí mismo, por persistir cuando las pantallas en blanco parecían ganar la batalla.

Este título lleva sus nombres grabados en cada página.

AGRADECIMIENTO

A la ULEAM, por ser el escenario donde forjé mis sueños profesionales.

A mi tutor, por sus valiosas enseñanzas y por empujarme a dar siempre un poco más.

A mis amigos de carrera, cómplices de desvelos y celebraciones.

A mi novia, por ser mi soporte emocional en los momentos más intensos.

Y al destino, por ponerme en el camino personas que hicieron esta meta más dulce.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El proyecto surge de la necesidad identificada de proteger los equipos informáticos esenciales para los estudiantes de TI de la ULEAM Extensión El Carmen. La alta dependencia de computadoras portátiles para el estudio, almacenamiento de proyectos y conexión a clases representa un riesgo significativo, ya que un incidente de seguridad o una falla eléctrica podría ocasionar la pérdida total de información.

Para abordar esta problemática, se diseñó un Plan de Contingencia basado en la norma ISO/IEC 27001:2022. Mediante la aplicación de una encuesta a 60 estudiantes y una entrevista al coordinador de la carrera, se identificó que, aunque algunos usuarios instalan software antivirus, la mayoría desconoce cómo actuar ante una emergencia, evidenciando la ausencia de protocolos establecidos.

En el análisis, se determinaron los riesgos más críticos: malware (47 %), fallas eléctricas (24 %) y robo o hurto (59 %). Si bien se cuenta con dispositivos de protección como reguladores de voltaje y sistemas de videovigilancia, no existe un plan formal para la recuperación de datos ni para el reemplazo ágil de equipos en caso de siniestro.

La propuesta presentada incluye tres componentes principales: capacitaciones para los usuarios, implementación de un sistema de copias de seguridad automatizadas y elaboración de un manual de respuesta a incidentes. El enfoque no es únicamente técnico, sino también educativo, con el objetivo de proporcionar seguridad a la comunidad estudiantil y fomentar la cultura de que la protección informática implica no solo prevenir problemas, sino también estar preparados para resolverlos de manera efectiva cuando ocurran.

El objetivo general de este proyecto es diseñar un Plan de contingencia para equipos informáticos de los estudiantes de TI de la ULEAM Extensión El Carmen, en el periodo 2024-2.

ABSTRACT

The project arises from the identified need to protect the essential computer equipment used by IT students at ULEAM Extensión El Carmen. The heavy reliance on laptops for studying, project storage, and attending classes represents a significant risk, as a security incident or power failure could result in the total loss of information.

To address this issue, a Contingency Plan was designed based on the ISO/IEC 27001:2022 standard. Through the application of a survey to 60 students and an interview with the program coordinator, it was identified that, although some users install antivirus software, the majority are unaware of how to act in an emergency, highlighting the absence of established protocols.

The analysis determined the most critical risks: malware (47%), power failures (24%), and theft or robbery (59%). While protective devices such as voltage regulators and surveillance systems are available, there is no formal plan for data recovery or rapid replacement of equipment in the event of an incident.

The proposed plan includes three main components: user training, the implementation of an automated backup system, and the development of an incident response manual. The approach is not solely technical but also educational, aiming to provide security for the student community and promote a culture in which IT protection involves not only preventing problems but also being prepared to resolve them effectively when they occur.

The general objective of this project is to design a Contingency Plan for the computer equipment of IT students at ULEAM Extensión El Carmen for the 2024-2 academic period.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

Este trabajo de titulación tiene como objetivo principal diseñar e implementar un Plan de Contingencia para los equipos informáticos de los estudiantes de Tecnologías de la Información (TI) en la ULEAM Extensión El Carmen, con el fin de garantizar la continuidad operativa y la protección de sus recursos tecnológicos ante posibles fallos, robos, ciberataques u otros incidentes.

Para lograr este propósito, se realizó un diagnóstico inicial mediante encuestas a estudiantes y entrevistas al coordinador de la carrera, identificando las principales vulnerabilidades, como la falta de protocolos de seguridad, la ausencia de copias de respaldo automatizadas y la carencia de capacitación en buenas prácticas digitales. Además, se llevó a cabo una auditoría basada en la norma ISO/IEC 27001:2022, que permitió evaluar el nivel de madurez en la gestión de seguridad de la información. Los resultados mostraron que, si bien existen medidas básicas de protección física (como reguladores de voltaje y cámaras de vigilancia), hay áreas críticas que requieren atención inmediata, como la prevención de incendios (24% de protección) y la seguridad contra malware (47%).

El estudio se estructura en seis capítulos:

- Capítulo I: Plantea la problemática, objetivos y justificación del plan de contingencia.
- Capítulo II: Fundamenta teóricamente el proyecto con base en estándares internacionales y antecedentes de planes similares en instituciones educativas.
- Capítulo III: Describe la metodología de investigación, combinando enfoques cualitativos (entrevistas) y cuantitativos (encuestas).
- Capítulo IV: Presenta la propuesta detallada, incluyendo fases de implementación, recursos necesarios y análisis de riesgos mediante matrices.

Capítulo V: Aquí se hace una revisión crítica de los resultados alcanzados, poniendo el foco en qué tanto se cumplieron los controles aplicados. Además, se dejan sobre la mesa algunas recomendaciones concretas, prácticas y, sobre todo, pensadas para reducir de manera real los riesgos que se encontraron.

Capítulo VI: En este punto se recogen las lecciones más valiosas que dejó la investigación y, a la vez, se plantea una especie de hoja de ruta con pasos estratégicos que buscan reforzar y dar más solidez a la seguridad tecnológica de la universidad.

Este proyecto no solo busca proteger los equipos informáticos, sino también fomentar una cultura de prevención entre los estudiantes, asegurando que su formación académica no se vea interrumpida por fallas técnicas o incidentes de seguridad. La implementación de este plan marca un precedente en la ULEAM, alineando sus procesos con normas internacionales y promoviendo un entorno educativo más resiliente y confiable.

1.2 Presentación del tema

Plan de contingencia para equipos informáticos de los estudiantes de TI de ULEAM Extensión El Carmen.

1.3 Ubicación y contextualización de la problemática

La ULEAM Extensión El Carmen es una institución de educación superior comprometida con la formación de profesionales en diversas disciplinas, entre ellas la Tecnología de la Información (TI). La Extensión El Carmen de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), situada en la intersección de la Avenida 3 de Julio y Carlos Aray (sector El Carmen), se consolida como un pilar fundamental en la formación de los profesionales que liderarán la transformación tecnológica de esta provincia en desarrollo. Durante el periodo lectivo 2024-2, su programa de Tecnologías de la Información cuenta con una comunidad de 239 estudiantes y 15 docentes, cuya actividad académica y práctica depende críticamente de la disponibilidad y confiabilidad de los recursos tecnológicos.

La extensión cuenta con un buen número de computadoras, con características modernas que calzan bien con lo que exige la malla curricular. La plena verdad es que esos

equipos son la base para que los estudiantes puedan cumplir con sus proyectos y entrar sin trabas a las plataformas virtuales. Pero, siendo sinceros, el mantenerlos en buen estado se ha vuelto un dolor de cabeza permanente para la institución.

En un mundo donde la tecnología se queda vieja apenas la compras y donde los riesgos en internet no paran de crecer, ya no hay cómo hacerse de la vista gorda: se necesita sí o sí un buen plan de contingencia para las computadoras de los estudiantes. No se trata solo de cuidar el fierro y estar parchando cuando se daña; la cosa va más allá. Ese plan también tiene que incluir la capacitación de los usuarios, para que aprendan a usar la tecnología de manera segura y se hagan responsables de cómo la manejan.

El gran reto para la ULEAM Extensión El Carmen está, por tanto, en asegurar que todo funcione sin interrupciones que afecten a las clases, a la vez que se protege la información de posibles brechas. Al final del día, poner en marcha una estrategia sólida no es solo una cuestión técnica, sino que es básico para exprimir al máximo las herramientas disponibles. La idea es crear, en definitiva, un entorno digital que sea seguro, de fiar y que, sobre todo, esté al servicio de una educación de calidad.

1.3.1 Problematización

En la ULEAM Extensión El Carmen, los estudiantes de Tecnología de la Información dependen en gran medida de sus equipos informáticos para desarrollar sus habilidades y completar sus tareas académicas. Sin embargo, no contar con un plan de contingencia para estos equipos representa un riesgo importante para que los estudiantes puedan seguir con su aprendizaje sin interrupciones.

Los equipos de cómputo, si no reciben mantenimiento seguido y no hay una estrategia clara para prevenir fallas, se vuelven presa fácil de todo tipo de problemas: desde daños en el hardware hasta ataques cibernéticos. Y siendo francos, el lío no es solo que la máquina se ponga lenta eso sería ver lo más simple. El verdadero asunto es que la seguridad de la información que usan los estudiantes queda en riesgo, y eso, la plena, puede afectar de forma seria su formación académica.

Como no hay reglas claras sobre cómo usar los equipos ni a quién acudir cuando algo falla, la verdad es que todo se maneja a la buena de Dios, puro improvisar. Y eso es un relajo. Imagina que, de repente, la compu se te cuelgue justo en la defensa de tu trabajo de fin de carrera o peor todavía, en medio de un examen en línea. Sin un protocolo que te respalde, el estudiante queda botado, cargando él solito con las consecuencias. Esa falta de respaldo, además de hacer que uno desconfíe de la tecnología, termina siendo un peso en la cabeza: genera estrés, desconcentra y al final afecta directamente el rendimiento.

En este contexto, armar un plan de contingencias serio ya no es un "sería bueno tenerlo". Es una necesidad urgente. La clave está en que sea un plan completo, que no solo se centre en mantener los equipos, sino también en reaccionar de inmediato cuando las cosas se complican. Algo coherente, que de verdad brinde protección.

El objetivo final es totalmente evidente: blindar el proceso educativo contra interrupciones, garantizando que el foco permanezca en el aprendizaje y no en la gestión de crisis evitables.

1.3.2 Génesis del problema

En un mundo cada vez más dependiente de la tecnología, la capacidad de los estudiantes de Tecnología de la Información para acceder a equipos informáticos confiables se ha convertido en un pilar fundamental de su formación académica. Sin embargo, a medida que estos dispositivos se vuelven esenciales para el aprendizaje, también se ven amenazados por una serie de riesgos que podrían comprometer su funcionamiento y, con ello, la calidad educativa que reciben los estudiantes.

A nivel mundial está clarito que las organizaciones serias le ponen prioridad total a contar con buenas medidas de seguridad. Y no es para menos, porque con lo sofisticados que se han vuelto los ciberataques y lo lleno de vulnerabilidades que está el mundo tecnológico de hoy, las empresas no se pueden dar el lujo de confiarse ni un rato.

En el ámbito educativo, la conciencia sobre la seguridad tecnológica no siempre ha tenido la misma fuerza. Esto se nota con claridad, sobre todo en instituciones que cuentan con

menos recursos o donde la capacitación en temas de ciberseguridad todavía es limitada y, en muchos casos, casi inexistente.

Si nos centramos en Ecuador, y en especial en la ULEAM Extensión El Carmen, la situación salta a la vista. Los estudiantes de TI dependen por completo de sus equipos. Para ellos no son simples herramientas, son la ventana a una educación actual y competitiva. Y sin un plan de contingencia, la verdad, todo queda al azar. Cualquier falla puede frenar en seco su proceso de aprendizaje.

La falta de mantenimiento preventivo, la vulnerabilidad frente a averías y la ausencia de protocolos de emergencia generan un ambiente cargado de incertidumbre. Y ojo, no es un problema que golpea solo a los estudiantes, al final termina debilitando la misión educativa de toda la institución.

Con lo rápido que avanza la tecnología, las universidades no pueden quedarse de brazos cruzados. Tienen que actuar con visión y proteger sus recursos como corresponde. Levantar un plan de contingencia para los equipos de TI va más allá de lo técnico, se convierte en un verdadero seguro de vida para la formación de los estudiantes, en una apuesta firme por el futuro de esos profesionales que se están preparando. Al fin y al cabo, es invertir en ellos y asumir un compromiso real con la excelencia académica.

1.3.3 Estado actual del problema

En la ULEAM Extensión El Carmen se observa un problema importante: no existen estrategias claras para proteger los equipos informáticos que usan los estudiantes de las carreras de Tecnologías de la Información y Software. La falta de un plan para situaciones imprevistas deja estos dispositivos expuestos a riesgos, tanto de daños físicos como de pérdida o compromisos de la información que contienen.

Al no aplicarse un mantenimiento preventivo adecuado los dispositivos sufren un deterioro acelerado; esto reduce su vida útil y limita la disponibilidad de recursos tecnológicos indispensables para el aprendizaje.

Asimismo la carencia de políticas de seguridad institucional propicia prácticas de riesgo como el uso de contraseñas débiles el acceso sin restricciones a redes o la conexión

indiscriminada de dispositivos externos. Estas vulnerabilidades no solo comprometen la información almacenada sino que incrementan la exposición del sistema ante ciberataques e infecciones de malware.

Este problema va más allá de lo técnico y termina impactando la calidad educativa. Cuando los equipos dejan de funcionar en momentos cruciales, los estudiantes tienen dificultades para terminar proyectos, asistir a clases en línea o llevar a cabo investigaciones. Sin un plan de contingencia sólido, estos riesgos siguen presentes y continúan amenazando la formación de los futuros profesionales del área.

Frente a esta situación, resulta urgente que la institución adopte medidas inmediatas para crear e implementar un plan de contingencia que no solo proteja los equipos, sino que también asegure la continuidad del aprendizaje en un entorno seguro y confiable.

1.4 Diagrama causa – efecto del problema

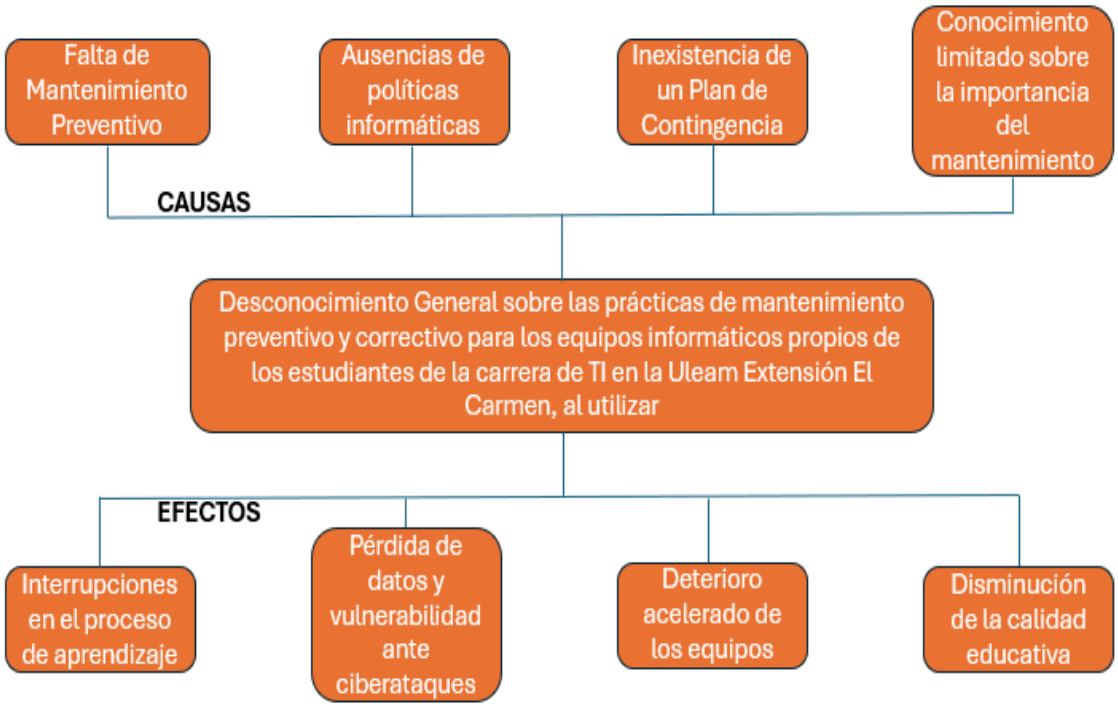


Ilustración 1 Diagrama Causa-Efecto del Problema

1.5 Objetivos

1.5.1 Objetivo general

Diseñar un Plan de contingencia para equipos informáticos de los estudiantes de TI de ULEAM Extensión El Carmen, en el periodo 2024 2.

1.5.2 Objetivos específicos

- Identificar las principales vulnerabilidades y riesgos asociados al uso de los equipos informáticos de los estudiantes de TI en la ULEAM Extensión El Carmen, mediante un análisis detallado de su estado actual y prácticas de uso.
- Fundamentar teóricamente el desarrollo del plan de contingencia a partir de una revisión seria de la literatura académica y de la normativa vigente en seguridad informática y gestión de recursos tecnológicos en entornos educativos. Esto, en pocas palabras, sirve para armar un marco sólido que dé sustento antes de ponerse manos a la obra.
- Diagnosticar la percepción y las necesidades de estudiantes y docentes respecto al uso de los equipos informáticos, mediante encuestas y entrevistas que permitan recoger información tanto cualitativa como cuantitativa, o sea, entender de verdad cómo viven y sienten su interacción con la tecnología.
- Desarrollar un plan de contingencia que no solo se quede en la teoría, sino que incorpore medidas preventivas y correctivas reales, con protocolos de mantenimiento, seguridad y respuesta ante incidentes. Todo ello basado en estándares reconocidos, pero pensado para que funcione de verdad en la práctica y sea aplicable en el día a día, no únicamente en el papel.
- Elaborar un documento final que refleje la implementación del plan de contingencia, detallando sus fases, los recursos necesarios y las recomendaciones para su correcta ejecución, con el objetivo de garantizar la protección y el buen funcionamiento de los equipos informáticos a largo plazo. La verdad es que nadie quiere llevarse sorpresas desagradables cuando dependen tanto de estos equipos.

1.6 Justificación

En la era digital actual, la tecnología constituye el núcleo de la educación moderna, especialmente en áreas como Tecnología de la Información. Para los estudiantes de TI de la ULEAM Extensión El Carmen, las computadoras representan más que simples herramientas

de clase; funcionan como un medio de trabajo y una conexión directa con los conocimientos necesarios para desarrollar un futuro profesional sólido en este campo.

El problema es que estos equipos están constantemente expuestos a diversos riesgos que terminan afectando tanto su funcionamiento como la calidad de la educación. No contar con un plan B ante cualquier falla no solo interrumpe el aprendizaje, sino que también puede ocasionar la pérdida de datos importantes, lo que impacta por igual a estudiantes y docentes.

En un entorno donde la tecnología es tan crucial, se da por hecho que es necesario contar con un plan que asegure que los equipos siempre funcionen y estén protegidos. Implementar un plan de contingencia no es solo un tema técnico; se convierte en algo imprescindible para la institución, de esos que no se pueden dejar de lado. No se trata únicamente de saber cómo reaccionar ante fallas, sino de fomentar desde ya una cultura de mantenimiento preventivo y de uso responsable de la tecnología.

Al final, lo que justifica este plan es sencillo: garantizar que la formación nunca se detenga. Todo apunta a proteger tanto la inversión educativa como el futuro de los estudiantes, evitando que un fallo técnico arruine semanas de trabajo. Además, contribuye a que los equipos tengan una vida útil más larga, lo que permite optimizar recursos y asegurar que estos futuros profesionales siempre cuenten con lo necesario para formarse. Visto así, parece puro sentido común. Por lo tanto, este trabajo no solo beneficiará a la generación actual de estudiantes, sino que también funcionará como un legado para las futuras cohortes, asegurando un entorno de aprendizaje seguro, eficiente y tecnológicamente sólido.

