UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR

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

PLAN DE RECUPERACIÓN DE DESASTRES PARA LA SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL LABORATORIO 1 DE LA CARRERA DE INGENIERÍA EN SOFTWARE DE LA ULEAM EXTENSIÓN EI CARMEN.

MOREIRA HUERTA ANGIE ELIZABETH
AUTORA

ING, POZO HERNANDEZ CLARA GUADALUPE, MG.
TUTORA

EL CARMEN, ENERO 2026

Certificación del director de trabajo de graduación

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

CERTIFICACIÓN

En calidad de docente tutor(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 **MOREIRA HUERTA ANGIE ELIZABETH**, 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 RECUPERACIÓN DE DESASTRES PARA LA SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL LABORATORIO 1 DE LA CARRERA DE INGENIERÍA EN SOFTWARE DE LA 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, 28 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 recuperación de desastres para la seguridad física de los equipos informáticos en el laboratorio 1 de la carrera de ingeniería en software de la Uleam extensión El Carmen.

Modalidad: Proyector Integrador

Autora: Moreira Huerta Angie Elizabeth

Tutora: Ing. Pozo Hernandez Clara Guadalupe, Mg.

Tribunal de Sustentación:

Presidente:

Ing. Reascos Pinchao Raul Saed, Mg.

Miembro:

Ing. Mendoza Villamar Rocio Alexandra, Mg.

Miembro:

Ing. Arévalo Hermida Rómulo Danilo, Mg.

Fecha de Sustentación:
19 de Febrero de 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 RECUPERACIÓN DE DESASTRES PARA LA SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL LABORATORIO 1 DE LA CARRERA DE INGENIERÍA EN SOFTWARE DE LA ULEAM EXTENSIÓN EI CARMEN., corresponde exclusivamente a: Moreira Huerta Angie Elizabeth con CI. 2350673006, y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Angie Elizabeth Moreira Huerta
C.I. 2350673006

Dedicatoria

A Dios por ser mi guía y apoyo eterno, por haberme otorgado fortaleza, el conocimiento y la resiliencia que han iluminado cada paso de este difícil trayecto académico.

A mis queridos padres, cuyo amor sin condiciones y sacrificios callados han sido la base de cada uno de mis éxitos desde mi nacimiento, sus bendiciones constantes me arropan, su fe en mí y sus palabras de aliento han sido mi fuerza en los momentos más difíciles. Esta tesis es mi ofrenda de gratitud por su entrega infinita. Los amo con todo mí ser.

A mi querido esposo, por su paciencia infinita, su comprensión incansable y su aliento incesante durante estos años de estudio, tu compañía ha sido mi sostén en cada desafío y la alegría detrás de cada logro.

Y a toda mi familia, por estar siempre cerca, animarme sin condiciones y ser parte esencial de este triunfo. Gracias por caminar junto a mí en cada etapa de este proceso.

Angie Moreira

Agradecimiento

Deseo manifestar mi agradecimiento más sincero a la Universidad por darme la oportunidad de conseguir este éxito académico, también agradezco a la carrera de Tecnologías de la Información por brindarme las habilidades y conocimientos que ahora respaldan mi vocación profesional.

También quiero expresar mi gratitud a todos los docentes, por compartir de manera generosa su conocimiento y su pasión por la enseñanza.

Para mi tutora de tesis, la Ing. Clarita Pazo Hernández, está destinado un reconocimiento especial, su orientación, instrucción y soporte constante fueron fundamentales para terminar este trabajo profundamente agradecida.

Angie Moreira

Índice de contenidos

Índice tablas

Índice gráfico e ilustraciones

Índice de anexos

Resumen

.

Este proyecto integrador propone el diseño de un Plan de Recuperación de Desastres enfocado en la protección física del equipamiento informático del Laboratorio 1 de la carrera de Ingeniería en Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. Para el diagnóstico de la problemática se empleó un enfoque cuantitativo, descriptivo y aplicado, apoyado en fuentes académicas confiables. Además, se realizó una entrevista al Ing. Jean Carlos Cedeño, responsable de los laboratorios, y una encuesta dirigida a una población finita de 149 estudiantes, con el objetivo de obtener información clara y precisa sobre el estado actual del laboratorio. Los resultados del diagnóstico evidenciaron como problema central la alta vulnerabilidad del laboratorio frente a constantes fallas eléctricas, la inexistencia de sistemas adecuados de protección eléctrica, como reguladores o fuentes de alimentación funcionales, y la ausencia de protocolos de seguridad física y mantenimiento preventivo. Como propuesta, se realizó una auditoría de seguridad física la cual abordo el análisis de los riesgos relacionados como robo, daño, incendio, inundación y el malware de estos riesgos, el malware y el incendio fueron clasificados como muy grave, el robo y la inundación como grave y el daño como un riesgo importante, tomando en cuenta estos resultados se emplea la metodología establecida en el estándar internacional NIST SP 800-34 Rev. 1 para diseñar un Plan de Recuperación de Desastres con la finalidad de garantizar la continuidad funcional del laboratorio y la protección de los activos tecnológicos ante situaciones adversos.

Abstract

This integrated project proposes the design of a Disaster Recovery Plan focused on the physical protection of the computer equipment in Laboratory 1 of the Software Engineering program at the Eloy Alfaro Lay University of Manabí, El Carmen Extension. A quantitative, descriptive, and applied approach was used to diagnose the problem, supported by reliable academic sources. In addition, an interview was conducted with Eng. Jean Carlos, the laboratory manager, and a survey was administered to a finite population of 149 students to obtain clear and precise information about the laboratory's current state. The diagnostic results revealed the central problem to be the laboratory's high vulnerability to frequent power outages, the lack of adequate electrical protection systems, such as voltage regulators or functional power supplies, and the absence of physical security and preventive maintenance protocols. As a proposal, a physical security audit was carried out which addressed the analysis of related risks such as theft, damage, fire, flood and malware. Of these risks, malware and fire were classified as very serious, theft and flood as serious and damage as a significant risk. Taking into account these results, the methodology established in the international standard NIST SP 800-34 Rev. 1 is used to design a Disaster Recovery Plan in order to guarantee the functional continuity of the laboratory and the protection of technological assets in adverse situations.

Capítulo I

1 Introducción

1.1 Introducción

Un proceso estratégico vital para detectar los riesgos y las debilidades que ponen en peligro los activos tecnológicos del laboratorio es el diseño de un Plan de Recuperación de Desastres que tiene como objetivo la seguridad física. Para la capacitación de profesionales, para que las actividades académicas se desarrollen con normalidad y para asegurar un ambiente eficaz en la institución, esta área es crucial; De este modo, se asegura que las herramientas tecnológicas estén siempre al alcance para el aprendizaje.

Después de haber llevado a cabo un análisis minucioso del estado actual del laboratorio 1, se examinaron y luego plantearon las necesidades concretas para robustecer la seguridad de los equipos informáticos en el laboratorio según la Información recopilada, se enfocó en implementar medidas de control para evitar el acceso no autorizado y el uso indebido del hardware, los cuales han sido identificados como las principales causas de incidentes técnicos pasados.

El objetivo de la realización de este proyecto es crear un ambiente más eficaz, salvaguardando la infraestructura y disminuyendo los peligros que generan efectos negativos en los activos, el análisis se enfocó en el laboratorio 1 de la carrera de Ingeniería en Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen en este, se examinaron varios niveles de riesgo relacionados con la falta de protocolos básicos de seguridad.

