UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

EXTENSIÓN EN EL CARMEN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

PROYECTO INTEGRADOR

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

PLAN DE CONTINGENCIA PARA SEGURIDAD DE INFORMACIÓN EN LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE INGENIERIA EN SOFTWARE DE LA ULEAM EXTENSIÓN EL CARMEN.

CAZA ROMERO DIANA PAOLA

AUTORA:

ING. POZO HERNANDEZ CLARA GUADALUPE, MG.

TUTORA

EL CARMEN, FEBRERO 2026

CERTIFICACIÓN DE TUTOR

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

CERTIFICACIÓN

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

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante **CAZA ROMERO DIANA PAOLA**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2025(1)-2025(2), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es " **PLAN DE CONTINGENCIA PARA SEGURIDAD DE IMFORMACION EN LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE INGENIERIA EN SOFTWARE 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, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

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

El Carmen, 29 de enero del 2026

Lo certifico,

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

TRIBUNAL DE SUSTENTACIÓN

Universidad Laica Eloy Alfaro de Manabí

Extensión El Carmen

Carrera de Ingeniería en Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Título del Trabajo de Titulación:
Plan De Contingencia Para Seguridad De Información En Los Laboratorios De Cómputo De La Carrera De Ingeniería En Software De La Uleam Extensión El Carmen.

Modalidad:
Proyector Integrador

Autora:
Caza Romero Diana Paola

Tutora:
Ing. Pozo Hernández Clara Guadalupe, Mg.

Tribunal de Sustentación:

Presidente: Ing. Reascos PInchao Raúl Saed _____

Miembro: Ing. Mendoza Villamar Rocío Alexandra _____

Miembro: Ing. Arévalo Hermida Rómulo Danilo _____

Fecha de Sustentación:

19 de febrero del 2026

DECLARACIÓN EXPRESA DE AUTORÍA

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 seguridad de información en los laboratorios de cómputo de la carrera de Ingenieria Software en ULEAM Extensión El Carmen, corresponde exclusivamente a: Caza Romero Diana Paola con CI. 1729975704 y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Caza Romero Diana Paola

C.I. 1729975704

DEDICATORIA

Este trabajo lo dedico, en primer lugar, a Dios, por ser el autor de mi vida, por concederme salud, fortaleza y sabiduría, y por permitirme llegar hasta este momento tan significativo de mi formación profesional. Gracias por ser mi guía constante, mi refugio en los momentos difíciles y el manantial de fe que me impulsó a no rendirme, brindándome siempre lo necesario para seguir adelante y alcanzar mis objetivos.

Con profundo amor y gratitud, dedico este logro a mi madre, mi pilar fundamental. Gracias por tu bendición diaria, por tu apoyo incondicional, tus consejos llenos de sabiduría y los valores que sembraste en mí desde el inicio. Tu amor, tu entrega y tu constante motivación han sido la fuerza que me ha acompañado en cada etapa de mi vida académica y personal, inspirándome a convertirme en la profesional que hoy soy.

A mi padre, por ser ejemplo de perseverancia, constancia y disciplina. Gracias por inculcarme valores, por tu esfuerzo incansable y por el amor y aliento que siempre me brindaste, guiándome con firmeza por el camino del crecimiento personal y profesional.

A mis hermanos, por caminar a mi lado, por sus consejos, regaños y opiniones sinceras, que en cada momento me ayudaron a avanzar y a cumplir una meta más en mi vida. Gracias por ser parte de este proceso y por su apoyo constante.

Finalmente, gracias a todos mis docentes, por compartir sus conocimientos, dedicación y sabiduría, contribuyendo de manera significativa a mi formación académica. De manera especial, agradezco a la Ingeniera Clara Pozo, por su invaluable guía, acompañamiento y compromiso durante la elaboración de este trabajo, haciendo posible su culminación exitosa.

Diana Caza

AGRADECIMIENTO

En primer lugar, agradezco a Dios por ser mi fortaleza en los momentos de dificultad, por guiarme con sabiduría y prudencia, y por brindarme la fe y la claridad necesarias para crecer día a día, tanto en lo personal como en mí que hacer profesional.

Expreso mi sincero agradecimiento a la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen, por abrirme sus puertas y permitirme formar parte de esta prestigiosa institución, donde pude cursar mi carrera profesional. De igual manera, agradezco a los docentes que, con vocación y compromiso, compartieron sus conocimientos, experiencia y apoyo constante, contribuyendo de manera significativa a mi formación académica y humana.

Agradezco de manera especial a mi tutora de tesis, la Ingeniera Clara Pozo, por brindarme la oportunidad de apoyarme en su capacidad profesional y vasto conocimiento. Gracias por su paciencia, dedicación y acompañamiento permanente durante todo el desarrollo de esta investigación. Sus orientaciones, metodología de trabajo, persistencia y motivación fueron fundamentales para la culminación exitosa de este proyecto. Su ejemplo ha fortalecido en mí valores esenciales como la responsabilidad, el rigor académico y la seriedad profesional, indispensables para mi crecimiento como futura ingeniera e investigadora. Muchas gracias a esta hermosa institución

Diana Caza

ÍNDICE DE CONTENIDOS

ÍNDICE TABLAS

ÍNDICE GRÁFICOS E ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto de titulación tuvo como objetivo diseñar un plan de contingencia basado en los lineamientos de la norma internacional ISO/IEC 27031, con la finalidad de fortalecer la seguridad de la información y garantizar la continuidad de los servicios de Tecnologías de la Información y Comunicación (TIC) en los laboratorios de cómputo de la carrera de Ingeniería en Software de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen.

La investigación se llevó a cabo a partir de un diagnóstico que mostró la falta de políticas de seguridades formales, el escaso conocimiento en el ámbito de la seguridad informática y la falta de procesos bien definidos para manejar incidentes tecnológicos, aspectos que aumentan el cuidado de la infraestructura tecnológica. El estudio se realizó con un enfoque tanto cualitativo como cuantitativo, y tuvo un alcance exploratorio y descriptivo, utilizando métodos como encuestas, entrevistas, observación directa y análisis de documentos. La información obtenida permitió llevar a cabo una auditoría de seguridad y crear un diagnóstico sobre la situación actual, así como una matriz de riesgos, identificando amenazas como el robo, el daño físico a los equipos y los ataques de malware, que pueden comprometer la continuidad de los servicios de TIC. Como consecuencia, se elaboró un plan de contingencia que incluye medidas preventivas, estrategias de respuesta ante incidentes, programas de capacitación y procedimientos para respaldar y recuperar información. Se llega a la conclusión de que la propuesta desarrollada ayuda a fortalecer la seguridad de la información y a asegurar la continuidad operativa de los servicios tecnológicos, siguiendo los principios establecidos en la norma ISO/IEC 27031 y contribuyendo a mejorar la gestión tecnológica dentro de la institución.

ABSTRACT

The present graduation project aimed to design a contingency plan based on the guidelines of the international standard ISO/IEC 27031, in order to strengthen information security and guarantee the continuity of Information and Communication Technology (ICT) services in the computer laboratories of the Software Engineering career of the Laica Eloy Alfaro University of Manabí (ULEAM), El Carmen Extension.

The research stemmed from a diagnostic assessment that revealed a lack of formal security policies, limited knowledge in the field of cybersecurity, and a lack of well-defined processes for handling technological incidents—factors that increase the vulnerability of the IT infrastructure. The study employed both qualitative and quantitative approaches and had an exploratory and descriptive scope, utilizing methods such as surveys, interviews, direct observation, and document analysis. The information gathered enabled a security audit and the creation of a diagnostic assessment of the current situation, as well as a risk matrix, identifying threats such as theft, physical damage to equipment, and malware attacks, which could compromise the continuity of ICT services. Consequently, a contingency plan was developed, encompassing preventative measures, incident response strategies, training programs, and procedures for backing up and recovering information. It is concluded that the proposed solution helps to strengthen information security and ensure the operational continuity of technological services, following the principles established in the ISO/IEC 27031 standard and contributing to improving technological management within the institution.

CAPÍTULO I:

1 INTRODUCCIÓN

1.1 Introducción

La aplicación de la Tecnologías de la Información y Comunicación (TIC) es esencial para el desarrollo de las actividades académicas y administrativas en las instituciones de educación superior. Los laboratorios de cómputo integra espacios estratégicos, ya que facilitan el acceso a recursos tecnológicos indispensables para la formación profesional; sin embargo, su operatividad puede verse afectada por incidentes que comprometan la continuidad de los servicios tecnológicos y la protección de la información

La Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen, particularmente en el área de Ingeniería en Software, ha detectado vulnerabilidades relacionadas con el manejo de incidentes tecnológicos, la gestión de accesos, la defensa contra software dañino y la reacción ante imprevistos. Estas circunstancias aumentan la probabilidad de paradas en los servicios académicos, lo que afecta el normal avance de las actividades de la institución. Ante esta situación, la norma ISO/IEC 27031 proporciona pautas para asegurar la preparación de las Tecnologías de la Información y Comunicación en el contexto de la continuidad del negocio, ofreciendo directrices para prevenir, enfrentar y recuperarse de incidentes que puedan afectar los servicios tecnológicos. Implementar esta norma posibilita la evaluación de riesgos, la definición de medidas de protección y la creación de planes de acción orientados a preservar la disponibilidad, integridad y confidencialidad de la información.

En este sentido, la presente investigación tiene como finalidad crear un plan de contingencia para los laboratorios de cómputo de la carrera de Ingeniería en Software de ULEAM, Extensión El Carmen, fundamentado en las orientaciones de la ISO/IEC 27031. Para ello, se adopta un enfoque de investigación aplicada, con un alcance exploratorio y un método cuantitativo, que facilita la identificación de posibles amenazas, la valoración del nivel de riesgo y la sugerencia de medidas técnicas, administrativas y operativas

Y sobre todo la estructura del estudio se organiza en capítulos que abordan la base teórica, el análisis metodológico sin embargo la implementación práctica del plan de contingencia, permitiendo presentar una solución posible al contexto institucional. Así, la investigación contribuye a reforzar la continuidad de los servicios de TIC en otras palabras mejorar la gestión de la seguridad de la información en el ámbito universitario.

1.2 Presentación del tema

Plan de contingencia para seguridad de información en los laboratorios de cómputo de la carrera de Ingeniería Software en ULEAM Extensión El Carmen

1.3 Ubicación y contextualización de la problemática

La Universidad Laica Eloy Alfaro de Manabí en la extensión El Carmen, cuenta con tres bloques principales. El primer bloque se encuentra ubicado en la zona de la granja, el segundo bloque está ubicado en las instalaciones del antiguo colegio Lastenia y el tercer bloque se encuentra en la planta central, en la provincia de Manabí, cantón El Carmen, específicamente en la parroquia El Carmen, en la avenida 3 de Julio y Carlos Alberto Aray.

Actualmente, la planta central está distribuida en dos edificaciones. En la primera funciona el área administrativa junto con las carreras de Finanzas y Contabilidad. En la parte superior se encuentran las carreras de Tecnología de la Información y Comunicación, y Software.

El lugar donde se realizará el proyecto integrador que se muestran en los anexos G de esta investigación cuenta con dos laboratorios para la carrera de Software los estudiantes emplean con frecuencia estos espacios. El segundo piso del edificio principal alberga los laboratorios. Para Acceder a ellos, hay que ingresar por la puerta principal luego subo las escaleras. Cuando llegue al segundo piso, encontrarás el Laboratorio 1 en la parte izquierda y el Laboratorio 2 en la parte derecha.

Laboratorio 1: tiene 24 computadoras en total de las cuales son de diferentes marcas las 18 son de marca y con procesador Intel® Core™ i7-10700 CPU @ 2.90GHz, RAM de 8.00 GB (7.69 GB usable), sistema operativo Windows 11 (versión 24H2). Hay 3 de marca LG con procesador 11th Gen Intel® Core™ i5-11400 @ 2.60GHz, RAM de 8.00 GB (7.77 GB usable), sistema operativo Windows 11 de 64 bits (basado en x64). El laboratorio cuenta con 1 de marca Beng con procesador 11th Gen Intel® Core™ i5-11400 @ 2.60GHz, RAM de 8.00 GB (7.77 GB usable), sistema operativo Windows 11 de 64 bits (basado en x64). También 1 de marca Dell con procesador Intel® Core™ i7-14700 @ 2.10GHz, RAM de 16.0 GB (15.7 GB utilizable), sistema operativo Windows 11 Pro de 64 bits (basado en x64).

1.4 Planteamiento del problema

1.4.1 Problematización

En la actualidad, se ha observado que muchos estudiantes hacen uso frecuente de los equipos de los laboratorios universitarios, lo cual, si no se realiza de manera adecuada, puede generar diversos riesgos de seguridad informática. Estos riesgos pueden provocar fallos en los equipos, pérdida de información importante, como tareas, archivos y actividades académicas, así como daños en los programas instalados. La falta de medidas preventivas ante estos incidentes podría afectar gravemente el desarrollo académico, ya que los equipos podrían quedar inoperativos y los datos adquiridos se perderían. Por esta razón, es fundamental estar preparados y contar con protocolos de prevención que permitan minimizar el impacto ante posibles fallos o ataques informáticos.

1.4.2 Génesis del problema

Las organizaciones enfrentan múltiples riesgos que amenazan su infraestructura tecnológica, como el robo de dispositivos, ataques en línea, fenómenos naturales y cambios climáticos. Estos eventos pueden afectar la operatividad de los sistemas, así como poner en peligro la seguridad de la información de la institución. Ante esta situación, es crucial reconocer, evaluar y disminuir estas potenciales amenazas, ya que podrían ocasionar la pérdida de documentos y datos importantes. la tecnología es clave para el avance y la evolución de las universidades. Por esta razón, es esencial entender cómo surgen los problemas de seguridad de la información e identificarlos, lo que permite gestionar vulnerabilidades, minimizar riesgos y reforzar la protección de los sistemas informáticos. En esta situación, el origen del problema se enfoca en la debilidad de la información que se guarda y se procesa en los laboratorios de cómputo de la carrera de Ingeniería en Software en la extensión universitaria de El Carmen.

1.4.3 Estado actual del problema

Hoy en día, los laboratorios uno y dos se emplean tanto para la carrera de Ingeniería en Software como para Tecnología de la Información y Comunicación. Estos espacios son utilizados por estudiantes de diferentes cursos y niveles de educación. Sin embargo, se ha observado una ausencia de control en el acceso a los laboratorios debido a la falta de medidas de seguridad definidas. A menudo, las puertas están abiertas y los equipos no tienen bloqueos de acceso, lo cual posibilita que cualquier usuario tenga la capacidad de manejarlos sin restricciones.

Esta situación constituye un peligro significativo para la seguridad de la información, ya que podría permitir el robo de datos, la desaparición de documentos o el mal uso de los dispositivos. Asimismo, los alumnos podrían entrar a sitios web no permitidos, debido a la vulnerabilidad a riesgos digitales.

1.5 Diagrama causa – efecto del problema

Árbol del problema

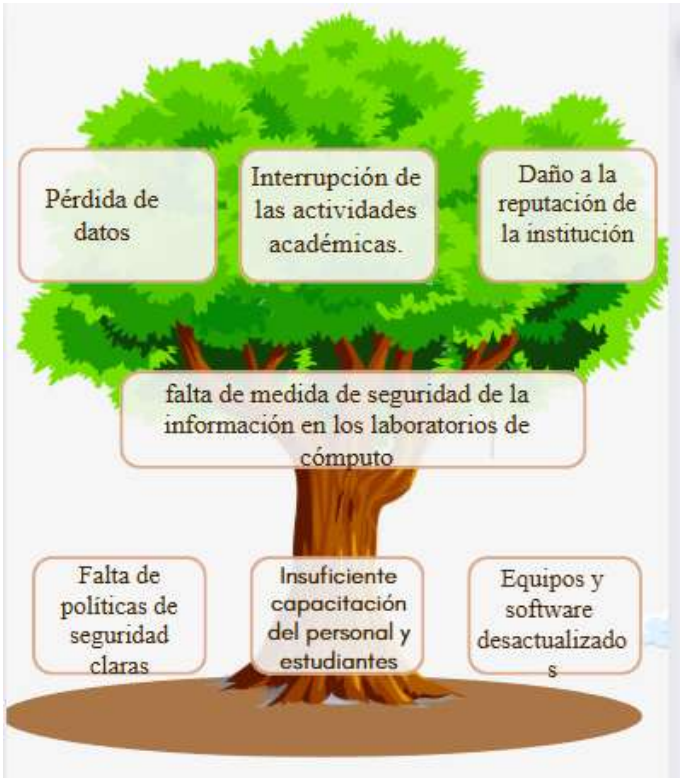


Ilustración 1 Árbol del problema

1.6 Objetivos

1.6.1 Objetivo general

Diseñar un plan de contingencia para seguridad de información en los laboratorios de cómputo de la carrera de Ingeniería Software en ULEAM Extensión El Carmen

1.6.2 Objetivos específicos

- Identificar los principales problemas relacionados con la seguridad lógica en el laboratorio de cómputo.
- Investigar informaciones relevantes sobre las variables vinculadas al plan de contingencia y la seguridad de la información.

- Diagnosticar la existencia de problemáticas reales de seguridad en el laboratorio, mediante la aplicación de encuesta y entrevistas a los estudiantes y docentes de las carreras de Ingeniería en software y Ingeniería tecnología de la información
- Evaluar el nivel de riesgo de seguridad lógica en los laboratorios de la ULEAM, extensión El Carmen.
- Desarrollar una estrategia de restauración de seguridad digital frente a emergencias que ayude a reducir los peligros y asegurar la continuidad de las operaciones del laboratorio, en cuanto a situaciones donde un riesgo significativo impacte en la información de los laboratorios.

1.7 Justificación

La presente investigación resulta fundamental debido a que la ausencia de conocimientos y prácticas adecuadas en seguridad de la información puede generar riesgos significativos, tales como el robo, pérdida o alteración de datos sensibles. En los laboratorios de cómputo de la carrera de Ingeniería de Software de la ULEAM, Extensión El Carmen, se han identificado deficiencias en la comunicación, el control y la gestión de la seguridad de la información, lo que incrementa la vulnerabilidad de los recursos tecnológicos y de la información institucional.

Ante esta problemática, se considera necesaria la elaboración de un plan de contingencia que permita prevenir, enfrentar y mitigar incidentes tecnológicos, garantizando la confidencialidad, integridad y disponibilidad de la información. La implementación de esta propuesta contribuirá al fortalecimiento de la continuidad operativa, la reducción de riesgos y la mejora de la gestión de seguridad en los laboratorios.

1.8 Impactos esperados

1.8.1 Impacto Social

El estudio actual tiene un efecto social significativo al ayudar a mejorar la seguridad de la información y la continuidad de los servicios tecnológicos dentro del ámbito universitario .La puesta en marcha de un plan de acción en los laboratorios de computación disminuirá los riesgos vinculados a la pérdida de información, interrupciones en las actividades académicas y debilidades tecnológicas, beneficiando de manera directa a alumnos, profesores y empleados administrativos .De igual manera, esta iniciativa fomenta una cultura de prevención,

responsabilidad y uso seguro de las herramientas tecnológicas, lo cual enriquece la calidad del proceso educativo y la salvaguarda de la información institucional.

El impacto social va más allá de la universidad, porque los saberes adquiridos se reproducirán en otros contextos personales y laborales. A largo plazo, esta medida promoverá una mayor conciencia colectiva sobre la importancia de proteger la información, lo que ayudará a crear una sociedad digital más segura y reducirá las vulnerabilidades institucionales.

1.8.2 Impacto tecnológico

El impacto tecnológico del plan de contingencia se manifiesta en la mejora y transformación de los sistemas tecnológicos existentes, garantizando que la infraestructura informática mantenga su operatividad, seguridad y disponibilidad incluso ante emergencias o amenazas a la integridad de los datos. La implementación de este plan no solo protege los recursos tecnológicos institucionales, sino que también fortalece la formación de los estudiantes al difundir conocimientos sobre normativas de seguridad y protocolos de actuación ante riesgos de pérdida de información.

De igual manera, la propuesta fomenta que se utilicen las herramientas tecnológicas de manera consciente, lo que favorece a la comunidad académica y al establecimiento con una cultura de ciberseguridad. Algunos de sus logros más sobresalientes son: la mejora en el uso eficiente de los recursos tecnológicos, el desarrollo de competencias digitales esenciales para el ámbito profesional y una correcta protección de la información personal e institucional. Efecto social

La elaboración y ejecución del Plan de Contingencia para la Seguridad de la Información en los laboratorios informáticos fortalecerá significativamente la cultura de ciberseguridad dentro de la comunidad académica. No solo se reforzará la protección de datos institucionales con esta iniciativa, sino que además promoverá un uso consciente de la tecnología entre estudiantes, docentes y personal administrativo. Se fomentará un comportamiento proactivo en la prevención de incidentes digitales al sensibilizar a los usuarios acerca de las amenazas asociadas con la pérdida o el robo de datos. Esta iniciativa contribuirá a capacitara profesionales más preparados para afrontar los desafíos de la época digital, desarrollando habilidades fundamentales en cuanto a seguridad informática que son esenciales tanto en el ámbito laboral como educativo.

1.8.3 Impacto ecológico

La ejecución del Plan de Seguridad de la Información en los laboratorios de computación de la Ingeniería en Software de la ULEAM, Sede El Carmen, produce un efecto ambiental considerable al aumentar la protección digital de los dispositivos y evitar perjuicios por ataques cibernéticos, malware o fallas de seguridad que podrían incapacitar los aparatos. Al proteger los sistemas tecnológicos y reducir los peligros, se alarga la vida útil del hardware, lo que a su vez reduce la producción de residuos electrónicos y promueve un uso más responsable de los recursos tecnológicos.

El plan también incluye protocolos concretos para afrontar catástrofes naturales, salvaguardando la infraestructura física de los laboratorios y la información crítica. Esta doble protección, tanto digital como física, no solo fortalece la seguridad tecnológica de la institución, sino que también promueve prácticas de responsabilidad ambiental en el área académica. La iniciativa ayuda a disminuir las consecuencias ambientales de las operaciones tecnológicas en universidades, al reducir la necesidad de sustituir con frecuencia los equipos y optimizar el ciclo de vida de los dispositivos. Esto está en consonancia con los principios de conservación de recursos y sostenibilidad.

CAPÍTULO II:

2 Marco teórico de la investigación

2.1 Antecedentes históricos

El concepto de plan de contingencia tiene sus orígenes en el pensamiento medieval, donde filósofos como Tomás de Aquino lo abordaron como parte fundamental de la condición humana, vinculándolo a la necesidad de adaptación ante lo imprevisto y a la dependencia de lo divino. En esta perspectiva filosófica, la contingencia representaba tanto la incertidumbre inherente a la existencia como la búsqueda constante de orden en los acontecimientos relevantes. Con el avance de las sociedades moderna, esta idea se transformó en aplicaciones prácticas durante el siglo veinte, cobrando gran importancia en tres áreas clave: la ciberseguridad, como una forma de resguardar sistemas; la administración empresarial, para asegurar una operativa continua; y la protección civil, como un método organizado para reaccionar ante situaciones de emergencia. Los planes de contingencia surgieron como herramientas estratégicas para abordar una variedad de riesgos, que van desde catástrofes naturales hasta fallos tecnológicos y crisis financieras. Hoy en día, estos protocolos se han establecido como elementos esenciales que dictan acciones y procedimientos ante situaciones de riesgo, buscando proteger tanto la integridad física de las personas como su seguridad, además de preservar los bienes materiales y el entorno. Su aplicación asegura una respuesta efectiva y coordinada frente a eventos inesperados, integrando preparación preventiva y capacidad de respuesta (Carrion , 2024).

La presente investigación se desarrolla en los laboratorios de cómputo de la carrera de Ingeniería en Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. Esta institución de educación superior brinda formación profesional en el área tecnológica, contando con infraestructura informática destinada al desarrollo académico de los estudiantes.

Actualmente, los laboratorios presentan debilidades relacionadas con la seguridad de la información y la continuidad de los servicios TIC, debido a la ausencia de políticas formales de contingencia, procedimientos documentados y mecanismos estructurados para la gestión de incidentes. Esta situación genera riesgos operativos que podrían afectar la disponibilidad, integridad y confidencialidad de la información institucional.

La ciberseguridad comenzó a tomar relevancia en la década de 1970, cuando surgieron los primeros virus informáticos, evidenciando la necesidad de proteger los sistemas

computacionales. Este problema llevó al desarrollo del primer software antivirus en los años 1980, marcando un avance significativo en la defensa contra amenazas digitales. Sin embargo, no fue hasta la década de 2000 cuando las empresas comenzaron a considerar la ciberseguridad como un elemento esencial dentro de sus estrategias corporativas. Este cambio de paradigma se debió principalmente al aumento considerable de ciberataques dirigidos contra sus redes corporativas. Estos incidentes demostraron claramente la urgencia de fortalecer los mecanismos de protección de la información, lo que impulsó: la creación de normativas y estándares de seguridad, el desarrollo de protocolos de seguridad más robustos, La implementación de tecnologías avanzadas para mitigar riesgos La adopción de mejores prácticas en entornos digitales, Estos avances han permitido establecer un marco de seguridad más completo para proteger la infraestructura tecnológica de las organizaciones en la era digital (Incibe, 2023).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Plan de contingencia informático y de seguridad de la información para los laboratorios de cómputo de la carrera de tecnologías de la información

Esta investigación, desarrollada en la Universidad Estatal del Sur de Manabí (UNESUM), Ecuador, implementó un plan de contingencia para proteger la información y equipos en los laboratorios de cómputo. Mediante una metodología mixta (cualitativa-cuantitativa) que incluyó métodos deductivos, estadísticos, bibliográficos y encuestas de evaluación de riesgos, se identificaron amenazas y se establecieron medidas de seguridad. Los resultados garantizaron la integridad de datos, disponibilidad de sistemas y continuidad operativa, mediante el análisis de vulnerabilidades, estrategias preventivas y protocolos de recuperación ante incidentes. El estudio proporciona un modelo aplicable para fortalecer la seguridad informática en instituciones educativas (Castro Baque S. , 2024).