1.7 Impactos esperados

1.7.1 Impacto tecnológico

El impacto tecnológico de implementar un plan de contingencia para los equipos informáticos de los estudiantes de TI en la ULEAM Extensión El Carmen es profundo y multifacético. Para empezar, asegura que el aprendizaje no se detenga en un entorno donde la tecnología se ha vuelto casi indispensable para adquirir conocimientos y habilidades. Al proteger los equipos de posibles fallos o incidentes, los estudiantes mantienen siempre a mano las herramientas necesarias para avanzar en su formación.

Además, un plan de contingencia impulsa el uso responsable y seguro de la tecnología, al mismo tiempo que genera conciencia sobre la importancia del mantenimiento preventivo y de una buena gestión de los recursos. Con ello no solo se alarga la vida útil de los equipos y se mejora su desempeño, sino que también se forma en los estudiantes una actitud de responsabilidad tecnológica que les servirá a lo largo de su carrera profesional.

Este enfoque integral, en definitiva, no solo resuelve problemas urgentes dentro de la institución, sino que también prepara a los futuros profesionales con competencias claves para el mundo laboral actual: saber reaccionar frente a incidentes tecnológicos y manejar los recursos digitales con eficiencia y seguridad.

En última instancia, este plan de contingencia posiciona a la ULEAM Extensión El Carmen como una institución que no solo se adapta a las exigencias tecnológicas del presente, sino que también anticipa y mitiga los riesgos del futuro, fortaleciendo así su compromiso con la excelencia educativa y la innovación tecnológica.

1.7.2 Impacto social

La implementación de un plan de contingencia para los equipos informáticos de los estudiantes de TI en la ULEAM Extensión El Carmen conlleva un impacto social significativo que va más allá del ámbito académico. En primer lugar, al asegurar la disponibilidad continua de los recursos tecnológicos, se promueve la equidad educativa al brindar a todos los estudiantes, independientemente de su situación socioeconómica, la oportunidad de acceder en igualdad de condiciones a herramientas fundamentales para su formación.

Al implementar un plan de contingencia, no solo se obtiene una guía para actuar en caso de fallas técnicas, sino que también se fortalece el sentido de comunidad dentro de la universidad. Este tipo de iniciativas fomenta una cultura de corresponsabilidad, donde estudiantes, docentes y personal administrativo valoran más los recursos compartidos y colaboran en su cuidado. Así, se refuerzan principios fundamentales como el respeto por lo común y la solidaridad, que son esenciales para la vida universitaria.

De igual forma, la universidad transmite un mensaje claro a su comunidad: se preocupa por sus miembros incluso en situaciones adversas. Esto genera confianza, fortalece los lazos institucionales y proyecta una imagen positiva hacia la sociedad. Los estudiantes, al vivir esta

experiencia, desarrollan una mayor conciencia y responsabilidad frente al uso de la tecnología, llevándose consigo valores que aplicarán en su vida profesional.

En definitiva, este plan trasciende lo técnico para convertirse en un motor de cambio cultural. Promueve resiliencia, inclusión y la participación activa de toda la comunidad universitaria en la construcción de un entorno educativo más sólido y sostenible.

1.7.3 Impacto ecológico

El impacto ecológico de implementar un plan de contingencia para los equipos informáticos de los estudiantes de TI en la ULEAM Extensión El Carmen es altamente significativo, ya que trasciende la simple gestión de recursos tecnológicos. Al fomentar un enfoque preventivo y responsable en el mantenimiento de los equipos, este plan contribuye directamente a la reducción de desechos electrónicos, uno de los principales retos ambientales de la actualidad.

Prolongar la vida útil de los dispositivos mediante cuidados y mantenimientos periódicos evita su reemplazo constante, lo cual representa un beneficio tanto para el presupuesto institucional como para la sostenibilidad del planeta. Cada equipo que se conserva en funcionamiento implica menos basura electrónica acumulada y, a su vez, una menor demanda de recursos naturales para la fabricación de nuevos dispositivos. En consecuencia, se optimizan los recursos y se disminuye la huella ambiental de la institución.

De esta manera, la universidad promueve una cultura donde la responsabilidad tecnológica está estrechamente vinculada con el compromiso ambiental. Este enfoque no se limita a lo institucional, sino que impacta también en la formación de los estudiantes, quienes al comprender la relación entre el cuidado de sus equipos y la protección del medio ambiente, adoptan prácticas más sostenibles. Así, se convierten en agentes de cambio capaces de generar transformaciones positivas en su entorno inmediato y en la sociedad en general.

En definitiva, este plan no solo garantiza la continuidad de las actividades académicas ante fallos técnicos, sino que también reafirma el compromiso de la ULEAM con la sostenibilidad. Demuestra que la tecnología y la protección ambiental pueden y deben ir de la mano para construir un futuro más responsable y sostenible.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

2.1.1 Plan de Contingencia para Equipos Informáticos

El desarrollo de los planes de contingencia para los equipos informáticos en universidades surge como una necesidad derivada de la creciente dependencia de la tecnología en las aulas. La presencia indispensable de estos recursos tecnológicos implica que cualquier fallo técnico o ataque cibernético puede paralizar las actividades académicas. Por lo tanto, se hace evidente la necesidad de implementar medidas preventivas y protocolos estructurados que aseguren la continuidad del funcionamiento de los sistemas.

La digitalización masiva a finales de los años noventa provocó un cambio profundo en las universidades, afectando desde la gestión académica hasta la administración institucional. Esta transformación obligó a las instituciones a enfrentar problemáticas que previamente no existían. Como respuesta, se fueron implementando progresivamente políticas de seguridad y protocolos de recuperación ante desastres. Sin embargo, fue únicamente hacia la década de 2010 cuando se adoptaron normativas internacionales, como la ISO 27001, para formalizar la gestión de la seguridad informática, incorporando planes integrales que abarcan hardware, software y aspectos humanos (Loaiza y Suasnabar, 2021).

Hoy estos planes integran no solo soluciones técnicas, sino también formación en ciberseguridad para estudiantes y el uso estratégico de infraestructuras cloud para redundancia de datos. El enfoque actual prioriza así una gestión holística que asegura tanto la protección como la recuperación ágil tras incidentes. Las instituciones que omiten estos mecanismos enfrentan riesgos sustanciales de pérdida informacional e interrupciones prolongadas en los procesos formativos (Herrera, 2021).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

2.2.1 Propuesta de Plan de Contingencia en la Universidad Estatal Sur de Manabí

El presente estudio aborda un tema de gran relevancia: la necesidad de implementar planes de contingencia para los equipos informáticos en las universidades. Un caso representativo es el

de la Universidad Estatal Sur de Manabí, donde la ausencia de una estrategia clara para proteger la infraestructura tecnológica y recuperar datos tras incidentes comprometía la continuidad de las actividades académicas.

La propuesta presentada establece medidas preventivas concretas, como la implementación de servidores redundantes para garantizar respaldo en caso de fallas y la realización periódica de copias de seguridad. El enfoque se centra particularmente en los estudiantes de TI, dado que son los principales usuarios de estos recursos y quienes, en el futuro, deberán gestionar situaciones de crisis. La aplicación del plan permitió mitigar los riesgos de pérdida de información por fallos técnicos o ciberataques, asegurando la continuidad de las actividades académicas (Quijije, 2022).

2.2.2 Implementación de un Plan de Continuidad Operativa en Instituciones Educativas

En esta investigación realizada en una institución educativa en Ecuador, se implementó un plan de continuidad operativa para equipos informáticos, centrado en el uso de tecnologías en la nube para respaldar los datos de los estudiantes y garantizar el acceso a herramientas digitales durante fallos del sistema. El estudio mostró una mejora significativa en la resiliencia de la infraestructura informática tras la implementación de soluciones basadas en servidores remotos y herramientas de colaboración en línea. (González y López, 2023)

2.2.3 Diseño de un Plan de Contingencia Informático para Universidades Públicas del Ecuador

Este estudio detalla un análisis exhaustivo de las universidades públicas de Ecuador, enfocándose en la vulnerabilidad de sus sistemas informáticos. Al final, la conclusión es bastante clara: no tener políticas de contingencia pone en serio peligro la integridad de toda la información académica y administrativa. Sin embargo, existen alternativas viables. La implementación de un plan de contingencia bien estructurado, que contempla protocolos de respuesta rápida, almacenamiento en la nube y revisiones periódicas, permitió reducir significativamente el riesgo de pérdida de información sensible (Guerra, 2022).

2.2.4 Evaluación de la Seguridad Informática en Universidades y Propuesta de Plan de Contingencia

En un estudio realizado sobre universidades en Ecuador, se identificó que la ausencia de un plan de contingencia sólido constituía el factor de mayor riesgo. La propuesta derivada de dicho análisis incluyó medidas concretas, tales como la implementación de firewalls especializados, la capacitación continua del personal técnico y la automatización de copias de seguridad en medios externos. La aplicación de estas medidas en un entorno piloto evidenció una reducción significativa de incidentes de seguridad y una estabilización notable de los servicios académicos en línea (Loaiza y Suasnabar, 2021).

2.2.5 Plan de Contingencia y Recuperación ante Desastres en Universidades

Este estudio se enfocó en desarrollar un plan de recuperación ante desastres para universidades en el contexto ecuatoriano. La investigación destacó cómo los sistemas de respaldo y las pruebas periódicas de restauración son esenciales para garantizar que los servicios académicos no se vean interrumpidos por fallos técnicos o desastres naturales. En particular, se abordó la necesidad de implementar políticas de ciberseguridad y copias de seguridad automáticas, que protegen los datos sensibles de los estudiantes y personal docente (Herrera, 2021).

2.3 Definiciones conceptuales

2.3.1 Definición de Plan de Contingencia

Un Plan de Contingencia es un conjunto de procedimientos y directrices diseñados para asegurar la continuidad de las operaciones y la recuperación rápida en caso de interrupciones o desastres. En el contexto de los equipos informáticos, este plan aborda cómo manejar situaciones como fallos de hardware, pérdida de datos o ataques cibernéticos. La implementación efectiva de un plan de contingencia permite mitigar el impacto de estos incidentes y proteger la integridad de la información. (Navarrete, 2023).

2.3.1.1 Importancia del Plan de Contingencia

La importancia de un Plan de Contingencia radica en su capacidad para reducir el riesgo de pérdidas significativas y asegurar la estabilidad operativa de una organización. Para las instituciones educativas, como la ULEAM Extensión El Carmen, tener un plan sólido es esencial para proteger los recursos informáticos y garantizar que las actividades académicas no se vean interrumpidas por problemas técnicos imprevistos (Guerra, 2022).

2.3.1.2 Características del Plan de Contingencia

Un Plan de Contingencia eficaz debe incluir varias características clave: debe ser claro y accesible, contemplar una evaluación continua de riesgos, y proporcionar procedimientos detallados para la recuperación de sistemas. Además, debe ser revisado y actualizado regularmente para adaptarse a nuevas amenazas y cambios en la infraestructura tecnológica. La participación del personal en la elaboración y ejecución del plan es fundamental para su éxito (Ponce, 2022).

2.3.1.3 Elementos del Plan de Contingencia

Según Guato (2023) los principales elementos de un Plan de Contingencia para equipos informáticos incluyen:

- **Política de recuperación de datos**: Directrices para la protección y restauración de información.
- **Evaluación de riesgos**: Identificación y análisis de posibles amenazas.
- **Procedimientos de recuperación**: Pasos específicos para restaurar sistemas y datos.
- **Entrenamiento y pruebas**: Capacitación del personal y simulaciones de incidentes.
- **Documentación**: Registros detallados de los procedimientos y recursos necesarios.

2.3.1.4 Fases del Plan de Contingencia

Según Correa (2024) el desarrollo de un Plan de Contingencia suele dividirse en las siguientes fases:

- **Preparación**: Identificación de riesgos y desarrollo de estrategias de respuesta.
- **Implementación**: Ejecución de los procedimientos y capacitación del personal.
- **Prueba y ajuste**: Realización de simulaciones para evaluar la eficacia del plan y hacer ajustes necesarios.
- **Mantenimiento**: Revisión periódica del plan para asegurar que siga siendo relevante y eficaz.

2.3.1.5 Ventajas y Desventajas del Plan de Contingencia

Entre las ventajas de un Plan de Contingencia se encuentran la reducción del tiempo de inactividad y la protección de los activos críticos. Sin embargo, los costos asociados con su implementación y mantenimiento pueden ser elevados. Además, la aceptación del personal y la capacitación adecuada son cruciales para el éxito del plan (Orjuela y Ruge, 2021).

2.3.1.6 Plan de Contingencia según Normas Internacionales

Según las normas internacionales, un Plan de Contingencia debe cumplir con ciertos estándares para garantizar una gestión efectiva de riesgos. Estas normas proporcionan un marco para la evaluación de amenazas y la implementación de medidas preventivas. El cumplimiento con estas directrices asegura que el plan sea integral y que proteja adecuadamente los recursos informáticos (Gonzabay, 2021).

2.3.1.7 Implementación de un Plan de Contingencia

Según Guerra (2022) la implementación de un Plan de Contingencia requiere un enfoque estructurado que incluye:

- **Desarrollo de políticas**: Establecimiento de directrices claras para la gestión de riesgos.

- **Asignación de responsabilidades**: Definición de roles y tareas para el personal encargado.

- **Desarrollo de procedimientos**: Creación de pasos detallados para la respuesta a incidentes.

- **Evaluación y ajuste**: Revisión continua del plan para mejorar su efectividad.

2.3.1.8 Mecanismos de Comunicación en el Plan de contingencia.

Según Orjuela y Ruge (2021) un aspecto crucial de un Plan de Contingencia es el establecimiento de mecanismos de comunicación efectivos para gestionar las emergencias y coordinar la respuesta durante un incidente. La comunicación debe ser clara, eficiente y oportuna para asegurar que todos los involucrados estén informados y puedan actuar de manera coordinada. Este mecanismo debe incluir:

 Canales de comunicación: es necesario establecer de manera clara los medios de comunicación que se utilizarán durante una crisis. Estos pueden incluir el correo institucional, la mensajería instantánea o las plataformas internas. Lo fundamental es garantizar que todos los usuarios tengan acceso a la información y disponer de múltiples canales para evitar situaciones de incomunicación.

 Roles y responsabilidades: cada integrante del equipo debe saber exactamente qué le toca hacer. O sea, quién comunica, cómo lo hace y a quién se dirige en medio de un incidente. Esa claridad evita confusiones y pérdida de tiempo.

 Protocolos de información: es necesario marcar un flujo claro para difundir datos críticos, cuidando que sean precisos, verificados y transmitidos en el momento justo.

 Comunicación externa: también hace falta pensar en cómo hablar con quienes están fuera de la institución, como proveedores, entes reguladores o incluso medios de comunicación. La idea es mantener la transparencia, pero al mismo tiempo controlar la narrativa para no generar alarmas innecesarias.

La comunicación efectiva mitiga la confusión y organiza la respuesta, reduciendo así el impacto del incidente y acelerando la recuperación. La revisión periódica y la simulación de estos protocolos resultan cruciales para preservar su utilidad operativa.

2.3.1.9 Evaluación y Pruebas del Plan de Contingencia

La fase de evaluación y pruebas es crucial para verificar la eficacia del plan de contingencia antes de enfrentarse a incidentes reales. Según un marco metodológico típico, se debe:

- **Ejecutar simulaciones o ejercicios de prueba** que involucren distintos escenarios de riesgo, como fallos de hardware, pérdida de acceso o incidentes de seguridad.

- **Realizar análisis post-ejecución** que permitan identificar debilidades, tiempos de respuesta y oportunidades de mejora continuas.

- **Documentar resultados** y generar acciones correctivas para optimizar el plan con base en los hallazgos.

Estas prácticas se alinean con modelos de continuidad de negocio utilizados en instituciones públicas de Ecuador, donde se incluye la revisión periódica, pruebas de restauración y formación del personal (Gambin y Macías, 2017).

2.3.2 Definición de Sistemas Informáticos

Su estructura tecnológica incluye desde el hardware, como las computadoras y servidores que utilizamos día a día, hasta las capas de software que permiten que todo funcione:

sistemas operativos, aplicaciones y bases de datos que sostienen nuestro trabajo académico y profesional. En el contexto educativo de la ULEAM Extensión El Carmen, estos sistemas se han vuelto fundamentales para sostener tanto la gestión académica como la administrativa, asegurando la continuidad operativa y facilitando el acceso ágil a la información para estudiantes, docentes y personal instituciona (Arco, 2024).

2.3.2.1 Importancia de los Sistemas Informáticos en la Educación

La implementación de sistemas informáticos en instituciones educativas es crucial para el desarrollo académico y administrativo. Estos sistemas permiten automatizar procesos, optimizar el acceso a la información y mejorar la comunicación entre estudiantes, profesores y el personal administrativo. Además, en tiempos de disrupciones tecnológicas, como ciberataques o fallos en la infraestructura, un sistema informático robusto permite la continuidad operativa, asegurando que las actividades educativas no se vean afectadas. Para la ULEAM Extensión El Carmen, esto significa poder garantizar un entorno de aprendizaje resiliente y seguro (Villamayor, 2024).

2.3.2.2 Características de los Sistemas Informáticos

Los sistemas informáticos presentan una serie de características fundamentales que garantizan su eficacia y funcionalidad. Estas incluyen la interactividad, ya que permiten la comunicación entre los diferentes componentes del sistema y sus usuarios; la flexibilidad, que les permite adaptarse a cambios tecnológicos y nuevas necesidades; y la seguridad, un aspecto vital para proteger la información sensible de estudiantes y profesores frente a amenazas externas. En un entorno educativo como el de la ULEAM Extensión El Carmen, estas características permiten una gestión eficiente de los recursos tecnológicos y aseguran que los estudiantes puedan acceder a las plataformas y servicios sin interrupciones. La integración de las Tecnologías de la Información y Comunicación (TIC) en el sistema educativo público de Ecuador ha marcado un cambio significativo en la manera en que se aborda el aprendizaje. La disponibilidad de información instantánea y recursos educativos en línea ha mejorado sustancialmente el acceso a conocimientos diversos, rompiendo barreras geográficas y económicas. Esta democratización del acceso a la información es un paso crucial hacia una educación más inclusiva y equitativa (Collahuazo, 2024).

2.3.2.3 Componentes de los Sistemas Informáticos

Según Grimalt y otros (2022), los componentes esenciales de un sistema informático se dividen en hardware, software, redes y recursos humanos:

- El hardware comprende todos los componentes físicos del sistema, incluyendo ordenadores, servidores, discos duros, chasis y cables, que constituyen la estructura necesaria para el funcionamiento del entorno informático.
- El software representa los sistemas operativos, programas y aplicaciones que permiten que el hardware funcione correctamente. Actúa como el componente intangible que da operatividad a los dispositivos físicos.
- Las redes constituyen la infraestructura de comunicación que conecta los dispositivos y permite el intercambio seguro de información. Su correcto funcionamiento es esencial para garantizar la continuidad y eficiencia de los servicios tecnológicos.
- El factor humano incluye a los técnicos y especialistas responsables de la administración, mantenimiento y mejora continua de los sistemas. Su participación es fundamental, ya que sin ellos los componentes físicos y digitales carecerían de operatividad y gestión adecuada.