El análisis permitió identificar las amenazas reales que representan un riesgo para los equipos de cómputo, lo cual posibilitó diseñar un plan de recuperación con reglas definidas para evitar inconvenientes y conocer cómo actuar en caso de que algo salga mal, garantizando que todos los sistemas estén funcionando apropiadamente y que el equipo tecnológico esté protegido a largo plazo, es imprescindible implementar estas estrategias en la infraestructura del laboratorio.

1.2 Presentación del tema

Plan de recuperación de desastres para la seguridad física de los equipos informáticos en el laboratorio 1 de la carrera de Ingeniería en Software de la ULEAM Extensión el Carmen.

1.3 Ubicación y contextualización de la problemática

Ilustración 1: Instalaciones de la ULEAM extensión el Carmen

Ilustración 2: Aspecto laboratorio 1 en la carrera de ingeniería de software.

Ilustración 3: Ubicación de la Universidad Laica Eloy Alfaro de Manabí – Extensión El Carmen.

La Universidad Laica Eloy Alfaro de Manabí Extensión "El Carmen" está ubicada en cantón el Carmen de la provincia de Manabí, en la avenida 3 de Julio; es una entidad académica enfocada a formar profesionales emprendedores y competentes. Brinda 11 carreras en áreas como ingeniería, salud, tecnología y contabilidad, cada programa cuenta con laboratorios especializados en particular.

La carrera Ingeniería de Software cuenta con dos laboratorios habilitados en la segunda planta del edificio principal, se tomó uno de los laboratorios el cual es identificado como "Laboratorio 1", el cual dispone de 25 computadoras distribuidas de la siguiente manera: 12 escritorios divididos en 3 filas de computadoras, en cada escritorio existen 2 computadoras para los estudiantes , sumando el escritorio y computadora del docente entre los 25 equipos de cómputo disponibles 20 son de la marca ASUS, 3 de la marca LG, 1 de la marca ACER y 1 de la marca BENQ, todas cuentan con una memoria RAM de 8 GB, tarjeta gráfica de Intel UHD 630 integrada, discos duros igual o mayores a 500 GB y procesadores desde Intel Core i5 hasta Intel Core i7 CPU con velocidades de hasta 2.90GHz.

1.4 Planteamiento del problema

1.4.1 Problematización

¿Cuáles son los principales riesgos que pueden comprometer la seguridad física de los equipos informáticos en el Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen y de qué manera un Plan de Recuperación de Desastres podría mitigar estos riesgos para garantizar su protección y funcionamiento óptimo?

1.4.2 Génesis del problema

El génesis del problema radica en la vulnerabilidad de los equipos informáticos del Laboratorio 1 ante eventos adversos como: desastres naturales, fallas humanas, incendios, inundaciones o robos esta vulnerabilidad puede deberse a factores como deficiencias en las medidas de seguridad física, o incluso la ausencia de una capacitación adecuada en manejo de riesgos. En aspectos geofísicos El Carmen en épocas de invierno sufre lluvias muy fuertes lo cual con el deterioro de las instalaciones puede causar humedad y puede por terminar en daños en los equipos tecnológicos en aspectos institucionales un mayor número de estudiantes puede abrir la puerta a más probabilidad de expansión de virus y finalmente en aspectos académicos muchas materias necesitan aplicaciones que consumen mucha memoria y a su vez provienen de páginas de dudosa procedencia, lo cual limita las funcionalidades de los equipos.

1.4.3 Estado actual del problema

Aunque el laboratorio opera normal actualmente, enfrenta serias deficiencias en la protección física de sus equipos, la carencia de mecanismos de vigilancia como: cámaras de seguridad y la ausencia de un control de acceso adecuado permite el ingreso de personas no autorizadas, elevando el peligro de hurtos, sabotaje al hardware o alteraciones no autorizadas del software. Así mismo, la falta de protecciones contra variaciones de voltaje y condiciones climáticas adversas pone en riesgo los dispositivos, pudiendo ocasionar daños permanentes y la perdida de datos importantes. Este escenario se ha agravado por la escasa supervisión de docentes o personal de vigilancia, lo que deriva en mal uso de los computadores, infección por malware mediante memorias USB y saturación de archivos innecesarios que perjudican la eficiencia del sistema.

El laboratorio cuenta con 25 computadoras, de las cuales 20 funcionan con normalidad, 3 presentan fallas recurrentes y 2 están inoperativas debido a daños en sus

componentes. La ausencia de personal dedicado a la supervisión y mantenimiento permite que los equipos deteriorados permanezcan sin reparación por largos periodos, afectando la disponibilidad para los estudiantes. Además, la falta de sistemas de alimentación ininterrumpida (UPS) o reguladores de voltaje los hace vulnerables a los frecuentes cortes de energía, lo que incrementa el riesgo de daños irreversibles en el hardware y la pérdida de datos. Esta situación no solo genera gastos adicionales, sino que también obliga a los alumnos a depender de sus propios dispositivos, evidenciando las carencias en la infraestructura de seguridad y mantenimiento del laboratorio.

1.5 Diagrama causa – efecto del problema

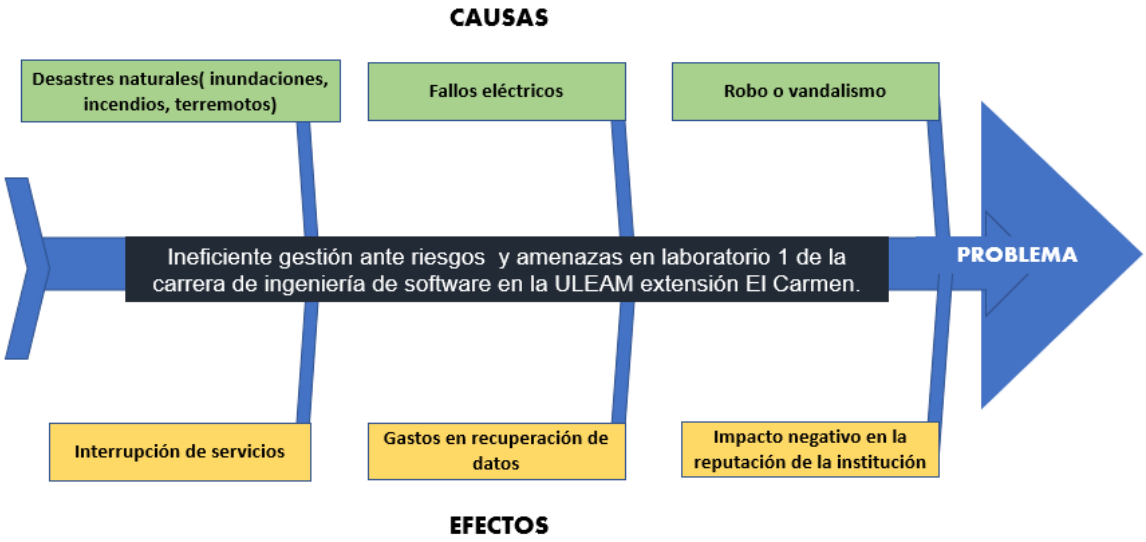


Ilustración 4: Árbol del problema

1.6 Objetivos

1.6.1 Objetivo general

Diseñar un plan de recuperación de desastres para la seguridad física de los equipos informáticos en el laboratorio1 de la carrera de ingeniería en software de la ULEAM extensión el Carmen

1.6.2 Objetivos específicos

- Identificar problemas que puedan afectar la integridad y seguridad física de los equipos tecnológicos en el laboratorio 1 de la carrera de ingeniería de software de la ULEAM Extensión El Carmen.