Plan de contingencias informáticas y la seguridad de la información en el consejo nacional electoral de la provincia de Santa Elena

Esta investigación, desarrollada en 2018 por el Ing. Carlos Renán Mero Suárez en el Consejo Nacional Electoral de Santa Elena (Ecuador), implementó un plan de contingencia para garantizar la protección de datos electorales. Mediante un análisis de riesgos y estrategias de seguridad informática, el estudio identificó vulnerabilidades críticas en los sistemas y estableció protocolos para asegurar la confidencialidad, integridad y disponibilidad de la información. Los resultados proporcionaron medidas efectivas para minimizar riesgos y

mantener la continuidad operativa del sistema electoral, fortaleciendo su capacidad de respuesta ante amenazas cibernéticas. El trabajo ofrece un modelo aplicable para la protección de datos en organismos electorales (Mero Suárez C. , 2018)**.**

Aanálisis de riesgo y diseño de plan de contingencia para recuperación ante desastres en florida education institute (fl-usa) según la norma ISO 24762-2008.

Se elaboró un plan de contingencia para el área de TI del Instituto de Educación de Florida (FEI) siguiendo la norma ISO 24762:2008. A través de métodos descriptivos y explicativos, se detectaron diversas amenazas cibernéticas, naturales y humanas mediante encuestas y análisis de documentos. Los hallazgos revelaron debilidades significativas en la gestión de la tecnología, lo que facilitó el desarrollo de estrategias para su mitigación, incluyendo protocolos de prevención y recuperación. La fase de implementación abarcó mejoras en las políticas de seguridad, formación del personal y procedimientos para asegurar la continuidad de las operaciones y la protección de datos frente a ciberataques, catástrofes y fallos técnicos. Este proyecto estableció un esquema de seguridad que cumple con estándares internacionales para proteger la infraestructura de TI de la institución (Montesdeoca, 2022).

Plan de contingencia de tecnología de la información

Este trabajo elaboró un esquema de contingencia tecnológica para el presupuesto de la Universidad Técnica de Ambato, que se concluyó en septiembre de dos mil veintidós. Siguiendo las directrices de las normas ISO/IEC 27001 y 27002, la investigación aplicó un enfoque de gestión de riesgos que detectó sistemas esenciales y debilidades en la infraestructura tecnológica del instituto. Entre los hallazgos más importantes, se crearon directrices para la copia de seguridad y recuperación de información, mejoras en la infraestructura tecnológica, además de un programa de ejercicios regulares. El esquema ofreció al apoyo UTA, que antes carecía de tales directrices, un sólido marco para asegurar la continuidad operativa frente a eventualidades tecnológicas, resguardando así sus procesos institucionales activas (Huilca Palacios, 2022).

Desarrollo de un sistema informático para el control de ventas en la pastelería adonis de la parroquia Abdón calderón del cantón Portoviejo

Objetivo principal: Implementar un sistema informático para automatizar el control de ventas en la pastelería Adonis, optimizando la gestión de inventario, registros de clientes y facturación. Quién lo realizó: Gema Monserrate Villacreses Muñiz, tutelada por el Ing. Omar Quimis Sánchez. Motivación: La operación manual generaba errores frecuentes y pérdidas

económicas. La autora buscó mejorar la operatividad del negocio. Metodología Se utilizó un enfoque mixto: encuestas a empleados, análisis de requerimientos y desarrollo en Visual Studio 2019 y MySQL, con validación de usuarios. Resultados Automatización de procesos, reducción de errores, mejora en el servicio al cliente y aceptación del sistema por los usuarios (Villacreses Muñoz, 2022).

2.3 Definiciones conceptuales

2.3.1 Plan de contingencia

Se define como una táctica de respaldo que detalla la manera en que una entidad reaccionará ante situaciones críticas que alteren sus planes iniciales. Comprende acciones preventivas, de reacción y de restauración para garantizar la capacidad de recuperación de la organización. se puede entender como una estrategia estructurada que incluye diversos procedimientos destinados a ofrecer soluciones alternativas. Esto facilita la rápida reanudación de los servicios de la entidad en caso de una interrupción, ya sea total o parcial. Este tipo de plan sirve como una herramienta que asegura que las funciones fundamentales de una empresa u organización continúen operando, incluso si se presenta una posible falla en los sistemas tecnológicos. En otras palabras, es un diseño que permite que su negocio o entidad funcione, aunque de manera limitada (López Cuadrado, 2015).

2.3.1.1 Objetivos del plan de contingencia

La meta fundamental de los planes de emergencia es asegurar que una organización mantenga su funcionamiento ante acontecimientos imprevistos que podrían cambiar en sus actividades esenciales. Estos planes se dividen en cuatro etapas clave: análisis de amenazas, formulación de tácticas de respuesta, verificación de eficacia y puesta en práctica. Un plan de emergencia eficaz debe abarcar áreas específicas que expliquen las medidas a tomar durante la asistencia inicial, la reacción ante la crisis y los pasos necesarios para la restauración. Asimismo, resulta fundamental identificar y documentar los instrumentos, herramientas y recursos tecnológicos que actualmente se utilizan para gestionar incidentes de seguridad informática (Ibarra Canseco, 2019)**.**

2.3.1.2 Plan de contingencia y sus relaciones con importancia en la gestión organizacional

La implementación de un plan de contingencia es vital para la gestión organizacional, ya que permite anticiparse a posibles crisis, asegurar la continuidad operativa y mantener la confianza de los elementos que demuestra un enfoque serio y oficial en una organización es su

capacidad para estar siempre lista ante cualquier situación inesperada o problemas en general, lo que le permite manejar estos desafíos, al menos temporalmente, mientras se presente la situación. Por lo tanto, es fundamental que se establezca un Plan de Contingencia de Tecnología de la Información de forma seria y meticulosa, de manera que implique, en mayor o menor medida, a toda la organización en el Plan de Prevención, Implementación y Recuperación, aunque se debe designar un grupo específico encargado de su diseño, aprobación y actualización (Huilca Palacios , 2022).

2.3.1.3 Tipos de planes de contingencia

Los tipos más importantes de planes de contingencia se centran en la restauración de datos y sistemas, la reacción ante urgencias y la reactivación de las operaciones, ordenados según. la gravedad de la contingencia. Según Castro Baque (2024), los planes de contingencia se clasifican en:

- **Planes de respaldo sobre todo en informática:** Estos planes se enfocan en la recuperación de datos y sistemas críticos en caso de incidentes o desastres informáticos.
- **Planes de emergencia:** Estos planes indican las acciones a realizar frente a situaciones urgentes que lleguen a impactar a la organización, como sucesos naturales, percances, etc.
- **Planes de recuperación:** Estos esquemas explican las acciones para rehacer las tareas y recobrar el orden luego de un percance o desastre.

2.3.1.4 Elementos del plan de contingencia

2.3.1.4.1 Análisis de riesgos

La evaluación del peligro se fundamenta en los datos recogidos durante la etapa de identificación, que ahora se transforman en insumos para tomar decisiones. Durante la etapa de análisis, se tienen en cuenta tres factores que ayudan a aproximar un valor objetivo del riesgo de la lista de peligros prioritarios: la posibilidad, el efecto y la exposición al riesgo. Estos factores permitirán al grupo coordinador clasificar los peligros, lo que le facilitará invertir más tiempo y esfuerzo en la gestión de los riesgos más significativos. Evaluación sistemática de amenazas potenciales y su impacto en la organización, identificando vulnerabilidades y probabilidades de ocurrencia (Huilca Palacios, 2022).

2.3.1.4.2 Identificación de recursos críticos

Determinación de los recursos indispensables (humanos, tecnológicos, financieros) necesarios para mantener las operaciones esenciales. Vinculado a la noción de reestructuración de procedimientos, se presenta el concepto de proceso crítico, que podemos entender como un conjunto de actividades que atraviesa transnacionalmente una empresa para crear un producto o brindar un servicio al cliente. La noción de transfuncionalidad se origina en el enfoque de especialización funcional dentro de una línea de producción en serie, donde cada tarea es realizada por un especialista altamente efectivo y eficiente. Este modelo ha permitido lograr avances significativos en la productividad. Los procesos críticos generalmente inician y concluyen con el cliente, ya sea que se empiecen debido a la identificación de una necesidad latente o de una solicitud precisa, y terminan con la oferta o la entrega de un producto o servicio (Betancourt Sánchez, 2017).

2.3.1.4.3 Plan de acción y recuperación

Consiste en desarrollar estrategias y procedimientos que permitan responder de manera efectiva y recuperar la operatividad tras la ocurrencia de incidentes o situaciones adversas. Esta fase contempla la asignación de responsabilidades, la organización de los tiempos y la definición de protocolos para el manejo de sistemas y recursos informáticos. También abarca la obtención y resguardo de copias de seguridad backups, así como el establecimiento de políticas, normas y procedimientos que garanticen la correcta ejecución y mantenimiento de dichos respaldos (Alberto Guerrero, 2023).

2.3.1.5 Implementación de gestión

2.3.1.5.1 Fases para la elaboración del plan de contingencia

Una de las etapas clave del Plan de Contingencia es la recopilación y verificación de la información que servirá para crear una guía práctica y de fácil comprensión para el personal del FCPC-UTA. Por ello, una etapa esencial de la metodología incluye un modelo estandarizado para documentar todos los acontecimientos establecidos que son parte del plan; de este modo se obtendrá un entregable que cumpla con las normativas y requisitos estipulados para este propósito. Se ha elaborado un modelo de Formato de Registro del Plan de Contingencia, que se detalla a continuación y que consta de las siguientes secciones (Huilca Palacios, 2020).

Ilustración 2 fases de plan de contingencia

2.3.1.5.2 Análisis de riesgos.

Es fundamental reconocer los peligros asociados a los procedimientos del proyecto y a los sistemas de comunicación e informáticos como parte del producto, así como establecer los criterios que indiquen cuándo se exceden los límites razonables. Deben aprovecharse las lecciones aprendidas y la información de proyectos pasados. La detección de riesgos necesita llevarse a cabo al comienzo del proyecto, durante las revisiones del progreso y en otros momentos donde se tomen decisiones importantes. La evaluación de riesgos debe enfocarse no solo en los aspectos económicos, temporales y del producto, sino también en áreas como la seguridad, el funcionamiento seguro, la responsabilidad profesional, la tecnología de la información, la salud laboral, el bienestar general y el impacto ambiental, considerando las normativas que se apliquen y aquellas que puedan surgir. Es crítico evaluar las interacciones entre los riesgos. Además, resulta útil detectar tecnologías nuevas y esenciales (Suárez, 2018).

2.3.1.6 Táctica de recuperación

Las tácticas de respaldo o de continuidad operativa se enfocan en identificar las prioridades y establecer, de manera lógica y ordenada, las alternativas que deben implementarse en primer lugar, así como los riesgos que requieren atención inmediata. Estas estrategias permiten definir el curso de acción más eficiente para minimizar el impacto de incidentes críticos. Asimismo, es indispensable determinar si las soluciones se aplicarán a gran escala, como en el caso de las estrategias de recuperación ante desastres para un centro de procesamiento de datos, con el fin de garantizar la pronta restauración de las operaciones esenciales y la protección de la información (Hermida, 2024).

2.3.1.7 Desarrollo de estrategia y procedimientos

Se entiende por recursos a los elementos y artículos que la entidad posee para manejar una situación de emergencia, los cuales requieren estar debidamente registrados, con su respectiva ubicación. Además, debe indicarse si están operativos o no, por lo que es necesario mantener una evaluación continua que identifique los recursos disponibles. Al desarrollar cualquier tipo de plan, es fundamental tener a disposición el equipo imprescindible, y el recuento debería incluir la totalidad de lo que se posee en lugar de lo que está previsto adquirir. Esto es crucial dado que las situaciones de emergencia pueden ocurrir justo antes de realizar una compra. Asimismo, se debe llevar a cabo un control regular de la operatividad del equipo, la reposición de botiquines, la fecha de caducidad de los extintores y el funcionamiento de linternas, sistemas de evacuación, alarmas, entre otros (Patricio, 2023).

2.3.1.8 Pruebas y entretenimiento

Análisis de debilidades internas que podrían ser aprovechadas por riesgos externos, teniendo en cuenta aspectos tecnológicos, humanos y organizativos. Para reducir estas debilidades, es fundamental desarrollar un enfoque completo de ciberseguridad que abarque la evaluación de riesgos, el mantenimiento proactivo, la formación del personal y la implementación de controles físicos y lógicos apropiados (Castro Baque S. G., 2024).

2.3.1.9 Plan de mantenimiento

El Departamento Administrativo asegurará evaluaciones del Plan de Contingencias al menos cada seis meses, realizadas por la Oficina de Informática, que requerirá la disponibilidad de su personal. Las correcciones necesarias serán realizadas por el encargado, quien informará a las áreas administrativas sobre los ajustes.

Según Huilca Palacios (2020), estas pruebas permiten verificar periódicamente la operatividad, actualización y viabilidad de los procedimientos establecidos en el plan. En este contexto, se contemplan las siguientes modalidades:

- Evaluaciones en formato impreso, donde el equipo asignado llevará a cabo evaluaciones trimestrales en cada área, incluyendo a todos los usuarios de la implementación del Plan. Estas sesiones revisarán procedimientos, viabilidad física y disponibilidad de equipos de protección.
- Las evaluaciones en tiempo real se realizan cada seis meses después de revisar las pruebas escritas. Durante este simulacro, se detiene la actividad en los departamentos y se instruye a todos sobre los procedimientos a seguir en una emergencia, como una

evacuación por fuego. También es importante practicar protocolos, como en caso de un corte de energía. Para seguir el Plan de Contingencias, se debe implementar cierta metodología.

2.3.2 Seguridad de la información

Es el grupo de acciones técnicas, administrativas y jurídicas que ayudan a una empresa a garantizar la privacidad, corrección y acceso al sistema de información. de los datos en una organización. Se basa en garantizar que la información sensible esté protegida contra accesos no autorizados, modificaciones no autorizadas o pérdida de disponibilidad. La seguridad de la información se ha vuelto crucial en nuestra sociedad conectada, aumentando con el uso generalizado de tecnología. Hoy en día, interactuamos con computadoras y dispositivos móviles para el trabajo, la educación, las compras y la vida diaria. Esto implica una necesidad necesaria debido a proteger nuestros datos en múltiples contextos, desde el hogar hasta lugares públicos (Del Pozo, 2023).

2.3.2.1 Principios fundamentales

Existen tres conceptos clave en seguridad de la información: la confidencialidad, integridad y disponibilidad, conocidos como la tríada de la CIA. Este modelo se utiliza desde hace más de 20 años para discutir la seguridad de los datos. La confidencialidad, relacionada pero no idéntica a la privacidad, implica proteger datos de personas no autorizadas. La confidencialidad se puede ver comprometida de varias formas, como la pérdida de dispositivos que contienen datos sensibles, la observación de contraseñas o ataques a sistemas. La integridad se refiere a proteger los datos de cambios no autorizados y a la capacidad de revertir cambios indeseados; esto es crucial, ya que datos alterados pueden llevar a decisiones equivocadas, como en el caso de resultados médicos. Finalmente, la disponibilidad se centra en el acceso a los datos cuando se necesitan, y su pérdida puede ser causada por problemas técnicos o ataques como el de denegación de servicio (Vega Briceño, 2021).

2.3.2.2 Amenazas

Considerando las argumentaciones presentadas, las amenazas, como se ha indicado anteriormente, se definen como la fuente o la causa de situaciones o incidentes no deseados que puedan ocasionar daños a los recursos informáticos de la entidad y, en consecuencia, a la misma. Entre estas amenazas, se destacan las más relevantes: la llegada y expansión del "malware" o "software malicioso", que son aplicaciones diseñadas para infiltrarse en los

sistemas sin el conocimiento de su propietario, con el fin de causar daños o alterar el funcionamiento del sistema y, por ende, de la organización (Quiroz & Macías, 2017).

2.3.2.3 Vulnerabilidades

Las redes presentan diversas vulnerabilidades que afectan la confidencialidad, integridad y disponibilidad de los sistemas. Una vulnerabilidad es una debilidad en un sistema informático que puede ser explotada por intrusos. Esto puede permitirles ejecutar comandos como otros usuarios, acceder a información confidencial o causar daños al sistema. Las vulnerabilidades tienen un ciclo de vida desde su detección hasta su corrección por parte de administradores o programadores. A menudo, estas fallas provienen de errores de diseño, programación o limitaciones tecnológicas, y pueden ser utilizadas para causar daños significativos (Olarte Quispe, 2021).

2.3.2.4 Tipo controles de seguridad

Existen algunos tipos de control de seguridad son los más importante las cuales son: controles físicos, lógico, administrativo, autenticación y autorización.

2.3.2.4.1 Controles físicos

Los controles de seguridad física constituyen las herramientas y los procedimientos específicos implementados para monitorear, disuadir y proteger a las personas y los espacios. Dichos controles pueden clasificarse en cuatro tipos generales (Condor Gordon, 2019).

- **Controles disuasivos:** su finalidad es evitar situaciones problemáticas mediante indicadores visibles de seguridad que hagan desistir a eventuales invasores. Ejemplos de esto son los carteles de “Zona prohibida”, obstáculos físicos y sistemas de alumbrado de seguridad.
- **Controles proactivos:** están enfocados en impedir entradas no permitidas o lesiones a los bienes y el personal. Ilustraciones de este tipo de control incluyen candados, tarjetas de entrada, vigilantes de seguridad y métodos de identificación.
- **Controles de detección:** permiten identificar intentos de intrusión o incidentes en el momento en que ocurren. Entre ellos se encuentran sensores de movimiento, cámaras de vigilancia y alarmas de intrusión.
- **Controles correctivos:** se implementan tras la ocurrencia de un incidente con el objetivo de reducir daños y restablecer la seguridad. Incluyen métodos de evacuación, planes de contingencia, respaldo de datos y estrategias de recuperación ante desastres.

2.3.2.4.2 Controles lógicos

El control de acceso lógico comprende políticas, procedimientos y otras actividades que forman parte del control de gestión de una organización. Restringe el uso de la información a individuos, grupos u organizaciones autorizados. Además, es un subconjunto de la seguridad que se ocupa de los procesos utilizados para restringir el acceso a los archivos y bases de datos de la computadora (Arévalo Cordovilla, 2022).

2.3.2.4.3 Controles administrativos

Los controles administrativos de seguridad consisten en: procedimientos operacionales, procedimientos de responsabilidad y suplementos de controles administrativos establecidos para proporcionar un nivel aceptable de seguridad para proteger los recursos de la organización. Además, los controles administrativos incluyen los procedimientos que se establecieron para asegurar que todo el personal que tiene acceso a los recursos tenga las autorizaciones requeridas (Condor Gordon, 2019).

2.3.2.4.4 Autenticación

Es el proceso de identificación de los usuarios basándose en su identificación como nombres de usuarios y contraseña protegiendo los sistemas informáticos como servidor y ordenador (Pozo Hernández et al., 2025).

2.3.2.4.5 Autorización

Garantiza que solo las personas autorizadas puedan acceder a los sistemas de seguridad y que puedan acceder con los permisos tomando en cuenta comprueba que los usuarios tengan un permiso autorizado

2.3.2.5 Cifrado y protección de la información

El cifrado transforma datos legibles texto plano en código ilegible texto cifrado para protegerlos. existen dos tipos de cifrado simétrico **(AES, DES):** Usa una misma clave para cifrar y descifrar es rápido, pero riesgoso si se pierde la clave y el Asimétrico (RSA, ECC) Emplea (Guardelli, 2024).

2.3.2.6 Políticas y normas de seguridad lógica

2.3.2.6.1 Políticas de contraseñas, acceso y uso

Las políticas de contraseñas, acceso y uso constituyen la base de la ciberseguridad en cualquier organización, ya que están diseñadas para proteger la información y los sistemas. De acuerdo con Sánchez (2022). estas políticas se clasifican en tres categorías principales: políticas de contraseñas, políticas de acceso y políticas de uso.

- **Políticas de contraseñas**: buscan asegurar que las claves de acceso sean fuertes y difíciles de comprometer. Esto se logra exigiendo una longitud mínima, combinaciones de caracteres mayúsculas, minúsculas, números, símbolos, prohibiendo el uso de información personal o palabras comunes, y promoviendo el cambio regular de contraseñas. Además, enfatizan la confidencialidad, instando a los usuarios a no compartirlas, escribirlas o almacenarlas de forma insegura, y a no reutilizarlas en múltiples servicios.
- **Políticas de acceso:** se basan en la idea del menor privilegio, asegurando que solo se den a los usuarios los permisos precisos para su trabajo. Esto requiere una autenticación fuerte, como la autenticación multifactorial, dar permisos según los roles, vigilar mucho las cuentas de administradores, regular el acceso remoto y usar cifrado para cuidar los datos en movimiento y guardados. También fijan acciones como bloquear cuentas después de varios intentos incorrectos.
- **Políticas de uso**: indican cómo los trabajadores deben usar los recursos tecnológicos de la compañía. Incluyen desde el uso ético y legal de software y hardware, hasta normas sobre el manejo del correo electrónico, la navegación web y los dispositivos móviles. Fomentan estar al tanto de peligros como el Phishing y lo importante que es la clasificación de la información. Algo esencial es la formación constante del personal para crear una cultura de seguridad y avisar de que el uso puede ser vigilado para asegurar que se cumple y que hay seguridad.

En conjunto, estas políticas forman un marco integral para minimizar los riesgos de seguridad, cumplir con las normativas y proteger los activos digitales de la organización

2.3.2.6.2 Normativas internacionales ISO/IEC 27001

El estándar internacional emitido por la ISO/IEC 27001 que describe cómo gestionar la seguridad en las organizaciones. La versión más reciente es de 2013 la primera versión es publicada en el año 2005 basada en las normas británicas BS 7799-2. Esta norma permite el aseguramiento, la confidencialidad, integridad y disponibilidad de los datos, así como los datos que se procesan. Permite a las organizaciones evaluar los riesgos y aplicar controles necesarios para reducirlos. La ISO/IEC 27001 se puede implementar en cualquier tipo de organización, privada, publica, pequeña, grande, permitiendo la certificación (Adriana, 2021).

2.3.2.7 Metodología

2.3.2.7.1 ISO/IEC 27031

Define la norma ISO/IEC 27031 es una norma internacional que proporciona directrices para la gestión de la continuidad de los servicios de Tecnologías de la Información y Comunicación (TIC), con el fin de asegurar que las organizaciones puedan prevenir, responder y recuperarse de incidentes que afecten la disponibilidad y continuidad de sus servicios tecnológicos críticos (ISO/IEC, 2011). las cuales conforma por cuatro Fases es Planificar , Implementar, revisar y mejorar (Lema Parco, 2025).

2.4 Conclusiones relacionadas al marco teórico

- En conclusión, contar con un Plan de Contingencia es fundamental para cualquier organización. Actúa como un escudo protector, permitiéndole anticipar y superar interrupciones. Este plan no es solo una reacción, sino una estrategia bien pensada que garantiza que las operaciones clave sigan funcionando, incluso cuando surgen problemas inesperados a través una evaluación de riesgos minuciosa, las instituciones universitarias pueden recuperarse rápidamente y mantener su estabilidad, asegurando su futuro en escenarios complejos.
- La seguridad de la información es absolutamente clave hoy en día. Se trata de proteger los datos para que sean confidenciales, íntegros y estén siempre disponibles. Para lograr esto, es esencial entender las amenazas y vulnerabilidades, y aplicar controles efectivos, tanto técnicos como de gestión. Adoptar buenas prácticas, como contraseñas robustas y el uso adecuado de los sistemas, es tan importante como seguir normas reconocidas como la ISO 27031. En definitiva, una buena seguridad informática no es solo para empresas, sino una habilidad crucial para proteger la información en nuestra día a día digital.
- Este proyecto se centró en la creación de un plan de contingencia enfocado en la seguridad lógica para los laboratorios lo principal fue buscar temas que nos lleven a la protección de los datos críticos, elevando la seguridad en los dispositivos y estableciendo un marco de respuesta ante riesgos. Además, este plan busca concienciar a los usuarios sobre las mejores prácticas de seguridad de la información.