En el contexto de los estudiantes de TI en la ULEAM Extensión El Carmen, estos componentes se integran para proporcionar un ambiente tecnológico adecuado para el aprendizaje y la investigación.

2.3.2.4 Fases de Implementación de un Sistema Informático

Según Sánchez (2021),la implementación de un sistema informático en una institución educativa sigue una serie de fases estructuradas, que incluyen:

1. **Planificación**: Se definen los objetivos del sistema y se identifican las necesidades tecnológicas de la institución.

2. **Desarrollo:** en primera instancia, se adquieren el hardware y el software necesarios. Posteriormente, se procede a ensamblar y configurar el sistema, ajustando cada componente para garantizar su correcto funcionamiento.

3. **Implementación:** a continuación, se instala el sistema en un entorno real y, al mismo tiempo, se entrena al personal técnico para que pueda manejarlo sin contratiempos.

4. **Evaluación**: finalmente, se revisa cómo está funcionando el sistema, auditando su rendimiento para asegurarse de que cumple los objetivos y opera correctamente.

Se audita el rendimiento del sistema para verificar el cumplimiento de objetivos y su funcionamiento óptimo.

2.3.2.5 Ventajas y Desventajas de los Sistemas Informáticos

Entre las principales ventajas de un sistema informático se destacan la eficiencia en la gestión de datos, la automatización de procesos y la capacidad de proteger la información académica y administrativa mediante mecanismos de seguridad. No obstante, también existen desventajas relevantes, como los altos costos de implementación y mantenimiento, así como el riesgo de brechas de seguridad cuando no se aplican las medidas adecuadas. En el caso de la ULEAM Extensión El Carmen, un sistema informático correctamente diseñado puede incrementar la productividad y resguardar los datos sensibles de los estudiantes; sin embargo, la disponibilidad limitada de recursos constituye un desafío significativo para garantizar su sostenibilidad operativa (Sánchez, 2021).

2.3.2.6 Sistemas Informáticos en la Nube

En los últimos años, el uso de sistemas en la nube ha revolucionado la gestión de la información en instituciones educativas. Este enfoque permite almacenar grandes cantidades de datos de manera remota, reduciendo la necesidad de infraestructuras físicas costosas. Además, la nube proporciona acceso continuo a la información desde cualquier lugar y dispositivo, lo cual es particularmente beneficioso para los estudiantes de TI en ULEAM Extensión El Carmen, ya que facilita el acceso a herramientas y recursos desde cualquier

ubicación geográfica. Sin embargo, es esencial garantizar la seguridad de los datos alojados en la nube para evitar brechas de seguridad (Barbosa y otros, 2023).

2.3.2.7 Mantenimiento de los Sistemas Informáticos

El mantenimiento de los sistemas informáticos es como llevar tu vehículo al taller de manera periódica. Si no lo haces, tarde o temprano surgirán problemas, y muchas veces de manera inesperada. La idea es que todo funcione sin contratiempos, asegurando que los equipos estén siempre listos para el estudio o el trabajo diario.

En la práctica, esto implica actualizar periódicamente tanto el software como el hardware, aplicar los parches de seguridad correspondientes y realizar revisiones regulares para identificar oportunamente posibles vulnerabilidades, de manera similar a la inspección preventiva de una infraestructura antes de una temporada de riesgo.

En la ULEAM Extensión El Carmen, contar con un plan de mantenimiento definido constituye una necesidad fundamental. Esto permite asegurar la operatividad continua de los sistemas durante la realización de proyectos y exámenes en línea por parte de los estudiantes de TI. Un mantenimiento adecuado garantiza que los equipos funcionen de manera eficiente, protegiendo la seguridad e integridad de los datos y permitiendo que el enfoque permanezca en el aprendizaje. La ausencia de mantenimiento incrementa el riesgo de fallos que podrían comprometer los sistemas y la información académica (Felices y López, 2023).

2.3.2.8 Seguridad de los Sistemas Informáticos

La seguridad informática es uno de los pilares más importantes en la gestión de sistemas informáticos, especialmente en el entorno educativo, donde se manejan datos personales y académicos sensibles. Las principales amenazas incluyen ciberataques, malware y phishing, que pueden comprometer la integridad de los sistemas. Para mitigar estos riesgos, las instituciones como la ULEAM Extensión El Carmen deben implementar medidas como el uso de firewalls, antivirus y protocolos de encriptación de datos, así como capacitar al personal y a los estudiantes en prácticas de ciberseguridad (Pozo y otros, 2025).

2.3.2.9 Interoperabilidad de los Sistemas Informáticos

La interoperabilidad de sistemas es la capacidad de que diferentes plataformas, aplicaciones y dispositivos puedan comunicarse, compartir datos y operar coordinadamente, lo cual es esencial en entornos educativos integrados. Un ejemplo de definición clara proviene de González (2023), quien señala que interoperabilidad incluye la habilidad de "transferir y traducir datos útiles" entre sistemas educativos digitales América Latina en Línea. También, en documentos sobre estándares tecnológicos, se menciona que la interoperabilidad facilita el intercambio seguro entre sistemas y dispositivos

2.3.3 Metodología de desarrollo.

Fases de la Norma ISO 27001

Ilustración 2 Fases de la Norma ISO 27001

2.3.3.1 Relación entre la Norma ISO/IEC 27001 y el Plan de Contingencia

Modelos académicos sobre continuidad de negocio también se sustentan en estándares ISO. Un estudio realizado en universidades ecuatorianas analiza la madurez del sistema de gestión de continuidad del negocio con base en normas internacionales, resaltando la necesidad de cláusulas documentadas, ejercicios de validación y auditorías internas como parte del ciclo continuo de mejora (Angulo et al., 2020).

2.4 Conclusiones del marco teórico

La revisión exhaustiva de los antecedentes históricos y de las investigaciones relacionadas revela que los planes de contingencia para equipos informáticos son elementos fundamentales para la continuidad operativa en instituciones educativas, como la ULEAM Extensión El Carmen. Estos planes no solo abordan la recuperación de datos tras incidentes tecnológicos, sino que también promueven una cultura de prevención y resiliencia ante las crecientes amenazas cibernéticas.

Queda claro que implementar estos planes de manera efectiva, combinando estrategias técnicas con capacitación en ciberseguridad, es algo indispensable para proteger nuestra infraestructura tecnológica. Esto se nota especialmente en el ámbito académico, porque mantener la integridad de los sistemas informáticos es fundamental para que estudiantes y docentes puedan trabajar y aprender sin interrupciones ni contratiempos.

Por otro lado, estudios recientes muestran que los sistemas de respaldo sólidos y el uso de tecnologías en la nube han cambiado bastante la manera de manejar datos y servicios en las universidades. No solo ayudan a recuperarse rápido ante cualquier fallo, sino que además permiten un acceso constante y seguro a la información, algo que hoy día resulta indispensable en la educación.

Implementar normas internacionales como la ISO 27001 es un paso muy importante, porque permite formalizar las políticas de seguridad de la institución. Esta tendencia hacia la estandarización muestra que se necesita un enfoque integral, que proteja los datos sensibles y asegure que todo funcione de manera estable, aspectos fundamentales para que la ULEAM Extensión El Carmen continúe avanzando tanto en lo académico como en lo administrativo.

Asimismo, el análisis conceptual del marco teórico ha permitido evidenciar que la existencia de un plan de contingencia articulado con sistemas informáticos sólidos no es únicamente una medida técnica, sino una herramienta estratégica para la gestión institucional. En contextos con limitaciones presupuestarias o infraestructura restringida, como ocurre en muchos centros de educación superior pública del Ecuador, contar con una planificación adecuada frente a interrupciones tecnológicas puede marcar la diferencia entre la continuidad o la parálisis de los procesos educativos.

En este sentido, resulta indispensable que las instituciones de educación superior desarrollen políticas claras de evaluación de riesgos, capacitación continua para el personal técnico y docente, y actualizaciones periódicas de sus planes de contingencia, con base en auditorías internas y en la evolución de las amenazas. El enfoque proactivo y preventivo debe reemplazar las respuestas reactivas, a fin de consolidar un ecosistema informático resiliente, sostenible y alineado con las necesidades actuales de la educación digital.

En definitiva, el conocimiento sistematizado en este capítulo establece los fundamentos conceptuales y metodológicos para diseñar un plan de contingencia contextualizado a la realidad de la ULEAM Extensión El Carmen. La articulación entre normativa internacional, mejores prácticas, antecedentes investigativos y componentes técnicos funciona como base estructural para el trabajo de campo subsiguiente y la formulación de una propuesta de mejora institucional viable.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

La prevención se reconoce como el instrumento más eficaz para afrontar contingencias en entornos tecnológicos. En este capítulo se presentan los hallazgos de una investigación exhaustiva que permitió el desarrollo de un plan de contingencia robusto y confiable.

Se analizaron diversos contextos y se identificaron los riesgos a los que están expuestos los equipos de computación de los estudiantes. Con base en esta información, se desarrollaron estrategias y procedimientos destinados a minimizar el impacto de posibles incidentes y garantizar la continuidad de las actividades académicas.

3.2 Tipos de investigación

3.2.1 Investigación cualitativa

La investigación cualitativa, como metodología, permite explorar y comprender a profundidad los significados, percepciones y comportamientos asociados a un fenómeno en particular, priorizando el análisis de datos no numéricos para interpretar la realidad desde la perspectiva de los involucrados. Este enfoque es especialmente valioso para detallar cómo se desarrollan ciertos eventos y para diseñar estrategias efectivas en respuesta a situaciones específicas (Satander Becas, 2021).

Este enfoque le dio mucha más solidez al marco teórico y nos permitió profundizar en conceptos clave como la seguridad informática, la continuidad operativa y la gestión de riesgos tecnológicos. Como parte del proceso, fue necesario mantener largas conversaciones con las autoridades académicas y administrativas, incluido el director de la extensión universitaria, para obtener información detallada sobre el estado de los equipos, las medidas de mantenimiento aplicadas y las prácticas de uso que ya estaban en funcionamiento.

De esos diálogos surgió un panorama revelador acerca de las debilidades del sistema y, sobre todo, de cómo percibe la comunidad universitaria la importancia de contar con un plan de contingencia. Los hallazgos señalaron con claridad en qué aspectos había que actuar con

urgencia y sirvieron de base para diseñar propuestas ajustadas al contexto real, asegurando que las soluciones no se vieran como parches momentáneos, sino como alternativas sostenibles y con verdadero sentido. Al final, la investigación cualitativa se convirtió en la herramienta que permitió comprender el problema en profundidad y construir respuestas coherentes con la realidad de la institución.

3.2.2 Investigación cuantitativa

La investigación cuantitativa, puede entenderse como un método riguroso orientado a recopilar datos medibles y objetivos que permitan analizar y comprender de manera estadística la problemática identificada. Este enfoque facilita la construcción de instrumentos como encuestas y cuestionarios diseñados para recopilar información de los 239 estudiantes y 15 docentes, permitiendo identificar patrones, vulnerabilidades y necesidades relacionadas con el manejo de los equipos informáticos.

Se emplearán herramientas estadísticas para el análisis de los datos, lo que permitirá presentar los hallazgos de manera clara mediante gráficos, tablas y análisis descriptivos. Este enfoque no solo otorga mayor objetividad al estudio, sino que también facilita la formulación de conclusiones y la propuesta de estrategias basadas en evidencia concreta, garantizando la efectividad del plan de contingencia. Además, el enfoque cuantitativo permite desarrollar hipótesis fundamentadas y responder preguntas relevantes, minimizando interpretaciones erróneas. De este modo, se genera información práctica y confiable que respalda la toma de decisiones basada en datos (Guillem, 2021).

3.2.3 Investigación descriptiva

La investigación descriptiva es una metodología que se centra en caracterizar y analizar fenómenos, poblaciones o contextos específicos mediante la observación sistemática de sus componentes. Este enfoque permite examinar en detalle los problemas y desarrollar modelos que faciliten su comprensión. Su objetivo principal es recopilar y procesar información de manera exhaustiva, identificando comportamientos y patrones subyacentes en el sistema. Esta información resulta fundamental para evaluar los problemas con criterio y proponer soluciones efectivas (Guevara y otros, 2020).

Se empleará una investigación descriptiva para examinar y detallar la situación de los equipos informáticos en la institución. El objetivo es recopilar datos concretos sobre el estado físico de los equipos, la frecuencia de uso, las políticas de mantenimiento existentes y las necesidades de los estudiantes. Este análisis permitirá observar la situación de manera objetiva y establecer bases sólidas para el diseño de propuestas viables que optimicen la utilización de los recursos.

Aplicar esta metodología también nos ayudará a identificar tanto las debilidades como, y esto es importante, las fortalezas de los sistemas informáticos de la ULEAM Extensión El Carmen. Además, nos brindará un respaldo firme para elaborar estrategias preventivas, porque el objetivo final es que los equipos continúen funcionando sin sobresaltos y que todo marche como debe ser.

3.3 Métodos de investigación

3.3.1 Método Inductivo

El método deductivo se basa en partir de conceptos generales, considerados válidos, para llegar a conclusiones más específicas mediante la aplicación de la lógica. Este enfoque permite estructurar el análisis de manera coherente, asegurando que los resultados sean consistentes al derivarse de la aplicación sistemática de principios generales (Gómez, 2021).

En este proyecto se parte de teorías y normativas existentes sobre seguridad informática y gestión de recursos, a partir de las cuales se derivan conclusiones más precisas. Este enfoque permite garantizar que las propuestas sean realistas, aplicables y pertinentes al contexto de la universidad, asegurando su utilidad y viabilidad operativa.

3.3.2 Método deductivo

El método deductivo se caracteriza por partir de premisas generales para llegar a conclusiones específicas, basándose en la reflexión lógica y la aplicación de principios preestablecidos. Este enfoque permite estructurar los análisis de manera coherente, obteniendo resultados válidos que se derivan de la aplicación sistemática de reglas generales (Gómez, 2021).

A partir de teorías y normativas generales sobre seguridad informática y gestión de recursos tecnológicos, se podrán derivar conclusiones específicas que se ajusten a la realidad de la institución. Para ello, se tomarán como referencia estándares internacionales, como la ISO/IEC 27001, y principios de gestión de riesgos, los cuales serán adaptados para el diseño de políticas y procedimientos que respondan a las necesidades de estudiantes y docentes.

Este enfoque permite organizar las soluciones de manera lógica, de modo que cada acción cuente con un respaldo teórico sólido y esté orientada a resolver los problemas identificados de forma práctica y eficaz.

3.3.3 Método analítico

El método analítico es fundamental para descomponer fenómenos complejos en elementos más manejables, identificando sus componentes y relaciones para obtener una comprensión profunda del objeto de estudio. Este enfoque implica el análisis sistemático de factores, causas y efectos para desarrollar una solución basada en evidencia y razonamiento crítico (Question Pro, 2023).

Este enfoque permite crear estrategias concretas y aplicar medidas de protección que realmente tengan sentido en el contexto de la institución.

Con este método, se pueden analizar las causas de los problemas que se repiten en los equipos, detectar los puntos más críticos dentro de la infraestructura tecnológica y revisar qué tan preparados están los estudiantes ante posibles contingencias. A partir de ese análisis, se puede armar un plan integral que no solo atienda las vulnerabilidades actuales, sino también los riesgos que podrían aparecer, mejorando así la seguridad y el funcionamiento de todo el sistema informático.

3.3.4 Método sintético

El método sintético permite consolidar información fragmentada en un todo coherente, reconstruyendo elementos esenciales para la comprensión integral de un fenómeno. Este enfoque es crucial para conectar teorías y datos aislados, transformándolos en un conocimiento estructurado y significativo que respalda el análisis y la toma de decisiones (Rodríguez y Pérez, 2024).

El método sintético facilita la integración de investigaciones previas y análisis fragmentados en una estrategia cohesionada. Por ejemplo, se puede resumir información clave sobre riesgos informáticos, políticas de seguridad y protocolos de mantenimiento, creando un marco completo que sustente las propuestas del plan. Este enfoque garantiza una visión amplia y fundamentada que abarca desde las necesidades específicas de los estudiantes hasta la proyección de soluciones viables.

3.4 Fuentes de información de datos

3.4.1 Fuente Primaria

Las fuentes primarias constituyen un recurso fundamental para comprender de manera directa la situación que enfrentan los estudiantes de TI de la ULEAM Extensión El Carmen en relación con el uso de sus equipos informáticos. La recolección de datos se llevará a cabo mediante entrevistas estructuradas y cuestionarios aplicados a los estudiantes, con el objetivo de identificar problemáticas recurrentes, tales como fallas técnicas, prácticas de uso inadecuadas y la ausencia de medidas preventivas de mantenimiento.

Se recopilará información detallada sobre aspectos como la frecuencia de averías de los equipos, sus métodos de almacenamiento y transporte, y las condiciones ambientales en las que operan. Adicionalmente, se realizarán entrevistas con representantes estudiantiles y técnicos especializados, con el fin de obtener una visión integral de las necesidades reales y de los recursos disponibles en la institución.

Esta metodología permitirá desarrollar un plan de contingencia basado en experiencias reales, contribuyendo a mantener los equipos en condiciones óptimas y garantizar su correcto funcionamiento, lo cual resulta fundamental para el desempeño académico de los estudiantes.

3.4.2 Fuente secundaria

Las fuentes secundarias son esenciales para complementar el análisis de las condiciones de los equipos informáticos personales de los estudiantes de TI en la ULEAM Extensión El Carmen. Estas fuentes, conformadas por libros, artículos académicos y reportes técnicos, aportan datos previamente recopilados y analizados por otros investigadores, lo que permite contextualizar la problemática desde perspectivas externas y generalizadas.

Se recurrirá a estudios previos sobre el uso, mantenimiento y vulnerabilidades de equipos informáticos personales en entornos educativos similares. Se considerarán referencias relacionadas con prácticas de gestión de riesgos tecnológicos y guías de mantenimiento preventivo dirigidas a estudiantes universitarios. Adicionalmente, se analizarán informes estadísticos y encuestas generales sobre la vida útil de laptops y otros dispositivos utilizados en el ámbito académico, con el objetivo de identificar patrones aplicables a la realidad de los estudiantes de la extensión. Esta información permitirá diseñar un plan de contingencia alineado con las necesidades institucionales y las mejores prácticas documentadas.

3.4.3 Encuestas

Para el desarrollo del Plan de Contingencia para Equipos Informáticos de los Estudiantes de TI de ULEAM Extensión El Carmen, se aplicó una encuesta a 239 estudiantes de la carrera. Este instrumento permitió recolectar datos sobre el estado actual de los equipos informáticos personales, las prácticas de mantenimiento implementadas, y las principales vulnerabilidades percibidas. Con los resultados, se pudo identificar patrones comunes y establecer prioridades para diseñar estrategias de contingencia efectivas (Hernández y Mendoza, 2023).

3.4.4 Entrevista

Las entrevistas son una herramienta clave para recopilar información directa y confiable mediante la interacción con los participantes, permitiendo explorar tanto sus comportamientos como sus percepciones sobre un tema. Este método facilita un entendimiento más profundo y personalizado del contexto investigado, integrando aspectos comunicativos en la recolección de datos (UPRRP, 2020).