- Investigar fuentes bibliográficas confiables basándome en las variables independiente (plan de recuperación ante desastres) y dependiente (seguridad física de los equipos tecnológicos) para fundamentar conceptualmente la investigación.
- Recopilar información mediante encuestas y entrevistas dirigidas a docentes, estudiantes y personal técnico del Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen.
- Realizar un análisis de riesgos para identificar las amenazas potenciales que puedan afectar la seguridad física de los equipos informáticos en el Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen.
- Definir protocolos de actuación ante emergencias en el laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen determinando roles y responsabilidades del personal durante una contingencia.
- Documentar el plan de recuperación ante desastres para facilitar copias al personal de mantenimiento y encargados del uso del Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen.

1.7 Justificación

El diseño de un Plan de Recuperación de Desastres (DRP) enfocado en el Laboratorio 1 de Ingeniería en Software de la ULEAM Extensión “El Carmen” resulta crucial para proteger y mantener en el tiempo los recursos tecnológicos que son el sustento de la formación profesional de los estudiantes. Estos equipos como la información que albergan son importantes para el desarrollo de prácticas en programación y desarrollo de software, por lo que su operatividad es indispensable y cualquier interrupción podría tener consecuencias en el proceso educativo y un impacto económico a la institución.

El estado actual de los equipos tecnológicos del laboratorio los evidencia a diversos riesgos, como fallas eléctricas, la humedad, los robos o deficiencias en su seguridad, lo que los hace vulnerables a daños constantes, al diseñar un plan de recuperación adecuadamente no solo contribuiría a la protestación y conservación de estos recursos esenciales, sino que también definiría procedimientos efectivos para restaurar las operaciones rápidamente ante cualquier incidente, asegurando así una disrupción mínima en las funciones académicas.

Este proyecto busca garantizar la protección de los equipos tecnológicos, además de también promover la excelencia académica y una gestión más eficaz de los recursos al optimizar los planes de contingencia ante emergencias. Al adoptar estas medidas, la Universidad refuerza su compromiso con una educación de calidad. La implementación del plan impactará positivamente a toda la comunidad universitaria y servirá como modelo para extender estas prácticas a otros laboratorios y espacios académicos, impulsando así el avance tecnológico de la institución.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Un proyecto como este generará un impacto tecnológico de gran nivel al proteger y fortalecer la infraestructura informática del laboratorio. Al incorporar medidas para evitar picos eléctricos, solucionar perdida de datos y redundancia de información en los ordenadores. Esto reducirá drásticamente los tiempos de inactividad mediante protocolos de recuperación rápida y copias de seguridad automatizadas, haciendo del laboratorio un entorno confiable y de alta disponibilidad para los estudiantes. Además, la integración de medidas de seguridad cibernética y física garantizará la protección de datos sensibles.

1.8.2 Impacto social

Su impacto directo es en el ámbito educativo garantizando la continuidad de los dispositivos y así evitando interrupciones en la formación académica de los estudiantes de ingeniaría de software, asegurando que las clases, proyectos y otras actividades académicas se lleven a cabo, que los docentes no tengan la necesidad de cambiar su cronograma de clases y las prácticas en programación se den de manera adecuada.

Un laboratorio funcional y seguro es crucial para estudiantes de escasos recursos que dependen de estos equipos para acceder a tecnología de punta. Ya que muchos estudiantes dependen netamente de los laboratorios al no contar con una laptop, con esto reduce la brecha tecnológica y evita la exclusión digital al garantizar que todos los alumnos tengan igual acceso a los recursos. Además, fomenta una cultura estudiantil de prevención de desastres en los laboratorios y cuidado de los equipos tecnológicos, haciendo tomar conciencia a estudiantes de la importancia de estas herramientas para su formación y futuro profesional

1.3.3 Impacto ecológico

Un plan de recuperación efectivo evita la obsolescencia programada prolongando la vida útil de los equipos su efecto es prevenir daños irreparables causados por amenazas como: fallas eléctricas, incendios o desastres naturales. Esto disminuye la generación de chatarra electrónica, que tiene residuos muy contaminantes por sus componentes tóxicos (plomo, mercurio, cadmio, litio). Al evitar cambiar recurrentemente de hardware, se reduce la huella ecológica asociada a la fabricación, transporte y disposición final de estos dispositivos.

Capítulo II

2 Marco teórico de la investigación

2.1 Antecedentes históricos

2.1.1 Plan de recuperación ante desastres (DRP)

La creación de los planes de recuperación ante desastres (DRP) ha ido desarrollándose continuamente, a raíz del progreso tecnológico y las demandas en constante cambio de la industria empresarial. Desde 1970, cuando las compañías comenzaron a depender más de los sistemas informáticos, se hizo evidente la necesidad de poner en marcha medidas que garanticen la continuidad operativa después de una crisis. Inicialmente, estos planos se fundamentaban en métodos físicos, tales como la redundancia de los equipos o el acceso a centros de datos secundarios, estos últimos fueron clasificados en tres modalidades: fría, templada o caliente, de acuerdo a su precio y velocidad de recuperación. La ley de 1983 de EE.UU. UU., que exigía a los bancos nacionales disponer con protocolos de respaldo verificables, fue un hito en la normalización y regulación de estos procedimientos. (Bigelow, 2025)

El Instituto de Recuperación de Desastres adaptó sus certificaciones para reflejar esta evolución a lo largo de la década de los 90, cuando el proceso de La recuperación ante desastres pasó de ser meramente técnico a una visión de continuidad del negocio que toma en cuenta todos los factores. La virtualización y el incremento de la capacidad de red durante la década del 2000 al 2010 han cambiado la protección de los datos. Hoy en día, los modelos como DRaaS (Disaster Recovery as a Service) son factibles gracias a la nube y ofrecen mayor agilidad y flexibilidad. No obstante, la externalización de estos servicios trae consigo nuevos retos, esto requiere auditorías rigurosas y protocolos de seguridad más robustos. La meta es salvaguardar información crítica ante amenazas crecientes. Esta evolución pone de manifiesto que se requieren tácticas más adaptables y resistentes (Council, 2020)

2.1.2 Seguridad física de equipos informáticos

Desde la era de los mainframes y minicomputadoras (1950 - 1970), las organizaciones implementaron protocolos de seguridad física para resguardar su infraestructura tecnológica. Estas medidas iban desde la instalación de sistemas de

vigilancia perimetral y personal de seguridad hasta la ubicación de equipos en áreas de acceso controlado, buscando prevenir actos de sabotaje, hurtos o malversaciones internas. Durante este periodo, se elaboraron prácticas como: Procedimientos de selección rigurosa para los funcionarios técnicos, igualmente la aplicación de estándares criptográficos (Data Encryption Standard, 1974). Estas medidas de seguridad física se unificaron estratégicamente con los progresos en criptografía, generando un perspectiva de protección multicapa que aseguraba la privacidad de la información seguridad física. (Belapurkar, 2022)

Desde los ochenta y principios de los noventa las empresas que fabrican computadoras personales introdujeron avances importantes en cuanto a la seguridad física, agregando cerraduras integradas en las carcasas de los dispositivos con el objetivo de impedir accesos no permitidos, ya sea cerrando el teclado o limitando la apertura de las cubiertas. Un hito importante ocurrió en 1992 cuando Kensington revolucionó el mercado con su sistema de seguridad para portátiles, introduciendo la famosa ranura para candados (laptop lock slot) junto con su candado MicroSaver, con el tiempo, este sistema evolucionó hacia diseños más compactos y resistentes, manteniéndose hasta la actualidad como una medida básica pero efectiva de disuasión contra robos en espacios públicos y entornos corporativos. (Smith, 2021)

2.2 Antecedentes de investigaciones relacionadas al tema presentado

2.2.1 Propuesta de un plan de contingencia y de recuperación de desastres frente a los riesgos informáticos del departamento de TICS