CAPÍTULO III:

3 Marco investigativo

3.1 Introducción

En este capítulo se explica la metodología utilizada para llevar a cabo la investigación titulada “Plan de contingencia para seguridad de la información en los laboratorios de cómputo de la carrera de Ingeniería en Software de la ULEAM, Extensión El Carmen”. Para el desarrollo del estudio se aplicó un enfoque de tipo aplicado, con carácter exploratorio y un método de análisis cuantitativo, ya que estos permitieron obtener información precisa y confiable.

Aquí se describen de forma clara el tipo y diseño de investigación seleccionados, la población y muestra a la que se dirigió el estudio, así como las herramientas, técnicas y procedimientos empleados para la recolección de datos. También se explican los pasos seguidos para el análisis de la información, procurando que los resultados sean válidos, confiables y útiles para la elaboración de un plan que responda a las necesidades detectadas y que pueda implementarse dentro del entorno institucional.

3.2 Tipo de investigación

3.2.1 Investigación aplicada

La investigación aplicada es un tipo de estudio que se centra en solucionar problemas verdaderos y concretos, usando ideas ya existentes para generar soluciones funcionales. A diferencia de la investigación teórica, esta no solo intenta comprender, sino actuar, siempre respetando las leyes y reglas que organizan la sociedad. Como estudiantes, nos permite llevar lo aprendido en clase a la vida diaria, garantizando que nuestras ideas sean útiles y estén de acuerdo con el marco legal (Castro Maldonado et al., 2022).

La investigación aplicada desempeñó un papel crucial para la solución de un problema específico relacionado con la seguridad de la información en los laboratorios de cómputo de la carrera de Ingeniería de Software en la ULEAM, extensión El Carmen. Se diseñó un plan de contingencia basado en la norma ISO 27031 y se mejoró la continuidad de los servicios TIC. Esta investigación permitió examinar la situación actual, detectar peligros y con base en normas e ideas de seguridad informática, se propuso un plan funcional que protegió los equipos y la información. No solo se estudió el problema, sino que se diseñó una solución concreta que puede implementarse en la institución. Para llevar a cabo esta investigación, se realizó un

proceso de análisis apoyado en la recolección de datos, lo que permitió establecer mejoras y plantear normas de seguridad.

3.2.2 Exploratoria

La investigación exploratoria es un tipo de estudio que se usa cuando el tema a investigar no está bien definido o no hay suficiente información disponible. Su objetivo es ayudarme a entender mejor el problema, conocer el contexto y reunir datos generales que me permitan enfocarlo con mayor claridad. No busca comprobar hipótesis, sino más bien generar ideas, identificar posibles causas y preparar el camino para una investigación más profunda (Achiri Taipe et al., 2021).

Se aplicó la investigación exploratoria como una primera etapa. Esta me permite conocer y comprender la situación actual de los laboratorios, ya que no existe suficiente información previa sobre cómo se gestionan los riesgos de seguridad. A través de entrevistas informales, observación directa y revisión de documentos institucionales, identifico los problemas más comunes y las posibles amenazas. Esta fase exploratoria es fundamental para delimitar el problema,

3.2.3 Investigación Cuantitativa

Cuantitativa Utiliza la recolección y el análisis de datos cuantitativos para identificar patrones y validar hipótesis preestablecidas. Emplea métodos estadísticos para el análisis de los datos (Sanca Tinta, 2011).

En este trabajo se realizó un estudio de corte práctico y exploratorio, usando un método cuantitativo para obtener datos útiles que ayuden a hallar posibles soluciones. Para hacer esto, se preparó una encuesta enfocada a los alumnos y los docentes de Desarrollo de Software y Tecnología de la Información, para saber su grado de entendimiento sobre la seguridad en los laboratorios. Con los datos recopilados, se pudo identificar un porcentaje importante de asistencia, lo cual ayudó a entender mejor cómo ven los alumnos el peligro y el uso seguro de los equipos que utilizan en esos sitios

3.3 Método(s) de investigación

3.3.1 Inductivo

El método inductivo se basa en partir de observaciones específicas para llegar a conclusiones generales. Esto implica recopilar datos particulares y buscar patrones que ayuden a formular hipótesis o teorías (Prieto et al., 2028).

En la investigación se utilizó este método inductivo, el cual me permitió analizar las situaciones mediante la recolección de información concreta sobre los laboratorios, como los incidentes de seguridad que fueron reportados, las entrevistas realizadas a los usuarios y el análisis de los documentos relacionados. A partir de este análisis identifiqué patrones que me permitieron comprender mejor la situación y formular conclusiones relevantes.

3.3.2 Analítico y sintético

El método analítico consiste en descomponer un problema en sus partes para estudiarlas por separado, mientras que el método sintético integra y organiza esa información fragmentada para obtener una visión completa del fenómeno (del Cid Flores, 2021).

En el trabajo, utilizó el método sintético para unir y organizar los datos recolectados sobre riesgos, recursos y normativas. Esto me permite construir un plan de contingencia coherente y adaptado a los laboratorios de cómputo de la carrera de Ingeniería en Software de la ULEAM, Extensión El Carmen. De esta manera, convierto información dispersa en una propuesta clara y estructurada para mejorar la seguridad de la información

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias – Fuentes secundarias si es que aplica los cuestionarios de Encuesta y Entrevista -Observación /Otras

3.4.1.1 Encuesta

Una encuesta es una herramienta que permite recopilar información mediante la realización de preguntas a un grupo de personas. Su finalidad es conocer sus opiniones, actitudes o comportamientos respecto a un tema específico. Resulta especialmente útil para analizar la percepción de grandes grupos y detectar patrones o tendencias comunes. (Medina Romero et al., 2023).

En este estudio, la encuesta se aplicó a los estudiantes de las carreras de Tecnología de la Información y Desarrollo de Software, con el propósito de evaluar su conocimiento y percepción sobre la seguridad en los laboratorios. Se consideraron los posibles riesgos asociados al uso de estos espacios.

3.4.1.2 Entrevista

La entrevista es una técnica para obtener información mediante una conversación entre dos personas: el entrevistador, que formula las preguntas, y el entrevistado, que responde. Su objetivo es conocer opiniones o datos específicos sobre un tema, aprovechando la comunicación directa para profundizar en aspectos importantes (Loaza Carrasco y otros, 2023).

La entrevista resulta clave pues consiente examinar qué puntos precisan optimizarse dentro de una institución, tomando como base la información dada por quienes están directamente implicados. Mediante la entrevista que se le hizo al encargado de los laboratorios, Jean Carlos, se lograron recopilar datos sobre las deficiencias que hay en los laboratorios, lo cual colaboró a identificar las áreas que urgen ser optimizadas e instaurar acciones correctivas.

3.5 Estrategia operativa para la recolección de datos

3.5.1 Población - Segmentación - Técnica de muestreo - Tamaño de la muestra

3.5.1.1 Población

La población es el conjunto completo de elementos que comparten alguna característica importante para el análisis que se realiza. Estos elementos pueden ser personas, objetos, eventos, seres vivos o incluso documentos, como pueden ser historias clínicas o registros. La población representa a todos aquellos que están involucrados o afectados por el fenómeno que se está investigando, y es sobre este grupo que se busca recopilar información y datos para analizarlos y obtener conclusiones confiables. (Toledo, 2021).

Para este caso de estudio, la población está compuesta por los usuarios habituales de los laboratorios de cómputo, específicamente los estudiantes y docentes de las carreras de Ingeniería en Tecnología de la Información (TI) y de Ingeniería en Software. Estos laboratorios son sitios fundamentales para hacer tareas de los estudio, prácticas y trabajos junto al saber y al entrenamiento laboral. En la carrera de TI, hoy existen 69 alumnos inscritos, mientras que en la carrera de Desarrollo de Software el número llega a 159 alumnos. En suma, la gente que estudia y usa estos laboratorios suma 228 alumnos.

Ambos grupos utilizan principalmente los laboratorios 1 y 2, que funcionan bajo un horario establecido previamente para organizar el acceso y garantizar un uso eficiente de los recursos disponibles. Este horario es gestionado y supervisado por los docentes responsables de cada carrera, quienes se encargan también de coordinar las actividades que se realizan en estos espacios.

3.5.1.2 Muestra

En el campo del estudio científico, una muestra es como una parte elegida sacada de un grupo mayor, y su fin es ayudar a entender un hecho sin tener que mirar cada caso. Esta elección se hace cuando estudiar todo el grupo no se puede hacer por temas de tiempo o de dinero.

Para que las conclusiones obtenidas sean válidas y generalizables, es fundamental que la muestra se elija siguiendo criterios metodológicos rigurosos, que aseguren su pertinencia y representatividad respecto al fenómeno observado (Solanet i Grau, 2020).

Fórmula de muestra Población finita

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

Tamaño de la población: 243 $ N = 243 $

nivel de confianza del 95% equivale $ Z = 1.96 $

Proporción: 50% equivale $ p = 0.5 $ (proporción estándar para máxima variabilidad).

Margen de error: 5% $ e $: margen de error, que serán ajustado.

n 150 tamaño de muestra resultado

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.5.2.1 Encuesta

La encuesta estuvo estructurada en 10 preguntas cerradas, principalmente de selección múltiple. Estas se organizaron en tres dimensiones: seguridad de la información, gestión de riesgos y continuidad de los servicios TIC. El instrumento se aplicó a los estudiantes de la carrera de Tecnología de la Información e Ingeniería de Software de la ULEAM, Extensión El Carmen, con el propósito de obtener información precisa y detallada sobre las condiciones de seguridad en los laboratorios de cómputo.

La encuesta fue diseñada como un análisis libre con alternativas variadas y se usó mediante la herramienta Microsoft Forms, lo cual ayudó a tener un control bueno del grado de

involucramiento y a hacer más fácil el conteo de los datos recopilados Para repartir, el link de la encuesta se les envió a los presidentes de cada curso, quienes se ocuparon de darlo a sus compañeros para juntar las respuestas necesarias.

Esta herramienta resultó fundamental para obtener información relevante sobre la seguridad en los laboratorios, evidenciando un alto nivel de desconocimiento entre los estudiantes, lo que permitió enfocar el análisis y las acciones posteriores de la investigación

3.5.2.2 Entrevista

La entrevista estuvo conformada por 11 preguntas abiertas dirigidas al encargado de los laboratorios, orientadas a conocer la situación actual, los procedimientos existentes y las medidas aplicadas ante incidentes tecnológicos.

Este instrumento constituyó una herramienta fundamental para comprender de manera más profunda las condiciones de seguridad presentes en los laboratorios de cómputo. A través de su aplicación, se evaluaron los riesgos a los que están expuestos los equipos y la información que gestionan.

Los resultados obtenidos permitieron identificar el estado de las medidas de seguridad implementadas, tales como políticas, protocolos e infraestructura tecnológica. Asimismo, se evidenció la necesidad de fortalecer los procesos de capacitación del personal, con el fin de garantizar el conocimiento adecuado y una preparación oportuna frente a posibles riesgos o incidentes.

3.5.3 Plan de recolección de datos

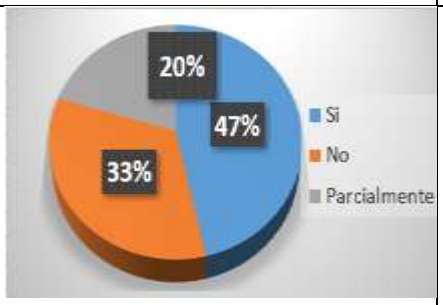
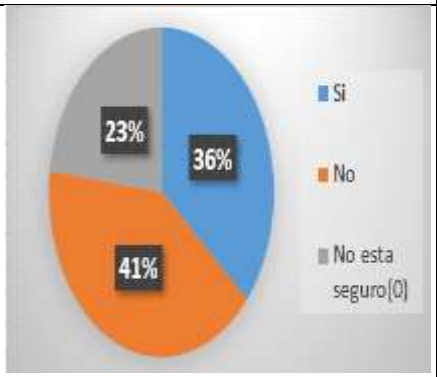
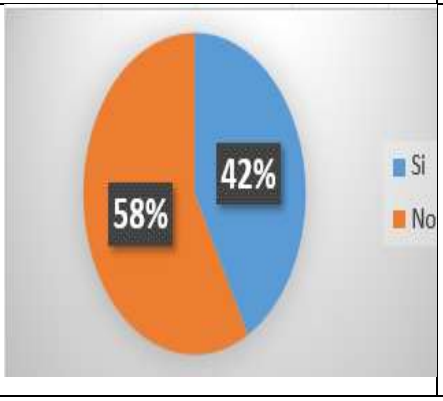
Responsable	Descripción	Actividad	Fecha
Diana Caza	Encuesta utilizada en Microsoft forms a los Estudiante de TI y Software	Aplicación de Encuesta	31-08-2025
Diana Caza	Entrevista presencial al Encargado de los laboratorios	Aplicación de Entrevista	29 -08-2025

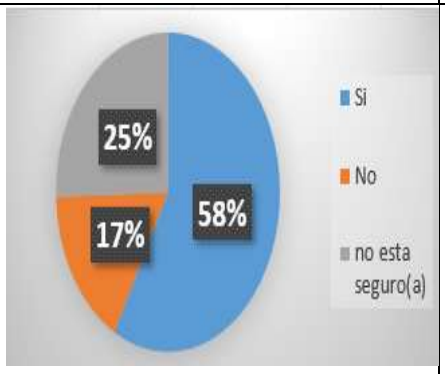
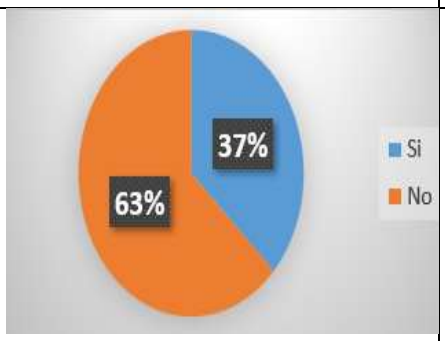
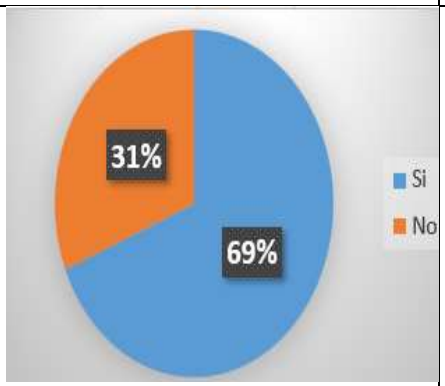
Tabla 1cronograma de recolección de datos

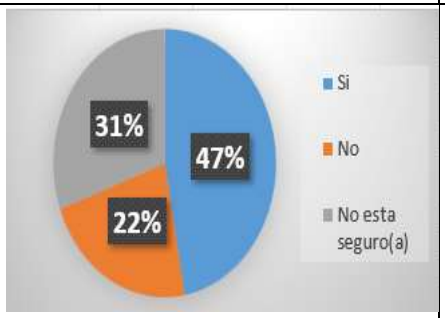
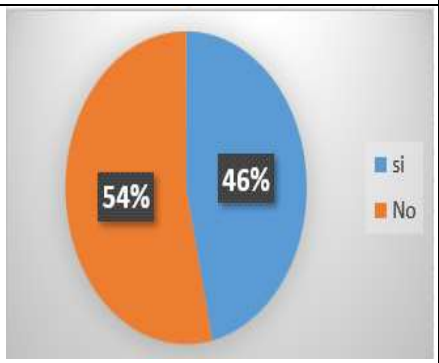
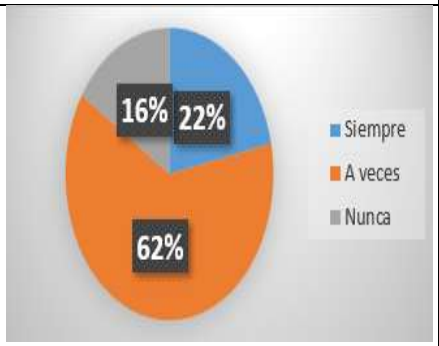
3.6 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos

3.6.1.1 Análisis de encuestas

Pregunta	Grafico	Interpretación
1.**¿Conoce usted las políticas de seguridad de la información implementadas en los laboratorios de cómputo?**		Casi la mitad de los estudiantes encuestados manifiestan conocer las políticas de seguridad de la información en los laboratorios de computo sin embargo la tercera parte de los encuestados no tiene conocimiento de las políticas de seguridad de la información no tiene ningún conocimiento.
2¿Considera que sus datos personales y académicos están protegidos al usar **los laboratorios de cómputo?**		Menos de la mitad de los estudiantes encuestados consideran que sus datos personales y académicos están protegidos al utilizar los laboratorios tomando en cuenta que casi la mitad de los estudiantes encuestados manifiestan que los datos no están protegidos tiene nivel de desconocimiento
3**¿Ha recibido alguna capacitación o charla informativa relacionada con la seguridad de la información en el uso d los laboratorios?**		Más de la mitad de los estudiantes encuestados han recibido algunas capacitaciones o charla informativa relacionada con la seguridad de la información en el uso de los laboratorios.

Pregunta	Grafico	Interpretación
4 ¿Considera que los equipos y el software de los laboratorios se encuentran actualizados y ofrecen un entorno seguro para trabajar?		La mayor parte de los estudiantes encuestados considera que los equipos y el software de los laboratorios se encuentran actualizados y ofrecen un entorno seguro para trabajar, sin embargo existe un porcentaje minoritario que manifiesta desconocimiento sobre las actualizaciones.
5¿Ha experimentado interrupciones en sus actividades académicas debido a problemas de seguridad de la información por ejemplo, virus, accesos no autorizados?		Un considerable porcentaje de encuestados Ha experimentado interrupciones en sus actividades académicas debido a problemas de seguridad de la información, por ejemplo, virus, accesos no autorizados tomando en cuenta que más de la mitad no ha tenido interrupciones en sus actividades académicas.
6 **¿Conoce usted las prácticas básicas para proteger su información personal y académica al utilizar los equipos de los laboratorios**		Los resultados evidencian que más de la mitad de los estudiantes encuestados demuestran que conocen las prácticas básicas para proteger su información personal y académica al utilizar los equipos de los laboratorios, Sin embargo, menos de la tercera parte no conoce de cómo proteger su información.

Pregunta	Grafico	Interpretación
7¿Considera que los laboratorios cuentan con los recursos necesarios para garantizar la seguridad de la información?		Se considera que la mayoría de n los encuestados reconoce que los laboratorios disponen de los recursos tecnológicos necesarios para las actividades académicas. La mitad de los encuestados responden de forma negativa entre no están seguros y considera que no hay seguridad.
8¿En caso de detectar un incidente de seguridad (como virus, accesos no autorizados, pérdida de información), ¿conoce el proceso para dar a conocer el incidente ?		Menos de la mitad de los estudiantes encuestados tiene conocimiento que en el caso de detectar un incidente de seguridad (como virus, accesos no autorizados, pérdida de información),si conoce el proceso para dar a conocer el incidente de los protocolos de detección y reporte de incidentes, sin embargo frente a más de la mitad que de cómo detectar un incidente de seguridad.
9¿Ha recibido instrucciones claras sobre cómo proteger la información en los laboratorios?		Una mínima parte de los encuestados Ha recibido instrucciones claras sobre cómo proteger la información en los laboratorios sin embargo más de la mitad de los encuestados indico que a veces dan instrucciones claras de cómo proteger la información.

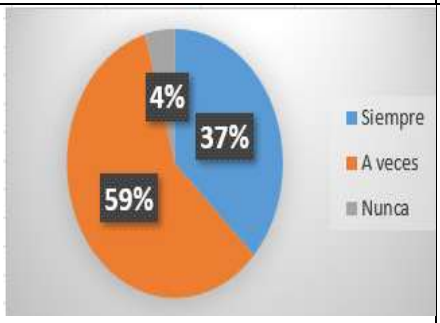
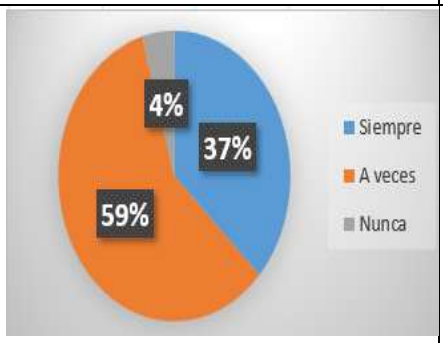
Pregunta	Grafico	Interpretación
10¿Consideras que el personal docente supervisa adecuadamente el uso seguro de los laboratorios?		Menos de la mitad de los estudiantes encuestados Consideras que el personal docente supervisa adecuadamente el uso seguro de los laboratorios sin embargo más de la mitad de los encuestados consideran que el personal docente no supervisa.
11¿Considera que las contraseñas que utiliza para acceder a los sistemas de los laboratorios son lo suficientemente seguras?		Menos de la mitad de los encuestados Considera que las contraseñas que utiliza para acceder a los sistemas de los laboratorios son lo suficientemente seguras tomando en cuenta que hay más de la mitad que considera que muchas veces no son seguras las contraseñas.

Tabla 2 resultado de la encuesta

3.6.1.2 Análisis de entrevista

Pregunta	Respuesta	Análisis
1¿Podría describir las políticas de seguridad de la información actualmente implementadas en los laboratorios de cómputo?	Actualmente no cuenta con política de seguridad.	considero preocupante que no existan políticas de seguridad, ya que esto puede afectar la protección de la información.
2 ¿Qué medidas preventivas se han tomado para evitar la pérdida de datos sensibles en los laboratorios?	Las políticas de seguridad que hay son general más solo no se cifran en los laboratorios.	Pienso que la falta de cifrado pone en riesgo los datos sensibles utilizados en los laboratorios.

Pregunta	Respuesta	Análisis
3¿Cómo se maneja la capacitación del personal y a los estudiantes en cuanto a la seguridad de la información en los laboratorios?	No se han capacitado.	Desde mi punto de vista, la ausencia de capacitación aumenta la posibilidad de errores y problemas de seguridad.
4 ¿Cuál es el proceso para la actualización de equipos y software en los laboratorios de cómputo y con qué frecuencia se realiza?	El proceso es cada inicio de semestre se hace una actualización que llega desde Manta y es una ISO 27001 que nos llegas desde de allá con los programa preinstalados.	Aunque se realizan actualizaciones semestrales, creo que deberían ser más frecuentes para evitar vulnerabilidades.
5 ¿Ha habido incidentes de interrupción de las actividades académicas debido a fallas de seguridad de la información en los últimos años? Si es así, ¿podría detallarlos?	No se han presentado.	El hecho de que no se hayan presentado incidentes es positivo, pero no garantiza que no existan riesgos.
6 ¿Existen protocolos específicos para el manejo de datos sensibles por parte de estudiantes y personal en los laboratorios?	No existe.	Considero que deberían existir protocolos claros para proteger la información sensible.
7 ¿Qué herramientas o software de seguridad se utilizan actualmente en los equipos de los laboratorios?	No solo el programa pre determinado que es el Windows defender en caso de antivirus.	Creo que depender solo de Windows Defender puede ser insuficiente para una protección adecuada.

Pregunta	Respuesta	Análisis
8 ¿Cómo se monitorea el cumplimiento de las políticas de seguridad por parte de los usuarios de los laboratorios?	No se realizan.	Pienso que el monitoreo es necesario para asegurar el buen uso de los recursos del laboratorio.
9 ¿Se realizan auditorías de seguridad de forma regular en los laboratorios? Si es así, ¿con qué frecuencia y cuáles son los hallazgos principales?	No existe.	Desde mi perspectiva, las auditorías ayudarían a detectar fallas y mejorar la seguridad.
10 ¿Qué mejoras o nuevas iniciativas considera prioritarias para fortalecer la seguridad de la información en los laboratorios a corto y mediano plazo?	Sería un proyecto a largo plazo ya que se necesitan crear las políticas internas de la seguridad de la información dentro de los laboratorios de la ULEAM.	Considero fundamental implementar políticas de seguridad lo antes posible.

Tabla 3 resultado de la entrevista

3.6.2 Presentación y descripción de los resultados obtenidos

De la respuesta a la pregunta 1 de la encuesta, se obtiene que menos de la mitad de los estudiantes manifiesta no conocer la política de seguridad. Por otro lado, el encargado de los laboratorios explicó en la pregunta 1 de la entrevista que el laboratorio no cuenta con políticas de seguridad establecidas.

En la pregunta 3 de la encuesta, más de la mitad de los estudiantes indicó no haber recibido capacitación relacionada con la seguridad de la información en el uso de los laboratorios. De manera similar, el encargado de los laboratorios señaló en la entrevista que actualmente no se han realizado capacitaciones sobre seguridad de la información.

Respecto a la pregunta 5 de la encuesta, menos de la mitad de los estudiantes reportó haber tenido inconvenientes en las actividades académicas. Sin embargo, el encargado de los

laboratorios manifestó en la entrevista que no se han presentado inconvenientes y que los dispositivos funcionan con normalidad.

Al final, en la pregunta 6 de la encuesta, los alumnos dijeron que hay una falta común sobre cómo proteger los datos básicos. Así, la respuesta a la pregunta 6 de la entrevista dice que no hay norma fija para usar datos, lo cual muestra las falencias actuales y la necesidad de implementar medidas para proteger los datos.