Para este estudio se llevaron a cabo entrevistas con un grupo de estudiantes de TI de la ULEAM Extensión El Carmen que usan sus propios equipos informáticos. La idea de estas conversaciones era conocer de primera mano las principales dificultades que enfrentan con el mantenimiento, el uso y la protección de sus dispositivos, así como entender cuáles son sus hábitos en materia de seguridad de la información. Toda la información recogida servirá como base sólida para elaborar un plan de contingencia que realmente se ajuste a sus necesidades y al contexto en el que se desenvuelven.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

La población se define como el conjunto de estudiantes matriculados en el periodo 2024-2, que asciende a 239 personas y el coordinador de la Carrera de TI y Software. Este grupo representa una muestra accesible y delimitada, lo que permite la implementación de instrumentos de recolección de datos. La caracterización de esta población es fundamental para identificar sus necesidades específicas en cuanto al uso y protección de equipos informáticos (Gómez, 2021).

3.5.2 Muestra

La población total, como se especificó anteriormente, está conformada por 239 estudiantes de la carrera de TI en la ULEAM Extensión El Carmen. Para este estudio, se seleccionó una muestra de 60 estudiantes, lo que representa un grupo suficientemente representativo para obtener resultados confiables sobre las condiciones y necesidades de los equipos informáticos. Esta selección se respalda en la fórmula de muestreo para poblaciones finitas**,** considerando un nivel de confianza del 95% y un margen de error del 10%, que indica que este número de participantes es adecuado para reflejar la realidad de toda la población. Cabe destacar que, además de las encuestas a los estudiantes, se realizó una entrevista con el coordinador de la carrera, lo que permitió obtener información más detallada sobre las políticas de seguridad informática y la gestión de los recursos tecnológicos (Guato, 2023).

3.5.3 Análisis de las herramientas de recolección de datos a utilizar

3.5.3.1 Cuestionario

Encuesta dirigida a: Estudiantes de la ULEAM Extensión el Carmen.

Objetivo: Evaluar las condiciones actuales de los equipos informáticos de los estudiantes de TI de la ULEAM Extensión El Carmen y la existencia de políticas de seguridad informática. Este análisis busca determinar el grado de preparación ante posibles contingencias, identificando las medidas necesarias para garantizar la protección y recuperación de los equipos en situaciones de riesgo o fallo, con el fin de diseñar un plan de contingencia adecuado que resguarde los recursos tecnológicos de los estudiantes y apoye su continuidad educativa.

Nombre de la empresa: Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen.

1. **¿Conoces algún plan de contingencia para equipos informáticos?**

   SI ( ) NO ( )

2. **¿Sabes cuáles son los procedimientos para seguir en caso de pérdida, daño o robo de tu equipo (computadora o laptop)?**

   SI ( ) NO ( )

3. **¿Tienes identificado un lugar seguro para guardar una copia de seguridad de tus archivos importantes?**

   SI ( ) NO ( )

4. **¿Has realizado alguna prueba de restauración de tus archivos desde la copia de seguridad?**

   SI ( ) NO ( )

5. **¿Conoces los riesgos más comunes que pueden afectar a tus equipos informáticos (virus, malware, etc.)?**

   SI ( ) NO ( )

6. **¿Utilizas software antivirus y antimalware actualizado en tu equipo?**

   SI ( ) NO ( )

7. **¿Has recibido capacitación sobre cómo identificar y reportar posibles amenazas a la seguridad informática?**

   SI ( ) NO ( )

8. **¿Sabes cómo activar el modo seguro en tu sistema operativo en caso de problemas?**

   SI ( ) NO ( )

9. **¿Tienes registrado el número de serie y otras características de tu equipo en caso de pérdida o robo?**

   SI ( ) NO ( )

10. **¿Consideras que la información almacenada en tu equipo es importante y requiere protección adicional?**

SI ( ) **NO ( )**

3.5.3.2 Guía de Entrevista

Entrevista dirigida a: Coordinador Académico de la carrera TI en la ULEAM Extensión El Carmen.

Objetivos: Objetivo: Analizar el estado actual de los equipos informáticos de los estudiantes de la carrera de TI en la ULEAM Extensión El Carmen, identificando las necesidades de seguridad y la preparación frente a situaciones de emergencia. Este estudio tiene como fin establecer las bases para el desarrollo de un plan de contingencia que garantice la continuidad operativa de los equipos, protegiendo los datos e infraestructura tecnológica ante posibles fallos, robos o desastres, y asegurando el funcionamiento adecuado de los sistemas durante el ciclo académico.

Nombre de la empresa: Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen.

1. **¿Conoces la existencia de un plan de contingencia para proteger tus equipos informáticos en caso de pérdida, robo o daño?**

---

2. **¿Has recibido alguna capacitación sobre cómo actuar en caso de un incidente de seguridad con tu equipo?**

---

3. **¿Sabes cómo realizar una copia de seguridad de tus archivos importantes?**

---

4. **¿Con qué frecuencia realizas copias de seguridad?**

5. **¿Tienes identificado un lugar seguro para almacenar tus copias de seguridad?**

6. **¿Has probado a restaurar tus archivos a partir de una copia de seguridad?**

7. **¿Utilizas contraseñas seguras y diferentes para cada una de tus cuentas?**

8. **¿Has instalado algún software de seguridad en tu equipo (antivirus, antimalware)?**

9. **¿Conoces los riesgos más comunes que pueden afectar a tus equipos informáticos (virus, phishing, etc.)?**

10. **¿Has reportado algún incidente de seguridad con tu equipo al personal encargado?**

3.5.3.3 Estructura de los instrumentos de recolección de datos aplicados

La recolección de datos para este estudio se llevó a cabo mediante una encuesta compuesta por 10 preguntas, cada una con opciones de respuesta cerradas. Una de las preguntas clave fue la número 1, que investigaba si los estudiantes conocían los procedimientos establecidos en el plan de contingencia de los equipos informáticos. Además, se incluyó una entrevista con los presidentes de la carrera de TI, también compuesta por 10 preguntas, para profundizar en las medidas de seguridad y protección de los equipos de los estudiantes, con el objetivo de evaluar la implementación de políticas de contingencia y su efectividad.

3.5.4 Plan de recolección de datos

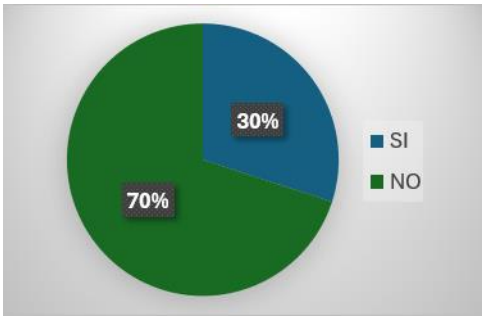
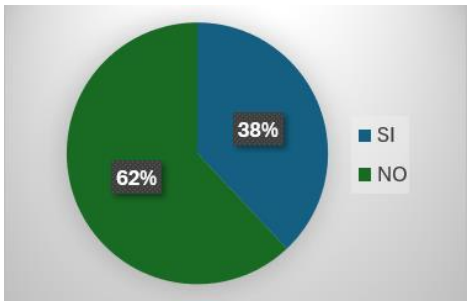
Día	Hora	Personal	Tipo de Instrumento
07/05/205	09-00 horas	Estudiantes de la Carrera de TI	Encuesta
08/05/2025	10-15 horas	Coordinador académico de la Carrera de TI	Entrevista

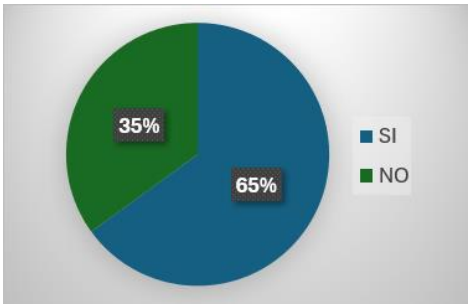
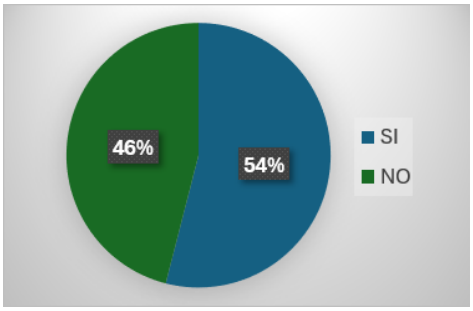
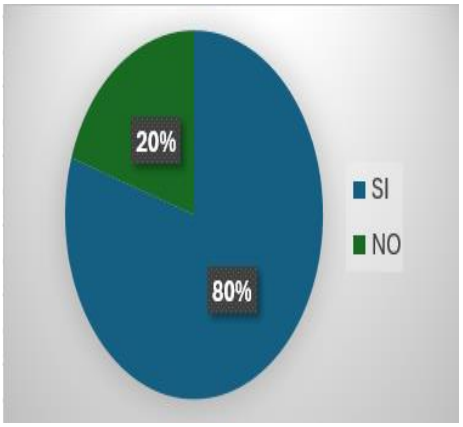
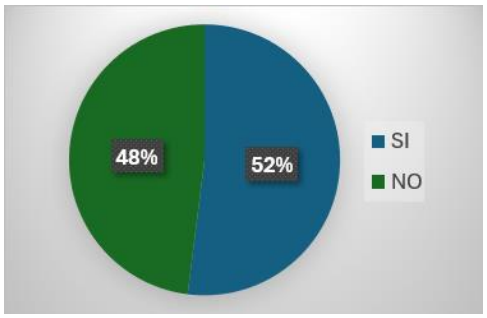
Tabla 1 Plan de Recolección de Datos

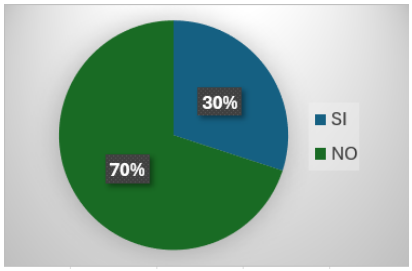
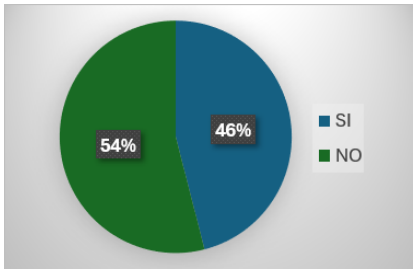
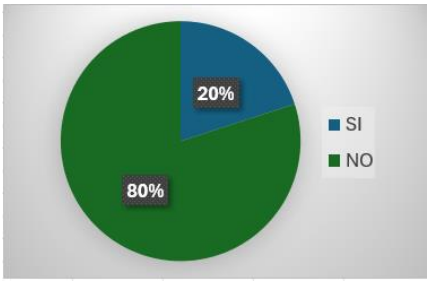
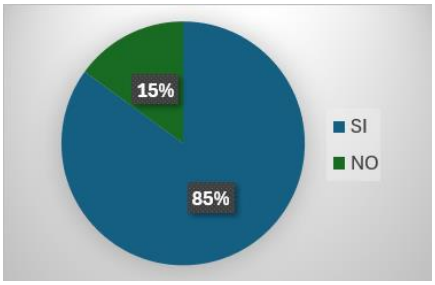
3.6 Análisis y presentación de resultados

3.6.1 Presentación y descripción de los resultados obtenidos

3.6.1.1 Encuesta aplicada a los estudiantes de la Carrera de TI de la ULEAM Extensión El Carmen.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
1. **¿Conoces algún plan de contingencia para equipos informáticos?**		De la muestra encuestada la gran mayoría desconoce lo que es un Plan de Contingencia para equipos informáticos.
2. **¿Sabes cuáles son los procedimientos para seguir en caso de pérdida, daño o robo de tu equipo (computadora o laptop)?**		Más de la mitad de los encuestados desconoce sobre los procedimientos a seguir en caso de pérdida, daño o robo de su equipo propio.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
3. **¿Tienes identificado un lugar seguro para guardar una copia de seguridad de tus archivos importantes?**		Más de la mitad de estudiantes si tiene identificado un lugar seguro para guardar archivos importantes de la copia de seguridad.
4. **¿Has realizado alguna prueba de restauración de tus archivos desde la copia de seguridad?**		Un poco más de la mitad de los estudiantes afirma que si ha realizado pruebas de como restaurar archivos desde la copia de seguridad.
5. **¿Conoces los riesgos más comunes que pueden afectar a tus equipos informáticos (virus, malware, etc.)?**		La gran mayoría de estudiantes si conoce cuales suelen ser los riesgos más comunes que pueden afectar los equipos informáticos.
6. **¿Utilizas software antivirus y antimalware actualizado en tu equipo?**		Un poco más de la mitad si usa una antivirus actualizado para su equipo.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
7. **¿Has recibido capacitación sobre cómo identificar y reportar posibles amenazas a la seguridad informática?**		La gran mayoría no ha recibido capacitaciones de como identificar posibles amenazas informáticas.
8. **¿Sabes cómo activar el modo seguro en tu sistema operativo en caso de problemas?**		Un poco más de la mitad de los estudiantes no sabe cómo activar el modo seguro en su sistema operativo.
9. **¿Tienes registrado el número de serie y otras características de tu equipo en caso de pérdida o robo?**		La gran mayoría no tiene registrado o apuntado el número de serie de su equipo informático.
10. **¿Consideras que la información almacenada en tu equipo es importante y requiere protección adicional?**		La gran mayoría de estudiantes si considera que es importante la información almacenada en sus equipos informáticos.

3.6.1.2 Entrevista aplicada al Coordinador de la Carrera de TI/Software de la ULEAM Extensión El Carmen.

PREGUNTAS	RESPUESTAS	CONCLUSIÓN
1. **¿Conoces algún plan de contingencia para equipos informáticos?**	SI	No existe conocimiento de un Plan de Contingencia Institucional de la ULEAM Extensión El Carmen, más bien usa un Plan de Contingencia Personal como uso de medida en este caso.
2. **¿Has recibido alguna capacitación sobre cómo actuar en caso de un incidente de seguridad con tu equipo?**	NO	No ha recibido una capacitación interna Institucional, las capacitaciones buscadas y recibidas se han realizado fuera de la ULEAM Extensión El Carmen.
3. **¿Sabes cómo realizar una copia de seguridad de tus archivos importantes?**	SI	Como Profesional en el Área de TI/Software si conoce y realiza los procesos correspondientes para las copias de seguridad.
4. **¿Con qué frecuencia realizas copias de seguridad?**	SI	Acorde a las necesidades puntuales que se presentes es el periodo de tiempo que realiza la copia de Seguridad.
5. **¿Tienes identificado un lugar seguro para almacenar tus copias de seguridad?**	SI	Las copias de Seguridad usualmente las Realizas en la Nube, aunque en ocasiones existen excepciones de realizarlo en un Disco Externo.
6. **¿Has probado a restaurar tus archivos a partir de una copia de seguridad?**	SI	En ocasiones en que el equipo a presentado fallas técnicas y necesita algún archivo de suma importancia.

PREGUNTAS	RESPUESTAS	CONCLUSIÓN
7. **¿Utilizas contraseñas seguras y diferentes para cada una de tus cuentas?**	SI	En cuentas que no almacenan información delicada utiliza la misma contraseña, pero en las de mucha importancia si utiliza contraseñas de mucha seguridad.
8. **¿Has instalado algún software de seguridad en tu equipo (antivirus, antimalware)?**	SI	Cuenta con Antivirus con Licencia porque así es la manera más segura de mantener la Seguridad de la Información.
9. **¿Conoces los riesgos más comunes que pueden afectar a tus equipos informáticos (virus, phishing, etc.)?**	SI	Cuenta con conocimiento de riesgo comunes informáticos por lo que siempre es bastante precavido al abrir un correo o instalar una aplicación.
10. **¿Has reportado algún incidente de seguridad con tu equipo al personal encargado?**	NO	Cuando existe un incidente siendo profesional en el área es quien se encarga de dar una pronta solución.

3.6.2 Presentación y descripción de los resultados obtenidos

El diagnóstico obtenido mediante una encuesta aplicada a estudiantes de Tecnologías de la Información de la ULEAM Extensión El Carmen reveló hallazgos críticos sobre su preparación frente a contingencias tecnológicas.

Principales hallazgos cuantitativos:

La mayoría desconoce la existencia y utilidad de un plan de contingencia para sus equipos (P1) y carece de protocolos de actuación ante pérdida, daño o robo de dispositivos (P2). Si bien una parte importante identifica lugares seguros para almacenar archivos y realiza pruebas de restauración (P3-P4), estas prácticas son autodidactas y no sistematizadas. Aunque reconocen riesgos digitales comunes (P5) y utilizan antivirus actualizados (P6), la mayoría no

ha recibido capacitación formal para identificar o reportar amenazas (P7). Se observan también carencias técnicas básicas: desconocimiento para activar el modo seguro del sistema operativo (P8) y ausencia de registro de números de serie de equipos (P9). Cabe destacar que existe conciencia sobre el valor de sus datos (P10), aunque sin traducción en prácticas robustas.

Hallazgos cualitativos (entrevista a especialista en TI):

Se confirmó que no existe un plan de contingencia institucional que haya sido socializado entre la comunidad académica. Las medidas de protección que se aplican, como la realización de copias de seguridad periódicas y el uso de software licenciado, son iniciativas propias del profesional entrevistado, basadas en su experiencia y formación externa, y no responden a políticas oficiales de la institución.

Conclusión integrada:

Los resultados demuestran que las prácticas de protección son individuales, empíricas y desarticuladas de una estrategia institucional. Esta brecha operativa evidencia la necesidad urgente de diseñar e implementar un plan de contingencia formal para equipos informáticos, que sistematice la seguridad tecnológica y operativa de los estudiantes de TI.

3.6.3 Informe final del análisis de los datos

A partir de los datos recopilados mediante la encuesta aplicada a los estudiantes de la carrera de Tecnologías de la Información de la ULEAM Extensión El Carmen, y complementados con la entrevista a un profesional del área de TI de la institución, se ha logrado identificar una realidad que amerita atención institucional prioritaria.

Los resultados de la encuesta resultaron reveladores. En una de las preguntas iniciales, referente al conocimiento sobre la existencia de un plan de contingencia para equipos informáticos, más del 80 % de los encuestados indicó desconocer el concepto, evidenciando un nivel generalizado de desconocimiento sobre un tema fundamental. Esta situación se confirmó con otra pregunta clave, relacionada con la capacitación proporcionada por la institución sobre cómo actuar ante fallos técnicos o pérdida de información, en la que la mayoría de los participantes señaló no haber recibido formación alguna al respecto.

La falta de conocimiento identificada resulta preocupante tanto a nivel académico como operativo, ya que la continuidad de las clases y la protección de la información personal y académica dependen en gran medida de la existencia de un plan de contingencia correctamente estructurado y comunicado. Esta situación se confirmó durante la entrevista con el especialista en TI, quien indicó que no existían documentos formales ni protocolos institucionales establecidos para guiar a los estudiantes en caso de emergencias tecnológicas, lo que representa un riesgo significativo.

A pesar del vacío institucional identificado, los resultados de la encuesta evidenciaron que los estudiantes han comenzado a desarrollar cierta cultura de autogestión. Por ejemplo, más de la mitad indicó realizar copias de seguridad de sus archivos importantes. Sin embargo, al consultar si estas acciones se efectuaban siguiendo alguna política institucional, la mayoría respondió que se realizaban de manera independiente, sin lineamientos ni respaldo oficial, lo que refleja iniciativa personal aunque sin coordinación institucional.