El proyecto en el departamento de Tics abordó la vulnerabilidad de sus sistemas ante amenazas informáticas y físicas mediante el desarrollo de un plan de contingencia basado en la metodología MAGERIT. Ante la falta de protocolos de seguridad y limitaciones presupuestarias que exponían a la institución a ciberataques y pérdida de datos, se identificaron 11 activos críticos, reduciendo amenazas en un 65% mediante controles de mitigación, transferencia y eliminación de riesgos. Los resultados demostraron optimización de tiempos de recuperación (RTO/RPO) para el 82% de los activos de alto riesgo, y la implementación de un plan integral con medidas técnicas y administrativas que garantizaron la continuidad operativa, estableciendo un precedente en gestión de riesgos para instituciones militares. (Morales, 2021)

2.2.2 Diseño de una solución integral de backup y disaster recovery

Un estudiante de la Universitat Oberta de Catalunya presenta un sistema integral de respaldo y recuperación ante desastres diseñado para garantizar la continuidad operacional de organizaciones frente a fallos críticos o emergencias, cumpliendo con los requisitos del Esquema Nacional de Seguridad (ENS), Ley Orgánica de Protección de Datos (LOPD) y Reglamento General de Protección de Datos (RGPD). Ante el desafío actual de entornos digitales con crecimiento exponencial de datos y amenazas cibernéticas; donde la ausencia de protocolos efectivos puede generar pérdidas millonarias en infraestructura y parálisis operacional. La solución propone un enfoque multicapa que combina: estrategias de backup automatizado, replicación en la nube y sistemas de conmutación por error, implementados mediante una prueba de concepto funcional. Los resultados obtenidos demuestran una arquitectura operativa que reduce significativamente los riesgos, optimiza los indicadores clave de recuperación (RTO/RPO), y cumple con estándares internacionales (ISO 22301) y directrices gubernamentales (MSPI del MinTIC), ofreciendo un modelo costo-efectivo y escalable para fortalecer la resiliencia en centros de datos y entornos corporativos. (Benítez, 2021)

2.2.3 Diseño y elaboración del plan de recuperación de desastres para el área TI de la Escuela Colombiana de Ingeniería Julio Garavito

Este proyecto desarrolló e implementó un Plan de Recuperación ante Desastres (DRP) para el área de Tecnologías de la Información de la Escuela Colombiana de Ingeniería Julio Garavito, con el propósito de asegurar la continuidad de sus operaciones académicas y administrativas frente a incidentes disruptivos como ciberataques, fallas técnicas o emergencias naturales, ante la falta de un protocolo formal para la recuperación en escenarios que amenazaba la prestación de servicios esenciales en un entorno de creciente vulnerabilidad digital, para determinar activos cruciales analizar riesgos y definir las métricas primordiales de recuperación (RTO/RPO), el proyecto empleó la metodología MAGERIT, la solución que se puso en práctica abarcó: (1) el diseño de estrategias de contingencia que contaban con infraestructura redundante en centros de datos alternativos, (2) la elaboración de protocolos para actuar inmediatamente y (3) la formación especializada del personal técnico. Los resultados validaron la efectividad del DRP al reducir significativamente los tiempos de inactividad y minimizar impactos financieros, demostrando no solo su viabilidad técnica sino la necesidad inmediata de su adopción para proteger los activos tecnológicos. (Amaya & Ángel, 2023)

2.2.4 Diseño del plan de recuperación de desastres informáticos para el centro de datos de la gobernación del departamento del Chocó

En este proyecto estratégico elaboró y se aplicó un sistema integral de operatividad continua para el centro de datos de la Gobernación del Chocó, con el objetivo de garantizar la disponibilidad ininterrumpida de servicios críticos mediante la adopción de los estándares del enfoque de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC. Enfrentando la preocupante fragilidad del sistema, como lo son la falta de políticas de seguridad, las constantes fallas operativas y la ausencia de un Plan de Recuperación ante Desastres (DRP), que se ha evidenciado en incidentes graves, como el colapso de bases de datos fundamentales, la propuesta tratada la apremiante necesidad de salvar información delicada y sostener los servicios del gobierno ante riesgos operativos y tecnológicos, a través de la implementación conjunta de las metodologías BIA (Análisis de Impacto al Negocio) y MSPI, se pudieron conseguir los siguientes objetivos: (1) determinación y categorización de activos vitales, (2) establecimiento de métricas esenciales para la recuperación (RPO/RTO), (3) creación de protocolos que siguen la norma ISO 22301:2019 para disminuir riesgos tecnológicos, humanos y eléctricos, y (4) desarrollo de un modelo escalable que redujo las vulnerabilidades encontradas en un 70%. Los resultados demostraron no solo la viabilidad técnica y operativa de la solución, sino su carácter prioritario para transformar la gestión tecnológica de la gobernación, mejorando significativamente la resiliencia institucional, protegiendo datos estratégicos. (Rios, 2020)

2.3 Definiciones conceptuales

2.3.1 Plan de Recuperación de Desastres (DRP)

2.3.1.1 Concepto de Plan de Recuperación de Desastres (DRP) vs BCP (Plan de Continuidad del Negocio)

Un DRP constituye un conjunto de protocolos estratégicos diseñados para implementarse ante situaciones críticas, funcionando como mecanismo de protección esencial cuando surgen emergencias. Mientras que un BCP se enfoca en mantener el negocio a flote durante una crisis, el DRP es ese plan de acción concreto que te dice qué hacer minuto a minuto cuando el desastre ya está ocurriendo: desde evacuar al equipo con seguridad hasta recuperar datos vitales o reemplazar equipos críticos. Cabe recalcar que ambos planes no operan de forma separada, sino como parte de un sistema integrado de gestión de crisis. El DRP representa el conjunto de medidas correctivas que se activan de

manera estructurada cuando la organización se enfrenta a una situación de caos, permitiendo una recuperación ordenada y eficiente. (Briceño, 2021)

2.3.1.2 Objetivos Plan de Recuperación de Desastres.

Un Plan de Recuperación ante Desastres consta de objetivos fundamentales y tiene como propósito establecer procesos robustos, eficientes y escalables para gestionar interrupciones de diversa índole (Saeed, 2022). Estos se listan a continuación:

- Garantizar una cobertura integral: El DRP debe abordar todas las fases de riesgos: la fase de activación, la fase de recuperación y la fase de reconstitución.
- Fomentar la preparación: La capacidad de respuesta ante potenciales crisis se garantiza a través de la planificación y simulacros regulares.
- Mejorar la comunicación: Resulta crucial desarrollar mecanismos claros de comunicación y roles definidos entre los asistentes.
- Emplear soluciones tecnológicas: El uso de instrumentos avanzadas (ej. replicación de datos, sistemas en la nube) permite reducir los tiempos de recuperación.
- Impulsar la mejora continua: El DRP necesita ser revisado periódicamente con el fin de ajustarse a cambios en el ambiente normativo, operativo y tecnológico.