3.6.3 Informe final del análisis de los datos

Los datos obtenidos mediante las encuestas y entrevistas permiten identificar un nivel preocupante en cuanto a la seguridad de la información en los laboratorios. Tanto los cuestionarios como las entrevistas coinciden en señalar la falta de protocolos establecidos que garanticen la protección adecuada de los datos. En particular, se destaca la ausencia de personal encargado específicamente de supervisar el cumplimiento de las normas de seguridad.

La entrevista con el docente encargado de los laboratorios confirmó que no existe normas claras y evidenció la necesidad de implementar medidas concretas para proteger la información de la institucional.

Por lo expuesto, se justifica plenamente la realización de este proyecto de titulación, ya que, a partir de los resultados obtenidos y las investigaciones realizadas, se podrá abordar y mejorar las deficiencias detectadas, tomando en cuenta especialmente las observaciones surgidas durante la entrevista.

CAPÍTULO IV:

4 Marco propositivo

4.1 Introducción

En el presente capítulo se desarrolla el diseño de un plan de contingencia para seguridad de información en los laboratorios de cómputo de la carrera de ingeniería en software de ULEAM extensión El Carmen. basándose en la seguridad lógica en el cual se desarrollará en los laboratorios 1 y 2 de la carrera software en la cual se evalúa el nivel de conocimiento de los estudiantes de ambas carreras tomando en cuenta se utilizará la metodología ISO/IEC27031 La metodología planteada es completa y facilita la anticipación y mitigación de posibles riesgos.

4.2 Descripción de la propuesta

En la presente propuesta se desarrolla un Plan de Contingencia para la Seguridad de la Información aplicado a los laboratorios de cómputo de la carrera de Ingeniería en Software de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen. El plan fue elaborado a partir de una auditoría con enfoque lógico y sistemático, cuyo propósito es garantizar la recuperación de la información y prevenir riesgos asociados a la pérdida, robo o uso indebido de los datos.

Para la elaboración del plan se empleó la metodología ISO/IEC27031 la cual permitió identificar, analizar y evaluar los riesgos presentes en los procesos tecnológicos, anticipar posibles incidentes y fortalecer las medidas preventivas y de respuesta, contribuyendo así a la continuidad y seguridad de los servicios TIC.

4.3 Determinación de recursos

4.3.1 Humanos

La siguiente tabla se detalla los recursos humanos que son parte del desarrollo del proyecto de titulación donde se especifica los roles que cumplen lo cual fue parte imprescindible para llevar la responsabilidad a lo largo de mi proyecto de titulación.

Recursos	**Función**	**Actividad**
Ing. Clara Pozo Hernández	Tutora	Participo desde el inicio de mi trabajo de titulación cual tomo un papel fundamental ser mi guía durante el proceso de titulación.

Ing. Jean Carlos Cedeño	Encargado de los laboratorios de la carrera TI y SW	Participo en la parte más importante dándome a conocer por medio de una entrevista fue Informante responsable de los laboratorios.
228 estudiantes	Estudiantes de la carrera de tu y software	Participaron en la parte de la encuesta cual se realizó en forms.
Diana Caza Romero	Investigadora	Realizando el proyecto integrador.

Tabla 4 Recurso humano

4.3.2 Tecnológicos

En esta tabla de recursos tecnológico se detallará las herramientas informáticas y de comunicación que fueron fundamentales para poder realizar cada proceso del proyecto de titulación del plan de contingencia para la seguridad de los laboratorios.

Cantidad	**Recurso**	**Actividad**
1	Laptop RYZEN 5 de 7000 series.	Es el material importante porque con esta herramienta me permite desarrollar el proceso de mi proyecto realizado paso a paso.
1	Teléfono móvil Redmi note 12 con grabado de voz y con cámara.	Esta herramienta nos perite poder tener evidencias visuales y grabación. también documentos importantes.
6 meses	Conexión a internet.	Recurso importante para buscar información.
1	Impresora Epson Smart panel.	Esta herramienta se utilizó para imprimir las preguntas para la entrevista.
1	Paquetes de Microsoft office.	Este paquete Microsoft se utilizó para el desarrollo de mi tesis con el Word y el Excel para ingresar datos y hacer grafica.

Tabla 5 Recurso Tecnológico

4.3.3 Económicos (presupuesto)

Se detalla el presupuesto de los materiales que se va a invertir para ser la auditoria de plan de contingencia

Cantidad	Descripción	Precio	Total
1	Laptop RYZEN 5 de 7000 series	600	600
1	Teléfono móvil Redmi note 12	300	300
7 meses	Servicio de internet	26	182
28 de viaje	Bus	0.80	22.40
2	Esfero	0.40	0,80
50	Impresiones	0.50	25

Tabla 6 Presupuesto Económico

4.4 Etapas de acción para el desarrollo de la propuesta

4.4.1 Programa de auditoría

Programa para elaboración de Plan de contingencia para seguridad de información en los laboratorios de cómputo de la carrera de Ingeniería Software en ULEAM Extensión El Carmen.		
Objetivos • Identificar riesgos de seguridad de la información en los laboratorios de cómputo de la carrera de Ingeniería en Software – ULEAM Extensión El Carmen, aplicando la metodología ISO/IEC 27031. • Desarrollar un plan de contingencia para garantizar la continuidad y protección de los datos fundamentales.		
Técnicas y Procedimientos	Ref.a papel	Fecha
• **Revisión de la metodología ISO/IEC 27031** • **Fase de Planificación** o Determinar los activos relevantes de la empresa o Valoración de riesgos o Determinar las amenazas a los que están expuestos los activos o Estimar los impactos potenciales y residuales	4411 4412 44131 4414 4415 4416 4417 51211	 03-10 -2025 04-10-2025 06-10-2025 10-11-2025 18-11-2025 26-11-2025

○ Estimar las salvaguardas de los activos • **Fase de Implementación y Operación**. ○ Elaborar el documento formal del Plan de Contingencia TIC (propósito, alcance, roles y responsabilidades). ○ Establecer el plan de comunicación y de respuesta ante incidentes ○ Capacitación del personal y estudiantes: ○ Pruebas de respaldo y recuperación: ○ Documentación operativa	51212 51213 51214	2-12-2026 3-12.2026 4-12-2026

4.4.1.1 Desarrollo

4.4.1.2 Revisión de la metodología ISO/IEC 27031

La preparación para la continuidad de los servicios de Tecnologías de la Información y la Comunicación ante posibles incidentes o desastres. Esta norma permitió aplicar principios, procesos y estrategias orientadas a mantener la disponibilidad, integridad y confidencialidad de la información, incluso en situaciones adversas.

Mediante su aplicación, se identificaron los activos críticos de los laboratorios de cómputo, se evaluaron los riesgos asociados a la interrupción de las operaciones y se definieron los procedimientos de respuesta, recuperación y las responsabilidades del personal, con el propósito de minimizar el impacto de los incidentes.

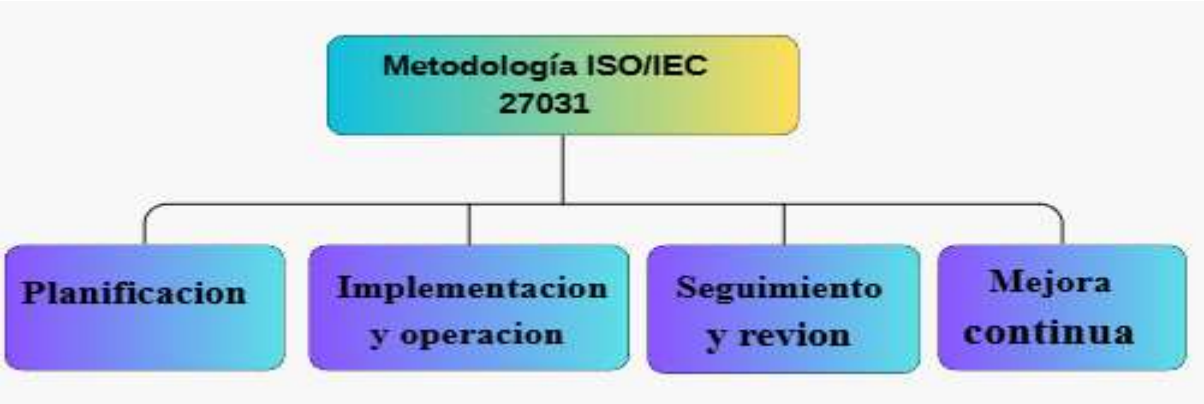


Ilustración 3 fases de la metodología ISO/IEC 27031

4.4.1.3 Planificación

4.4.1.3.1 Determinar los activos relevantes de la empresa

4.4.1.3.1.1 Activos físicos

En la tabla 7 se identifican los principales activos de los laboratorios de cómputo, incluyendo computadoras de escritorio, sus características técnicas, ubicación y periféricos. Esta información es clave para garantizar el correcto funcionamiento de los servicios y la seguridad de los datos.

Ubicación de laboratorio 1 201						
N	**Código de serie**	**Nombre de Activo**	**Descripción Técnicas**	**Periféricos Asociados**	**Marca**	**Modelo**
01	074213	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Teclado genérico y Mouse Genius	LG	19EN336
02	074504	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Genius	ASUS	VP228
03	074507	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor Dell, Teclado y Mouse Genius	Dell	E1913FS
04	074497	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Speedmind	ASUS	VP228
05	074385	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Adikt@	ASUS	VP228
06	074381	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Mouse y Speedmind Teclado Genius	ASUS	VP228
07	074494	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Speedmind	ASUS	VP228
08	074479	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Mouse y Sin Teclado	LG	VP228
09	074506	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Teclado y Mouse genius	LG	20MK400H-B
10	074496	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Speedmind	ASUS	VP228
11	074501	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado Speedmind y sin Mouse	ASUS	VP228
12	074500	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS , Teclado y Mouse Genius	ASUS	VP228
13	074503	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Moditor ASUS, Teclado Speedmind y mouse adikt@	ASUS	VP22

14	074502	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Mouse Genius y Teclado Speedmind	ASUS	VP228
15	074499	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Genius	ASUS	VP228
16	074405	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado Speedmind y Mouse genius	Asus	VP228
17	074534	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Mouse Genius y teclado Speedmind	LG	W1742ST
18	072002	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitto BENQ, Teclado y Mouse Genius	BENQ	ET-002-B
19	074397	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Tclado Y Mouse Speedmind	ASUS	VP228
20	074095	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado genérico y Mouse Tech	ASUS	VP228
21	074079	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monotor ASUS, Mouse Genius y Teclado Speedmind	ASUS	VP228
22	074408	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Genius	ASUS	VP228
23	074412	Computada de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Speedmind	ASUS	VP228
N	**Código de serie**	**Nombre de Activo**	**Descripción Técnicas**	**Periféricos Asociados**	**Marca**	**Modelo**
24	074498	Computadora	Procesador Intel i7, Ram 16MG.	Teclado y Mouse Genius	ASUS	VP228
25	073816	Rack	Estructura metálica para organizar equipos de TI (servidores, red).	Switches, Routers y Cableado	Microtk	Crs326-24g-24s+rm
26	077184	Aire Acondicionado	Controla la temperatura lo que protege a los equipos	Filtros de Aire	Green Air	Lmvc060cc201
27		Proyector	Proyección de imágenes o video desde la computadora	Contol	Epson	EX9240

Ubicación de laboratorio 2 209

N	**Código de serie**	**Nombre de Activo**	**Descripción Técnicas**	**Periféricos Asociados**	**Marca**	**Modelo**

28	31120	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor	Dell	D17S
29	31115	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
30	31133	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
31	31119	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
32	31130	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
33	31134	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
34	31116	Computadora de escritorio	Procesador i7,Ram 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
35	31127	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
36	31118	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
37	31125	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
38	31123	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
39	31131	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
40	31129	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
41	31126	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
42	31128	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
43	31122	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
44	31132	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
N	**Código de serie**	**Nombre de Activo**	**descripción Técnicas**	**Periféricos Asociados**	**Marca**	**Modelo**
45	31121	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S
46	31125	Computada de Escritorio	Procesador i7, RAM 16MG	Mouse, Teclado y Monitor Dell	Dell	D17S

47	072001	Rack	Estructura metálica, conexión redundante de energía	Switches, Routers y Cableado	Microtk	Crs326-24g-24s+rm
48	No tiene	Aire Acondicionado	Sistema de climatización para salas de servidore	Filtros de Aire Control	Green Air	Lmvc060cc201
49	074483	Proyectores	Proyector HD, conectividad HDMI y Wi-Fi	Cables de conexión y Control	Epson	EX9240

Tabla 7 identificación de activos

4.4.1.3.1.2 Activos lógicos

En la tabla 8 se obtienen los activos lógicos.

Código	**Activo Lógico Identificado**	**Ubicación Equipo Asociado**	**Descripción o Función**	**Usuarios**	**Estado Actual**	**Licencia Versión**
Al -01	Sistema Operativo Windows 11	Desde la A1asta la A 20 tienen los equipos	Sistema base para ejecución de software educativo	Estudiantes	Operativo	Licencia institucional
AL-02	Microsoft Office	Todos los equipos	Paquete ofimático para tareas académicas	Usuarios del laboratorio	Operativo	Licencia institucional
AL-03	antivirus	servidor principal	protección contra malware y ataques	departamento ti	Activo	versión 10.5
AL-04	Base de Datos Académica (MySQL)	Servidor académico	Almacena registros de estudiantes	Administrador de sistemas	Activo	MySQL 8.4.6 (LTS)
AL-05	Configuración de Red VLAN	Switch central	Segmenta tráfico por áreas	Técnico de redes	Vigente	NA

Tabla 8 identificación activos lógico

4.4.1.4 Valoración de activos

La siguiente tabla 9 presenta la valoración de activos según su nivel de riesgo, permitiendo identificar la gravedad de posibles incidentes que afecten la seguridad de la información y la continuidad operativa de los laboratorios de cómputo.

VA	Valor del Activo	Descripción
1	**Muy Bajo**	Activo con escasa relevancia en la gestión de información. Su pérdida no afecta los procesos académicos ni la seguridad de los datos.
2	**Bajo**	Activo afecta mínimamente las operaciones, puede volver a su estado sin intervenir con la continuidad del servicio.
3	**Medio**	Activo necesario para el funcionamiento regular de los sistemas informáticos. Su ausencia momentánea puede impactar de manera parcial las labores académicas o administrativas.
4	**Alto**	Activo fundamental para la protección o manejo de información sensible. Su mal funcionamiento se detiene el procedimientos críticos y demanda intervención urgente.
5	**Muy Alto**	Activo Es crítico para la institución; su pérdida genera graves consecuencias operativas, económicas o legales en el funcionamiento de los laboratorios, afectando de manera grave el rendimiento académico.

Tabla 9 Valor de Activo

Se realizó la evaluación de los activos de acuerdo con su nivel de criticidad, conforme a lo establecido en la Tabla 10.

Tipo de activo	Ubicación	Valor			
		D	I	C	VA
Sistema Operativo Windows/Linux	Lab1	5	4	4	4.3
Software de gestión académica	Lab1	5	5	5	5.0

Aplicaciones de programación (IDE, compiladores)	Lab1	3	4	4	3.6
Base de datos institucional	Lab1	5	5	5	5.0
Herramientas ofimáticas	Lab1	4	3	3	3.3
Sistema de copias de seguridad (Backups)	Lab1	5	5	4	4.6
Antivirus / Sistema de seguridad informática	Lab2	4	4	4	4.0
Software de control de red (Firewall, Router virtual)	Lab2	4	5	4	4.3
Acceso a las plataformas académicas	Lab2	4	4	4	4.0
Documentos digitales y reportes académicos	Lab2	3	4	4	3.6
Pantallas	Lab2	3	3	3	3.0
Computadoras	Lab2	5	4	4	4.3

Tabla 10 Valoración de activos

4.4.1.5 Determinar las amenazas a los que están expuestos los activos

La Tabla 11 presenta la identificación de las amenazas a las que se encuentran expuestos los activos de los laboratorios de cómputo. Este análisis constituye un elemento fundamental dentro del proceso de gestión de riesgos, ya que permite identificar los posibles eventos que podrían afectar la operatividad, disponibilidad e integridad de los recursos tecnológicos. De igual manera, ayuda en el desarrollo de tácticas preventivas y correctivas que fortalecen el plan de contingencia.

Activos Lógicos	**Amenazas**
Sistema operativo (Windows/Linux)	Malware robo daño de equipo
Software académico (licencias y programas de laboratorio)	Malware robo daño de equipo
Base de datos de usuarios o estudiantes	Datos de equipo, robo
Servidor de respaldo (backups)	Daño malware
Red local (LAN/Wi-Fi)	Daño robo
Sistema operativo (Windows/Linux)	malware, daño
Documentos digitales y reportes académicos	Daño, Robo
Pantallas	Daño, Robo

Computadoras	Daño, Robo, Malware

Tabla 11 Identificando los posibles riesgos

4.4.1.5.1 Elaboración de instrumentos

Para la presente investigación, se elaboraron tres cuestionarios de evaluación de riesgos basados en la norma ISO/IEC 27031, enfocados en las amenazas de robo, daño de equipos y malware. Cada instrumento incluyó 25 preguntas tipo sí y no, orientadas a verificar los controles de confidencialidad, integridad y disponibilidad de la información.

Los resultados permitieron determinar el nivel de exposición e impacto de los riesgos, facilitando la priorización de medidas preventivas y correctivas en los laboratorios de cómputo

Cuestionario para Analizar Riesgos			C1 1-3
Preguntas (Malware)	**Respuesta**		**Observaciones**
	Si	**No**	
1. ¿Existe una política de seguridad definida para la protección contra malware?			
2. ¿Se cuenta con un software antivirus actualizado en los equipos del laboratorio?			
3. ¿Los usuarios tienen restricciones para la instalación de software no autorizado?			
4. ¿Se realizan análisis periódicos para detectar posibles infecciones?			
5. ¿Existen medidas para prevenir ataques de phishing dentro de la red del laboratorio?			
6. ¿Se cuenta con control de acceso para evitar el uso no autorizado de los dispositivos?			
7. ¿Los sistemas operativos están actualizados con parches de seguridad?			
8. ¿Se han identificado incidentes previos de malware en el laboratorio?			
9. ¿Los estudiantes reciben capacitación sobre buenas prácticas de seguridad informática?			
10. ¿Las redes Wi-Fi cuentan con medidas de protección contra accesos no autorizados?			
11. ¿Se utilizan herramientas de monitoreo para detectar comportamiento sospechoso en los equipos?			
12. ¿Existe un procedimiento de respuesta en caso de infección por malware?			
13. ¿Se aplican filtros de contenido para prevenir el acceso a sitios maliciosos?			
14. ¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?			
15. ¿El tráfico de red es monitoreado para detectar actividad sospechosa?			
16. ¿Los dispositivos USB están restringidos para evitar infecciones?			
17. ¿Los archivos de descarga son verificados antes de su uso?			
18. ¿Se han realizado auditorías previas que detecten vulnerabilidades en la lógica de seguridad?			
19. ¿Existen políticas de gestión de actualizaciones para reducir riesgos de infección?			
20. ¿Se implementan registros de actividad para identificar intentos de acceso sospechosos?			
21. ¿Los accesos a cuentas institucionales están protegidos con autenticación de múltiples factores?			
22. ¿Los servidores del laboratorio tienen protecciones específicas contra ataques externos?			
23. ¿Se han documentado procedimientos de limpieza y eliminación de malware en los equipos?			
24. ¿Se cuenta con herramientas de análisis forense para detectar el origen de una infección?			
25. ¿Las medidas de seguridad actuales han sido probadas mediante pruebas de penetración?			
Realizado por **Fecha:**			
Revisado por: **Fecha:**			

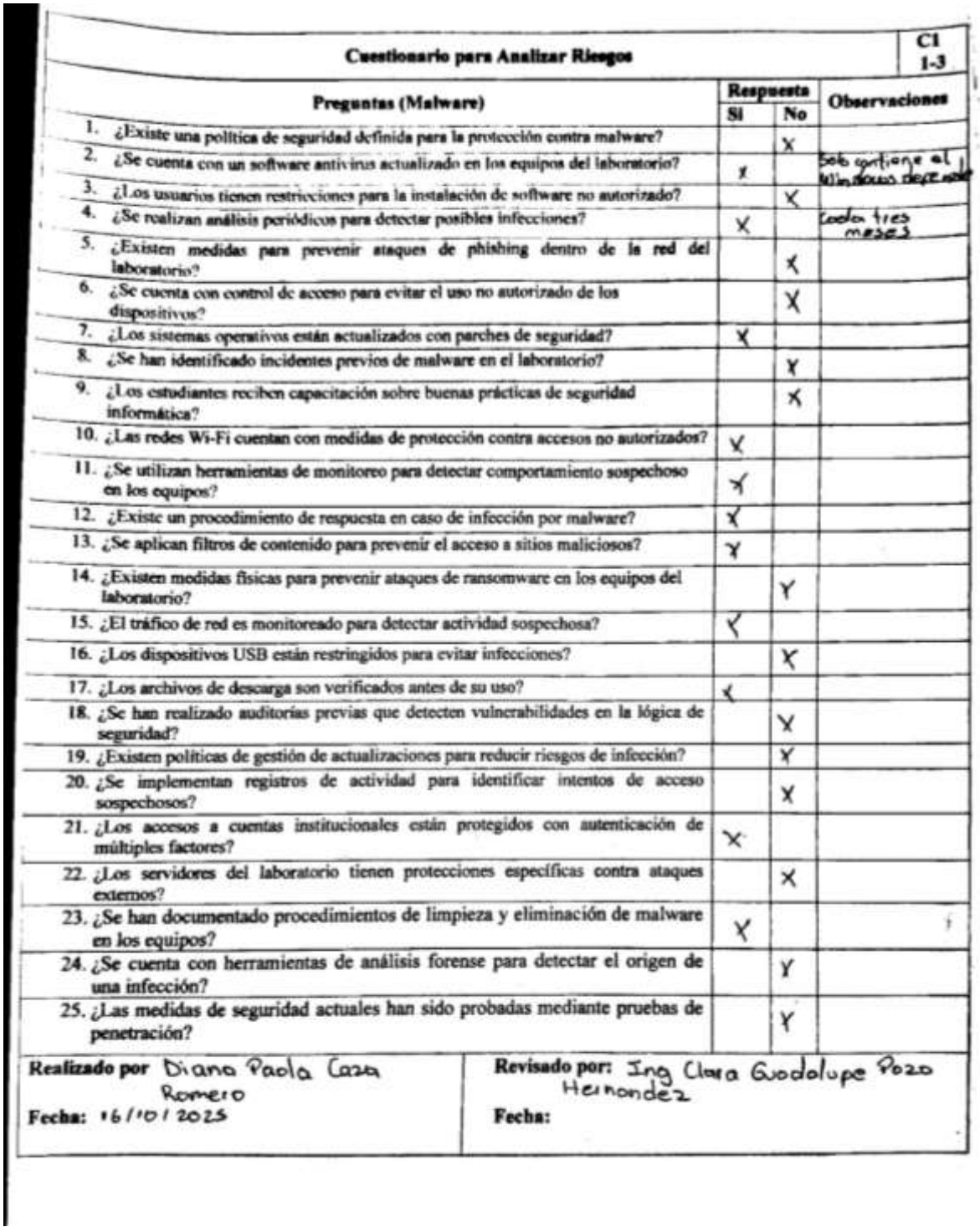
Ilustración 4 *instrumento*

4.4.1.5.2 Ejecución

Una vez elaborados los instrumentos de evaluación, se aplicaron en los laboratorios de cómputo con el fin de identificar riesgos. Se realizó una inspección técnica para verificar los controles de seguridad físicos y lógicos, así como una entrevista al encargado, quien aportó información sobre las condiciones operativas y de seguridad de los equipos.

A través de la evaluación y las respuestas recibidas, se finalizaron los formularios sobre robo, daño a equipos y malware, lo que facilitó el análisis de la situación actual de las medidas de control puestas en marcha. Asimismo, se llevó a cabo un cuestionario técnico de 25 preguntas con la colaboración del coordinador del programa, lo que ayudó a detectar peligros y a establecer un diagnóstico global del grado de seguridad de la infraestructura tecnológica.