Algo similar ocurre con las prácticas relacionadas a la seguridad informática. La pregunta "¿Utiliza usted antivirus actualizado en sus dispositivos?" mostró respuestas positivas en más del 60% de los casos, lo cual indica una conciencia individual sobre los riesgos tecnológicos. Sin embargo, en la entrevista, al consultarle al profesional "¿Se brinda capacitación sobre cómo identificar y reportar amenazas informáticas?", la respuesta fue negativa, dejando en evidencia una ausencia institucional de formación preventiva en seguridad digital.

Finalmente, en la encuesta, la pregunta "¿Considera que la información almacenada en sus equipos merece una protección especial?" obtuvo mayoritariamente respuestas afirmativas, lo que evidencia una valoración consciente de los recursos informáticos por parte de los estudiantes. No obstante, esta percepción no se refleja en acciones sistemáticas ni en una cultura de prevención respaldada por la institución.

En conclusión, la evidencia recogida a través de la encuesta y la entrevista demuestra la inexistencia de un Plan de Contingencia institucional para los equipos informáticos de los estudiantes, por lo que se hace urgente crearlo con toda su estructura, es decir que este proyecto es factible realizarlo e implementarlo y al final obtener conclusiones y recomendaciones del mismo, con él se marcaría una investigación que en un futuro se podría actualizar.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

El presente capítulo expone el desarrollo de una propuesta técnica y estratégica orientada al diseño de un plan de contingencia para los equipos informáticos de los estudiantes de la carrera de Tecnología de la Información de la ULEAM Extensión El Carmen. Esta iniciativa surge como respuesta a la necesidad detectada en el análisis diagnóstico, donde se evidenció la ausencia de lineamientos institucionales claros para enfrentar situaciones que comprometan la disponibilidad, integridad y continuidad operativa de los dispositivos personales utilizados con fines académicos.

El plan se fundamenta en la gestión proactiva de riesgos tecnológicos, respaldado metodológicamente por la norma internacional ISO/IEC 27001:2022, reconocida por su rigor en la seguridad de la información. Esta norma ha permitido estructurar un conjunto de medidas preventivas y correctivas para anticipar, mitigar y responder de manera efectiva ante incidentes como fallos técnicos, ciberataques o pérdida de datos.

Este capítulo detalla además los recursos humanos, tecnológicos y financieros que hicieron viable la propuesta, junto con las fases de desarrollo guiadas por el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar, Actuar). Este marco no solo asegura solidez técnica, sino que facilita una implementación progresiva en el entorno académico, fomentando así una cultura de seguridad digital entre los estudiantes.

4.2 Descripción de la propuesta

La propuesta presentada consiste en el diseño de un Plan de Contingencia para los equipos informáticos personales de los estudiantes de la carrera de Tecnología de la Información de la ULEAM Extensión El Carmen. Esta iniciativa surge a partir de la identificación de un problema: la mayoría de los estudiantes carece de una guía que indique cómo actuar ante fallas o compromisos de sus equipos, incluyendo laptops y ordenadores de sobremesa, los cuales se han convertido en herramientas esenciales para el desarrollo académico.

El objetivo principal es garantizar que los dispositivos se encuentren siempre disponibles, funcionen correctamente y puedan recuperarse rápidamente en caso de fallas. Para ello, se incorporan principios de gestión de riesgos, continuidad operativa y buenas prácticas en el manejo de la información, permitiendo prevenir incidentes y establecer procedimientos adecuados de respuesta ante eventualidades.

La metodología se basa en el enfoque de mejora continua propuesto por la norma ISO/IEC 27001:2022, adaptado al contexto de los estudiantes universitarios. Esto permite implementar medidas preventivas, como copias de seguridad automáticas, software de protección y talleres de ciberseguridad, junto con protocolos definidos para enfrentar situaciones críticas, tales como pérdida de datos, ataques de malware o fallas de hardware. El objetivo es no solo prevenir incidentes, sino también garantizar una respuesta efectiva ante cualquier eventualidad.

Finalmente, el plan contempla un conjunto de recomendaciones prácticas y sostenibles, pensadas desde una perspectiva educativa y realista, de modo que puedan ser adoptadas progresivamente por los estudiantes y eventualmente promovidas desde la institución como parte de una cultura de protección tecnológica.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recursos	Función	Actividad
1	Ing. Bladimir Mora	Coordinador Académico de la Carrera TI/Software	Participará de la Entrevista como Coordinador Académico.
1	Neicer Zambrano	Investigador	Consultará las bases teóricas que sustentan la propuesta.
60	Estudiantes de la Carrera TI/Software	Estudiantes de la Carrera Período 2024-2	Será la población participe de la encuesta para la obtención de datos.

Tabla 2 Recursos Humanos

4.3.2 Tecnológicos

Cantidad	Recursos	Actividad
1	Portátil Dell core i5 16 GB de RAM	Equipo informático utilizado para el desarrollo de la investigación.
1	Celular TECNO POVA 5	Móvil usado para la toma de evidencias durante la realización de la investigación.
1	Impresora EPSON L210	Equipo para las hojas de la encuesta, entrevista y tesis.
1	Programa Microsoft Excel	Usado para la tabulación de datos de las encuestas y entrevista.
1	Programa Microsoft Word	Usado para la redacción del Proyecto de Titulación.
10 meses	Conexión a Internet	Usado para investigar sobre el tema del proyecto de titulación

Tabla 3 Recursos Tecnológicos

4.3.3 Económicos

Cantidad	Descripción	Precio	Subtotal
1	Portátil Dell core i5 16 GB de RAM	765.00$	765.00$
1	Celular TECNO POVA 5	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 la elaboración del Plan de Contingencia, se adopto como marco metodológico el ciclo PHVA (Planificar-Hacer-Verificar-Actuar), alineado con los lineamientos de la norma internacional ISO/IEC 27001:2022, referente fundamental en la gestión de la seguridad de la información. En la fase inicial se realizó un diagnóstico exhaustivo de los equipos utilizados por los estudiantes de TI en la ULEAM Extensión El Carmen. Se aplicaron cuestionarios especializados para recopilar información sobre la antigüedad de los dispositivos, la realización de copias de seguridad, la frecuencia de fallas y las medidas de seguridad implementadas. Este análisis permitió identificar puntos críticos y establecer las bases para un plan de contingencia funcional y efectivo.

Con la información recopilada, se diseñó el plan incorporando acciones tanto preventivas como correctivas. La propuesta contempla talleres sobre buenas prácticas en seguridad digital, implementación de software antivirus actualizado, recomendaciones para el uso de reguladores de corriente y rutinas periódicas de respaldo en la nube. El objetivo es doble: prevenir la ocurrencia de incidentes y, en caso de que se presenten, garantizar una recuperación rápida y eficiente.

Para validar la efectividad del plan, se consultó a expertos en seguridad informática, gestión de riesgos y docencia universitaria. Su evaluación confirmó que el plan se encuentra alineado con la norma ISO/IEC 27001 y que resulta factible en el contexto de los estudiantes de extensión universitaria. Además, se proporcionaron recomendaciones orientadas a optimizar la gestión de incidentes y el seguimiento de las prácticas implementadas.

Finalmente, se procedió a la fase de ejecución. Con base en las recomendaciones recibidas, se incorporaron las mejoras necesarias y se elaboró un plan de implementación progresiva. Este incluye actividades de sensibilización, monitoreo continuo del estado de los equipos y la creación de protocolos para responder de manera rápida ante eventos adversos, tales como daños físicos, pérdida de datos o ciberataques. De esta manera, el plan no solo constituye un documento, sino una guía concreta para la acción efectiva.

Este enfoque integral busca consolidar una cultura de responsabilidad y resiliencia tecnológica, entendiendo que la seguridad comienza desde el cuidado individual, pero se fortalece con el apoyo institucional.

4.4.1 Fase 1 Planificar

4.4.1.1 Programa de Auditoría

Programa de auditoría informática de seguridad de la información plan de contingencia (ISO/IEC 27001:2022 y Ciclo PHVA)		
Objetivo • Evaluar la implementación y eficacia del Plan de Contingencia basado en el ciclo PHVA y alineado a ISO/IEC 27001:2022. • Identificar riesgos y vulnerabilidades en la protección de equipos informáticos y datos estudiantiles.		
Técnicas y procedimientos		
Actividad	**Ref. a Papel**	**Fecha**
1.1 Revisar ISO/IEC 27001:2022 (Anexo A)	4.4.1.2	28/04/2025
1.2 Auditoría inicial (diagnóstico de equipos y prácticas)	4.4.1.3	04/05/2025
1.3 Análisis de contexto (vulnerabilidades y controles existentes)	4.4.2	30/05/2025
2.1 Elaborar cuestionarios para validación de expertos	4.4.3	03/06/2025
2.2 Aplicar análisis de riesgos (simulacros de contingencia)	4.4.3.2	06/06/2025
2.3 Tabulación de resultados (matriz de riesgos)	4.4.3.3	10/06/2025
2.4 Evaluación de impacto (efectividad de capacitaciones y respaldos)	4.4.3.4	13/06/2025
2.5 Valoración final de riesgos (priorización)	4.4.3.5	16/06/2025
2.6 Elaborar informe de auditoría (hallazgos y recomendaciones)	5.1	17/06/2025

Tabla 5 Programa de Auditoría

4.4.1.2 Revisión ISO/IEC 27001

La norma ISO/IEC 27001:2022 constituye el estándar internacional más reconocido para la gestión de la seguridad de la información, proporcionando un marco sistemático para la protección de los activos digitales de una organización, incluidos los equipos informáticos utilizados por estudiantes en entornos académicos. Esta norma establece los requisitos para crear, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), aplicando el enfoque de mejora continua basado en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar).

La estructura de la norma se organiza en diez cláusulas principales que abarcan desde el contexto de la organización y el liderazgo, hasta la planificación, el soporte operativo, la evaluación y la mejora continua. Adicionalmente, incluye un Anexo A con 93 controles distribuidos en cuatro áreas clave: organizativa, de personal, tecnológica y física, que funcionan de manera integral para garantizar la confidencialidad, integridad y disponibilidad de la información. La revisión de la norma ISO/IEC 27001:2022 permitió adaptar sus lineamientos al contexto académico específico, guiando el diseño del plan de contingencia bajo estándares internacionales de gestión de riesgos y continuidad operacional (Calder, 2022).

4.4.1.3 Auditoría Inicial

La auditoría inicial constituye un proceso esencial para determinar el estado actual de los controles de seguridad implementados en los equipos informáticos de los estudiantes de la carrera de Tecnología de la Información en la ULEAM Extensión El Carmen. Esta fase se llevó a cabo mediante un análisis de brechas (GAP Analysis), con el propósito de identificar las discrepancias existentes entre las prácticas actuales y los requisitos establecidos por la norma ISO/IEC 27001:2022 (International Organization for Standardization, 2022).

El análisis de brechas consiste, básicamente, en comparar la situación actual con la situación deseada. Nos permite identificar claramente dónde estamos y hacia dónde debemos avanzar. Esta comparación es fundamental, porque ayuda a detectar las fallas en las medidas de seguridad existentes, o incluso la ausencia de algunas, y nos brinda una guía concreta para implementar mejoras de manera efectiva (Mora, 2022).

Se utilizará una escala de niveles de madurez con el objetivo de evaluar el grado de implementación de los controles de seguridad. Esta evaluación considera no solo la existencia de los controles, sino también su documentación, ejecución efectiva y revisión periódica para su mejora continua. Este enfoque permite identificar áreas de debilidad y fortalezas en la gestión de la seguridad de la información de manera práctica y sistemática.

Nivel de Madurez	**Descripción**
Nivel 0 - No existencia	No se ha implementado ningún control.
Nivel 1 - Ad hoc	Existe reconocimiento parcial de la necesidad del control, sin aplicación sistemática.
Nivel 2 - Ejecutado	Los controles están presentes, pero no documentados formalmente.
Nivel 3 - Definido	Los controles están implementados y documentados.
Nivel 4 - Manipulable y Medible	Se aplica un control interno sistemático para supervisar los controles.
Nivel 5 - Optimizado	Los controles están completamente integrados y continuamente optimizados.

Tabla 6 Nivel de Madurez

Nivel Medio Cumplimiento = Puntuación total de cada Control /Número 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 evaluación incluyó los siete capítulos principales de la norma ISO/IEC 27001:2022, entre los cuales se destacan: el entendimiento del contexto organizacional, el liderazgo, la planificación, el soporte, la operación, la evaluación del desempeño y la mejora continua del SGSI. Cada requisito fue operacionalizado mediante preguntas específicas que permitieron cuantificar su grado de cumplimiento (International Organization for Standardization, 2022).

Paralelamente, se diseñó un instrumento de evaluación pormenorizado que incluyó indicadores como:

- Identificación de objetivos del SGSI
- Delimitación del alcance del sistema
- Existencia de políticas de seguridad formalizadas
- Asignación explícita de roles y responsabilidades
- Mecanismos de supervisión y revisión interna

La aplicación de este instrumento permitió establecer una línea base del cumplimiento normativo en la institución y definir prioridades para la implementación del plan de contingencia.

Este diagnóstico preliminar no solo facilitó el diseño estratégico de medidas correctivas y preventivas, sino que también generó insumos técnicos valiosos para la posterior ejecución del análisis de riesgos (Mora, 2022).

N.º	**Capítulo**	**Descripción breve**
1	Alcance	Define los límites de aplicación del SGSI.
2	Referencias normativas	Muestra otras normas complementarias requeridas.

N.º	Capítulo	Descripción breve
3	Términos y definiciones	Proporciona el vocabulario técnico usado en la norma.
4	Contexto de la organización	Analiza factores internos y externos que afectan al SGSI.
5	Liderazgo	Establece el compromiso de la alta dirección con la seguridad de la información.
6	Planificación	Reconoce riesgos y oportunidades para definir objetivos del SGSI.
7	Apoyo (Soporte)	Incluye recursos, competencia, concienciación, comunicación y documentación.
8	Operación	Aborda la implementación y control de los procesos de seguridad.
9	Evaluación del desempeño	Define cómo medir, analizar y evaluar el SGSI.
10	Mejora	Establece acciones para mejorar continuamente el sistema.

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

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

Requisito ISO 27001	Preguntas para Evaluación	Cumplimiento
4. 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 la disponibilidad de los equipos?	

	3. ¿Se han identificado posibles amenazas o riesgos para los equipos informáticos?	
Requisito ISO 27001	**Preguntas para Evaluación**	**Cumplimiento**
5. Liderazgo	1. ¿La dirección ha establecido objetivos para el plan de contingencia alineados con las necesidades académicas?	
	2. ¿Se asignan recursos adecuados para mantener el plan de contingencia?	
	3. ¿La dirección revisa periódicamente la eficacia del plan?	

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

4.4.1.4 Ejecución

La entrevista al Ing. Jean Carlos Cedeño quien es el encargado de los laboratorios de la carrera TI en la ULEAM Extensión El Carmen, tuvo como fin principal obtener detalles sobre la seguridad actual, las normativas aplicables, los documentos esenciales y el cumplimiento de la norma ISO 27001:2022.

Ilustración 3 Fotografía de Entrevista

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

Los datos que se recopilaron se trabajaron en Microsoft Excel para ver qué tanto se cumplían los requisitos, usando una evaluación de brechas basada en un modelo de madurez por niveles, que va del 0 al 5.

El procedimiento se desarrolló de la siguiente manera:

- Primero, se calculó el promedio ponderado de cada requisito.

- Luego, se cuantificó la brecha (GAP) dividiendo ese promedio entre 5 y expresando el resultado como un porcentaje de déficit.

Los resultados mostraron que la ULEAM Extensión El Carmen cumple con la mayoría de los requisitos de la norma, logrando un nivel de madurez global que refleja, en buena medida, su alineación con el estándar internacional.

Requisitos	Pregunta	Cumplimiento	Observación	Promedio	Estado GAP	Brecha	Estado de Madurez
4. Contexto de la Organización	1. ¿Están identificados los objetivos del plan de contingencia para los equipos informáticos de los laboratorios?	4	Tema de mante	4,666667	93%	7%	CUMPLE
	2. ¿Se han identificado cuestiones internas y externas que podrían afectar la disponibilidad de los	5					
	3. ¿Se han identificado posibles amenazas o riesgos para los equipos	5					
5. Liderazgo	1. ¿La dirección ha establecido objetivos para el plan de contingencia alineados con las necesidades	5		3,666667	73%	27%	CUMPLE
	2. ¿Se asignan recursos adecuados para mantener el plan de contingencia?	2					
	3. ¿La dirección revisa periódicamente la eficacia del plan?	4					

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

Cumplimiento de controles

Este marco, definido por la norma ISO, ofrece un conjunto de controles y prácticas recomendadas para fortalecer la gestión de la seguridad de la información en organizaciones. Su estructura incluye múltiples cláusulas que cubren distintos ámbitos de protección de datos. A continuación, se detallan los requisitos de cumplimiento de controles alineados con la norma ISO 27002:

Numeral	Cláusulas	Descripción
A5	Políticas de Contingencia	Protocolos para responder a emergencias y minimizar impactos.
A6	Organización	Estructura de roles y responsabilidades en seguridad de la información.
A7	Recursos Humanos	Gestión de riesgos asociados a empleados (formación, contratación, desvinculación).
A8	Gestión de Activos	Inventario y protección de datos, software y hardware críticos.
A9	Control de Acceso	Restricciones para garantizar que solo personal autorizado acceda a recursos.
A10	Seguridad Física	Protección de instalaciones contra accesos no autorizados o daños.
A11	Operaciones	Procedimientos seguros en sistemas (monitoreo, malware, logs).
A12	Copias de Seguridad	Respaldos periódicos para recuperar datos ante pérdidas.
A13	Incidentes	Detección, reporte y manejo de brechas de seguridad.
A14	Continuidad	Planes para mantener operaciones durante crisis.

Numeral	Cláusulas	Descripción
A15	Cumplimiento	Alineación con leyes, regulaciones y estándares aplicables.

Tabla 11 Descripción de Cláusulas según la norma ISO

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

Numeral	Cláusula	Requisito	CUMPLE
A5	Políticas de Contingencia	1. ¿Existe una política documentada para el plan de contingencia de equipos?	
		2. ¿Se revisa periódicamente la política de contingencia?	
A6	Organización	1. ¿Hay responsables designados para cada laboratorio?	
		2. ¿Existen procedimientos para coordinar entre los 3 laboratorios?	
A7	Recursos Humanos	1. ¿El personal y estudiantes conocen sus roles en el plan?	
		2. ¿Se capacita a los usuarios sobre el uso correcto de los equipos?	
A8	Gestión de Activos	1. ¿Hay un inventario detallado de equipos por laboratorio?	
		2. ¿Se clasifican los equipos por criticidad académica?	

Tabla 12 Diseño de instrumentos de controles

4.4.1.5 Ejecución

Se llevó a cabo una entrevista con al Ing. Jean Carlos Cedeño responsable de los equipos informáticos de la carrera TI en la ULEAM Extensión El Carmen, para recabar datos específicos sobre la implementación de los controles de seguridad exigidos por la norma ISO 27001 y el estado de su cumplimiento.

Ilustración 4 Fotografía de Entrevista

Tabulación de datos del cumplimiento de controles de la Norma ISO 27001

El procesamiento de datos se ejecutó en Microsoft Excel para verificar el cumplimiento de los controles de la norma ISO 27001 en la ULEAM Extensión El Carmen. Se implementó un código de evaluación con valores: Sí (1), No (0) y No aplica (2) por cada control.