2.3.1.3 Importancia de un Plan de Recuperación de Desastres.

Para garantizar la estabilidad operativa de una entidad ante eventualidades inesperadas como ataques cibernéticos, desastres naturales, averías de equipos o cualquier otra dificulta que obstaculice el funcionamiento habitual, resulta fundamental planificar la recuperación frente a desastre, las organizaciones los negocios y las instituciones se exponen a riesgos importantes sin un plan estructurado, tales como interrupciones del servicio por mucho tiempo, pérdidas de datos, perjuicios económicos y deterioro de la reputación. Un DRP bien diseñado permite minimizar el tiempo de inactividad, proteger los datos críticos, cumplir con normativas legales, y fortalecer la confianza de clientes, socios y reguladores al demostrar preparación y resiliencia. (Bhat, 2025)

2.3.2 Componentes Fundamentales del Plan de Recuperación de Desastres

2.3.2.1 Personal y Roles

La planificación y coordinación de la recuperación ante desastres es una tarea prudentemente compleja para una organización. Requiere amplios esfuerzos de diferentes

equipos para elaborar un plan que puede ser complicado, pero debe tener un proceso de ejecución detallado paso a paso. (Awasthi, 2020)

A continuación, proporciona una lista posible de equipos que pueden ayudar en la planificación y ejecución de la recuperación ante desastres

Equipo	Rol/Líder	Responsabilidades Clave
Gerente de Proyectos	Gerente de Proyecto	Coordina el esfuerzo general, gestiona tiempos y presupuesto, establece estructura de reportes y actualizaciones al comité ejecutivo.
Equipo de Gestión de Crisis	Chief Operating Officer (COO)	Toma decisiones clave en crisis, declara desastre, define estrategia de comunicación interna y externa, activas estrategias de respuesta.
Equipo de Apoyo Administrativo	Jefe de Administración	Establece el centro de comando, gestiona suministros y apoya logísticamente a otros equipos.
Equipo de Evaluación de Daños	Jefe de Instalaciones	Analiza el impacto en infraestructura, equipos y seguridad, recomendando acciones de recuperación.
Equipo de Coordinación de Recuperación	Consultor Externo o Coordinador Interno	Facilita la comunicación entre áreas técnicas y usuarios, con apoyo de consultores externos si es necesario.
Equipo de Apoyo a Recursos Humanos	Jefe de Recursos Humanos	Gestiona temas laborales, seguros, nóminas y contratación de personal temporal.
Equipo de Restauración del Sitio	Director de Instalaciones	Evalúa daños y supervisa la recuperación de instalaciones físicas.
Equipo de apoyo al transporte	Jefe de Administración	Coordina logística, alojamiento y transporte de personal/equipos.
Equipo de restauración del sistema	Jefe de Tecnología (TI)	Recupera operaciones de sistemas críticos: redes, servidores, telecomunicaciones y soporte a usuarios finales.

Tabla 1: Roles DRP. Elaboración propia basada en **(Awasthi, 2020)**

2.3.2.2 Inventario de Activos

El inventario de activos es un pilar fundamental de cualquier DRP efectivo, ya que permite identificar con precisión todos los recursos críticos de la organización: equipos físicos, datos digitales y documentación esencial. Este registro detallado que debe incluir descripciones técnicas, ubicaciones exactas, niveles de criticidad y relaciones de dependencia no solo agiliza la recuperación operativa tras una crisis, sino que también sirve como herramienta preventiva al revelar vulnerabilidades potenciales. Un inventario bien estructurado debe ser dinámico y escalable, capaz de adaptarse a los cambios tecnológicos y organizacionales, con actualizaciones que garanticen su precisión. En una emergencia, un plan de recuperación exitoso radica precisamente en la capacidad de responder tres preguntas clave: ¿qué activos poseemos?, ¿dónde se encuentran? y ¿en qué condiciones están? Por ello, lejos de ser un mero requisito administrativo, el inventario de activos se erige como un instrumento estratégico que sustenta la continuidad del negocio y minimiza el impacto operacional y financiero ante eventualidades disruptivas. (PRIA, 2020)

2.3.2.3 Procedimientos de Backup

Los respaldos de datos garantizan la disponibilidad de información crítica ante fallos técnicos, ciberataques o emergencias. Sin copias de seguridad confiables, las empresas no solo pierden datos valiosos, también la confianza de clientes y socios. Su función va más allá de preservar información: permiten reanudar operaciones con rapidez, minimiza el impacto de una crisis. En el ámbito de la gestión de datos, existen diversas estrategias de respaldo: a) El respaldo completo: almacenamiento local. b) Los respaldos incremental y diferencial: almacena únicamente las modificaciones. c) Las copias por instantáneas (snapshots): capturan el estado del sistema en momentos específicos. d) La protección continúa de datos (CDP): permite restaurar la información en tiempo real. e) Las soluciones en la nube: respaldo remoto. f) Finalmente, el respaldo híbrido, que combina almacenamiento local y remoto. Cada tipo de respaldo presenta ventajas y limitaciones. (Stephen, 2023)

2.3.3 Procedimiento de recuperación basada en NIST sp 800-34 Rev.1 (Implementación del DRP)

Ilustración 5: Procedimiento de implementación DRP. Elaboración Propia.

2.3.3.1 Preparación y Autorización

La participación de todas las áreas de la organización y de cada nivel jerárquico es fundamental para establecer una planificación efectiva de recuperación ante desastres. Es indispensable que la alta dirección y los distintos responsables comprendan la importancia de este proceso, ya que solo así podrán asignar adecuadamente los recursos, el tiempo y la atención necesarios. Este compromiso no solo refleja la voluntad de contar con un plan formal, sino que también facilita su desarrollo al promover la colaboración entre departamentos y asegurar el acceso a los medios requeridos. Sin una preparación adecuada, cualquier intento de respuesta ante un incidente será desorganizado y podría agravar la situación. Por ello, un componente esencial es la elaboración de un plan de respuesta a incidentes, acompañado de la capacitación del personal encargado y la provisión de herramientas forenses. (Bacula Systems S.A., 2023)

2.3.3.2 Análisis de Impacto y Riesgos

El análisis de riesgos e impactos en la implementación del DRP es una etapa esencial que detecta y examina los eventuales efectos de una interrupción en los sistemas críticos de una organización, además de las debilidades que podrían intensificar el

impacto. Este análisis establece el orden de recuperación de cada sistema o servicio en función de su relevancia para las operaciones comerciales, calculando el Tiempo Máximo Tolerable de Interrupción (MTD) y el Objetivo de Tiempo de Recuperación (RTO). (Briceño, 2021)

2.3.3.2.1 Análisis de Impacto en el Negocio (BIA)

El BIA ayuda a determinar qué sucedería si algo sale mal, dónde se encuentran tus alternativas de emergencia y cómo mantener funcionando lo más relevante. Primero, determina cuáles son las actividades y activos esenciales para tu empresa. Después, se examina la interdependencia de los procesos y se evalúa el efecto que tendría su indisponibilidad a lo largo del tiempo. Las Las organizaciones, debido a esta perspectiva estructurada, están más capacitadas para reaccionar frente a crisis como pandemias, ciberataques o desastres naturales sin tener que recurrir a la improvisación. El BIA, en esencia, ofrece una ruta clara para salvar lo más preciado y garantizar la continuidad de la empresa en los momentos más difíciles. (Taarup, 2020)

2.3.3.2.2 Definición de métricas

Las métricas RPO, RTO, MTD y WRT son indicadores fundamentales en el marco de la continuidad del negocio y la recuperación de desastres (DRP), ya que determinan los límites de tolerancia frente a una interrupción y fijan las metas de recuperación. Estas métricas posibilitan la medición del impacto de un suceso y orientan la puesta en marcha de tácticas efectivas. Su adecuada delimitación garantiza que el DRP sea realista, eficaz y esté en sintonía con los requisitos empresariales. (INCIBE, 2020)