Ilustración 5 entrevista al encargado



Cuestionario para Analizar Riesgos			C1 1-3
Preguntas (Malware)	**Respuesta**		**Observaciones**
	Si	**No**	
1. ¿Existe una política de seguridad definida para la protección contra malware?		X	
2. ¿Se cuenta con un software antivirus actualizado en los equipos del laboratorio?	X		Solo cuenta el Windows Defender
3. ¿Los usuarios tienen restricciones para la instalación de software no autorizado?		X	
4. ¿Se realizan análisis periódicos para detectar posibles infecciones?	X		Cada tres meses
5. ¿Existen medidas para prevenir ataques de phishing dentro de la red del laboratorio?		X	
6. ¿Se cuenta con control de acceso para evitar el uso no autorizado de los dispositivos?		X	
7. ¿Los sistemas operativos están actualizados con parches de seguridad?	X		
8. ¿Se han identificado incidentes previos de malware en el laboratorio?		X	
9. ¿Los estudiantes reciben capacitación sobre buenas prácticas de seguridad informática?		X	
10. ¿Las redes Wi-Fi cuentan con medidas de protección contra accesos no autorizados?	X		
11. ¿Se utilizan herramientas de monitoreo para detectar comportamiento sospechoso en los equipos?	X		
12. ¿Existe un procedimiento de respuesta en caso de infección por malware?	X		
13. ¿Se aplican filtros de contenido para prevenir el acceso a sitios maliciosos?	X		
14. ¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?		X	
15. ¿El tráfico de red es monitoreado para detectar actividad sospechosa?	X		
16. ¿Los dispositivos USB están restringidos para evitar infecciones?		X	
17. ¿Los archivos de descarga son verificados antes de su uso?	X		
18. ¿Se han realizado auditorías previas que detecten vulnerabilidades en la lógica de seguridad?		X	
19. ¿Existen políticas de gestión de actualizaciones para reducir riesgos de infección?		X	
20. ¿Se implementan registros de actividad para identificar intentos de acceso sospechosos?		X	
21. ¿Los accesos a cuentas institucionales están protegidos con autenticación de múltiples factores?	X		
22. ¿Los servidores del laboratorio tienen protecciones específicas contra ataques externos?		X	
23. ¿Se han documentado procedimientos de limpieza y eliminación de malware en los equipos?	X		
24. ¿Se cuenta con herramientas de análisis forense para detectar el origen de una infección?		X	
25. ¿Las medidas de seguridad actuales han sido probadas mediante pruebas de penetración?		X	

Realizado por Diana Paola Caza Romero
Fecha: 16/10/2025

Revisado por: Ing Clara Guadalupe Pozo Hernandez
Fecha:

Ilustración 6Checklist respuesta obtenidas

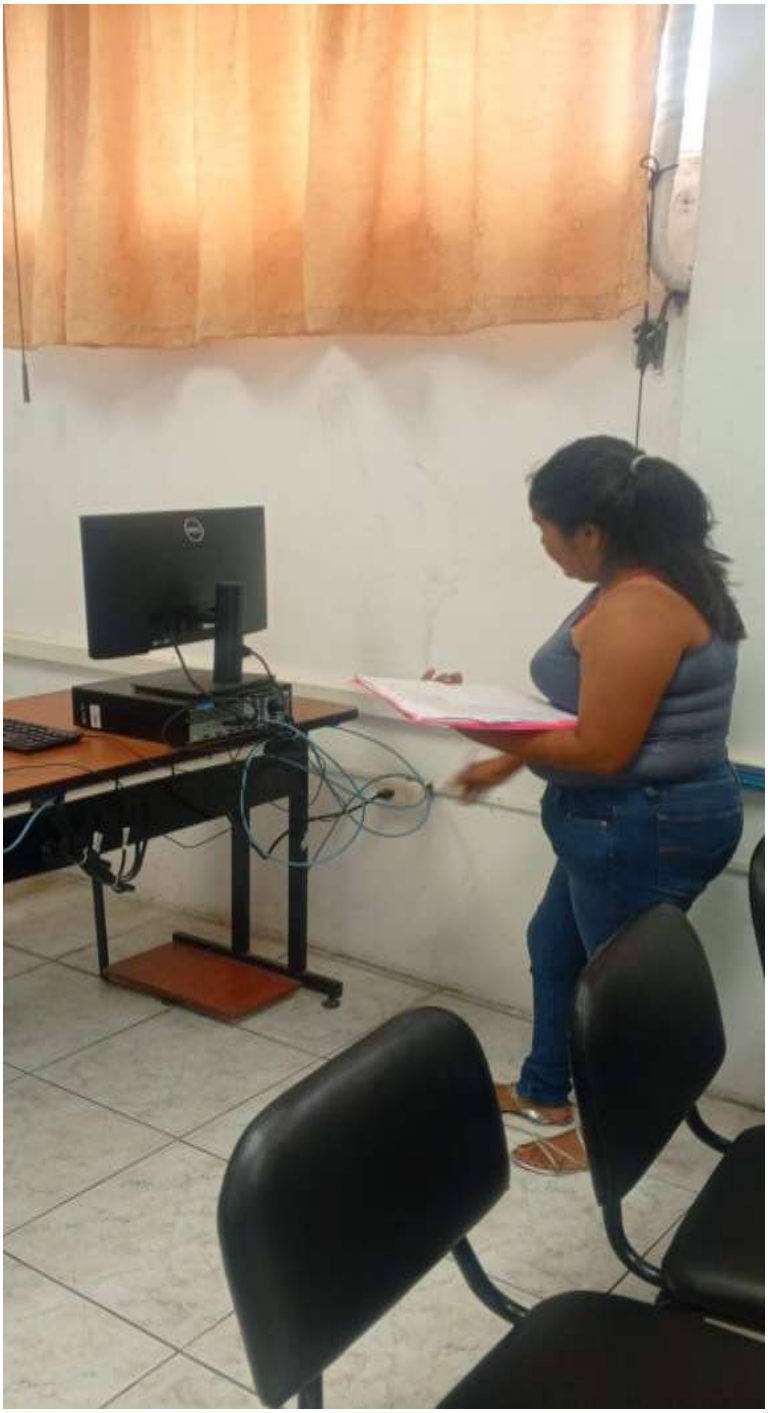


Ilustración 7 inspección de equipos para controlar el estado del equipo y su seguridad informática.

4.4.1.6 Tabulación

Para la tabulación de los resultados se utilizó Microsoft Excel, lo que permitió organizar y sistematizar los datos obtenidos de la matriz de evaluación de controles de seguridad en los laboratorios. Con el apoyo del coordinador académico se validó la información recopilada.

El estudio se llevó a cabo utilizando un formato organizado en el que se anotaron todas las interrogantes y sus respectivas respuestas, asignando los siguientes valores: 0 = Riesgo, 1 = Seguridad y 2 = No aplica.

La utilización de Excel hizo más sencillo el tratamiento exacto de la información y ayudó a determinar el grado de unión de medidas de seguridad en los laboratorios de informática.

Valoración	Niveles
0	Riesgo
1	Seguridad
2	No aplica

Tabla 12 tabla de valoración de nivel de riesgo

Se empleó la siguiente escala de valoración para la obtención y análisis de resultados, la cual permitió clasificar los equipos según su nivel de riesgo y estado de funcionamiento. Los resultados obtenidos se presentan en la ilustración 12.

	RIESGO ROBO			
N	PREGUNTA	lab1	lab 2	0
1	¿Existe cámara de seguridad instalada en el laboratorio?	1	1	1
2	¿Las cámaras de seguridad están funcionando correctamente?	1	1	2
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?	1	1	
4	¿Existe responsable de la seguridad de los laboratorios?	1	1	
5	¿Existen procedimientos para reportar un robo?	1	1	
6	¿Se han registrado incidentes previos de robo en los laboratorios?	2	2	
7	¿Los activos del laboratorio cuentan con medidas de protección física actualme	1	0	
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?	2	1	
9	¿Los equipos están identificados con códigos o etiquetas?	0	1	
10	¿Se mantiene un registro actualizado de las personas que acceden a los laborat	1	0	
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta área?	1	0	
12	¿Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus	2	2	
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorio	2	2	
14	¿Hay restricciones para la salida de equipos del laboratorio?	1	1	
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?	1	1	
16	¿Se verifica el estado y funcionamiento de los equipos físicos en el laboratorio?	1	1	
17	¿Existe un sistema de comunicación rápida para reportar incidentes?	1	1	
18	¿Los accesos principales están bajo vigilancia constante?	0	0	
19	¿Se cuenta con sistemas de alarma en los laboratorios?	0	0	
20	¿Los equipos están atados o asegurados básicamente?	2	0	
21	¿Se han registrado informes de robo recientemente?	2	0	
22	¿Hay dispositivos de rastreo en los equipos?	2	0	
23	¿Los laboratorios tienen sensores de movimiento?	1	1	
24	¿Existen protocolos claros para la investigación de incidentes?	0	0	
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?	1	1	
	TOTAL CONTROLES NO APLICADOS:	7	3	
	TOTAL DE CONTROLES EVALUADOS	18	22	
	TOTAL CONTROLES SEGURIDAD:	14	13	
	TOTAL CONTROLES RIESGO:	4	9	
	PORCENTAJE SEGURIDAD	78%	59%	68%
	PORCENTAJE RIESGO	22%	41%	32%
		100%	100%	

Ilustración 8 tabulación de resultado

Para la elaboración de la matriz de riesgos, se tomó como punto de partida el nivel de impacto, considerado un parámetro esencial dentro del proceso de evaluación. Este nivel fue determinado con base en los criterios previamente definidos, los cuales se detallan a continuación.

Valor de Impacto	Descripción
1	No afecta las actividades; los procesos continúan con normalidad y sin alteraciones.
2	Causa efectos menores que no interrumpen el desarrollo normal de las actividades.
3	Provoca una interrupción parcial, rápida y controlada que afecta temporalmente las operaciones.
4	Provoca una perturbación noble que interrumpe temporalmente las actividades institucionales.
5	Genera un impacto severo que paraliza totalmente las operaciones, ocasionando pérdidas críticas.

Tabla 13Valoracion de impacto

El nivel de impacto se determinó aplicando los parámetros definidos previamente, evaluando los riesgos de daño de equipos, malware y robo en función de las dimensiones de confidencialidad, disponibilidad e integridad de los activos. Los resultados obtenidos se muestran en la siguiente tabla:

riesgos	CONFIDENCIALIDAD	DISPONIBILDAD	INTEGRIDAD	PROMEDIO
DAÑO DE EQUIPOS	1	3	4	3
MALWARE	5	5	5	5
ROBO	4	4	3	4

Tabla 14nivel de impacto

Para la valoración del riesgo, se consideraron los porcentajes obtenidos en los controles asociados a los riesgos identificados, tales como robo, daño de equipos y malware. Con base en los cuestionarios aplicados en los laboratorios 1 y 2, se obtuvo un promedio general de los resultados, el cual permitió identificar el nivel de exposición de cada amenaza.

Posteriormente, estos valores fueron analizados conforme a una escala de clasificación establecida según el rango porcentual correspondiente, tal como se presenta en la siguiente tabla:

ESCALA PARA ASIGNAR VALOR DE APARICIÓN		
NIVEL DE APARICIÓN (PROBABILIDAD)		
1	MAS BAJO	1%-10%
2		10%-30%
3		30%-50%
4		50%-75%
5	MÁS ALTO	75%-100%

Tabla 15nivel de probabilidad

A continuación, se presenta la matriz de riesgos, la cual relaciona el nivel de impacto con la probabilidad de ocurrencia, considerando los valores previamente calificados. Esta herramienta permite visualizar y clasificar los riesgos según su nivel de gravedad, tal como se muestra en la siguiente tabla:

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

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Tabla 16 clasificar los riesgos según su nivel de gravedad

Una vez determinada la probabilidad y la gravedad (impacto), se calculó el nivel de riesgo mediante la multiplicación de ambos valores. Este resultado permitió clasificar cada amenaza según su nivel de criticidad, facilitando la priorización de medidas preventivas y correctivas dentro de los laboratorios de cómputo

MATRIZ DE RIESGOS				
RIESGO	**Aparición** probabilidad	**Gravedad (Impacto)**	**Valor del Riesgo**	**Nivel de Riesgo**
DAÑO DE EQUIPOS	5	3	15	Muy grave
MALWARE	4	5	20	Muy grave
ROBO	4	4	16	Muy grave

Tabla 17 Matriz de riesgo

En la tabla de riesgo observamos el total de seguridad que ahí en los laboratorios y de nivel de riesgo estamos expuesto este total se dio mediante a los cuestionarios.

RIESGOS	%SEGURIDAD	% RIESGO
DAÑO DE EQUIPO	78%	22%
ROBO	68%	32%
MALWARE	58%	43%
PROMEDIO	68%	32%

Ilustración 9 porcentaje de seguridad y riesgos

4.4.1.7 **Estimar las salvaguardas de los activos**

A continuación, se presenta la tabla correspondiente a la estimación de las salvaguardas de los activos, en la cual se detallan las medidas de protección existentes y las recomendaciones propuestas para reducir los riesgos identificados.

Riesgos	**Causas identificadas**	**Salvaguarda**
Malware	• No tiene política de seguridad	• Implementar política de seguridad contra malware.

	• Instalación de software no autorizado • Falta de medidas anti phishing • Antecedentes de incidentes de malware • Falta de capacitación en seguridad informática • Ausencia de medidas físicas contra ransomware • Falta de auditorías de vulnerabilidades • Ausencia de políticas de actualización • No existe monitoreo ni registros de actividad • Servidores sin protección contra ataques externos • Ausencia de herramientas de análisis forense • No se realizan pruebas de penetración	• Limitar la instalación de programas no autorizados. • Implementar filtros y estrategias contra el phishing. • Emplear EDR y optimizar la supervisión del antivirus. • Formar a los usuarios en aspectos de ciberseguridad. • Asegurar físicamente dispositivos y copias de seguridad. • Realizar revisiones y evaluaciones de vulnerabilidades. • Aplicar actualizaciones y parches de forma regular. • Activar registros y seguimiento de actividades. • Configurar cortafuegos, IDS/IPS y fortalecer servidores. • Establecer herramientas fundamentales de análisis forense. • Llevar a cabo pruebas de penetración de manera regular.
Daño de equipo	• Falta de protección contra sobrecargas eléctricas • Exposición a humedad o líquidos • Apagado inadecuado de los equipos • Falta de control de amenazas ambientales • Conexiones eléctricas sin revisión periódica	• Instalar reguladores, UPS y protectores de voltaje. • Mover dispositivos y utilizar resguardos contra la humedad. • Diseñar métodos de desconexión adecuados y entrenar a los usuarios. • Ejecutar manejo ambiental (circulación de aire, temperatura, organización). • Realizar inspecciones eléctricas y mantenimiento preventivo.

	• Ingreso de alimentos o bebidas al área	• Prevenir el ingresos de alimentos a los laboratorios
Robo	• Historial de robos en los laboratorios • Inadecuado control de acceso • Equipos sin identificación o etiquetado • Mala gestión de apagado y almacenamiento de equipos • Acceso de estudiantes externos sin registro • Falta de vigilancia en accesos principales • Ausencia de sistemas de alarma • Equipos sin anclaje o aseguramiento físico • Registros recientes de incidentes de robo • Equipos sin dispositivos de rastreo • Falta de protocolos para investigar incidentes	• Documentación de incidentes. • Sistema de acceso mediante identificaciones. • Etiquetas de dispositivos. • Proceso para cerrar el laboratorio. • Registro de ingreso de externos. • Cámaras de vigilancia. • Alarmas antirrobo. • Cables de seguridad para equipos. • Reporte inmediato de incidentes. • Software de rastreo en equipos. • Protocolo de investigación de robos.

Tabla 18 controles y salvaguardia de activo

CAPÍTULO V:

5 Informe de auditoría

Dirigido a: Dr. Temístocles Bravo Decano de la ULEAM Extensión El Carmen

Objetivos:

- Identificar riesgos de seguridad de la información en los laboratorios de cómputo de la carrera de Ingeniería en Software – ULEAM Extensión El Carmen, aplicando la metodología ISO/IEC 27031
- Elaborar un plan de contingencia para garantizar la continuidad y protección de la información crítica.

Alcance:

La presente auditoría se desarrolló conforme a los lineamientos establecidos por la metodología ISO/IEC 27031, adaptándola al entorno académico de los laboratorios de cómputo. El proceso incluyó actividades clave para evaluar el estado actual de la seguridad de la información

- Revisión de la metodología ISO/IEC 27031
- Fase de Planificación
- Determinar los activos relevantes de la empresa
- Valoración de riesgos
- Determinar las amenazas a los que están expuestos los activos
- Estimar los impactos potenciales y residuales
- Estimar las salvaguardas de los activos
- Fase de Implementación y Operación
- Establecer el plan de comunicación y de respuesta ante incidentes.
- Elaborar el documento formal del Plan de Contingencia TIC (propósito, alcance, roles y responsabilidades).
- Capacitación de formación a los estudiantes:
- Evaluación de respaldo y recuperación.

- Documentación operativa al personal asociado

Personal Relacionado:

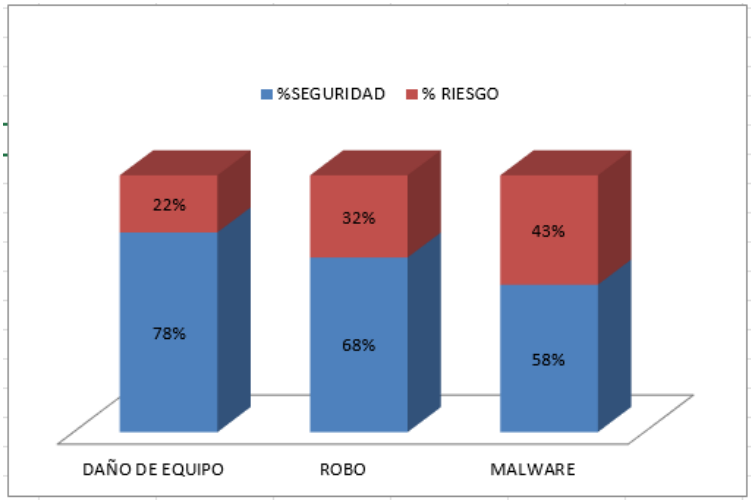
- Coordinador de la Carrera de Ingeniería en Software
- Estudiantes de la disciplina colaborando en revisiones técnicas
- Docentes encargados del manejo de los laboratorios.

5.1 Hallazgos

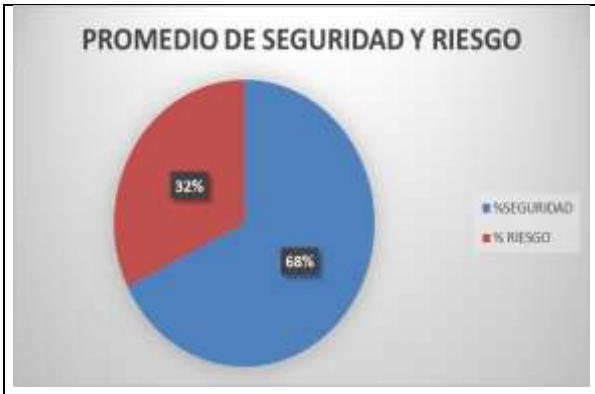
El análisis evidencia que los laboratorios presentan niveles de riesgo entre importantes y muy graves frente a las amenazas de malware, robo y daño de equipo, lo que demuestra una alta vulnerabilidad y debilidades en los controles actuales de seguridad. Aunque en algunos casos los riesgos asociados a malware y daño de equipo se mantienen en rangos moderados, igualmente requieren atención inmediata para evitar afectaciones a la continuidad operativa.

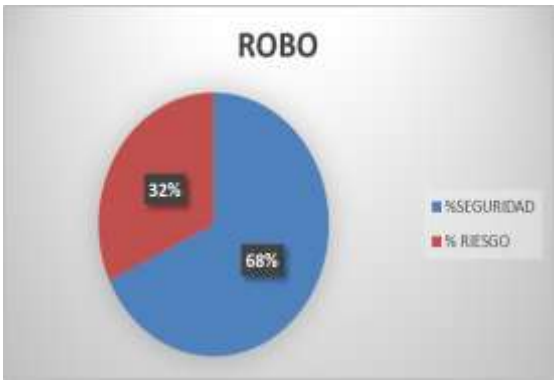
En resumen, los hallazgos muestran la imperante necesidad de reforzar la seguridad digital, optimizar los métodos de gestión y implementar acciones correctivas que se alineen con los principios de la norma ISO/IEC 27031.

5.1.1 Hallazgos de seguridad de riesgos



5.1.2 Resultado de riesgo global

	Los resultados de la auditoría evidencian que, a pesar de existir controles de seguridad básicos, persisten vulnerabilidades críticas que comprometen la continuidad operativa de los laboratorios. La presencia de estos riesgos latentes demanda la ejecución inmediata de acciones correctivas y preventivas, lo cual fundamenta la necesidad de implementar un plan de contingencia que asegure la integridad de los servicios TIC ante posibles incidentes.

Robo	**Causa**
	• No existen cámara de seguridad • Falta de medidas de seguridad • No cuenta con sistemas de alarmas • No existe un control de acceso • No cuentan con dispositivos de rastreo • No existen protocolos para incidentes
El riesgo frente al robo se clasifica como muy alto, ya que el nivel de riesgo supera considerablemente a las medidas de seguridad existentes. Esta situación evidencia vulnerabilidades críticas debido a la insuficiente infraestructura de seguridad, lo que podría ocasionar pérdidas económicas y afectar la continuidad operativa si no se refuerzan los controles preventivos y de vigilancia	
Daño de Equipo	**Causa** • No tener registros de mantenimiento previos. • El uso inadecuado de los dispositivos • Mal control de revisión eléctrica

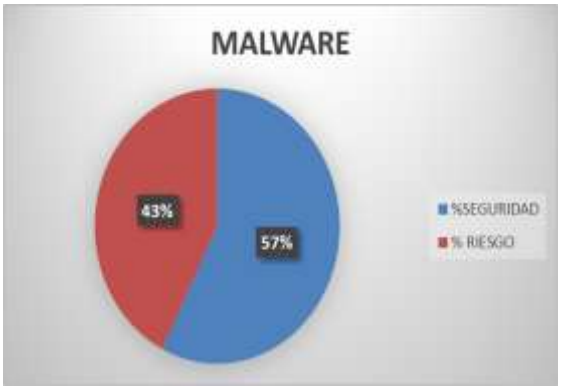
<table>
<tr><td> 
</td><td>• No existe responsable del área
• Fallas frecuentes en equipos
• Problemas de estructuras</td></tr>
<tr><td colspan="2">El daño de los equipos presenta un riesgo bajo, lo que evidencia un nivel de seguridad aceptable en el manejo de los recursos tecnológicos. Sin embargo, se recomienda continuar reforzando las acciones preventivas de mantenimiento y control para evitar fallas que puedan afectar la continuidad del servicio.</td></tr>
<tr><td>Malware
 
</td><td>Causa
• No existen protección de acceso
• Los archivos de instalación no son verificados
• No tienen acceso de identificación</td></tr>
<tr><td colspan="2">El riesgo de infección por malware ha sido clasificado como alto, lo que corresponde a un riesgo muy importante según la escala establecida.</td></tr>
</table>

Tabla 19 resultado de riesgo global

5.1.3 Conclusión

En respuesta a los objetivos planteados, se concluye que la identificación y evaluación de los activos tecnológicos permitió reconocer de manera clara su nivel de criticidad dentro de los laboratorios de cómputo. Asimismo, el análisis de amenazas y riesgos evidenció los principales eventos que podrían afectar la continuidad operativa, la disponibilidad y la integridad de la información. Estos resultados facilitaron la definición de medidas preventivas

y correctivas orientadas a minimizar el impacto de posibles incidentes. En conjunto, el cumplimiento de los objetivos establecidos contribuyó al fortalecimiento del plan de contingencia, proporcionando una base técnica y metodológica para mejorar la seguridad de la información y garantizar la continuidad de los servicios tecnológicos

5.1.4 Recomendaciones

Una vez identificados los riesgos que pueden afectar a los laboratorios de cómputo, se recomienda la implementación formal del plan de contingencia propuesto, con el fin de mitigar los efectos derivados de incidentes como el daño de equipos, el robo y la presencia de malware. Igualmente, se recomienda la creación y distribución de este diseño entre los alumnos, con el objetivo de mejorar su comprensión sobre seguridad digital y fomentar una cultura de precaución en los laboratorios.

Adicionalmente, se recomienda considerar el siguiente plan de contingencia

Se aplique todas las directrices de seguridad establecidas, de manera que sirva como una herramienta de apoyo para la respuesta oportuna y la solución eficaz ante la ocurrencia de cualquier riesgo, contribuyendo así a la protección de los recursos tecnológicos y a la continuidad de los servicios.

5.1.4.1 Plan de contingencias

Fase 2 Implementación operativa

5.1.4.1.1 Elaborar el documento formal del plan de continuidad TIC (propósito, alcance, roles y responsabilidades).

En este apartado se elabora el documento formal del Plan de Continuidad TIC, donde se especifican los objetivos, el ámbito de aplicación, así como las funciones y deberes designados para asegurar la persistencia de los servicios tecnológicos en la entidad frente a eventuales situaciones adversas.

PLAN DE CONTINGENCIA ANTE MALWARE

1. Datos Generales

Institución: _____

Área: Tecnologías de la Información

Documento: Plan de Contingencia ante Malware

Responsable: Coordinación / Departamento TIC

Fecha: _____

Versión: 1.0

2. Introducción

El uso de las tecnologías de la información en los laboratorios de cómputo y áreas administrativas de la institución es fundamental para el desarrollo de las actividades académicas y administrativas. Sin embargo, el acceso constante a internet, el uso de dispositivos de almacenamiento externo y la instalación de software incrementan el riesgo de infecciones por malware.

En respuesta a esta circunstancia, se crea el actual Plan de Contingencia contra Malware, que determina normas, reglas y roles para reaccionar de forma adecuada y eficiente ante casos de software dañino, con el propósito de salvaguardar los datos institucionales y asegurar la continuidad de las operaciones.

3. Objetivos

3.1 Objetivo General

Establecer un conjunto de procedimientos claros para la detección, contención, erradicación y recuperación ante incidentes de malware que afecten los sistemas informáticos de la institución**.**

3.2 Objetivos

- Reconocer rápidamente eventos vinculados al malware.
- Disminuir las consecuencias y la difusión del software dañino.
- Recobrar los sistemas y datos comprometidos.
- Reforzar las estrategias preventivas de seguridad informática.