Metodología aplicada:

1. Conteo del total de controles evaluados y excluidos.

2. Cálculo de controles conformes (restando los excluidos al total).

3. Determinación del porcentaje de cumplimiento vs. no cumplimiento.

Numeral	Cláusula	Requisito	CUMPLE
A5	Políticas de Contingencia	1. ¿Existe una política documentada para el plan de contingencia de equipos?	1
		2. ¿Se revisa periódicamente la política de contingencia?	1
A6	Organización	1. ¿Hay responsables designados para cada laboratorio?	1
		2. ¿Existen procedimientos para coordinar entre los 3 laboratorios?	1
A7	Recursos Humanos	1. ¿El personal y estudiantes conocen sus roles en el plan?	1
		2. ¿Se capacita a los usuarios sobre el uso correcto de los equipos?	1
A8	Gestión de Activos	1. ¿Hay un inventario detallado de equipos por laboratorio?	1
		2. ¿Se clasifican los equipos por criticidad académica?	1
A9	Control de Acceso	1. ¿Existen controles para prevenir daños intencionales a equipos?	1
		2. ¿Se registra el uso de equipos por estudiantes?	0

Tabla 13 Datos de la institución

Nivel de Madurez

Tras evaluar los controles, se cuantificó el porcentaje de requisitos cumplidos y no cumplidos. Este análisis permitió:

1. Medir el nivel de conformidad con la norma ISO 27001 para cada requisito.

REQUISITO DE ISO 27001	CUMPLE LA NORMA	BRECHA
4. La Organización y su Contexto	93%	7%
5. Liderazgo	73%	27%
6. Planificación	73%	27%
7. Soporte	67%	33%
8. Operación	53%	47%
9. Evaluación y desempeño	60%	40%
10. Mejora	100%	0%
Promedio Requisitos	**74%**	**26%**

Tabla 14 Nivel de madurez de requisitos

2. Identificar la brecha de cumplimiento mediante los porcentajes obtenidos.

Cláusulas	CUMPLE	NO CUMPLE
A5. Políticas de Contingencia	100%	0%
A6. Organización	100%	0%
A7. Recursos Humanos	100%	0%
A8. Gestión de Activos	100%	0%
A9. Control de acceso	50%	50%

Cláusulas	CUMPLE	NO CUMPLE
A10. Seguridad Física	50%	50%
A11. Operaciones	100%	0%
A12. Copias de Seguridad	0%	100%
A13. Incidentes	50%	50%
A14. Continuidad	100%	0%
A15. Cumplimiento	100%	0%
PROMEDIO:	**77%**	**23%**

Tabla 15 Nivel de Madurez de Controles

Conclusión

En la fase inicial se realizó una auditoría basada en los lineamientos de la norma ISO 27001. Este proceso fue fundamental para evaluar el Plan de Contingencia implementado en la ULEAM Extensión El Carmen, donde se verificó el cumplimiento de los controles y requisitos de seguridad informática establecidos. Los resultados de la auditoría determinaron que la institución cuenta con un elevado nivel de madurez en su gestión de seguridad de la información.

4.4.2 Análisis del Contexto

Se evaluó el contexto interno y externo de la ULEAM Extensión El Carmen conforme a los lineamientos de la norma ISO/IEC 27001:2022, con el objetivo de identificar los factores que pueden influir en la seguridad de la información y en la continuidad operativa de los equipos informáticos utilizados por los estudiantes de la carrera de Tecnologías de la Información. Este análisis permitió reconocer riesgos, oportunidades y necesidades de protección frente a eventos disruptivos.

Contexto externo	
Aspecto	**Detalle**
Partes interesadas	- **Estudiantes de TI:** principales usuarios de los equipos informáticos. - **Docentes y personal técnico:** responsables del uso, monitoreo y mantenimiento. - **Proveedores externos:** encargados del suministro de repuestos, soporte técnico y licencias de software. - **Autoridades académicas:** responsables de la toma de decisiones institucionales.
Entorno político, legal y contractual	- **Político:** Autonomía académica universitaria. - **Legal:** Cumplimiento de la Ley Orgánica de Educación Superior (LOES), normativas internas ULEAM, y política de gestión tecnológica. - **Contractual:** Contratos con proveedores de tecnología, internet y mantenimiento técnico.
Entorno competitivo	Instituciones de educación superior cercanas como la Universidad Técnica Estatal de Quevedo (UTE) o extensiones del Instituto Superior Tecnológico Tsáchila que también ofrecen carreras tecnológicas.
Entorno económico	La mayoría de los estudiantes pertenecen a estratos socioeconómicos medio y medio-bajo, lo que limita en ocasiones el acceso a equipos personales. Por ello, los laboratorios institucionales cumplen una función esencial.
Entorno tecnológico	La institución cuenta con laboratorios equipados con computadoras de escritorio, red local, servicios de internet, cámaras de videovigilancia y software especializado. No obstante, el mantenimiento preventivo y correctivo enfrenta limitaciones presupuestarias que impactan en la sostenibilidad operativa.
Entorno social y ambiental	La comunidad estudiantil está integrada predominantemente por jóvenes provenientes de El Carmen y zonas aledañas. Se observan iniciativas incipientes para fomentar la conciencia ambiental, particularmente en reciclaje de componentes electrónicos, aunque sin un programa institucional formalizado.

Tabla 16 Contexto Externo ULEAM Extensión El Carmen

Contexto interno	
Aspecto	**Descripción**
Partes interesadas	- **Coordinación de carrera TI:** responsable de coordinar el uso de laboratorios. - **Docentes:** usuarios directos y responsables del uso académico de los equipos. - **Técnicos en sistemas:** encargados del mantenimiento de hardware y software. - **Estudiantes:** usuarios frecuentes que requieren continuidad operativa.
Misión y Visión institucional	- **Misión:** Formar profesionales integrales, competentes y comprometidos con el desarrollo local y nacional, mediante una educación de calidad. - **Visión:** Ser una institución líder en formación superior, innovación y responsabilidad social.
Organización, procesos y funciones	**- Procesos estratégicos:** Planificación académica, inversión en infraestructura tecnológica, asignación de recursos. **- Procesos operativos:** Uso diario de laboratorios, prácticas de programación, simulaciones de redes y ciberseguridad. **- Procesos de apoyo:** Soporte técnico, gestión de inventarios, seguridad física.
Recursos disponibles	- **Infraestructura:** Tres laboratorios equipados con computadoras de escritorio, switches, routers, cámaras de vigilancia y proyectores. - **Personal:** Técnico informático responsable, docente coordinador de TI, personal de limpieza y seguridad. - **Servicios:** Acceso a internet institucional, software educativo licenciado, sistema de autenticación unificado.
Tecnología vigente	- **Equipos:** computadoras de escritorio marca DELL (modelo 2024), routers TP-Link, switches Cisco. - **Software:** Windows 10 Pro, Linux Ubuntu, simuladores de redes (Packet Tracer), entornos de programación (Visual Studio, NetBeans), y plataformas de aprendizaje como Moodle. - **Sistemas complementarios:** antivirus ESET, cámaras de seguridad, sistema de respaldo de datos local.

Tabla 17 Contexto Interno ULEAM Extensión El Carmen

4.4.3 Justificación Técnica del Plan de Contingencia

La necesidad de implementar un Plan de Contingencia para los equipos informáticos de los estudiantes de TI de la ULEAM Extensión El Carmen surge como respuesta a la creciente dependencia de la tecnología en los procesos académicos y a los riesgos latentes que comprometen la disponibilidad, integridad y confidencialidad de los recursos tecnológicos.

Desde una perspectiva técnica, se justifica esta propuesta por varios factores concretos evidenciados durante la auditoría inicial y el análisis contextual realizado. Se identificaron deficiencias críticas en los procedimientos de respaldo y recuperación de información, junto con la ausencia de protocolos de respuesta ante fallos de hardware, incidentes de malware o interrupciones eléctricas. Estas vulnerabilidades comprometen directamente la continuidad académica, particularmente durante evaluaciones en línea, prácticas de laboratorio y defensas de trabajos finales.

Incidente ilustrativo

Durante el segundo semestre de 2024, una subida de tensión en el Laboratorio de Informática 2 afectó gravemente tres estaciones de trabajo, inutilizándolas por más de una semana. Este evento evidenció la falta de medidas preventivas básicas —como reguladores de voltaje o sistemas UPS— y la inexistencia de procedimientos documentados para responder ante emergencias técnicas.

Alineación con marco normativo

Con base en los principios de la norma ISO/IEC 27001:2022 (específicamente el control A.5.29 sobre continuidad operativa), el plan propuesto establece protocolos estandarizados, reduce tiempos de respuesta y garantiza la resiliencia de los procesos académicos frente a fallas técnicas previsibles.

Estrategias de mitigación

El análisis de riesgos reveló alta exposición a amenazas físicas (humedad, polvo, accesos no controlados), reforzando la necesidad de implementar controles ambientales, técnicos y administrativos. La propuesta incorpora:

- Creación de imágenes de respaldo (*ghosting*)
- Inventario técnico actualizado
- Pruebas periódicas de restauración de sistemas
- Esquema definido de roles y responsabilidades durante emergencias

Por lo tanto, este plan no solo representa una herramienta de gestión, sino un componente técnico esencial para asegurar la resiliencia operativa de los laboratorios de informática de la extensión universitaria, salvaguardando la infraestructura tecnológica y, por ende, la calidad del proceso educativo.

4.4.4 Elaboración de Cuestionarios para Analizar Riesgos

Se diseñó un cuestionario dividido en cinco bloques temáticos con el objetivo de identificar los principales riesgos que afectan a los equipos informáticos utilizados por los estudiantes de la carrera de Tecnologías de la Información en la ULEAM Extensión El Carmen. El instrumento de evaluación consta de 75 ítems distribuidos en cinco dimensiones críticas:

- **15 ítems** sobre daños físicos a equipos
- **15 ítems** sobre riesgo de incendios
- **15 ítems** sobre vulnerabilidad ante inundaciones
- **15 ítems** sobre prevención y respuesta ante robos
- **15 ítems** relacionados con infecciones por malware o software malicioso

Cada dimensión evalúa aspectos específicos de vulnerabilidad, medidas preventivas y protocolos de respuesta ante incidentes que podrían comprometer la operatividad tecnológica de los laboratorios.

Para la construcción de los cuestionarios, se diseñaron dos matrices complementarias: una matriz general enfocada en la evaluación global de los riesgos que afectan a los equipos informáticos y una matriz específica orientada a analizar de manera individual cada laboratorio de la institución donde se encuentran instalados dichos equipos.

4.4.4.1 Ejecución de los cuestionarios para analizar riesgos

Se realizó una evaluación de los equipos informáticos ubicados en los tres laboratorios de la ULEAM Extensión El Carmen, considerando los riesgos asociados al robo, daños físicos, incendios, inundaciones y malware. El propósito fue determinar el nivel de seguridad y el grado de exposición al riesgo en cada uno de estos espacios tecnológicos.

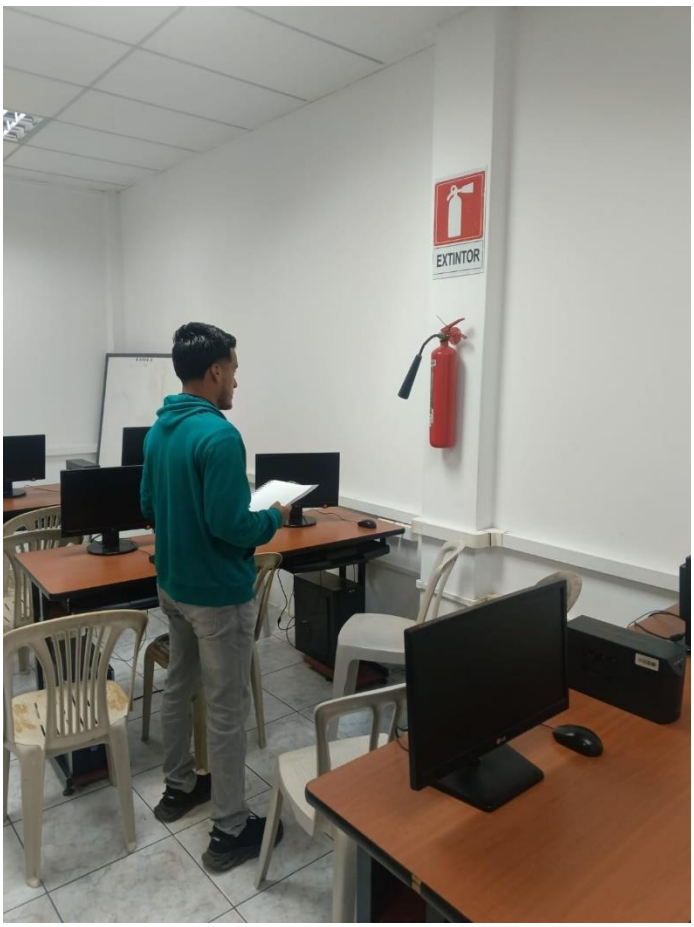
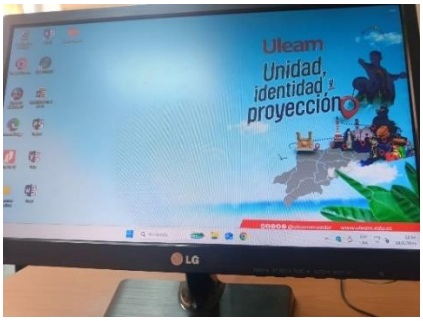
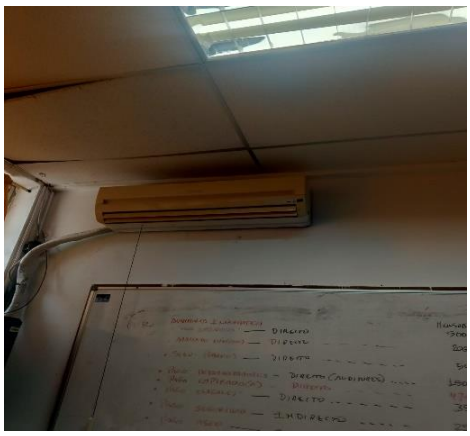


Ilustración 5 Ejecución de Cuestionarios para Analizar Riesgos

4.4.4.2 Aplicación de Análisis de Riesgo

Se efectuó un recorrido por la ULEAM Extensión El Carmen, durante el cual se llevó a cabo una entrevista con el responsable de los equipos informáticos de cada laboratorio, con el objetivo de analizar los controles que se encuentran en funcionamiento.

Fotografía	Descripción
	Extintores revisados y en funcionamiento.
	Las Computadoras no cuentan con claves de acceso.
	Aires acondicionados para garantizar la adaptación del clima para mejor funcionamiento de los equipos.
	Reguladores de Energía en cada uno de los equipos informáticos para evitar daños que puedan causar cortes eléctricos.

Fotografía	Descripción
	Cableado perfectamente estructurado y ordenado para un correcto funcionamiento.
	Breque regulador de energía, para así evitar algún tipo de incendio que pueda llegar a provocar un cortocircuito.
	Luces de emergencia que se activan en el momento que ocurre un corte eléctrico.
	Cámara de seguridad para el monitorio de cómo es el uso de cada uno de los equipos informáticos.

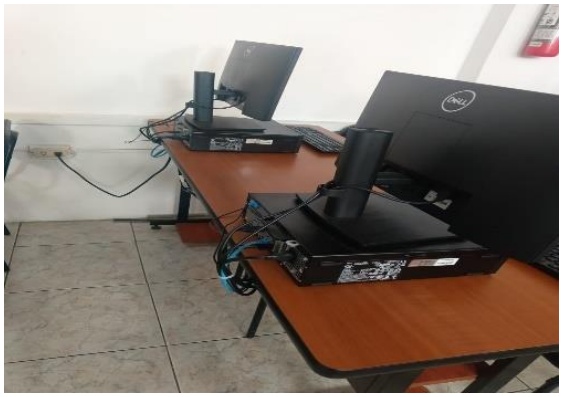
Fotografía	Descripción
	En caso de presentarse un Incendio el detector de humo emitirá la alarma.
	El Orden de todos los equipos dentro de los laboratorios.

Tabla 18 Aplicación de Análisis de Riesgo

4.4.4.3 Evaluación de Recursos Disponibles para Contingencia

La elaboración de un plan de contingencia efectivo requiere partir del reconocimiento de los recursos con los que actualmente cuenta la institución para enfrentar posibles incidentes. Esta evaluación técnica permite dimensionar las capacidades reales de respuesta, identificar brechas y priorizar adecuadamente las acciones correctivas o preventivas dentro del plan.

- Durante las visitas técnicas a los tres laboratorios de informática de la ULEAM Extensión El Carmen, se levantó un inventario detallado de activos físicos, lógicos y humanos disponibles para enfrentar situaciones críticas como fallas de hardware, cortes eléctricos, ataques de malware o desastres naturales. Entre los recursos identificados se incluyen:
- Actualmente, solo hay tres laptops institucionales asignadas a la coordinación académica, por lo que no hay disponibilidad inmediata para emergencias en los laboratorios.

- En cuanto a los sistemas de respaldo de información, no existen copias de seguridad automatizadas. Depender únicamente del almacenamiento local en cada equipo se vuelve un problema, más aún porque no hay políticas ni frecuencias de backup definidas.
- El soporte técnico también es limitado: solo hay un técnico para toda la extensión universitaria, lo que dificulta atender incidencias que ocurran al mismo tiempo.
- Sobre los recursos energéticos, únicamente un laboratorio cuenta con UPS funcional y sin registros de pruebas de autonomía mientras que los demás operan sin ninguna estabilización eléctrica.
- Finalmente, no existen manuales ni protocolos documentados para contingencias; cuando surge algún problema, el personal docente suele resolverlo de manera empírica o improvisada.

En conjunto, esta situación evidencia vulnerabilidades importantes en los mecanismos actuales de recuperación y mitigación, dejando a la infraestructura tecnológica expuesta a riesgos operativos significativos. Por eso, el plan de contingencia deberá priorizar no solo el diseño de procedimientos claros, sino también la adquisición, el mantenimiento y el fortalecimiento de recursos, con el fin de garantizar que el sistema se mantenga sostenible ante cualquier interrupción crítica.

4.4.4.4 Tabulación de Análisis de Riesgos

Se empleó Microsoft Excel para organizar y tabular los datos obtenidos a partir de los instrumentos aplicados en los 3 laboratorios de la ULEAM Extensión El Carmen. Asimismo, las respuestas de los cuestionarios fueron clasificadas utilizando una escala de valores: 0 para indicar peligro, 1 para seguridad y 2 para no aplica.