2.3.3.2.2.1 Objetivo de tiempo de recuperación (RTO)

Es el período máximo que una empresa puede tolerar sin que un sistema, aplicación, activo o servicio esté operativo después de un desastre o falla crítica. Establecer un RTO adecuado implica considerar los recursos disponibles tanto financieros como humanos, ya que estos influyen directamente en las estrategias que se pueden implementar para garantizar la continuidad del negocio. En este sentido, es recomendable adoptar un enfoque escalonado: iniciar con soluciones accesibles, como respaldos en ubicaciones externas o la priorización de riesgos más probables, e ir avanzando hacia estrategias más robustas, como la replicación de datos en tiempo real o el uso de infraestructuras en la nube. La clave está en definir RTO realistas y ajustarlos conforme evoluciona el entorno y se fortalecen los planes de recuperación, asegurando así una respuesta eficaz ante cualquier crisis. (Seco, Martins, & Netto, 2024)

2.3.3.2.2.2 Objetivo del punto de recuperación (RPO).

El RPO, o punto de recuperación objetivo, establece el tiempo máximo que una organización es capaz de permitir perder información después de una catástrofe, lo cual define la periodicidad con la que estas copias de seguridad deben hacerse, estas decisión es estratégica y debe equilibrar el costo de implementación con el nivel de riesgo que se puede asumir un RPO menos extenso supone hacer respaldos más seguidos o incluso replicación en tiempo real, lo cual implica gastos más altos por otro lado, un RPO más amplio ofrece estrategias más simples y baratas, pero a su vez con mayor riesgo de perder información. (EAR/PILAR, 2025)

2.3.3.2.2.3 Tiempo de recuperación de trabajo (WRT)

El Work Recovery Time (WRT) es el periodo necesario para restablecer completamente los procesos operativos y de negocio una vez que la infraestructura tecnológica ha sido recuperada, es decir, después de alcanzado el RTO. Mientras que el RTO se centra en la restauración técnica como servidores, sistemas y redes, el WRT abarca las actividades posteriores necesarias para volver a la normalidad, tales como la validación de datos, la reconexión de usuarios y la reactivación de flujos de trabajo. El WRT, junto con el RTO, permite calcular el Tiempo Máximo Tolerable de Inactividad (MTD), mediante la fórmula: MTD = RTO + WRT. (Nikolovski, Milenkovski, Petreska, & Slavkovska, 2024)

2.3.3.2.2.4 Tiempo de inactividad máximo tolerable (MTD)

El *MTD* (Tiempo Máximo Tolerable de Inactividad) es el límite crítico que una organización puede soportar sin operar, esto antes de que se produzcan consecuencias graves e irreversibles, como la pérdida de clientes y perdida de datos y esto trae consigo consecuencias más pequeñas como ventas fallidas, el RTO siempre debe ser menor que el MTD para evitar riesgos. Por ejemplo, si una empresa logra restablecer sus sistemas técnicos en 2 horas (RTO), pero necesita 3 horas adicionales para reanudar completamente sus operaciones (WRT) su MTD será de 5 horas, esta métrica combinada es fundamental para diseñar planes de continuidad del negocio realistas y efectivos. (INCIBE, 2020)

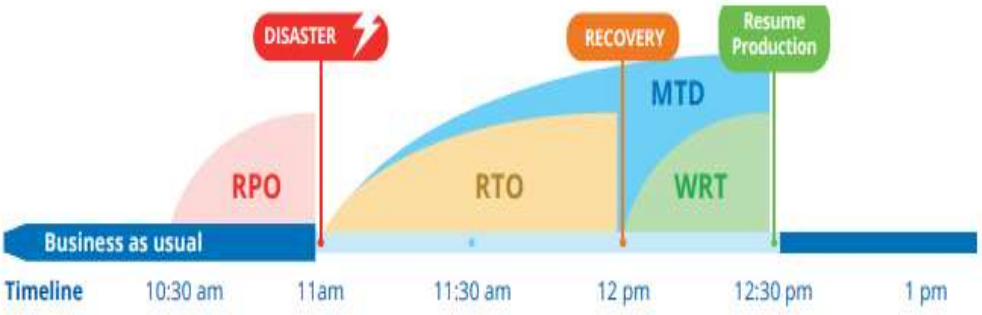


Ilustración 6: Recuperación ante desastres. Extraído de: (Ramiro, 2020)

2.3.3.3 Diseño de Estrategias de Recuperación

Estrategias	Acciones	Descripción
Procedimientos Técnicos	Copias de seguridad y restauración	Implementar políticas de respaldo regulares y pruebas de restauración para asegurar la disponibilidad de datos.
	Planes de recuperación de sistemas (SRP)	Documentar procesos para recuperar servicios tecnológicos, estableciendo objetivos de tiempo y punto de recuperación (RTO y RPO).
	Pruebas periódicas	Realizar simulacros y pruebas de recuperación para validar la eficacia de los procedimientos y realizar ajustes necesarios.
Roles y Comunicaciones	Definir roles y responsabilidades	Asignar tareas específicas a miembros del equipo para garantizar una respuesta organizada.
	Plan de comunicación	Establecer protocolos de comunicación internos y externos, incluyendo canales, mensajes clave y frecuencias de actualización.
	Capacitación y simulacros	Entrenar al personal en los procedimientos de comunicación y realizar ejercicios para evaluar la preparación.
Proveedores Alternos	Identificar proveedores críticos	Determinar qué servicios o productos son esenciales para las operaciones.
	Evaluar y seleccionar alternativas	Investigar y establecer relaciones con proveedores que puedan sustituir a los actuales en caso de interrupciones.
	Formalizar acuerdos	Establecer contratos o memorandos de entendimiento que definan los términos de colaboración en situaciones de emergencia.

Tabla 2: Estrategias de recuperación. Elaboración propia basada en **(Bacula Systems S.A., 2023)**

2.3.3.4 Documentación del Plan

La documentación exhaustiva de incidentes constituye un pilar fundamental dentro de los procesos de recuperación ante desastres, conforme establece el estándar NIST SP 800-34. Cada integrante del equipo de contingencia tiene la obligación de registrar meticulosamente todas las acciones ejecutadas, dificultades enfrentadas y conocimientos adquiridos durante las operaciones de recuperación, información que debe ser remitida al Coordinador para su análisis e incorporación al plan. Esta documentación necesita abarcar informes posteriores a eventos, resultados de pruebas de validación, un compendio de lecciones aprendidas y registros cronológicos pormenorizados de actividades, además funciona como un fundamento para auditorías, formación y mejoras continuas del plan. (Swanson, Bowen, Phillips, Gallup, & Lynes, Contingency Planning Guide for Federal Information Systems, 2010)

2.3.3.5 Pruebas y Simulacros

Los análisis del Plan de Recuperación ante Desastres (DRP) son un elemento fundamental con el fin de garantizar su eficacia continua, estos deben llevarse a cabo de manera periódica, al menos cada semestre, mediante distintos métodos como recorridos teóricos, simulaciones de desastres o pruebas completas de conmutación. La meta consiste en garantizar que el plan evidencie adecuadamente las modificaciones en la organización, mantenga actualizadas las listas de contactos y configuraciones, y pueda llevarse a cabo sin problemas en cualquier instante, asimismo es necesaria la intervenciones de todos los encargados del plan, puesto que las pruebas no solo confirman que el plan es operativo, sino que también robustecen la preparación institucional ante situaciones de emergencia reales. (ITA, 2020)

Las simulaciones o simulacros constituyen una herramienta esencial dentro del ciclo de pruebas de un Plan de Recuperación ante Desastres (DRP), ya que permiten evaluar el funcionamiento integral del plan sin afectar las operaciones normales de la organización. En estas pruebas, se recrea de manera controlada un escenario de desastre con el objetivo de comprobar la respuesta coordinada de todos los elementos involucrados. Durante una simulación, deben examinarse aspectos clave como la infraestructura como: tecnología (hardware y software), infraestructura, el desempeño del personal, los canales de comunicación, los procedimientos documentados, los suministros disponibles, los servicios esenciales (electricidad y transporte); para asegurar la funcionalidad de la organización. (Rene, 2024)