4. Alcance

- El presente Plan de Contingencia es aplicable a:
- Laboratorios de cómputo institucionales.
- Equipos administrativos y académicos.

- Servidores y conexión local.

Quienes usan son estudiantes y docentes

5. Idea central

El software malo es todo programa hecho para causar daño. Su meta es estropear computadoras, tomar datos, parar servicios, o dar entrada sin permiso. Los tipos más comunes de software malo son virus, secuestro de datos, espías, caballos de Troya, y bichos de red.

6. Roles y responsabilidades del plan de contingencia

Reporte de los Usuario	• inmediatamente cualquier anomalía detectada en el equipo. • Suspender Reportar el uso del equipo afectado. • No instalar software ni conectar dispositivos externos sin autorización
Técnico TIC	• Verificar la existencia del incidente. • Separar el aparato dañado de la red. • Usar programas de revisión y borrado de software malicioso. • Anotar todos los sucesos del problema.
Responsable TIC	• Coordinar las acciones de respuesta. • Permitir de nuevo los sistemas y la información. • Notificar a los jefes de la entidad si el problema es muy grave.

Tabla 20 roles y responsabilidades del plan de contingencia

7. Identificación del Incidente

Se considerará un incidente de malware cuando se presenten una o más de las siguientes situaciones:

- Lentitud inusual del sistema.
- Aparición de ventanas emergentes sospechosas.
- Bloqueo o cifrado de archivos.
- Alertas emitidas por el antivirus.
- Fallos reiterados del sistema operativo**.**

Procedimiento de Respuesta ante Malware

8.1 Hallazgo

La persona usuaria y avisa al experto de Sistemas sobre el modo extraño del aparato dañado.

8.2 Parada

• El dispositivo se separa sin demora de la red de la institución.

• Se impide la entrada al sistema que tiene problemas

8.3 Análisis

- Identificación del tipo de malware.
- Evaluación del nivel de impacto del incidente (bajo, medio o alto).

8.4 Erradicación

- Ejecución de antivirus y herramientas antimalware actualizadas.
- Quitar archivos dañados.
- Si el problema es muy serio, se debe borrar todo y poner el sistema de nuevo.

8.5 recuperación

- Poner la información de nuevo usando respaldos.
- Poner solo programas que tienen permiso.
- Verificación del correcto funcionamiento del equipo.

8.6 Cierre del Incidente

Registro del incidente en el informe técnico correspondiente.

- Evaluación de las causas y aplicación de mejoras preventivas.

9. Plan de Comunicación

REPORTE DE INCIDENCIAS EN EQUIPO DE LABORATORIO DE COMPUTO

Nombre del Docente encargado

Institución Fecha: de entrega

REGISTRO DE INCIDENTE							
FECHA	DESCRIPCION DE INCIDENTE	CODIGO DE EQUIPO	NOMBRE DEL QUE REPORTA	FIRMA DE ENTREGADO DEL DIRECTOR	SOLUCIÓN	FECHA SOLUCIÓN	Equipo:

Ilustración 10 reporte de incidente del plan se comunicación

Cadena de notificación:

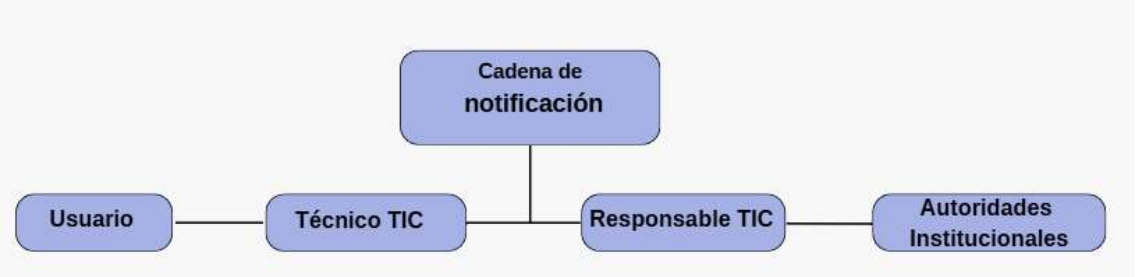


Ilustración 11 notificación de malware

En caso de incidentes críticos que afecten el desarrollo de las actividades académicas, se emitirá un comunicado interno informando las acciones a tomar.

10. Pasos para Evitar Riesgos

- Se debe usar un antivirus que esté al día.
- Es bueno actualizar los sistemas y programas a tiempo.
- No se permiten bajar cosas si no están dadas por la empresa.

- Se necesita enseñar lo básico de cuidar la información.
- Se deben tener reglas firmes sobre cómo usar las máquinas de la entidad.

11. Manejo de Respaldo de Datos

- Hacer copias de seguridad de datos importantes con regularidad.
- Guardar estos respaldos en lugares fuera de la red que sean seguros.
- Revisar si las copias guardadas sirven bien cada cierto tiempo.

12. Evaluación y Mejora Continua

El presente plan será evaluado de forma semestral o anual, con el propósito de actualizar los procedimientos conforme a nuevas amenazas informáticas y mejorar la capacidad de respuesta ante incidentes de malware.

13. Aprobación y Vigencia

El presente Plan de Contingencia entra en vigencia a partir de su aprobación por las autoridades competentes y será de cumplimiento obligatorio para todos los usuarios de los sistemas informáticos institucionales.

Firma Responsable TIC: _____

Fecha: _____

PLAN DE CONTINGENCIA ANTE ROBO

1. Datos Generales

Institución: _____

Área: Tecnologías de la Información

Documento: Plan de Contingencia ante Robo

Responsable: Coordinación / Departamento TIC

Fecha: _____

Versión: 1.0

2. Introducción

Los equipos tecnológicos y recursos informáticos representan activos fundamentales para el desarrollo de las actividades académicas y administrativas de la institución. La posibilidad de robos de equipos, dispositivos de almacenamiento o componentes tecnológicos constituye una amenaza que puede afectar la continuidad operativa, la seguridad de la información y el normal desarrollo de las funciones institucionales.

En este contexto, se elabora el presente Plan de Contingencia ante Robo, su fin es fijar pasos claros y bien puestos. Estos pasos son para evitar robos. También son para responder y volver a la normalidad luego de que quiten bienes de tecnología.

3. Objetivos

3.1 Objetivo General

Establecer acciones y procedimientos que permitan responder de manera oportuna Es si ocurren robos de equipos de tecnología. Se busca bajar el daño en el trabajo. También se busca reducir el costo y el riesgo a la información guardada

3.2 Objetivos Específicos

- Prevenir la sustracción de equipos y recursos tecnológicos de los laboratorios de cómputo.
- Actuar de forma inmediata ante la detección de un robo, siguiendo los protocolos establecidos.
- Recuperar la operatividad de los servicios tecnológicos afectados en el menor tiempo posible.
- Fortalecer los controles de seguridad institucionales para reducir riesgos futuros.

4. Alcance

- El presente plan es aplicable a:
- Laboratorios de cómputo..

- Equipos de cómputo, dispositivo de apoyo y sitios para guardar datos..
- Usuarios: estudiantes, docentes y personal administrativo.

5. Marco Conceptual

El robo se define como tomar sin permiso cosas de la institución. Esto incluye máquinas de cómputo, partes de tecnología y aparatos con datos del centro. Dicho acto daña el tener los medios y pone en riesgo los datos guardados.

6. Roles y Responsabilidades

Usuario	• Reportar inmediatamente la pérdida o sustracción de equipos. • No alterar el área donde ocurrió el incidente. • Colaborar con la información requerida
Técnico TIC	• Verificar el inventario de equipos. • Detectar los medios dañados. • Bloquear entradas, perfiles o máquinas sacar, si es necesario.
Responsable TIC	• Coordinar la respuesta institucional. • Gestionar la reposición de equipos. • Informar a las autoridades correspondientes. • Autoridades Institucionales • Autorizar acciones legales o administrativas. • Coordinar con seguridad interna o entidades externas

7. Identificación del Incidente

- Se considera un incidente de robo cuando:
- Se detecta la ausencia de equipos o dispositivos.
- Existen daños en cerraduras, puertas o ventanas.
- Se ve que tocaron área prohibidas sin permiso.

8. Procedimiento de Respuesta ante Robo

8.1 Detección

El usuario o responsable del área informa inmediatamente al Técnico TIC y a la autoridad correspondiente sobre el robo.

8.2 Contención

Asegurar el área afectada.

- No cambie las pruebas que haya. Limite quién entra al sitio del fallo.

8.3 Análisis

- Use la lista para saber qué cosas faltan.
- Vea cuánto afecta esto al trabajo y a la defensa.
- Compruebe si los datos en las máquinas robadas son clave.

8.4 Acciones Correctivas

- Deshabilitar cuentas de usuario asociadas a los equipos robados.
- Cambiar las claves secretas de la institución.
- Avisar a los cargos directivos si es necesario.

8.5 Recuperación

- Devolver los datos desde respaldos guardados.
- Reponer equipos nuevos para reanudar las labores.
- Configurar de nuevo los sistemas y los permisos.

8.6 Cierre del Incidente

- Elaborar informe del incidente.
- Actualizar el inventario de activos.
- Proponer mejoras de seguridad física.

REPORTE DE INCIDENCIAS EN EQUIPO DE LABORATORIO DE COMPUTO

Nombre del Docente encargado

Institución Fecha: de entrega

REGISTRO DE INCIDENTE							
FECHA	DESCRIPCION DE INCIDENTE	CODIGO DE EQUIPO	NOMBRE DEL QUE REPORTA	FIRMA DE ENTREGADO DEL DIRECTOR	SOLUCIÓN	FECHA SOLUCIÓN	Equipo:

9. Plan de Comunicación

Cadena de notificación:

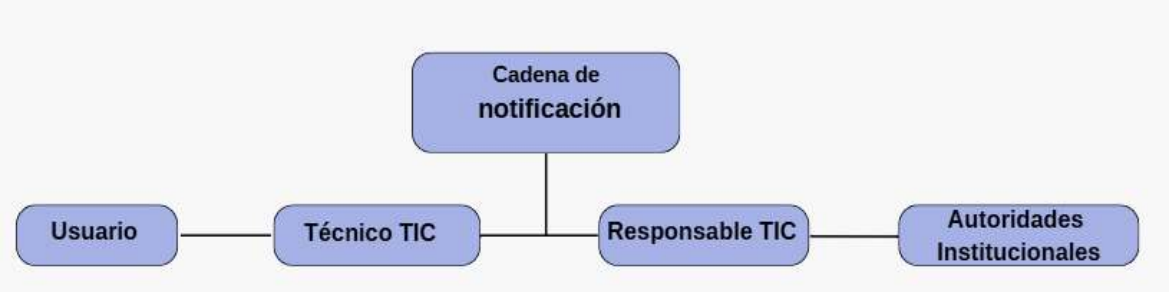


Ilustración 12 cadena de notificación robo

En robos de alto impacto se emitirá un comunicado interno y, de ser necesario, se activarán procedimientos legales.

10. 10. Acciones de Cuidado

- Limitar quién entra a los cuartos y a las oficinas.
- Usar cierres, cámaras para ver, y ruidos de alerta.
- Tener una lista al día de todo el aparato.
- Poner etiquetas claras y anotar todos los aparatos.
- Tener reglas firmes para prestar y usar lo que tenemos.

11. Manejo de Respaldo

- Hacer copias de lo importante a intervalos fijos.
- Guardar esas copias en un sitio que esté bien cuidado
- Verificación de disponibilidad de la información.

12. Revisión y Progreso Constante

Este plan se mirará cada cierto tiempo. El fin es hacer mejores los puntos de seguridad física. También se busca hacer más fuerte cómo reaccionamos a robos.

13. Aprobación y Vigencia

El presente Plan de Contingencia ante Robo entra en vigencia a partir de su aprobación oficial y es de cumplimiento obligatorio para toda la comunidad institucional.

Firma Responsable TIC: _____

Fecha: _____

PLAN DE CONTINGENCIA ANTE DAÑO DE EQUIPO

1. Datos Generales

Institución: _____

Área: Tecnologías de la Información

Documento: Plan de Contingencia ante Daño de Equipo

Responsable: Coordinación / Departamento TIC

Fecha: _____

Versión: 1.0}

2. Introducción

Los equipos informáticos constituyen un recurso esencial para el desarrollo de las actividades académicas y administrativas de la institución. El uso constante de estos equipos, así como factores externos como fallas eléctricas, manipulación inadecuada o desgaste natural, pueden ocasionar daños en el hardware o software, afectando la continuidad de los servicios tecnológicos.

Por esta razón, se crea este Plan de Emergencia por Fallas de Máquinas. Su fin es fijar pasos claros. Estos pasos sirven para ver, atender y arreglar fallas o daños en las herramientas de tecnología. Esto baja el daño a la labor diaria. También asegura que la entidad siga funcionando.

3. Objetivos

3.1 Objetivo General

Establecer acciones y normas. Estos deben permitir reaccionar a tiempo y bien ante fallas en los aparatos de cómputo. Esto garantiza que sigan las labores de enseñanza y de oficina.

3.2 Objetivos Específicos

- Detectar oportunamente daños en equipos informáticos.
- Reducir el tiempo de inactividad de los sistemas afectados.
- Proteger la información almacenada en los equipos.
- Garantizar la recuperación y restablecimiento del servicio.

4. Alcance

El presente plan aplica a:

Laboratorios de cómputo.

Equipos administrativos y académicos.

Hardware y software institucional.

Usuarios: estudiantes, docentes y personal administrativo.

5. Marco Conceptual

El Daño de equipo se nombra a toda rotura real o digital. Esto detiene que un aparato de cómputo trabaje bien. Causas varias lo provocan a uno. Hay fallas de luz. También hay fallos del programa. El desgaste de piezas es un factor. El manejo erróneo daña cosas. Los accidentes suman a esto. Todo esto toca el acceso a las herramientas de la técnica.

6. Roles y Responsabilidades

Roles	**Responsabilidades**
Usuario	• Reportar inmediatamente cualquier falla o daño detectado. • Suspender el uso del equipo afectado. • No intentar reparaciones sin autorización
Técnico TIC	• Diagnosticar el daño del equipo. • Verificar si el fallo es del equipo o del programa. • Hacer tareas de arreglar y mantenoimiento. • Anotar lo que pasó.
Responsable TIC	• Coordinar la reparación o reposición del equipo.

	• Autorizar el uso de equipos de respaldo. • Informar a las autoridades si el daño es crítico.

7. Identificación del Incidente

Se considera un daño de equipo cuando se presentan:

- Fallas de encendido o apagados repentinos.
- Errores frecuentes del sistema operativo.
- Mire daños claros en partes de máquinas.
- Los aparatos externos no funcionan bien. Esto incluye el teclado, la pantalla, el ratón y la máquina de copias.
- Los datos se borran. o puede que la información se dañe y no sirva.

8. Procedimiento de Respuesta ante Daño de Equipo

8.1 Detección

El usuario informa al Técnico TIC sobre la falla o daño detectado en el equipo.

8.2 Contención

- Suspender el uso del equipo afectado.
- Desconectar el equipo de la red eléctrica y de datos si es necesario.
- Evitar daños adicionales.

8.3 Análisis

- Diagnóstico técnico del equipo.
- Verificar qué falló de la máquina o el programa (hardware o software).
- Mirar qué tan malo es el efecto en el trabajo diario. Esto puede ser poco, normal o muy grande.

8.4 Acciones Correctivas

- Reparación del componente dañado.
- Poner de nuevo el programa o ajustarlo bien.
- Si el daño es muy fuerte, cambiar la máquina entera.

8.5 Recuperación

- Devolver los datos usando copias guardadas antes.
- Verificación del funcionamiento del equipo.
- Reincorporación del equipo al servicio.

8.6 Cierre del Incidente

Uleam
UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

REPORTE DE INCIDENCIAS EN EQUIPO DE LABORATORIO DE COMPUTO

Nombre del Docente encargado

Institución Fecha: de entrega

REGISTRO DE INCIDENTE

FECHA	DESCRIPCION DE INCIDENTE	CODIGO DE EQUIPO	NOMBRE DEL QUE REPORTA	FIRMA DE ENTREGADO DEL DIRECTOR	SOLUCIÓN	FECHA SOLUCIÓN	Equipo:

Ilustración 13 reporte de cierre de incidente

- Actualización del inventario de equipos.
- Recomendaciones para prevenir futuros daños.

9. Plan de Comunicación

Cadena de notificación:

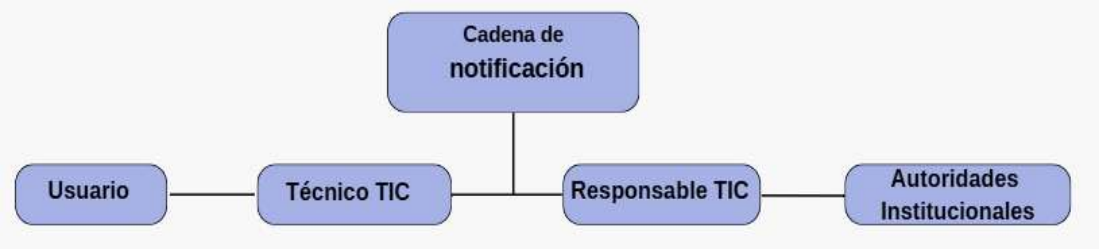


Ilustración 14cadena de notificación de daño de equipo

Cuando el daño afecte el desarrollo de actividades académicas, se emitirá un comunicado interno informando las medidas adoptadas.

10. Medidas Preventivas

- Mantenimiento preventivo periódico de los equipos.
- Utilización apropiada de los recursos tecnológicos.
- Reguladores de voltaje, UPS.
- Formación elemental para los usuarios.
- Políticas para el uso y la protección de los equipos.

11. Manejo de copias de seguridad

- Respaldo regular de datos críticos.
- Guarda segura de las copias de seguridad.
- ensayos periódicos para la recuperación de datos.

12. Evaluación y Mejora Continua

El presente plan será evaluado periódicamente con el fin de mejorar los procesos de mantenimiento, prevención y respuesta ante daños de equipos tecnológicos.

13. Aprobación y Vigencia

El presente Plan de Contingencia ante Daño de Equipo entra en vigencia a partir de su aprobación por las autoridades institucionales y es de cumplimiento obligatorio para todos los usuarios.

Firma Responsable TIC: _____

Fecha: _____

5.1.4.1.2 Plan de comunicación y de respuesta ante incidentes

Esta fase tiene como finalidad definir el plan de comunicación y de respuesta ante incidentes, orientado a garantizar una actuación rápida, coordinada y eficaz frente a eventos que comprometan la seguridad de la información o los activos tecnológicos.

PLAN DE COMUNICACIÓN Y DE RESPUESTA ANTE INCIDENTES

Fecha de Elaboración: Diciembre 08, 2025

Elaborado por: Diana Caza

Revisado Por: Clara Poso

1. **Objetivo**

Establecer las directrices para garantizar una comunicación rápida, clara y eficiente ante incidentes que afecten la seguridad lógica del laboratorio de la ULEAM, asegurando la continuidad operativa de los sistemas, plataformas académicas y servicios tecnológicos.

1. **Alcance Esta política es aplicable a:**

- El personal del equipo de Tecnologías de la Información (TI).
- Maestros encargados de los laboratorios informáticos.
- Estudiantes que utilizan los recursos informáticos.
- Personal administrativo vinculado con servicios digitales institucionales

2. **Roles y Responsabilidades**

Rol	**Responsabilidades**
Coordinador de Carrera	Reportar incidentes, comunicar avances, validar información oficial hacia la comunidad académica.
Docente responsable de laboratorio	Registrar fallas, informar el estado de las plataformas y canalizar los reportes de los estudiantes.
Equipo Técnico de TI	Examinar, atender y solucionar incidentes; implementar medidas de seguridad; generar informes técnicos.
Los Usuarios estudiantes y docentes	Informar sobre irregularidades, emplear los canales de comunicación oficiales y acatar las instrucciones dadas.

3. **Canales de Comunicación Oficiales**

Para garantizar una comunicación segura y oportuna, se establecen los siguientes medios:

- **Correo institucional** (@uleam.edu.ec)
- **Plataformas de mensajería institucional** WhatsApp Business institucional o Microsoft Teams
- **Plataformas académicas**: Moodle
- **Página web institucional** o panel informativo digital
- **Sistema de tickets o registro de incidencias** (si aplica)

4. Procedimiento de Comunicación ante Incidentes

5. **Detección del incidente**

   El usuario, docente o personal TI identifica una falla o anomalía en el sistema.

6. **Documentación del incidente**

   Se documenta en el sistema de incidentes o a través del correo institucional.

7. **Alerta al Coordinador de TI**

   El maestro responsable o el usuario informa de manera formal sobre el incidente observado**.**

8. **Delegación del incidente al equipo de técnicos**

   departamento de TI determina la gravedad y designa a los responsables.

9. **Comunicación a los usuarios afectados**

   Se informa sobre el incidente, servicios afectados y acciones iniciales.

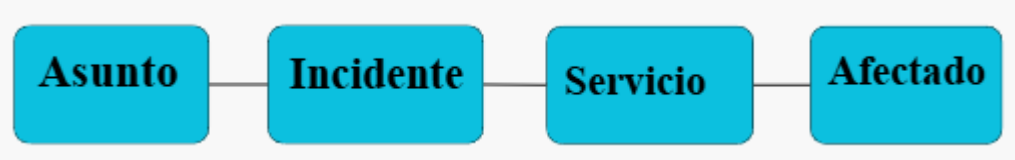
10. **Actualización del estado del suceso**

    Se informa el progreso de acuerdo con la disponibilidad de datos.

11. **Cierre y resolución**

    Después de que se resuelva el problema, se información que el servicio ha sido restaurado y se guarda el incidente.

12. Plantilla de Mensaje para Comunicaciones



Cuerpo del mensaje:

- **Servicios afectados:** _____
- **Descripción del incidente:** _____
- **Acciones en curso:** _____
- **Tiempo estimado de solución:** _____
- **Recomendaciones a los usuarios:** _____

13. Frecuencia de Comunicaciones

- **Estado general de plataformas:** semanal
- **Notificación de mantenimientos programados:** mínimo 48 horas antes
- **Comunicación de incidentes:** inmediata, al momento de ser detectado
- **Actualización de incidentes activos:** según evolución (mínimo cada 2 a 4 horas para casos críticos)

14. . Cumplimiento y Revisión

Esta política será revisada anualmente por el Departamento de TI y la Coordinación de Carrera para garantizar su vigencia y alineación con las normas universitarias y mejores prácticas de seguridad lógica.

15. Vigencia

El presente documento entra en vigencia a partir de su aprobación por la administración de la ULEAM y permanecerá activo hasta su reemplazo o actualización.

Ilustración 15 tabla ante incidente

5.1.4.2 Capacitación del personal y estudiantes

Se establecen las acciones de capacitación dirigidas a personal y estudiantes, con el fin de garantizar el conocimiento, la correcta aplicación de los procedimientos y la respuesta adecuada ante incidentes que puedan afectar la continuidad de los servicios TIC

CAPACITACIÓN DEL PERSONAL Y ESTUDIANTES

1. Objetivo

Fortalecer las competencias del personal y los estudiantes en el uso seguro, eficiente y responsable de los recursos tecnológicos de la institución.

2. Público

- Personal de administración y docente
- Alumnos de bachillerato

3. Contenido

- Prácticas adecuadas de seguridad informática.
- Uso apropiado de laboratorios y equipos informáticos.
- Manejo de acceso a plataformas, cuentas y contraseñas.
- Protocolos para situaciones de incidentes tecnológicos.
- Reglas institucionales para la utilización de TIC.

4. Metodología

- Charlas breves
- Talleres prácticos
- Demostraciones
- Material digital (guías, videos, infografías)

5. Recursos

- Laboratorio de cómputo
- Proyector y pantalla
- Material digital
- Facilitador / técnico TIC

6. Evaluación

- Cuestionario corto
- Actividades prácticas
- Registro de asistencia

Ilustración 16instrumento de capacitación

5.1.4.3 Pruebas de respaldo y recuperación

Se describen las pruebas de respaldo y recuperación que se realizarán para asegurar la disponibilidad y restauración oportuna de los datos y sistemas críticos ante posibles incidentes

1. Objetivo

Evaluar la eficacia del sistema de respaldo y recuperación, garantizando que la información crítica pueda restaurarse de forma segura, íntegra y en el menor tiempo posible.

1.Alcance

Tipos de Pruebas

a) Prueba de Respaldo:

- Verificar que los archivos se copien correctamente.
- Confirmar almacenamiento en los medios definidos.
- Validar la periodicidad del respaldo.

b) Prueba de Recuperación:

- Restaurar un respaldo total o parcial.
- Verificar integridad y consistencia de los datos recuperados.

2. Alcance

Las pruebas se llevan a cabo en:

- Respaldo de bases de datos.
- Documentos de tipo académico y administrativo.
- Ajustes del sistema operativo.
- Plataformas institucionales archivos que se comparten, sistemas internos, Moodle.