Cuestionario para Alizar Riesgos	**Laboratorio 1**	**Laboratorio 2**	**Laboratorio 3**
Daños de Equipos			
1. ¿Se utilizan protectores de voltaje en las estaciones de trabajo?	1	1	1
2. ¿Se realiza mantenimiento preventivo a los equipos con frecuencia?	0	0	0
3. ¿Los equipos están expuestos a calor, polvo o humedad en los laboratorios?	1	1	1
4. ¿Se manipulan adecuadamente los cables de alimentación y datos?	1	1	1
5. ¿Se reportan fallos técnicos apenas ocurren?	1	1	1
6. ¿Los estudiantes reciben instrucciones claras sobre el uso correcto del equipo?	0	0	0

Tabla 19 Tabulación de Análisis de Riesgos

Escala de Probabilidad de Ocurrencia

Para estimar la probabilidad de aparición de los riesgos identificados en el análisis, se aplicó una tabla con cinco niveles, basada en rangos porcentuales. Esta escala permite asignar un valor numérico según la frecuencia estimada de ocurrencia, distribuyéndose de la siguiente manera:

Escala para determinar el valor de Ocurrencia		
Nivel de Ocurrencia (probabilidad):		
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 Valor de Ocurrencia

Nivel de Gravedad (Impacto)

Para valorar la magnitud del impacto ante la ocurrencia de un riesgo, se aplicó una escala de cinco niveles. Esta tabla permite clasificar el grado de afectación en función de las consecuencias que podrían presentarse, como se detalla a continuación:

Escala de impacto		Consideraciones por nivel:
Nivel 1	Muy bajo	Cierre temporal de instalaciones o afectación menor que no impide la continuidad de actividades. La interrupción no supera las 8 horas y los daños a los activos son limitados, sin repercusión significativa en la operatividad general.
Nivel 2	Bajo	Interrupciones o daños que requieren atención específica pero no comprometen la operación general de la institución. El impacto se circunscribe a áreas o servicios no críticos.

Escala de impacto		Consideraciones por nivel:
Nivel 3	Medio	Afectaciones que demandan intervenciones técnicas importantes para restablecer la normalidad operativa. Inciden en servicios clave pero sin colapsar la infraestructura tecnológica principal.
Nivel 4	Alto	Daños graves con interrupciones relevantes, que exigen respuestas inmediatas y podrían comprometer la continuidad operativa.
Nivel 5	Muy alto	Daños irreversibles en las instalaciones, que las vuelven inhabitables. Pérdida o destrucción total de datos y activos, sin posibilidad de recuperación.

Tabla 21 Escala de Impacto

Clasificación del Nivel de Riesgo

El riesgo se agrupa en distintas categorías según el grado de impacto que pueda generar, asignándole un color representativo y estableciendo las medidas correspondientes para su tratamiento, como se detalla a continuación en ambas tablas:

Riesgo	Color	Rango	Medidas
Muy Grave		De 15 a 25	Implica un nivel de riesgo crítico que exige atención inmediata previo a la ejecución de cualquier actividad del proyecto. Requiere la implementación de medidas preventivas urgentes y control riguroso mediante protocolos estandarizados.
Importante		De 9 a 12	Necesita acciones preventivas obligatorias y supervisión constante de las variables asociadas durante todo el ciclo de vida del proyecto.
Apreciable		De 3 a 8	Puede mitigarse mediante medidas preventivas, siempre que su aplicación sea técnicamente viable y económicamente sostenible.

Riesgo	Color	Rango	Medidas
Marginal		De 1 a 2	No demanda medidas inmediatas, pero debe ser objeto de observación continua para evitar su evolución a niveles superiores.

Tabla 22 Escala Nivel de Riesgo

Nivel de Riesgo	Descripción	Medidas de Tratamiento
BAJO	Riesgos con una probabilidad de ocurrencia muy baja o baja y/o un impacto muy bajo. Su materialización no genera interrupciones significativas ni pérdidas mayores.	Pueden ser aceptados o gestionados mediante controles rutinarios. Se requiere monitoreo periódico para asegurar que no escalen. No se necesitan acciones inmediatas o recursos adicionales.
MODERADO	Riesgos con una probabilidad de ocurrencia moderada y/o un impacto bajo a medio. Su materialización puede causar interrupciones menores o pérdidas recuperables, pero no compromete la continuidad operativa crítica.	Elaboración de planes de acción documentados con controles preventivos y correctivos Gestión a cargo de equipos operativos con supervisión directa de la coordinación Monitoreo continuo y reporting periódico del estado del riesgo
ALTO	Riesgos con probabilidad de ocurrencia alta o muy alta y/o impacto medio a alto. Su materialización puede generar interrupciones operativas	Exigen atención prioritaria y la asignación de recursos dedicados. Se deben desarrollar planes de contingencia detallados y realizar simulacros. La gestión requiere el

	significativas, pérdidas cuantificables o afectar la reputación institucional. Exigen atención prioritaria y asignación de recursos específicos.	involucramiento de la alta dirección y revisiones frecuentes.
Nivel de Riesgo	**Descripción**	**Medidas de Tratamiento**
CRÍTICO	Riesgos con una probabilidad de ocurrencia alta o muy alta y/o un impacto muy alto. Su materialización puede causar daños irreversibles, interrupciones prolongadas o la paralización total de las actividades, con graves consecuencias financieras, operativas o reputacionales.	Demandan una respuesta inmediata y la implementación de planes de emergencia. La máxima dirección debe estar directamente involucrada en la toma de decisiones y en la asignación de todos los recursos necesarios para mitigar el impacto y asegurar la recuperación.

Tabla 23 Clasificación del Nivel de Riesgo

4.4.4.5 Evaluación del impacto en el análisis de riesgos

Para determinar el impacto asociado a distintos tipos de riesgo como daño a los equipos, incendio, inundaciones, robo y malware, se utilizó Microsoft Excel como herramienta de cálculo. El análisis consideró tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. Estos aspectos fueron evaluados con base en los datos recogidos en los 3 laboratorios, permitiendo así asignar un valor de impacto a cada tipo de riesgo identificado.

Resultados del impacto según categoría de riesgo:				
Riesgo	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Impacto Total**
Daños de Equipos	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 Análisis de Riesgos

4.4.4.6 Evaluación de los riesgos

El proceso de valoración comenzó con la identificación y conteo de los controles marcados como "No Aplica" (valor 2). Posteriormente, se determinó el número total de controles efectivamente evaluados, restando aquellos que no aplicaban del total general.

Se procedió a contabilizar tanto los controles que representan condiciones de seguridad como aquellos considerados riesgos. Con estos datos, se calculó el porcentaje de seguridad dividiendo el número de controles seguros entre el total de controles evaluados. De igual manera, se obtuvo el porcentaje de riesgo mediante la división del total de controles de riesgo sobre el mismo total evaluado.

Finalmente, se estableció un promedio general que incluyó los totales de seguridad y riesgo, así como sus respectivos porcentajes.

Pregunta Daños de Equipos	Laboratorio 1	Laboratorio 2	Laboratorio 3
12. ¿El software instalado presenta errores por mal uso o instalación indebida?	1	1	1
13. ¿Se realizan respaldos antes de manipular el sistema operativo?	0	0	0
14. ¿El ambiente donde se encuentran los equipos es seguro y controlado?	1	1	1
15. ¿Los equipos son utilizados únicamente para fines académicos?	1	1	1
Total Controles No Aplica:	0	0	0
Total Controles Evaluados:	15	15	15
Total Seguridad	10	10	10
Total Riesgo:	5	5	5
Porcentaje Seguridad	67%	67%	67%
Porcentaje Riesgo:	33%	33%	33%

Tabla 25 Evaluación de Riesgos

4.4.4.7 Matriz de riesgos

Se elaboró una matriz de riesgos en Microsoft Excel para los eventos de daño a equipos, incendio, inundaciones, robo y malware. En primer lugar, se evaluó la probabilidad de ocurrencia de cada riesgo tomando como referencia el porcentaje de incidencia. A continuación, se estimó su impacto considerando los principios de confidencialidad, integridad y disponibilidad de la información.

El valor del riesgo fue calculado multiplicando la probabilidad de aparición por el nivel de impacto determinado. Con base en ese resultado, se clasificó cada riesgo dentro de un nivel específico, al que se le asignó un color representativo según su gravedad.

Riesgo	Probabilidad	Impacto	Valor del Riesgo	Nivel
Daños de Equipos	3	3	9	Importante
Incendio	2	3	6	Apreciable
Inundaciones	3	1	3	Apreciable
Robo	4	4	15	Importante
Malware	2	4	9	Apreciable

Tabla 26 Matriz de Riesgo

CAPÍTULO V

5 EVALUACIÓN DE RESULTADOS

5.1 Informe de Auditoría

Dirigido a:

Ing. Jean Carlos, Responsable de Infraestructura Tecnológica, ULEAM Extensión El Carmen.

Tipo de auditoría:

Auditoría de seguridad informática física y lógica aplicada a los laboratorios de computación de la carrera de Tecnologías de la Información.

Motivo:

Cumplir con los requerimientos del trabajo de titulación correspondiente al diseño e implementación de un Plan de Contingencia para Equipos Informáticos, aplicando principios de la norma ISO/IEC 27001:2022.

Objetivos:

- Evaluar el nivel de madurez en la gestión de seguridad de los equipos informáticos de los laboratorios de la ULEAM Extensión El Carmen.

- Identificar los principales riesgos y determinar el grado de exposición de los activos frente a eventos que comprometan su disponibilidad, integridad y confidencialidad.

Alcance:

- Revisión de los requisitos aplicables de la norma ISO/IEC 27001:2022.

- Ejecución de una auditoría inicial en los tres laboratorios de informática.

- Aplicación de instrumentos de recolección de información (entrevista, cuestionario y observación directa).

- Análisis de contexto y categorización de amenazas.
- Evaluación del nivel de madurez por requisitos y controles.
- Elaboración de matriz de riesgos.
- Valoración del impacto y probabilidad.
- Propuesta de medidas correctivas y de mejora.

Personal involucrado:

- Coordinador académico
- Responsable de laboratorios
- Estudiantes asistentes técnicos

5.2 Presentación y monitoreo de resultados

5.2.1 Requisito ISO/IEC 27001:2022

Requisito	Cumplimiento (%)	Nivel de madurez
4. Contexto de la organización	93.3%	Cumple
5. Liderazgo	73.3%	Cumple
6. Planificación	78.3%	Cumple
7. Soporte	70.0%	Cumple
8. Operación	60.0%	Parcialmente
9. Evaluación del desempeño	66.7%	Parcialmente
10. Mejora	60.0%	Parcialmente

Tabla 27 Requisito ISO/IEC 27001:2022

Promedio general: 71.6% – Nivel de cumplimiento: Medio.

5.2.2 Interpretación y causas por requisito

- **Contexto de la organización (93.3% – Cumple):** Se ha identificado adecuadamente el entorno interno y externo que influye en la seguridad.
  Causas del éxito: Análisis contextual bien definido y documentado.

- **Liderazgo (73.3% – Cumple):** Existe compromiso directivo en el manejo de la seguridad.
  Causas de brecha: La política de seguridad no ha sido difundida formalmente a todos los actores.

- **Planificación (78.3% – Cumple):** Se han definido objetivos, pero no están vinculados a indicadores.
  Causas de brecha: Falta establecer criterios de riesgo aceptable y una declaración de aplicabilidad clara.

- **Soporte (70.0% – Cumple):** Se reconocen recursos, pero no hay control sobre competencias.
  Causas de brecha: Ausencia de evidencia sobre la formación técnica y concienciación del personal.

- **Operación (60.0% – Parcial):** Existen procesos, pero son inconsistentes.
  Causas: No hay seguimiento continuo ni documentación actualizada sobre los procesos críticos.

- **Evaluación del desempeño (66.7% – Parcial):** No se realizan auditorías internas planificadas.
  Causas: Ausencia de un cronograma y responsables definidos para seguimiento.

- **Mejora (60.0% – Parcial):** Hay iniciativas, pero no están sistematizadas.
  Causas: No existen procesos formales de mejora continua ni gestión de no conformidades.

5.3 Evaluación de Controles

5.3.1 Principales controles evaluados

Control	Cumplimiento (%)	Nivel de madurez
A.5 Políticas de Contingencia	50%	Bajo
A.6 Organización de la Seguridad	50%	Bajo
A.7 Seguridad de Recursos Humanos	50%	Bajo
A.8 Gestión de Activos	50%	Bajo
A.9 Control de Accesos	66%	Medio
A.10 Criptografía	33%	Muy bajo
A.11 Seguridad Física y del Entorno	66%	Medio
A.12 Seguridad en las Operaciones	66%	Medio
A.13 Seguridad en las Comunicaciones	83%	Alto
A.14 Adquisición y desarrollo de sistemas	33%	Muy bajo
A.15 Relación con Proveedores	33%	Muy bajo
A.16 Gestión de Incidentes	50%	Bajo
A.17 Continuidad del Negocio	33%	Muy bajo
A.18 Cumplimiento	33%	Muy bajo

Tabla 28 Principales Controles Evaluados

Promedio general de cumplimiento: 51.7% – Nivel de madurez: Bajo-Medio.

5.4 Análisis de Riesgo

Riesgo	Nivel de seguridad	Nivel de riesgo	Causas identificadas
Daño de equipos	Medio	Importante	Sin mantenimiento programado, exposición a polvo.
Incendio	Bajo	Muy grave	No hay detectores, ni extintores accesibles.
Inundaciones	Bajo	Muy grave	No hay sistemas de drenaje ni protección física.
Robo	Medio	Importante	Accesos sin control, ausencia de cámaras.
Malware	Bajo	Muy grave	No se usan antivirus, navegación libre, dispositivos externos sin restricción.

Tabla 29 Análisis de Riesgo

Evaluación general del riesgo: 44% – Muy grave.

5.5 Conclusiones y Recomendaciones

La auditoría evidencia un nivel medio de madurez en requisitos y bajo en controles, lo cual es un riesgo para la continuidad académica y operativa de los laboratorios.

Los riesgos más críticos identificados son incendios, malware e inundaciones, que requieren acciones inmediatas.

Se recomienda:

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) formal.

Crear y socializar políticas de seguridad institucionales.

Establecer medidas físicas (extintores, UPS, alarmas) y lógicas (antivirus, backups, control de accesos).

Realizar capacitaciones periódicas para estudiantes y docentes.

Definir e implementar un plan de mejora continua y un cronograma de auditorías internas.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Gracias al compromiso institucional de la ULEAM Extensión El Carmen, especialmente al apoyo del responsable de los laboratorios de informática, fue posible llevar a cabo una auditoría integral que permitió diagnosticar las debilidades en materia de seguridad de los equipos utilizados por los estudiantes de la carrera de Tecnologías de la Información.

- Se construyó una base teórica sólida, fundamentando las variables de estudio: Plan de Contingencia como variable dependiente y los equipos informáticos del área académica como variable independiente. Esta revisión se sustentó en bibliografía reciente y relevante, lo que facilitó el desarrollo del marco teórico con una estructura clara, contenido pertinente y redacción académica precisa.

- La recopilación de información mediante entrevistas al personal responsable y la aplicación de instrumentos de evaluación permitió identificar con claridad el estado actual de los laboratorios en cuanto a su exposición frente a riesgos como incendios, malware, daños físicos, inundaciones y robos. El análisis de los datos permitió comprender de manera objetiva los factores críticos que afectan la disponibilidad, integridad y confidencialidad de los activos tecnológicos.

- Al aplicar la norma ISO/IEC 27001:2022 como marco metodológico, se evaluó qué tan bien se cumplen los requisitos y controles clave del SGSI. La evaluación mostró que, aunque hay avances en la organización de la seguridad y en algunas prácticas operativas, todavía existen deficiencias en áreas sensibles, como la planificación ante emergencias, la capacitación del personal y la gestión de incidentes. Por este motivo se pudo realizar un plan de contingencia el cuál se lo puede apreciar en el Anexo 1.

- Finalmente, se elaboró un informe de auditoría que expuso los hallazgos más relevantes y se diseñó una propuesta de plan de contingencia orientada a mejorar la seguridad de los equipos informáticos. Este trabajo aporta herramientas útiles para fortalecer la infraestructura tecnológica y fomentar una cultura preventiva entre los usuarios de los laboratorios.

6.2 Recomendaciones

Se recomienda que la ULEAM Extensión El Carmen adopte formalmente el Plan de Contingencia propuesto**,** el cual permitirá reducir la exposición a eventos como incendios, malware y fallas eléctricas, garantizando así la continuidad operativa de los laboratorios.

Es fundamental que se implemente un proceso de capacitación permanente dirigido a estudiantes, técnicos y docentes sobre buenas prácticas en seguridad informática. Esta acción no solo previene errores humanos, sino que promueve la responsabilidad compartida en el uso de los recursos tecnológicos.

Se recomienda la creación e institucionalización de políticas internas de seguridad de la información que definan explícitamente roles, normas de uso, controles de acceso y protocolos de respuesta ante incidentes. La existencia de este marco normativo consolida la gobernanza tecnológica institucional.

Adicionalmente, la carrera de Tecnologías de la Información podría integrar estas auditorías como parte de sus prácticas académicas, permitiendo que los estudiantes participen en proyectos reales que fortalezcan su formación profesional mientras contribuyen con soluciones concretas a su institución.

Finalmente, es recomendable que se actualicen periódicamente los inventarios, se instalen mecanismos básicos de protección física y lógica, y se adopte un enfoque de mejora continua para que el sistema de seguridad informática evolucione junto a las necesidades educativas.

BIBLIOGRAFÍA

7 Bibliografía

Angulo Murillo , N., Cárdenas Encalada , J., y Bolaños Burgos , F. (2020). LA CONTINUIDAD DE NEGOCIO EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL ECUADOR. CASO DE ESTUDIO. *Revista Científica Multidisciplinaria Arbitrada Yachasun, 4*, 88–123. https://doi.org/10.46296/yc.v4i7.0036

Angulo, N., Cárdenas, J., y Bolaños, F. (2020). *LA CONTINUIDAD DE NEGOCIO EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL ECUADOR. CASO DE ESTUDIO.* Guayaquil: REVISTA CIENTÍFICA MULTIDISCIPLINARIA ARBITRADA YACHASUN. https://www.researchgate.net/publication/343477058_LA_CONTINUIDAD_DE_NEGOCIO_EN_LAS_INSTITUCIONES_DE_EDUCACION_SUPERIOR_DEL_ECUADOR_CASO_DE_ESTUDIO

Arco, J. B. (2024). *Sistemas Informáticos.* Síntesis. https://www.casadellibro.com/ebook-sistemas-informaticos-ebook/9788413575032/13521755?msockid=3805ab0c60f569d40b3cbe4f619a686f

Atehortúa, F., Bustamante, R., y Valencia, J. (2008). *Sistema de gestión integral: una sola gestión, un solo equipo.* Medellín, Colombia: Universidad de Antioquia. https://books.google.com.ec/books/about/Sistema_de_gesti%C3%B3n_integral_Una_sola_ge.html?id=15nVyh1Fn6MC&redir_esc=y

Barbosa, G. M., Estupiñan, B. L., y Estupiñan, B. J. (2023). *El uso de la nube distribuida para el control de la información académica en la educación superior.* (Vol. 3). Grupo Editorial SAPIENZA. https://doi.org/https://doi.org/10.56183/iberoeds.v3i1.603

Calder, A. (2022). *Nine Steps to Success: An ISO 27001 Implementation Overview* (4 ed.). Cambridgeshire: IT Governance Publishing.