2.3.3.6 Mantenimiento y Mejora Continua

El DRP debe ser dinámico y permanentemente actualizado para mantener su efectividad, ya que cambios en el personal, infraestructura, equipos y servidores; pueden volver obsoletos los protocolos existentes. (Borrego & Vivar, 2022)

2.3.4 Seguridad física de los equipos informáticos

La seguridad física prioriza la protección de tres activos fundamentales: personas, datos y equipos. Las personas constituyen el principal foco de protección por su valor irremplazable, especialmente cuando poseen conocimientos especializados. Es crucial que todos los empleados sepan y estén capacitados en los procedimientos actuales. Herramientas como las listas de contactos, las evaluaciones de riesgo y las prioridades de protección deben ser revisadas con regularidad, un plan sólido debe abarcar las tres etapas críticas: prevenir (acciones proactivas), intervenir (actuar durante la emergencia) y recuperarse (recuperar materiales dañados), asegurando de esta manera la seguridad del patrimonio frente a cualquier eventualidad. La utilidad práctica del DRP está directamente relacionada con su continua adaptación a la realidad institucional y con el entrenamiento constante del equipo encargado. (Briceño, 2021)

2.3.4.1 Amenazas naturales, humanas, técnicas

Una amenaza se define como un factor impredecible, que, al materializarse, puede explotar vulnerabilidades y ocasionar daños significativos a los sistemas de información. Estas se clasifican generalmente en tres categorías principales: incidentes accidentales, ataques y fallos técnicos. Los incidentes accidentales abarcan fenómenos naturales, como desastres meteorológicos que pueden afectar la infraestructura física, o fallas técnicas inesperadas, como interrupciones prolongadas del suministro eléctrico, por otro lado, los ataques implican la intervención de agentes externos maliciosos que buscan explotar vulnerabilidades de seguridad y por último los fallos técnicos son impredecibles sobre los equipos y pueden comprometer la disponibilidad, integridad o confidencialidad de los sistemas y datos. (Mena & Ordóñez, 2021)

Los desastres naturales muestran nuevas vulnerabilidades frente a las fuerzas de la naturaleza, donde fenómenos como huracanes, terremotos e inundaciones se manifiestan cada vez con características únicas que demandan respuestas rápidas y diferentes, al contrario, de los eventos predecibles como los ciclones tropicales que permiten activar protocolos preventivos de evacuación y protección de equipos, eventos

como los sismos repentinos solo dejan como recurso la solidez estructural de las instalaciones y la eficiencia de los equipos de emergencia, enseñando que, si bien no se puede controlar estos fenómenos, sí se puede fortalecer continuamente los sistemas de prevención y respuesta. . (Hodgson, Clark-Ginsberg, Haldeman, Lauland, & Mitch, 2022)

2.3.4.2 Vulnerabilidades

Una vulnerabilidad es cualquier fallo o debilidad en un sistema que pueda ser aprovechado para comprometer su seguridad o funcionamiento, estas vulnerabilidades pueden manifestarse de múltiples formas, poniendo en riesgo la integridad física de los equipos informáticos y la continuidad operativa de la institución. Por ejemplo, a nivel técnico sería un software obsoleto o mala configuración puede dejar expuestos los sistemas a ataques o fallos críticos, mientras que, en el ámbito físico la ubicación inadecuada de los equipos o la falta de sistemas de climatización adecuados pueden provocar daños irreversibles en el hardware, Asimismo las vulnerabilidades organizativas, como la ausencia de protocolos claros para emergencias o la falta de capacitación del personal, pueden agravar los riesgos, retrasando la respuesta ante incidentes. (Briceño, 2021)

2.3.4.3 Ciberseguridad

La ciberseguridad actúa como un sistema de defensa integral para proteger la información y los sistemas tecnológicos contra amenazas crecientes. Como señalan (Pinchao, Hernández, & Minaya Macías, 2024), consiste en "un conjunto de procedimientos y herramientas implementados para proteger la información generada y procesada a través de dispositivos electrónicos" (p. 20). Este concepto abarca múltiples temas como: la seguridad de redes, programas malignos, hacking, continuidad operacional. Además, funciona como un ecosistema de protección que salvaguarda datos en tránsito e información almacenada, más que una medida técnica es una estrategia permanente que combina prevención, monitoreo constante y protocolos de respuesta rápida, evidenciando su papel crítico en la preservación de activos digitales personales, corporativos y gubernamentales.

2.3.5 Protección física del hardware

2.3.5.1 Seguridad de componentes internos

Los ataques más frecuentes al hardware de dispositivos se dividen en dos categorías principales. En primer lugar, los accidentes físicos, como derrames de líquidos,

golpes o exposición a temperaturas extremas, que pueden dañar irreparablemente los componentes de hardware. En segundo lugar, las modificaciones no autorizadas, donde el hardware o software es alterado para realizar funciones distintas a las previstas por el fabricante. Las consecuencias de las modificaciones maliciosas realizadas, como la instalación de componentes de hardware adulteradas, pueden convertir un computador en un gran dolor de cabeza. Por otro lado, la fragilidad física del hardware lo hace vulnerable a factores ambientales y accidentes cotidianos, lo que subraya la necesidad de mantener los dispositivos en condiciones óptimas y adquirir componentes únicamente de fuentes confiables. (B-safe, 2020)

2.3.5.2 Seguridad en entornos de almacenamiento

Para lograr que la seguridad de la información este segura es necesario identificar y proteger los datos confidenciales, estudiando su ubicación, vías de acceso y condiciones de retención, los más significativos abarcan la corrupción, el extravío de datos, la falta de confidencialidad y una liberación anticipada por lo tanto es fundamental poner en marcha controles que mantengan la integridad y accesibilidad de los datos, supervisar la recuperación y las copias de seguridad, cifrar información crítica, eliminar los datos con seguridad al final de su vida útil y asegurar la resiliencia frente a fallos mediante planes de continuidad y respaldos guardados en lugares seguros. Asimismo es necesario hacer seguimiento a la obsolescencia de los dispositivos, revisar con regularidad los servicios en la nube y emplear software de protección como antivirus y antimalware para proteger la información necesario hacer seguimiento a la obsolescencia de los dispositivos, revisar con regularidad los servicios en la nube y emplear software de protección como antivirus y antimalware para proteger información institucional. (red.tic, 2021)

2.3.5.3 Seguridad en infraestructuras de redes y dispositivos

Debido a la mayor complejidad de las infraestructuras de conexión y los equipos, , es necesario un enfoque integral de seguridad que abarca hardware, software, protocolos y políticas. Las organizaciones deben adoptar estrategias proactivas, incluyendo investigación continua, formación del personal y preparación ante ciber amenazas y desastres naturales. Esto requiere soluciones tecnológicas avanzadas, planes de contingencia robustos y capacitación constante. Además, el anclaje físico de servidores y equipos en racks o data centers es clave para evitar movimientos no deseados, vibraciones o accesos no autorizados, garantizando su estabilidad y seguridad operativa. (Lara, 2023)

2.3.6 Control de Acceso

Los controles de acceso se fundamentan en cuatro funciones esenciales: permitir, denegar, limitar y revocar el acceso, sirven para salvaguardar activos que tengan un gran valor para las instituciones. Al permitir el acceso autoriza a usuarios específicos o grupos a utilizar ciertos recursos físicos o digitales, mientras que denegarlo restringe dicho acceso, siendo común configurar los sistemas para denegar por defecto y solo permitir accesos explícitamente a personal autorizado. Al restringir el acceso, se sugiere imponer limitaciones parciales, como autorizaciones diversas para cada rol, usando biometría, aplicaciones o llaves con varios niveles de autorización en espacios físicos. (Briceño, 2021)