3. Tipos de Pruebas

a) Verificación de Respaldo:

- Confirmar que los archivos se copian de manera adecuada.
- Verificar el almacenamiento en los medios establecidos.
- Confirmar la periodicidad de la copia de seguridad**.**

b) Prueba de recuperación:

- Reestablecer una copia de seguridad total o parcial.
- Comprobar que los datos recuperados sean íntegros y consistentes.
- Comprobar el tiempo de restauración.

4. Procedimiento

Etapa 1: Preparación

- Detección de información esencial.

- Establecimiento de rutas para el almacenamiento.
- Comprobación de las herramientas de respaldo..
- Notificación a las áreas involucradas.

Fase 2: Implementación de la copia de seguridad

- Ejecutar la copia de acuerdo con lo que estipula la política.
- Anotar la fecha, el tamaño y el lugar del respaldo.
- Elaborar el informe pertinente**.**

Fase 3: Prueba de restauración

- Elegir un punto de restauración.
- Recuperar la información en un entorno seguro.
- Confirmar la integridad y documentación de los resultados.

Fase 4: Comprobación y conclusión

- Contrastar datos originales con los restaurados.
- Descubrir fallos y oportunidades de mejora.
- Redactar el informe final.

5. Recursos requeridos

- Software de respaldo.
- Discos o servidores externos.
- Personal técnico.
- Entorno de pruebas.
- Políticas institucionales de respaldo.

6. Indicadores

- Porcentaje de respaldos que resultaron exitosos.
- Tiempo de restauración.
- Errores identificados.
- Grado de integridad del respaldo que ha sido restaurado.

7. Periodicidad

- Respaldo: diario, semanal o mensual.
- Evaluación de restauración: trimestral o semestral.

8. Resultados entregables

- Registro de respaldo.
- Informe de recuperación.
- Recomendaciones.

- Actualización de procedimientos.

Ilustración 17 instrucción de recuperación

5.1.4.4 Documentación operativa

Se recopila y organiza la documentación operativa necesaria para el correcto funcionamiento y mantenimiento de los sistemas TIC, asegurando que los procedimientos, guías y registros estén disponibles y actualizados para su consulta y ejecución

- **Procedimiento Operativo: Respaldo Diario de Información**

Responsable: Administrador de Sistemas

1.Propósito

Garantizar la integridad y disponibilidad de la información generando respaldos diarios de los datos críticos almacenados en los servidores institucionales.

2.Alcance

Se aplica a los servidores que almacenan sistemas de aprendizaje virtual, administrativo y académico.

3. Responsables

- Administrador de Sistemas
- Técnico de Soporte

4. Procedimiento

1. Verificar el estado del almacenamiento de respaldo.
2. Lleve a cabo el script de copia de seguridad automática.
3. Comprobar que el respaldo se haya terminado sin equivocaciones.
4. Registre el procedimiento en el formato de registro de respaldo.
5. Notificar al jefe de TI sobre fallas.

5. Registros asociados

- Formato REG --: Registro de Respaldo Diario.

Ilustración 18instrumento operativo

CAPÍTULO VI:

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

A partir del análisis realizado, se determinó que el objetivo planteado fue satisfactoriamente cumplido, dado que se identificaron diversas deficiencias en la seguridad lógica de los laboratorios de cómputo. Entre las principales se evidencian la ausencia de políticas formales de seguridad de la información, el uso inadecuado de credenciales de acceso, la limitada gestión de controles de seguridad y la inexistencia de procedimientos definidos para la atención de incidentes. Estas falencias incrementan significativamente el riesgo de pérdida, alteración o acceso no autorizado a la información académica e institucional.

Se determina que el propósito planteado fue logrado, pues se recopiló información relevante sobre la gestión de riesgos, la seguridad de la información y los planos de contingencia a partir del análisis documental y bibliográfico. Esta fundamentación teórica fue posible que se fortaleciera el marco conceptual de la investigación y que se reconocieran prácticas adecuadas y directrices que se pueden aplicar a los laboratorios de computación en el universitario.

Se determina que el propósito se cumplió, ya que se evidencia la presencia de problemas reales en términos de seguridad lógica, a partir del diagnóstico realizado a través de entrevistas y encuestas dirigidas a profesores y alumnos de las carreras Ingeniería en Tecnologías de la Información e Ingeniería de Software. Los hallazgos muestran un nivel restringido de comprensión acerca de la seguridad informática y la falta de protocolos definidos para prevenir, detectar y reaccionar frente a incidentes informáticos.

Por último, tras evaluar el nivel de riesgo en seguridad lógica, se concluye que el objetivo fue alcanzado, ya que se identifican riesgos de niveles medio y alto en los laboratorios informáticos. Estos constituyen una posible amenaza para la confidencialidad, la integridad y la disponibilidad de los datos. Esto evidencia que es necesario poner en marcha un plan de contingencia para mitigar los efectos, mejorar la seguridad y asegurar que los laboratorios sigan funcionando.

6.2 Recomendaciones

A la Universidad Laica Eloy Alfaro de Manabí – Extensión El Carmen implementar formalmente el plan de contingencia propuesto para la seguridad de la información y la continuidad de los servicios TIC en los laboratorios de cómputo, asegurando su publicidad, aplicación y cumplimiento por parte de docentes, estudiantes y personal administrativo, de acuerdo con los lineamientos de la norma ISO/IEC 27031.

Con el objetivo de reforzar la prevención y la respuesta frente a sucesos que puedan perjudicar las actividades académicas, se le pide la coordinación de ingeniería en software que promueva programas de capacitación periódica para estudiantes y profesores acerca de seguridad de información, continuidad de servicios TIC y buenas prácticas informáticas.

Al Departamento de Tecnologías de la Información realizar mantenimientos preventivos y correctivos de manera continua a los equipos de cómputo, sistemas de red y plataformas tecnológicas de los laboratorios, así como implementar controles de acceso, gestión de usuarios, copias de seguridad y actualización constante del software de seguridad.

A los estudiantes usuarios de los laboratorios de cómputo cumplir responsablemente con las políticas y normas de seguridad establecidas por la institución, hacer un uso adecuado de los recursos tecnológicos y reportar oportunamente cualquier incidente, anomalía o situación de riesgo que pueda afectar la seguridad de la información o la continuidad de los servicios.

BIBLIOGRAFÍA

Achiri Taipe, M., & Batalla Diaz, A. (2021). *investigacion exploratoria y correlacional.*

Achiri Taipe, M., & Batalla Diaz, A. J. (2021).

Adriana, O. A. (2021). *PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES.* bogota: https://repository.unad.edu.co/bitstream/handle/10596/41984/aonatear_3ago2021.pdf?sequence=1&isAllowed=y.

Alberto Guerrero, J. (2023). *PLAN DE CONTINGENCIA INFORMATICO Y SEGURIDAD DE LA INFORMACION.* hospitalcmpcuruman. https://doi.org/https://hospitalcmpcurumani.gov.co/wp-content/uploads/2020/05/plan_de_contingencia_informatico_y_seguridad_de_la_informacion1.pdf

ANCAJIMA MENDOZA , M. (28 de 4 de 2019). *PROPUESTA DE IMPLEMENTACIÓN DE seguridad informatica de las tic DE LA I.E.SAN MIGUEL ARCÁNGEL, CATACAOS - PIURA*. ULADECH Católica - Universidad Católica Los Ángeles de Chimbote %: https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/9386/CONTROL_SEGURIDAD_ANCAJIMA_MENDOZA_MARIA_ALEJANDRA.pdf?s

Arévalo Cordovilla, F. (2022). *seguridad fisica y logica* . https://sga.unemi.edu.ec/media/archivologo/2022/07/19/archivologocompendio_2022719165425.pdf.

Arias,, F. (2017). Revista RECITIUTM. *Revista Electrónica de Ciencia y Tecnología del Instituto Universitario de Tecnología de Maracaibo*, 20. https://doi.org/http://d1wqtxts1xzle7.cloudfront.net/85198345/92-501-1-PB-libre.pdf?1651278966=&response-content-disposition=inline%3B+filename%3DEfectividad_y_eficiencia_de_la_investiga.pdf&Expires=1748194372&Signature=EJY5zk~7fuI8CAcn6OxOn5uQypZAzUxXDIY9liWCBlTGEMVuEXj

Betancourt Sánchez, G. A. (2017). *IDENTIFICACIÓN, LEVANTAMIENTO Y PROPUESTA DE MEJORA DE LOS PROCESOS CRÍTICOS DE LA EMPRESA LA EMPRESA.*

PUCE. https://doi.org/https://repositorio.puce.edu.ec/items/a1a0ec02-ea81-42b9-b718-c06b6731f292

Calderon Lopez, D. X., & Suntaxi Oña, D. K. (2019). *PROPUESTA PARA EL ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS LABORATORIOS DE COMPUTACIÓN DE LAS FACULTADES DE INGENIERÍA DE SISTEMAS DE LAS UNIVERSIDADES DE QUITO.* quito: file:///C:/Users/Personal/Downloads/CD-2103.pdf.

CAMPOZANO , Y., & CASTRO , S. (22 de enero de 2025). *PLAN DE CONTINGENCIA INFORMÁTICO Y DE SEGURIDAD DE LA INFORMACIÓN PARA LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN*. repositorio digital Unesum: http://repositorio.unesum.edu.ec/handle/53000/7264

Carrion , B. F. (06 de marzo de 2024). *Repositorio Institucional de la Universidad Politécnica Salesiana.* dspace: http://dspace.ups.edu.ec/handle/123456789/27657

Castro Baque , S. (2024). *PLAN DE CONTINGENCIA INFORMÁTICO Y DE SEGURIDAD DE LA INFORMACIÓN PARA LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN.* jipijapa: https://repositorio.unesum.edu.ec/bitstream/53000/7264/1/CASTRO%20BAQUE%20SULLY%20GABRIELA.pdf.

Castro Baque , S. (15 de diembre de 2024). *repositorio.unesum*. PLAN DE CONTINGENCIA INFORMÁTICO Y DE SEGURIDAD DE LA INFORMACIÓN PARA LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN: https://repositorio.unesum.edu.ec/bitstream/53000/7264/1/CASTRO%20BAQUE%20SULLY%20GABRIELA.pdf

CASTRO BAQUE, S. (2024). *PLAN DE CONTINGENCIA INFORMÁTICO Y DE SEGURIDAD DE LA INFORMACIÓN PARA LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN.* unesum. https://doi.org/https://repositorio.unesum.edu.ec/bitstream/53000/7264/1/CASTRO%20BAQUE%20SULLY%20GABRIELA.pdf

Castro Baque, S. G. (2024). *PLAN DE CONTINGENCIA INFORMÁTICO Y DE SEGURIDAD DE LA INFORMACIÓN PARA LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN.* unesum. https://doi.org/https://repositorio.unesum.edu.ec/bitstream/53000/7264/1/CASTRO%20BAQUE%20SULLY%20GABRIELA.pdf

Chicano Tejada, E. (2023). *Auditoría de seguridad informática. IFCT0109.* https://www.google.com.ec/books/edition/Auditor%C3%ADa_de_seguridad_inform%C3%A1tica_IFC/SRLLEAAAQBAJ?hl=es&gbpv=1&dq=Seguridad+de+la+red+interna&printsec=frontcover.

cisco. (2024).

Condor Gordon, E. G. (2019). *DISEÑO DE UN SISTEMA DE SEGURIDAD FÍSICA PARA LA EPN.* quito: https://bibdigital.epn.edu.ec/bitstream/15000/11148/1/T2467.pdf.

Condor Gordon, E. G. (2019). *DISEÑO DE UN SISTEMA DE SEGURIDAD FÍSICA PARA LA EPN.* quito: https://bibdigital.epn.edu.ec/bitstream/15000/11148/1/T2467.pdf.

Carrión Hermida, B. (2024). *PROPUESTA DE UN PLAN DE EMERGENCIA Y CONTINGENCIA EN UN.* universidad tecnica selestina . https://doi.org/https://dspace.ups.edu.ec/bitstream/123456789/27657/1/UPS-GT005097.pdf

Castro Maldonado, J., Gómez Macho, L., & Camargo Casallas, E. (2022). *La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI.* https://revistas.udistrital.edu.co/index.php/Tecnura/article/view/19171/18635.

Castro Marquina, L. (2013). *DISEÑO DE UN SGCN PARA LA RENIEC.* universidad catolica . https://doi.org/https://tesis.pucp.edu.pe/server/api/core/bitstreams/d501e63a-3d83-4530-b341-035789dbd5b2/content

del Cid Flores, J. (2021). *Escuela de Contaduría Pública y Auditoria Seminario Integrador Profesional.* https://www.studocu.com/gt/document/universidad-de-san-carlos-de-guatemala/seminario-integrador-profesional/metodologia-de-la-investigacion/50955121?utm_source=chatgpt.com.

Del Pozo, M. (2023). *gestion de archivo.* https://www.google.com.ec/books/edition/Gesti%C3%B3n_de_archivos/7hHTEAAAQBAJ?hl=es&gbpv=1&dq=Definici%C3%B3n+de+seguridad+de+la+informaci%C3%B3n&pg=PA53&printsec=frontcover.

Haro Sarango, A., & Chisag Pallmay, E. (2024). *Tipos y clasificación de las investigaciones.* file:///C:/Users/Diana/Downloads/Dialnet-TiposYClasificacionDeLasInvestigaciones-9541046%20(1).pdf.

Intriago , J., Quimis , J., Choez, C., & Marcillo, M. (2023). Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información. *Journal TechInnovation*, 79-84.

Lema Parco, O. (2025). *Propuesta de un sistema de seguridad de la información para una Empresa de Telecomunicaciones bajo la Norma ISO/IEC 27005.* quito: http://repositorio.uisrael.edu.ec/bitstream/47000/4305/1/UISRAEL-EC-MASTER-SEG-INF-PRO-378.242-2025-004.pdf.

Ortiz Alulema, I. (2020). *Implementación de la Norma ISO 31000:2009 en la administración del riesgo de lavado de activos y del financiamiento de delitos, en bancos privados de Ecuador.* universidad andina simon bolivar. https://doi.org/https://repositorio.uasb.edu.ec/bitstream/10644/7760/1/T3349-MAE-Ortiz-Implementacion.pdf

PACHECO POZO, D. (2016). *PROPUESTA DE UN PLAN DE CONTINGENCIA DE TI PARA LA EMPRESA LOGICIEL.* bibdigita. https://doi.org/https://bibdigital.epn.edu.ec/bitstream/15000/15030/1/CD-6841.pdf

Quiroz, S., & Macías, D. (2017). *Seguridad en informática: consideraciones.* manabi: file:///C:/Users/Diana/Downloads/Dialnet-SeguridadEnInformatica-6137824.pdf.

Tapia Farinango, :. (2023). *Evaluación del plan de contingencia ante emergencias de la Facultad de Ingeniería en.* Atención Prehospitalaria y en Emergencias. https://doi.org/https://www.dspace.uce.edu.ec/server/api/core/bitstreams/985a2758-3bcd-4a95-baf4-2359e2d52362/content

Toledo, M. (2021). *Técnicas de Investigación Cualitativas y Cuantitativas.* https://core.ac.uk/download/pdf/80531608.pdf.

Vega Briceño, E. (2021). SEGURIDAD DE LA INFORMACIÓN. En E. Vega Briceño, *SEGURIDAD DE LA INFORMACIÓN* (pág. 112). file:///C:/Users/Personal/Downloads/SEGURIDAD-INFORMACION.pdf.

Vega Briceño, E. (2021). *SEGURIDAD DE LA INFORMACIÓN.* https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf.

Freire, F. (3 de enero de 2017). *PLAN DE CONTINGENCIA ANTE CIBERATAQUES*. DSpace en espol: https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf

Guardelli, E. (2024). *Ciberseguridad en la Atención Sanitaria : Protección* . https://www.google.com.ec/books/edition/Ciberseguridad_en_la_Atenci%C3%B3n_Sanitaria/Wc8UEQAAQBAJ?hl=es&gbpv=1&dq=Cifrado+y+protecci%C3%B3n+de+la+informaci%C3%B3n&pg=PT97&printsec=frontcover.

Hecker, R. (25 de julio de 2002). *journals.sagepub.* Planificación de contingencias para la gestión del laboratorio: evaluación ambienta: https://journals.sagepub.com/doi/pdf/10.1016/S1535-5535-04-00173-X

Hermida, B. F. (2024). *PROPUESTA DE UN PLAN DE EMERGENCIA Y CONTINGENCIA EN UN CONDOMINIO UBICADO EN LA CIUDAD DE JIPIJAPA.* Guayas Ecuador : https://dspace.ups.edu.ec/bitstream/123456789/27657/1/UPS-GT005097.pdf.

Huilca Palacios , J. (2022). *Plan de contingencia de tecnologia de la informacion.* fondouta. https://doi.org/https://fondouta.ec/wp-content/uploads/2023/02/PLAN-DE-CONTINGENCIA-DE-TECNOLOGIA-DE-LA-INFORMACION-FONDO-UTA-signed-signed-signed.pdf

Huilca Palacios, J. (2020). *nstituto Nacional de Desarrollo y Conservación Forestal de Áreas Protegidas y Vida Silvestre. (2020*. PLAN DE CONTINGENCIA Y informatico: https://icf.gob.hn/wp-content/uploads/2021/08/Plan-de-Contingencias-ICF-2020.pdf

Huilca Palacios, J. (2020). *Plan de contingencia de tecnologias de la información.* FONDO-UTA.

Huilca Palacios, J. (2022). *PLAN DE CONTINGENCIA* . VERSION 1.0 -. https://doi.org/https://fondouta.ec/wp-content/uploads/2023/02/PLAN-DE-CONTINGENCIA-DE-TECNOLOGIA-DE-LA-INFORMACION-FONDO-UTA-signed-signed-signed.pdf

Huilca Palacios, J. (2022). PLAN DE CONTINGENCIA DE. En J. HUILCA PALACIOS, *GENETRIX SOFTWARE & LEARNING* (pág. 47). file:///C:/Users/Personal/Downloads/PLAN-DE-CONTINGENCIA-DE-TECNOLOGIA-DE-LA-INFORMACION-FONDO-UTA-signed-signed-signed.pdf.

Huilca Palacios, J. (2022). *Plan de contingencia de tecnologias de la informacion.* FONDO-UTA. https://doi.org/https://fondouta.ec/wp-content/uploads/2023/02/PLAN-DE-CONTINGENCIA-DE-TECNOLOGIA-DE-LA-INFORMACION-FONDO-UTA-signed-signed-signed.pd

Ibarra Canseco, S. (2019). *"DISEÑO DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL.* Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Gerencia de Sistemas de Información. https://doi.org/http://repositorio.uta.edu.ec/handle/123456789/30475

Incibe. (05 de 12 de 2023). *Pasado, presente y futuro de la seguridad de la información.* Empresas | INCIBE: https://www.incibe.es/empresas/blog/pasado-presente-y-futuro-de-la-seguridad-de-la-informacion

Loaza Carrasco, R., Martel Carranza, C., & Castillo Acobo, R. (2023). *TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN.* http://coralito.umar.mx:8383/jspui/bitstream/123456789/1539/1/80-M%C3%A9todolog%C3%ADa%2Bde%2Bla%2Binvestigaci%C3%B3n.pdf.

López Cuadrado, J. L. (2015). *PLAN DE CONTINGENCIA DE TECNOLOGIAS DE LA INFORMACIÓN EN ENTORNOS DISTRIBUIDOS.* Universidad Carlos III de Madrid.

Medina Romero, M., Rojas Leon, R., & Bustamante Hoces, W. (2023). *TÉCNICAS E INSTRUMENTOS DE.* http://coralito.umar.mx:8383/jspui/bitstream/123456789/1539/1/80-M%C3%A9todolog%C3%ADa%2Bde%2Bla%2Binvestigaci%C3%B3n.pdf.

Mero Suarez , C. (2018). *PLAN DE CONTINGENCIAS INFORMÁTICAS Y LA SEGURIDAD DE LA INFORMACIÓN EN EL CONSEJO NACIONAL ELECTORAL DE LAPROVINCIA DE SANTA ELENA.* ambato: https://dspace.uniandes.edu.ec/bitstream/123456789/9060/1/TUAEXCOMMIE004-2018.pdf.

Mero Suárez, C. (28 de 5 de 2018). *dspace.uniandes*. Repositorio Digital Uniandes: https://dspace.uniandes.edu.ec/handle/123456789/9060

Mero Suárez, C. R. (1 de septiembre de 2018). *Plan de contingencias informáticas y la seguridad de la información en el Consejo Nacional Electoral de la provincia de Santa Elena*. repositorio digital uniandes : https://dspace.uniandes.edu.ec/handle/123456789/9060

Montesdeoca, B. (20 de septiembre de 2022). *ANALISIS DE RIESGO Y DISENO DE PLAN DE CONTINGENCIA PARA RECUPERACION ANTE DESASTRES EN FLORIDA EDUCATION INSTITUTE (FL-USA) SEGUN LA NORMA ISO 24762-2008*. file:///C:/Users/Personal/Downloads/t2063si.pdf.

Olarte Quispe, P. B. (2021). *Seguridad informática y la vulnerabilidad del sistema de información inalámbrico en la Municipalidad Provincial de La Convención, periodo* . Santa Ana, La Convención, Cusco: https://repositorio.ulp.edu.pe/bitstream/handle/ULP/49/T142_73185092_B_PAUL%20OLARTE.pdf?isAllowed=y&sequence=1.

OÑATE ARBOLEDA, A. (2021). *PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES.* bogota: https://repository.unad.edu.co/bitstream/handle/10596/41984/aonatear_3ago2021.pdf?sequence=1&isAllowed=y.

ORTEGA VENTURA, C. (2024). *"DISEÑO DE UN MARCO DE SEGURIDAD MEDIANTE EL USO DE ESTÁNDARES INTERNA PROCESOS DE DESARROLLO Y DESPLIEGUE DE SISTEMAS INFORMÁTICOS DENTRO DE UNA UNIVERSIDAD PÚBLICA"CIONALES PARA OPTIMIZAR.* https://www.dspace.espol.edu.ec/bitstream/123456789/65847/3/T-115141%20POSTG143%20GARZON-ORTEGA.pdf.

PACHECO POZO, D. (2016). *PROPUESTA DE UN PLAN DE CONTINGENCIA DE TI PARA LA EMPRESA LOGICIEL.* bibdigital.epn. https://doi.org/https://bibdigital.epn.edu.ec/bitstream/15000/15030/1/CD-6841.pdf

Patricio, T. F. (2023). *Evaluación del plan de contingencia ante emergencias de la Facultad de Ingeniería en.* quito:

https://www.dspace.uce.edu.ec/server/api/core/bitstreams/985a2758-3bcd-4a95-baf4-2359e2d52362/content.

Postigo Palacio, A. (2020). *seguridad de la informacion.* https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=Seguridad+de+Inform%C3%A1ticos&ots=-IZUij6Rg0&sig=GqVqrWNeLcae4WOTAsa4KsISLyI#v=onepage&q=Seguridad%20de%20Inform%C3%A1ticos&f=false.

Postigo Palacio, A. (2020). *seguridad de la informacion.* https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=Seguridad+de+Inform%C3%A1ticos&ots=-IZUij6Rg0&sig=GqVqrWNeLcae4WOTAsa4KsISLyI#v=onepage&q=Seguridad%20de%20Inform%C3%A1ticos&f=false.

Postigo Palacio, A. (2020). *seguridad de la informacion.* https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=Seguridad+de+Inform%C3%A1ticos&ots=-IZUij6Rg0&sig=GqVqrWNeLcae4WOTAsa4KsISLyI#v=onepage&q=Seguridad%20de%20Inform%C3%A1ticos&f=false.

Pozo Hernández, C. G., Reascos Pinchao , R. S., & Minaya Macías, R. W. (2025). *Fundamentos de Seguridad Informática y Ciberseguridad.* Manabi: GESICAP.

Prieto, A., Díaz, D., & Santiago, R. (2028). *Metodologías inductivas El desafío de enseñar mediante el cuestionamiento y los retos.* file:///C:/Users/Diana/Downloads/MetodologiasInductivas.pdf.

Sanca Tinta, M. (2011). *Tipos de investigación científica.* http://www.revistasbolivianas.ciencia.bo/pdf/raci/v12/v12_a11.pdf?fbclid=IwAR0kLP7YobJz6CzHlath64ZEiYArh8EgbGoxih_wLUAoyepczuzudL5JhBs.

Sánchez Paredes, V. (2022). *POLÍTICAS DE SEGURIDAD INFORMÁTICA Y VULNERABILIDADES EN EL SISTEMA PARA GENERAR CITAS Y PAGOS DE FACTURACIÓN DEL CONCESIONARIO AMBACAR.* Ambato.

Sánchez Vargas, L. (2019). *FUNDAMENTOS PARA LA ELABORACIÓN DE PLANES ESTRATÉGICOS.* Editorial UNADSello Editorial UNAD]. https://doi.org/Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54931

Santos Llanos, D. (2024). *Gestión de riesgos de seguridad de información, bajo el estándar ISO/IEC 27005:2022, aplicando ontologías de dominio.* lima : https://www.proquest.com/openview/1f67a69b17da1d9af327d201e59c3547/1?cbl=2026366&diss=y&pq-origsite=gscholar.