Collahuazo, J. D. (2024). Integración de las Tecnologías de la Información y las Comunicaciones en el Sistema de Educación Pública Ecuatoriano: Una Revisión Sistemática. Polo del Conocimiento, 9(10). *Integration of Information and Communications Technologies in the Ecuadorian Public Education System: A Systematic Review.* Universidad Estatal de Milagro UNEMI, Milagro. https://polodelconocimiento.com/ojs/index.php/es/article/view/8203/html

Correa, W. D. (2024). Diseño e implementación de una Red BGP para un plan de contingencia en el sistema decomunicación de la empresa Grupo Faysal S.A.C, 2023 [Tesis de Maestría, Universidad Tecnológica de Perú]. *Diseño e implementación de una Red BGP para un plan de contingencia en el sistema de comunicación de la empresa Grupo Faysal S.A.C, 2023.* Repositorio Digital, Lima. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/9229/W.Correa_Tesis_Titulo_Profesional_2024.pdf?sequence=1&isAllowed=y

Felices, M. d., y López, M. J. (2023). *Formación de la identidad docente durante la pandemia. Evaluación de una experiencia* (Vol. 27). Miscelánea. https://doi.org/https://doi.org/10.30827/profesorado.v27i3.21270

Gambin, B., y Macías, L. (2017). *MARCO DE TRABAJO PARA LA GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS ESTUDIO UNIVERSIDAD DEL MAGDALENA.* Barranquilla: FUNDACIÓN UNIVERSIDAD DEL NORTE DIVISIÓN DE INGENIERÍAS MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA . https://manglar.uninorte.edu.co/bitstream/handle/10584/8539/134004.pdf?isAllowed=y&sequence=1&utm_source=chatgpt.com

Gómez, G. (2021). *Métodos y técnicas de investigación utilizados en los estudios sobre comunicación en España* (12 ed., Vol. 1). Revista Mediterránea De Comunicación. https://doi.org/https://doi.org/10.14198/MEDCOM000018

Gonzabay, R. E. (2021). Desarrollo de un plan de contingencias informático para el centro de datos y comunicaciones de la empresa AGUAPEN-EP mediante el uso de normas internacionales[Exámen Complesivo, UNIVERSIDAD ESTATAL]. *DESARROLLO DE UN PLAN DE CONTINGENCIAS INFORMÁTICO PARA EL CENTRO DE*

DATOS Y COMUNICACIONES DE LA EMPRESA AGUAPEN-EP MEDIANTE EL USO DE NORMAS INTERNACIONALES. Repositorio Digital, La Libertad. https://repositorio.upse.edu.ec/bitstream/46000/7724/1/UPSE-TTI-2022-0023.pdf

González, H., y López, J. (2023). Plan de Emergencia y Contigencia. *PLAN DE EMERGENCIA Y CONTINGENCIA.* Uiversidad Central del Ecuador, Quito. https://repositorio.uce.edu.ec/archivos/dsaltamirano/facebook/5.FIQ_PLAN_DE_EMERGENCIA_Y_CONTINGENCIA_2023_SCPSSOA-1.pdf

González, X. (2023). *Interoperabilidad digital en software educativo para la didáctica.* AmeliCA Foro Ciber. https://www.forociber.cl/foro/site/docs/20240322/20240322150520/edicion_construyendo_la_ciberseguridad_en_chile_v2.pdf?utm_source=chatgpt.com

Grimalt, C., Marqués, L., Palau, R., Holgado, J., Valls, C., y Hernández, C. (2022). *Tecnología educativa para los retos de la era digital.* OCTAEDRO. https://www.redage.org/publicaciones/tecnologia-educativa-para-los-retos-de-la-era-digital

Guato, H. G. (2023). Plan de contingencia ante amenazas naturales y antrópicas de los talleres tecnológicos de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato[Tesis de Maestría, UNIVERSIDAD TÉCNICA DE AMBATO]. *PLAN DE CONTINGENCIA ANTE AMENAZAS NATURALES Y ANTRÓPICAS DE LOS TALLERES TECNOLÓGICOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO.* Repositorio Digital, Ambato. https://repositorio.uta.edu.ec/bitstream/123456789/39987/1/t2418poi.pdf

Guerra, J. X. (2022). DISEÑO DE UN PLAN DE CONTINGENCIA DE TI PARA MINIMIZAR RIESGOS[Tesis de Maestría, UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ]. *DISEÑO DE UN PLAN DE CONTINGENCIA DE TI PARA MINIMIZAR RIESGOS OPERATIVOS EN LA CARRERA TECNOLOGÍAS DE LA INFORMACIÓN.* Repositorio Digital, Jipijapa.

https://repositorio.unesum.edu.ec/bitstream/53000/3547/1/GUERRA%20CARVAJAL%20JONATHAN%20XAVIER.pdf

Guevara, G. P., Verdesoto, A. E., y Castro, N. E. (2020). *Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción)* (Editorial Universitaria ed., Vol. 4). Revista Científica de la Investigación y el Conocimiento. https://dialnet.unirioja.es/servlet/revista?codigo=26323

Guillem, M. (2021). *Desde la mirada del investigador: retos, desafíos y decisiones Neuroedu.* Barcelona: NEdu. https://www.ub.edu/neuroedu/desde-la-mirada-del-investigador/

Hernández, R., y Mendoza, C. (2023). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* (Q. e. ed.), Ed.) McGraw-Hill Interamericana. https://doi.org/https://doi.org/10.13140/RG.2.2.36135.11689

Herrera, J. H. (2021). Identificación de escenarios de riesgo e implementación de contingencias en la empresa Eulen del Perú Servicios complementarios S.A. [Tesis de Título Profesional, Universidad Continental]. *Identificación de escenarios de riesgo e implementación de contingencias en la empresa Eulen del Perú Servicios complementarios S.A.* Repositorio Digital, Arequipa. https://repositorio.continental.edu.pe/bitstream/20.500.12394/10440/1/IV_FIN_107_TSP_Herrera_Pelaez_2021.pdf

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Ginebra: ISO. https://www.iso.org/standard/82875.html

Loaiza, A., y Suasnabar, V. (2021). Ciberseguridad y planes de contingencia en universidades [Tesis de Maestría, Universidad Continental]. *Plan de continuidad operativa de la Municipalidad Distrital de Chancay ante sismo de gran magnitud, 2021.* Repositorio Digital, Lima. https://repositorio.continental.edu.pe/bitstream/20.500.12394/10471/2/IV_PG_MGRD_TI_Loaiza_Suasnabar_2021.pdf

Mora, C. (2022). *Modelo de análisis de madurez de la seguridad de la información basado en la norma ISO 27001:2022.* Ibarra, Ecuador: Universidad Técnica del Norte. https://repositorio.utn.edu.ec/handle/123456789/13938

Navarrete, O. S. (2023). LA CONTINUIDAD DEL NEGOCIO BASADO EN ISO 22301 EN LOS SERVICIOS TECNOLÓGICOS DEL GAD MUNICIPAL DEL CANTÓN MOCACHE,2023 [Exámen Complesivo, UNIVERSIDAD TÉCNICA DE BABAHOYO]. *LA CONTINUIDAD DEL NEGOCIO BASADO EN ISO 22301 EN LOS SERVICIOS TECNOLÓGICOS DEL GAD MUNICIPAL DEL CANTÓN MOCACHE,2023.* Repositorio Digital, Los Ríos. http://dspace.utb.edu.ec/bitstream/handle/49000/14950/E-UTB-FAFI-SIST.INF-000188.pdf?sequence=1&isAllowed=y

Orjuela, M. A., y Ruge, M. A. (2021). Propuesta de implementación del plan de emergencias y contingencias para la empresa[Tesis de EspecializaciónUniversidad ECCI]. *Propuesta de implementación del plan de emergencias y contingencias para la empresa Inversiones Jomayosa SAS basado en la norma ISO 45001:2018.* Repositorio Digital, Bogotá. https://repositorio.ecci.edu.co/server/api/core/bitstreams/62a442ce-85a1-4d43-a2ad-022e09d75648/content

Ponce, B. C. (2022). ELABORACIÓN DE UN PLAN DE CONTINGENCIA INFORMÁTICO PARA EL CENTRO DE MOVIMIENTO DE MUJERES DE LA CIUDAD DE JIPIJAPA[Tesis de Titulación, UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ]. *ELABORACIÓN DE UN PLAN DE CONTINGENCIA INFORMÁTICO PARA EL CENTRO DE MOVIMIENTO DE MUJERES DE LA CIUDAD DE JIPIJAPA.* Repositorio Digital, Jipijapa. https://repositorio.unesum.edu.ec/bitstream/53000/4322/1/Ponce%20Macias%20Brigitte%20Carolina.pdf

Pozo, C. G., Reascos, R. S., y Minaya, R. W. (2025). *Fundamentos de Seguridad Informática.* Ediciones GESICAP. 77 pp. https://www.researchgate.net/publication/389395515_Fundamentos_de_Seguridad_Informatica_y_Ciberseguridad

Question Pro. (2023). QuestionPro Sitio Web: https://www.questionpro.com/blog/es/metodo-analitico/

Quijije, H. B. (2022). Propuesta de Plan de Contingencia en la Universidad Estatal Sur de Manabí, [Tesis de Maestría, UNESUM]. *PLAN DE CONTINGENCIA PARA ASEGURAR LA INTEGRIDAD DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ.* Repositorio Digital, Jipijapa. https://repositorio.unesum.edu.ec/bitstream/53000/3559/1/Quijije%20Quiroz%20Hilda%20Brigitte_PDF.pdf

REVISTA CAMPUS VIRTUALES. (2022). *REVISTA CIENTÍFICA IBENOAMERICANA DE TECNOLOGÍA EDUCATIVA* (Vol. 11). https://doi.org/10.54988/cv.2022.2.1081

Rodríguez , A., y Pérez, A. O. (2024). *Métodos científicos de indagación y de construcción del conocimiento* (Vol. 82). Revista Ean. https://doi.org/https://doi.org/10.21158/01208160.n82.2017.1647

Sánchez, V. (2021). Análisis, diseño e implementación de un sistema informático de notas académicas para el. *Análisis, diseño e implementación de un sistema informático de notas académicas para el Colegio Pedagógico La Casita Mágica, de Rivera – Huila.* Universidad Nacional Abierta y a Distancia - UNAD, Neiva. https://repository.unad.edu.co/bitstream/handle/10596/41729/vsanchezco.pdf?isAllowed=y&sequence=3

Santos, F., y Guzmán, H. (2022). *Análisis de la efectividad de los sistemas informáticos en la educación superior.* Universidad Técnica Particular de Loja.

Satander Becas. (2021). *Investigación cualitativa y cuantitativa: características, ventajas y limitaciones.* WMCCF (Web del Maestro CMF). https://webdelmaestrocmf.com/portal/investigacion-cualitativa-y-cuantitativa-caracteristicas-ventajas-y-limitaciones/

UPRRP. (2020). *DEGI*. Proceso de entrevista individual y grupos focales.: https://graduados.uprrp.edu/

Villamayor, L. E. (2024). *Transformación digital en la educación superior: Un estudio de caso en la Facultad de Ciencias Económicas Filial Caaguazú* (Vol. 5). LATAM. https://doi.org/https://doi.org/10.56712/latam.v5i4.2501

ANEXOS

Anexo 1 : Plan de Contingencia

Contenido

PLAN DE CONTINGENCIA PARA EQUIPOS INFORMÁTICOS

Carrera de Tecnología de la Información y Software – ULEAM Extensión El Carmen

1. Introducción

Este plan tiene como objetivo garantizar la disponibilidad, integridad y confidencialidad de los equipos informáticos personales de los estudiantes ante incidentes como:

- Fallos técnicos (hardware/software).
- Ataques de malware o ransomware.
- Pérdida/robo de dispositivos.
- Cortes eléctricos o desastres naturales.

Se basa en el análisis de riesgos realizado (Capítulo IV) y sigue los lineamientos de la ISO/IEC 27001:2022.

---

2. Alcance

- **Cobertura**: Estudiantes de la carrera de TI y Software de la ULEAM Extensión El Carmen.
- **Dispositivos**: Laptops, computadoras de escritorio y datos académicos almacenados.
- **Exclusiones**: Equipos institucionales de laboratorios (ya auditados).

---

3. Equipo de Respuesta

Rol	Responsable	Función
Coordinador	Ing. Bladimir Mora (Coordinador Académico)	Supervisar la implementación del plan.
Soporte Técnico	Ing. Jean Carlos Cedeño (Responsable de laboratorios TI)	Asesorar en recuperación de datos y reparaciones.
Comunicación	Docente designado	Informar a estudiantes sobre incidentes.
Estudiantes	Usuarios de equipos	Aplicar medidas preventivas y reportar incidentes.

4. Identificación de Riesgos y Medidas

Basado en la matriz de riesgos (Capítulo IV), se priorizan:

Riesgo	Probabilidad	Impacto	Medidas Preventivas	Medidas Correctivas
Malware	Alta (4)	Crítico (5)	- Instalar antivirus (Ej: ESET). - Bloquear USB no autorizados. - Capacitar en phishing.	- Aislar equipo infectado. - Restaurar desde backup.
Robo/Pérdida	Media (3)	Alto (4)	- Uso de candados físicos. - Registro de seriales.	- Bloquear equipo remotamente (Find My Device). - Reportar a autoridades.
Daños físicos	Media (3)	Medio (3)	- Protectores de voltaje. - Zonas libres de líquidos.	- Reparación con proveedores autorizados.
Corte eléctrico	Baja (2)	Alto (4)	- UPS o reguladores. - Guardar trabajo frecuentemente.	- Usar energía alternativa (batería laptop).

---

5. Procedimientos de Actuación

5.1. Para Infección por Malware

1. **Aislar**: Desconectar el equipo de la red.
2. **Escanear**: Usar herramientas como Malwarebytes.
3. **Restaurar**: Recuperar datos desde la última copia de seguridad (backup).
4. **Reportar**: Notificar al soporte técnico.

5.2. Para Robo o Pérdida

1. **Bloquear**: Usar herramientas como Find My Device (Windows) o Find My Mac.
2. **Cambiar contraseñas**: De cuentas académicas (correo, Moodle).
3. **Denunciar**: Presentar reporte policial y a la universidad.

5.3. Para Fallos de Hardware

1. **Diagnóstico**: Usar herramientas como HWMonitor.
2. **Reparación**: Acudir a técnicos autorizados (lista de proveedores en Anexo A).
3. **Préstamo temporal**: Solicitar equipo de reserva (si aplica).

---

6. Recursos Necesarios

- **Tecnológicos**:
  - Software antivirus (licencias gratuitas para estudiantes).
  - Plataforma de backups en la nube (Google Drive, OneDrive).
- **Humanos**: Talleres trimestrales de ciberseguridad.
- **Económicos**: Presupuesto para reparaciones urgentes (según Tabla 5 del Capítulo IV).

---

7. Comunicación

- **Interna**:
  - Grupo de WhatsApp/Teams para alertas.
  - Correo institucional para reportes.
- **Externa**: Contacto con proveedores de soporte técnico externo.

---

8. Capacitación y Simulacros

- **Talleres semestrales**:
  - Uso seguro de dispositivos.
  - Creación y restauración de backups.
- **Simulacro anual**: Simulación de ataque de ransomware para evaluar respuestas.

---

9. Monitoreo y Mejora Continua (PHVA)

- **Planificar**: Revisar matriz de riesgos cada 6 meses.
- **Hacer**: Implementar medidas nuevas (ej: nuevo software de backup).
- **Verificar**: Auditorías internas (según ISO 27001).
- **Actuar**: Actualizar el plan con lecciones aprendidas.

Elaborado por: Zambrano Vera Neicer Daniel

Revisado por: Ing. Bladimir Mora

Fecha: 24/07/2025

ANEXO 1 Plan de Contingencia

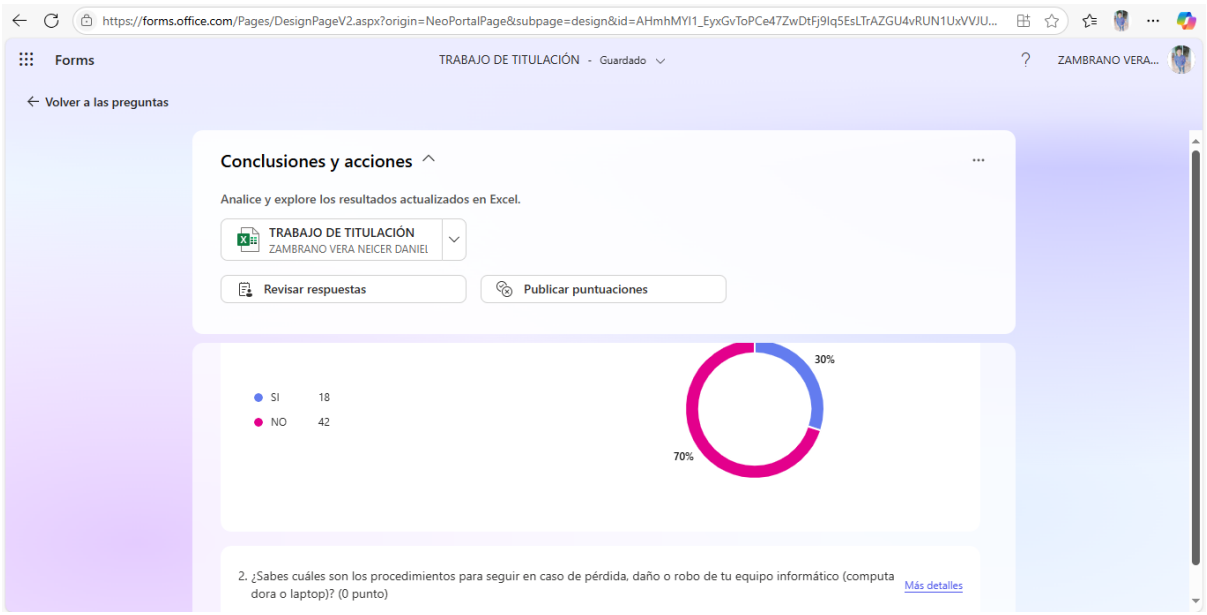
Anexo 2 : Anti plagio

ANEXO 2 Certificado de Antiplagio

Anexo 3 : Entrevista con el Coordinador de la Carrera de TI y Sotfware.

ANEXO 3 Entrevista Coordinador de la Carrera TI y Software

Anexo 4 : Encuesta a los estudiantes de TI y Software de la ULEAM Extensión El Carmen.



ANEXO 4 Encuesta a los estudiantes de TI y Software de la ULEAM Extensión El Carmen.

Anexo 5 : Cuestionarios de Análisis de Riesgos

Cuestionario para Analizar Riesgos			C1
Daños de Equipos	Respuestas		Observaciones
	SI	NO	
1. ¿Se utilizan protectores de voltaje en las estaciones de trabajo?			
2. ¿Se realiza mantenimiento preventivo a los equipos con frecuencia?			
3. ¿Los equipos están expuestos a calor, polvo o humedad en los laboratorios?			
4. ¿Se manipulan adecuadamente los cables de alimentación y datos?			
5. ¿Se reportan fallas técnicas apenas ocurren?			
6. ¿Los estudiantes reciben instrucciones claras sobre el uso correcto del equipo?			
7. ¿Existen normativas visibles sobre el uso adecuado de los equipos?			
8. ¿Los equipos son apagados correctamente después del uso?			
9. ¿Hay incidentes frecuentes de caídas o golpes a los dispositivos?			
10. ¿Se almacenan bebidas o alimentos cerca de los computadores?			
11. ¿Los periféricos (mouse, teclado, audífonos) presentan daños visibles frecuentes?			
12. ¿El software instalado presenta errores por mal uso o instalación indebida?			
13. ¿Se realizan respaldos antes de manipular el sistema operativo?			
14. ¿El ambiente donde se encuentran los equipos es seguro y controlado?			
15. ¿Los equipos son utilizados únicamente para fines académicos?			
Realizado por:	**Revisado por:**	**Observaciones:**	
Fecha:	**Fecha:**		

ANEXO 5 Cuestionarios Para Analizar Riesgos

8 Glosario

V