Solanet i Grau, A. (2020). *El muestreo.* https://openaccess.uoc.edu/server/api/core/bitstreams/c3270301-454c-4126-bb9d-7c9bbf89dab4/content.

Suárez, C. R. (2018). *Plan de contingencias informáticas y análisis de riesgos.* https://dspace.uniandes.edu.ec/handle/123456789/9060?utm_source=chatgpt.com.

Vasquez Ramirez, A. A., & Guanuchi Orellana, L. M. (2023). *MÉTODOS DE INVESTIGACIÓN CIENTÍFICA.* https://unglueit-files.s3.amazonaws.com/ebf/b1d763e3953440199ad2b90c990cf3fa.pdf.

Vieites, A. (2013). *Auditoria de seguridad informatica* . Una entidad puede hacer uso de herramientas para la identificación de debilidades, las cuales permiten conocer la condición actual de un sistema y fortalecer su protección, comprobando que los sistemas de seguridad operan de manera adecuada. Además, estas.

Villacreses Muñoz, G. M. (2022). "DESARROLLO DE UN SISTEMA INFORMÁTICO PARA EL CONTROL DE VENTAS EN LA PASTELERÍA ADONIS DE LA PARROQUIA ABDÓN CALDERÓN DEL CANTÓN PORTOVIEJO". En G. M. VILLACRESES MUÑIZ, *"DESARROLLO DE UN SISTEMA INFORMÁTICO PARA EL CONTROL DE VENTAS EN LA PASTELERÍA ADONIS DE LA PARROQUIA ABDÓN CALDERÓN DEL CANTÓN PORTOVIEJO"* (pág. 176). https://repositorio.unesum.edu.ec/bitstream/53000/3565/1/VILLACRESES%20MU%c3%91IZ%20GEMA%20MOSERRATE.pdf.

ANEXOS

Anexo A: Aprobación de tema

Universidad Laica Eloy Alfaro de Manabí

Periodo 2025-1 - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Estimad@
Docente y Estudiante
Uleam

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

Tema: PLAN DE CONTINGENCIA PARA SEGURIDAD DE INFORMACIÓN EN LOS LABORATORIOS DE CÓMPUTO DE LA CARRERA DE INGENIERÍA EN SOFTWARE DE ULEAM EXTENSIÓN EL CARMEN

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

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

Apellidos y nombres del tutor asginado: POZO HERNANDEZ CLARA GUADALUPE

Apellidos y nombres del estudiante: CAZA ROMERO DIANA PAOLA

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2025-1

Anexo B Instrumento entrevista

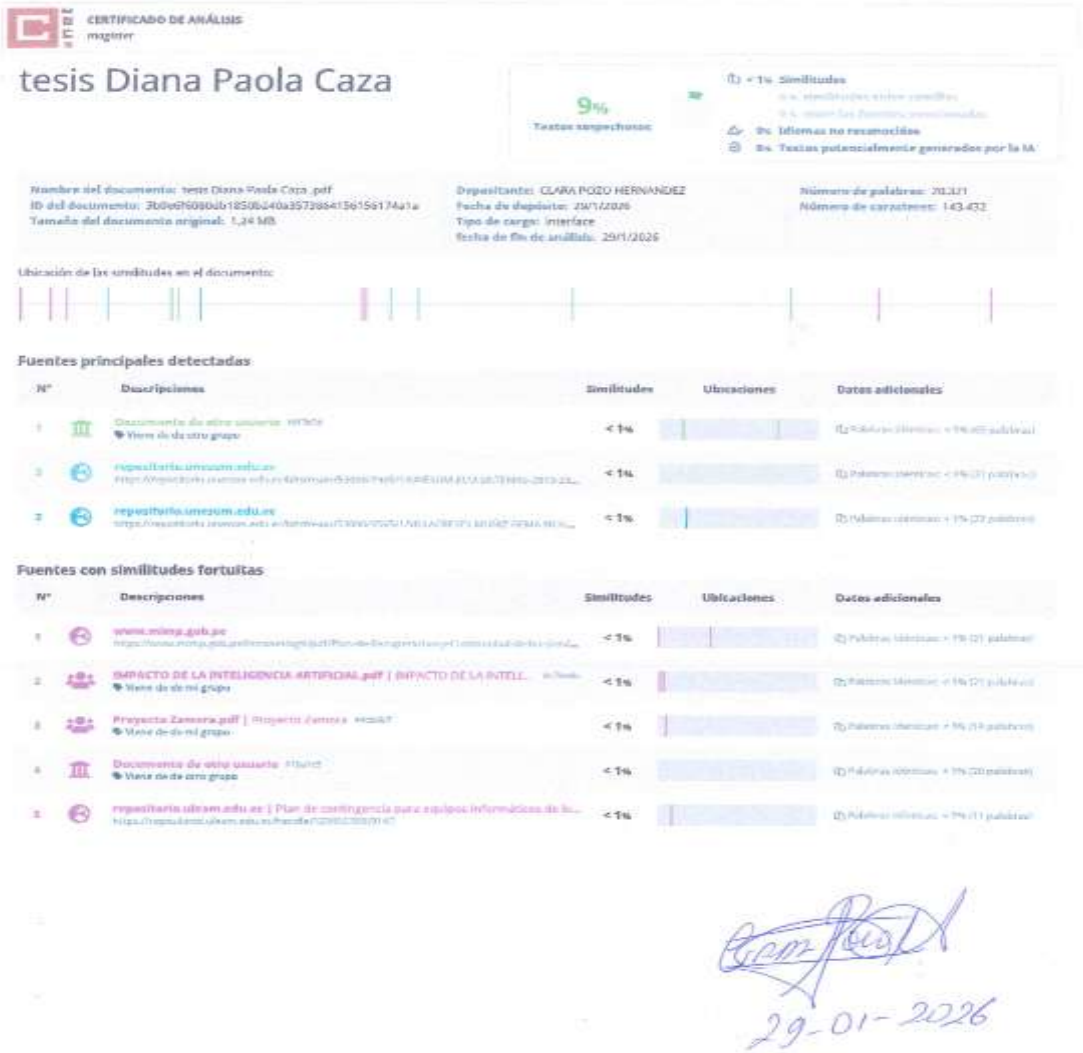
Dirigido a Jean Carlos Cedeño	**Fecha**
Objetivo Identificar el estado actual de las medidas de seguridad en los laboratorios de cómputo, analizando políticas, protocolos, infraestructura y capacitación, para determinar los puntos críticos a abordar en el plan de contingencia que garantice la protección de datos y continuidad operativa.	
1¿Podría describir las políticas de seguridad de la información actualmente implementadas en los laboratorios de cómputo? **2 ¿Qué medidas preventivas se han tomado para evitar la pérdida de datos sensibles en los laboratorios?** **3¿Cómo se maneja la capacitación del personal y a los estudiantes en cuanto a la seguridad de la información en los laboratorios?** **4 ¿Cuál es el proceso para la actualización de equipos y software en los laboratorios de cómputo y con qué frecuencia se realiza?** **5 ¿Ha habido incidentes de interrupción de las actividades académicas debido a fallas de seguridad de la información en los últimos años? Si es así, ¿podría detallarlos?** **6 ¿Existen protocolos específicos para el manejo de datos sensibles por parte de estudiantes y personal en los laboratorios?** **7 ¿Qué herramientas o software de seguridad se utilizan actualmente en los equipos de los laboratorios?** **8 ¿Cómo se monitorea el cumplimiento de las políticas de seguridad por parte de los usuarios de los laboratorios?** **9 ¿Se realizan auditorías de seguridad de forma regular en los laboratorios? Si es así, ¿con qué frecuencia y cuáles son los hallazgos principales?** **10 ¿Qué mejoras o nuevas iniciativas considera prioritarias para fortalecer la seguridad de la información en los laboratorios a corto y mediano plazo?**	

Anexo C Instrumento encuesta

Cuestionario para Analizar Riesgos			C1 1-3
Preguntas (Malware)	**Respuesta**		**Observaciones**
	Si	**No**	
1. ¿Existe una política de seguridad definida para la protección contra malware?			
2. ¿Se cuenta con un software antivirus actualizado en los equipos del laboratorio?			
3. ¿Los usuarios tienen restricciones para la instalación de software no autorizado?			
4. ¿Se realizan análisis periódicos para detectar posibles infecciones?			
5. ¿Existen medidas para prevenir ataques de phishing dentro de la red del laboratorio?			
6. ¿Se cuenta con control de acceso para evitar el uso no autorizado de los dispositivos?			
7. ¿Los sistemas operativos están actualizados con parches de seguridad?			
8. ¿Se han identificado incidentes previos de malware en el laboratorio?			
9. ¿Los estudiantes reciben capacitación sobre buenas prácticas de seguridad informática?			
10. ¿Las redes Wi-Fi cuentan con medidas de protección contra accesos no autorizados?			
11. ¿Se utilizan herramientas de monitoreo para detectar comportamiento sospechoso en los equipos?			
12. ¿Existe un procedimiento de respuesta en caso de infección por malware?			
13. ¿Se aplican filtros de contenido para prevenir el acceso a sitios maliciosos?			
14. ¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?			
15. ¿El tráfico de red es monitoreado para detectar actividad sospechosa?			
16. ¿Los dispositivos USB están restringidos para evitar infecciones?			
17. ¿Los archivos de descarga son verificados antes de su uso?			
18. ¿Se han realizado auditorías previas que detecten vulnerabilidades en la lógica de seguridad?			
19. ¿Existen políticas de gestión de actualizaciones para reducir riesgos de infección?			
20. ¿Se implementan registros de actividad para identificar intentos de acceso sospechosos?			
21. ¿Los accesos a cuentas institucionales están protegidos con autenticación de múltiples factores?			
22. ¿Los servidores del laboratorio tienen protecciones específicas contra ataques externos?			
23. ¿Se han documentado procedimientos de limpieza y eliminación de malware en los equipos?			
24. ¿Se cuenta con herramientas de análisis forense para detectar el origen de una infección?			
25. ¿Las medidas de seguridad actuales han sido probadas mediante pruebas de penetración?			
Realizado por **Fecha:**			
Revisado por: **Fecha:**			

Anexo D Fotografía

Anexo E Certificación de coincidencia académica



CERTIFICADO DE ANÁLISIS
magister

tesis Diana Paola Caza

9%
Textos sospechosos

< 1% Similitudes
0% Idiomas no reconocidos
0% Textos potencialmente generados por la IA

Nombre del documento: tesis Diana Paola Caza .pdf
ID del documento: 3b0e9f6080db1850b240a3573984f3615617441a
Tamaño del documento original: 1,24 MB

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 29/1/2026
Tipo de carga: interface
Fecha de fin de análisis: 29/1/2026

Número de palabras: 20.321
Número de caracteres: 143.432

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario #f7b67d Viene de otro grupo	< 1%		
2	repositorio.unesum.edu.ec https://repositorio.unesum.edu.ec/bitstream/53000/7449/1/UNESUM-ECUADOR-2019-23...	< 1%		
3	repositorio.unesum.edu.ec https://repositorio.unesum.edu.ec/bitstream/53000/5026/1/UNESUM-ECUADOR-2019-23...	< 1%		

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.minp.gob.pe https://www.minp.gob.pe/Informacion/gestion/Plan-de-Contingencia-para-Equipos-Informaticos-de-la-...	< 1%		
2	IMPACTO DE LA INTELIGENCIA ARTIFICIAL.pdf (IMPACTO DE LA INTELL... Viene de de mi grupo	< 1%		
3	Proyecto Zamora.pdf (Proyecto Zamora #f0d6f7 Viene de de mi grupo	< 1%		
4	Documento de otro usuario #7bcfcf Viene de de otro grupo	< 1%		
5	repositorio.uleam.edu.ec (Plan de contingencia para equipos informáticos de la... https://repositorio.uleam.edu.ec/handle/123456789/3167	< 1%		

29-01-2026

Anexo F Cuestionario lleno

Cuestionario para Analizar Riesgos			C1 I-3
Preguntas (Malware)	**Respuesta**		**Observaciones**
	Si	**No**	
1. ¿Existe una política de seguridad definida para la protección contra malware?		X	
2. ¿Se cuenta con un software antivirus actualizado en los equipos del laboratorio?	X		Solo contiene el Windows defe
3. ¿Los usuarios tienen restricciones para la instalación de software no autorizado?		X	
4. ¿Se realizan análisis periódicos para detectar posibles infecciones?	X		Cada tres meses
5. ¿Existen medidas para prevenir ataques de phishing dentro de la red del laboratorio?		X	
6. ¿Se cuenta con control de acceso para evitar el uso no autorizado de los dispositivos?		X	
7. ¿Los sistemas operativos están actualizados con parches de seguridad?	X		
8. ¿Se han identificado incidentes previos de malware en el laboratorio?		X	
9. ¿Los estudiantes reciben capacitación sobre buenas prácticas de seguridad informática?		X	
10. ¿Las redes Wi-Fi cuentan con medidas de protección contra accesos no autorizados?	X		
11. ¿Se utilizan herramientas de monitoreo para detectar comportamiento sospechoso en los equipos?	X		
12. ¿Existe un procedimiento de respuesta en caso de infección por malware?	X		
13. ¿Se aplican filtros de contenido para prevenir el acceso a sitios maliciosos?	X		
14. ¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?		X	
15. ¿El tráfico de red es monitoreado para detectar actividad sospechosa?	X		
16. ¿Los dispositivos USB están restringidos para evitar infecciones?		X	
17. ¿Los archivos de descarga son verificados antes de su uso?	X		
18. ¿Se han realizado auditorías previas que detecten vulnerabilidades en la lógica de seguridad?		X	
19. ¿Existen políticas de gestión de actualizaciones para reducir riesgos de infección?		X	
20. ¿Se implementan registros de actividad para identificar intentos de acceso sospechosos?		X	
21. ¿Los accesos a cuentas institucionales están protegidos con autenticación de múltiples factores?	X		
22. ¿Los servidores del laboratorio tienen protecciones específicas contra ataques externos?		X	
23. ¿Se han documentado procedimientos de limpieza y eliminación de malware en los equipos?	X		
24. ¿Se cuenta con herramientas de análisis forense para detectar el origen de una infección?		X	
25. ¿Las medidas de seguridad actuales han sido probadas mediante pruebas de penetración?		X	

Realizado por Diana Paola Caza Romero	**Revisado por:** Ing Clara Guadalupe Pozo Hernandez
Fecha: 16/10/2025	**Fecha:**

Cuestionario para analizar Riesgos			C1 2-3
Preguntas (Robo)	**Respuesta**		**Observaciones**
	Si	**No**	
1. ¿Existe cámara de seguridad instalada en el laboratorio?	✓		
2. ¿Las cámaras de seguridad están funcionando correctamente?	✓		
3. ¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?	✓		
4. ¿Existe responsable de la seguridad de los laboratorios?	✓		
5. ¿Existen procedimientos para reportar un robo?	✓		
6. ¿Se han registrado incidentes previos de robo en los laboratorios?		✓	
7. ¿Los activos del laboratorio cuentan con medidas de protección física actualmente?	✓		
8. ¿Existe un control de acceso restringido para el ingreso a los laboratorios?		✓	
9. ¿Los equipos están identificados con códigos o etiquetas?		✓	
10. ¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?	✓		
11. ¿Existe un sistema de registro actualizado sobre el ingreso a esta área?	✓		
12. ¿Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?		✓	
13. ¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?		✓	
14. ¿Hay restricciones para la salida de equipos del laboratorio?	✓		
15. ¿Existen mecanismos para monitorear la actividad dentro del laboratorio?	✓		
16. ¿Se verifica el estado y funcionamiento de los equipos físicos en el laboratorio?	✓		
17. ¿Existe un sistema de comunicación rápida para reportar incidentes?	✓		
18. ¿Los accesos principales están bajo vigilancia constante?		✓	
19. ¿Se cuenta con sistemas de alarma en los laboratorios?		✓	
20. ¿Los equipos están atados o asegurados básicamente?		✓	
21. ¿Se han registrado informes de robo recientemente?		✓	
22. ¿Hay dispositivos de rastreo en los equipos?		✓	
23. ¿Los laboratorios tienen sensores de movimiento?	✓		
24. ¿Existen protocolos claros para la investigación de incidentes?		✓	
25. ¿Se aplican sanciones o medidas disciplinarias en casos de hurto?	✓		

Realizado por Liana Paola Cano Romero

Fecha: 16/10/2025

Revisado por: Ing. Clara Guadalupe Pozo Hernandez

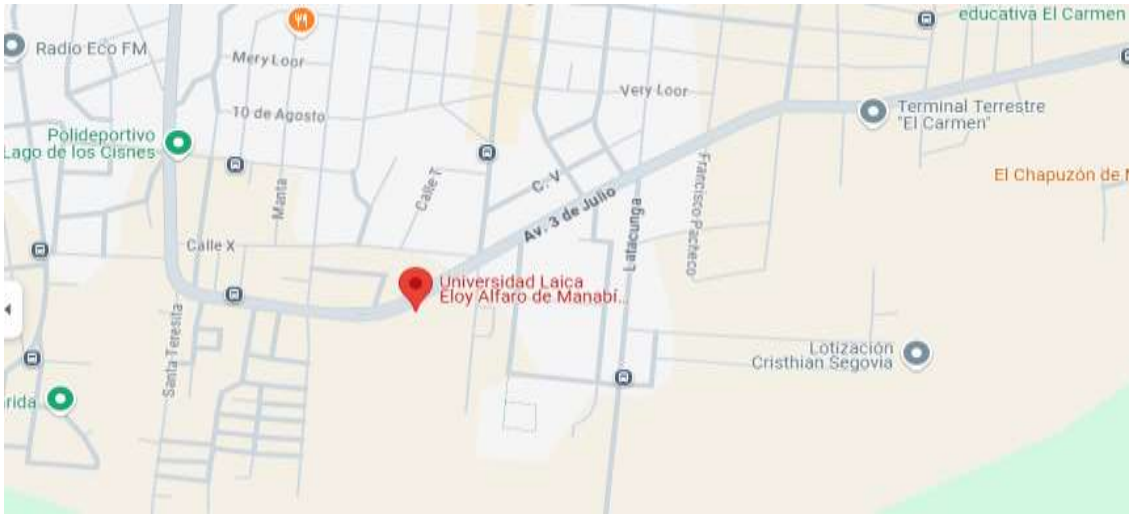
Fecha:

Cuestionario para Analizar Riesgos			CI 3-3
Preguntas (Daño)	**Respuesta**		**Observaciones**
	Sí	**No**	
1. ¿Las superficies de trabajo donde se ubican los equipos son adecuadas?	X		
2. ¿Se han reportado daños por caídas o golpes?	X		
3. ¿Los periféricos del equipo (teclado, monitor y mouse) presentan signos de mal uso?	X		
4. ¿Se realizan inspecciones para detectar desgaste o fallas en los equipos?	X		
5. ¿El sistema de cableado está organizado adecuadamente?	X		
6. ¿Se cuenta con protección contra sobrecarga eléctrica?		X	No cuentan los UPS
7. ¿Los equipos de los laboratorios se utilizan siguiendo las medidas de seguridad física para prevenir daños?	X		
8. ¿Existen registros de mantenimiento preventivo de los equipos?	X		
9. ¿Hay señales visibles de maltrato físico en los equipos?	X		
10. ¿Los equipos están expuestos a humedad o líquidos?		X	
11. ¿Los equipos tienen ventilación suficiente para evitar sobrecalentamientos?	X		
12. ¿Se han identificado equipos con fallas recurrentes?	X		
13. ¿Se han implementado procedimientos para reportar daños?	X		
14. ¿Los equipos se apagan correctamente después de su uso?		X	
15. ¿Se han reportado incidentes debido al uso inadecuado de los dispositivos en el laboratorio?	X		
16. ¿Se han tomado medidas para reducir las amenazas ambientales que afectan a los equipos?		X	
17. ¿Se da mantenimiento preventivo periódico a los equipos?	X		
18. ¿Los usuarios tienen normas claras sobre el cuidado de los dispositivos?	X		
19. ¿Las conexiones eléctricas son revisadas regularmente?		X	
20. ¿Se han encontrado problemas en la estructura del laboratorio?	X		
21. ¿El laboratorio tiene cableado estructurado?	X		
22. ¿Se controla la temperatura y ventilación del laboratorio?	X		
23. ¿Se permite el ingreso de alimentos o bebidas?		X	
24. ¿Hay un responsable designado para el cuidado del equipo?	X		
25. ¿Se inspeccionan los equipos al final de cada jornada?	X		

Realizado por Dicen, Paula Cazo Romero
Fecha: 16/09/2025

Revisado por: Ing Clara Guadalupe Pozo Hernández
Fecha:

Anexo G evidencia del lugar de la investigación


Radio Eco FM
Mery Loor
10 de Agosto
Polideportivo
Lago de los Cisnes
Manta
Calle Y
C. V
Av. 3 de Julio
Latacunga
Francisco Pacheco
Calle X
Universidad Laica
Eloy Alfaro de Manabí
Santa Teresita
Lotización
Cristhian Segovia
Vety Loor
Terminal Terrestre
"El Carmen"
educativa El Carmen
El Chapuzón de

GLOSARIO

Activo de información: Elemento que posee valor para la institución y requiere protección, como datos, equipos, software, redes y documentación.

Amenaza: Evento o acción potencial que puede afectar negativamente la seguridad de la información o la continuidad de los servicios TIC.

Análisis de riesgos: Proceso sistemático para identificar, evaluar y priorizar riesgos considerando amenazas, vulnerabilidades, impacto y probabilidad.

AES Estándar de Cifrado Avanzado

Backup (Respaldo de información) Copia de seguridad de los datos que permite su recuperación ante pérdidas, daños o fallos del sistema.

Ciberataques: Acciones malintencionadas realizadas a través de medios digitales con el fin de dañar, robar o alterar sistemas informáticos o información.

Continuidad de servicios TIC: Capacidad de mantener o restablecer los servicios tecnológicos críticos tras un incidente disruptivo.

Control de acceso: Mecanismo que regula el ingreso y uso de sistemas, equipos o información solo a usuarios autorizados.

Contingencia; Es un evento que puede suceder o no. Se refiere a una situación de riesgo o una emergencia imprevista que obliga a cambiar los planes originales**.**

Deficiencia: Como vimos antes, es una falla, imperfección o falta de algo necesario. Es cuando algo es insuficiente o no alcanza el nivel que debería tener.

Directrices: Conjunto de normas, orientaciones o lineamientos que indican cómo deben realizarse determinadas acciones o procedimientos.

Divulgación: Acción de difundir o dar a conocer información a un grupo de personas de forma clara y accesibl**e.**

Disponibilidad: Principio de la seguridad de la información que garantiza que los activos estén accesibles cuando se requieran.

DES Estándar de Cifrado de Datos

Gestión de incidentes : Proceso estructurado para manejar incidentes de seguridad y minimizar su impacto en la continuidad de los servicios.

Infraestructura: Conjunto de recursos físicos y tecnológicos necesarios para el funcionamiento de una organización o sistema, como equipos, redes y software**.**

Incidente de seguridad: Evento que compromete o pone en riesgo la confidencialidad, integridad o disponibilidad de la información.

Integridad: condición de mantenerse completo, correcto y sin alteraciones.

ISO/IEC 27031: Norma internacional que proporciona directrices para la preparación y continuidad de las tecnologías de la información y la comunicación.

Laboratorios de cómputo: Espacios académicos equipados con infraestructura tecnológica para actividades educativas y de investigación.

Lógico: Algo que tiene sentido, coherencia o que sigue las reglas de la razón.

La dependencia de lo divino: Creencia o actitud de confiar en una fuerza superior o espiritual para afrontar situaciones de la vida.

Malware: Software malicioso diseñado para dañar sistemas, robar información o interrumpir servicios tecnológicos.

Matriz de riesgos: Herramienta que permite evaluar y priorizar riesgos según su impacto y probabilidad de ocurrencia.

Operatividad: Capacidad de un sistema, proceso u organización para funcionar de manera correcta, eficiente y continua.

Plan de contingencia: Conjunto de procedimientos y acciones destinadas a responder ante incidentes y asegurar la continuidad de los servicios TIC.

Proactiva: Actitud orientada a anticiparse a los problemas y actuar de manera preventiva antes de que ocurran.

Paradigma: Modelo, enfoque o forma de pensar que sirve como referencia para comprender o interpretar una realidad.

Plan: Es un modelo o guía detallada que se elabora para lograr un objetivo.

Particulares; Se refiere a cosas o personas específicas, propias o privadas

Recuperación de servicios: Proceso de restablecimiento de sistemas y servicios tecnológicos después de un incidente.

Respuesta ante incidentes: Acciones coordinadas para detectar, contener, mitigar y solucionar incidentes de seguridad.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo.

Seguridad de la información: Protección de la información para preservar su confidencialidad, integridad y disponibilidad.

Servicios TIC: Conjunto de recursos tecnológicos que apoyan los procesos académicos y administrativos.

Sensibilizar: Hacer que las personas tomen conciencia sobre un tema, problema o riesgo, fomentando una actitud responsable**.**

Vulnerabilidad: Debilidad en un sistema o proceso que puede ser aprovechada por una amenaza.

Vulnerabilidad: Debilidad o punto frágil que puede ser aprovechado para causar daño, especialmente en sistemas, personas u organizaciones**.**