2.3.7 Normativas

La norma ISO 27001, una norma internacional para los Sistemas de Gestión de Seguridad de la Información (SGSI), ofrece un marco adaptable que resguarda datos importantes en organizaciones de todas las dimensiones, resultando especialmente útil para aquellas con gran exposición a peligros relacionados con la seguridad, dado un escenario en el que las amenazas informáticas son impredecibles o ineludibles, ha llegado a ser fundamental su implementación para asegurar una respuesta eficaz frente a incidentes, obtener la certificación ISO 27001, a pesar de la demanda de trabajo, ofrece beneficios estratégicos en tres ámbitos esenciales confianza de los clientes (ventajas comerciales), protección de activos críticos (tranquilidad) y procesos estandarizados para gestionar riesgos (eficiencia operativa).). (NQA, 2022)

El NIST SP 800-34 es un manual federal que define técnicas para la planificación de contingencias en sistemas de información, con el objetivo de preparar, responder y recuperarse ante interrupciones a través de temporales como la reubicación en lugares alternativos, el uso de equipos sustitutivos o métodos manuales. Su enfoque estructurado abarca un procedimiento de siete etapas: 1) establecer políticas de contingencia, 2) efectuar análisis de impacto empresarial (BIA) para jerarquizar sistemas fundamentales, 3) instaurar controles preventivos, 4) diseñar estrategias de recuperación rápida, 5) elaborar planos minuciosos (ISCP), 6) comprobar a través de pruebas y formación, y 7) mantener los planos al día. (Connor, 2023)

2.4 Metodología aplicada: NIST sp 800-34 Rev.1

Ilustración 7. Marco de seguridad NIST. Obtenido de: **(National Institute of Standards and Technology, 2024)**

2.5 Conclusiones relacionadas al marco teórico en referencia al tema planteado.

- El Plan de Recuperación ante Desastres (DRP) se ha transformado en un componente crucial para asegurar que las organizaciones mantengan su capacidad continuidad operativa y sean robustas ante acontecimientos inesperados, Si se implementa de manera adecuada se puede transformar un hipotético incidente crítico en un procedimiento de recuperación bien organizados y eficiente, lo que disminuye el impacto sobre las operaciones de la entidad. El DRP tiene que ser considerado como un proceso dinámico que fortalece la capacidad de anticipación, respuesta y aprendizaje institucional frente a amenazas cada vez más complejas.
- La seguridad física es la primera barrera de protección para garantizar la integridad de los datos, los equipos tecnológicos y personas que

conforman la institución. Su adecuada implementación incluye control de acceso, protecciones del hardware, mitigación de amenazas naturales, humanas y técnicas, es fundamental para prevenir daños materiales, robos o interrupciones operativas. Además, mejora la capacidad de respuesta y recuperación, al controlar y reducir las amenazas de índole física y organizativa.

- La eficacia del DRP se incrementa cuando se combina con medidas para la seguridad física, lo que genera un ambiente de protección de seguridad física lo cual produce un entorno de salvaguardas integral que cuenta tanto el espacio físico como el digital que incluye tanto el espacio físico como el digital, la seguridad física es el primer nivel de defensa para la protección de las personas, los datos y los equipos reforzarla es fundamental para asegurar la continuidad, Detectar y Mitigar las amenazas humanas, naturales, físicas y técnicas debe ser un componente esencial del proceso de gestión de riesgos.
- La metodología empleada para desarrollar el DRP, que se fundamenta en un enfoque estructurado por etapas (preparación, planificación, respuesta y mejora continua), no solo posibilita una respuesta efectiva ante situaciones de emergencia, sino que también impulsa una cultura organizacional enfocada en la prevención, la resiliencia y el perfeccionamiento constante, este esquema metodológico garantiza que los procesos estén en concordancia con las necesidades operativas y las modificaciones tecnológicas o institucionales.

Capítulo III

3 Marco investigativo

3.1 Introducción

En este capítulo, se establecen las bases metodológicas para el desarrollo del proyecto "Plan de Recuperación de Desastres para la Seguridad Física de los Equipos Informáticos en el Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen". Este capítulo detalla el enfoque metodológico empleado, los tipos de investigación, los métodos utilizados, las fuentes de información y las herramientas para la recolección de datos y análisis de datos. Su objetivo principal es proporcionar un marco estructurado que permita identificar los riesgos y vulnerabilidades del laboratorio, así como fundamentar la propuesta de un plan de recuperación ante desastres.

La investigación se caracteriza por combinar enfoques aplicados, cuantitativos y descriptivos, lo que permite no solo analizar la situación actual del laboratorio, sino también proponer soluciones prácticas y medibles. Además, nos permite partiendo de una fórmula de obtención de muestra en una población objetivo hacer la aplicación de encuestas a docentes y estudiantes, y entrevistas a un integrante del personal técnico, en estas se recopiló información fundamental sobre las condiciones de seguridad física, vulnerabilidades, los riesgos presentes y las experiencias de los involucrados.

El análisis de las opciones globales se hizo visible a partir de la tabulación de los resultados en tablas y gráficos, mientras que la triangulación de las encuestas y entrevistas permitió verificar los datos cruzada mente y conseguir los resultados derivados del uso de las herramientas, este diseño metodológico no solamente señala los puntos débiles del laboratorio en la actualidad, sino que además pretende sugerir soluciones que fomenten la continuidad de las operaciones, estableciendo así los cimientos para un DRP eficaz y ajustado lo que demanda la institución.

3.2 Tipo de investigación

3.2.1 Investigación Aplicada

La investigación aplicada tiene como finalidad emplear el conocimiento científico para dar solución a problemas reales. Se orienta a generar resultados útiles que puedan ser implementados en áreas prácticas. (González, 2021). Este tipo de investigación fue esencial porque el proyecto no solo se orientó a teorizar, sino a implementar soluciones

reales para la seguridad física de los equipos. Estuvo directamente alineada con los objetivos del proyecto, que incluyeron la definición de estrategias, protocolos y roles. Al tratarse de un plan de recuperación de desastres, requirió acciones prácticas y verificables, como la implementación de protocolos de respaldo, sistemas de protección eléctrica y medidas contra robos.

3.2.2 Investigación Cuantitativa

La investigación cuantitativa se centra en la medición numérica y el análisis estadístico para comprender y explicar fenómenos. Este enfoque utiliza datos estructurados recolectados mediante herramientas estandarizadas como encuestas y entrevistas. Su objetivo principal es obtener resultados objetivos que puedan ser generalizados a poblaciones amplias. (Carazas, Huiza, Martínez, Barrios, & Quispe, 2024). En este proyecto, se utilizó el tipo de investigación cuantitativa para recopilar y analizar datos de manera objetiva y medible, que se obtuvieron de la aplicación de instrumentos como encuestas y entrevistas dirigidas a estudiantes, docentes y personal técnico, permitiendo obtener datos numéricos sobre las condiciones del laboratorio, la frecuencia de fallas, y el nivel de riesgo percibido.

3.2.3 Investigación Descriptiva

La investigación descriptiva se enfoca en detallar las características esenciales de un fenómeno o grupo homogéneo, a partir de criterios sistemáticos que permiten comprender su estructura o comportamiento, utilizando métodos como encuestas para obtener una descripción precisa y sistemática. Su finalidad es ofrecer información clara, organizada y comparable, útil para otros estudios. (Alban, Arguello, & Molina, 2020). Este tipo de estudio posibilitó el reconocimiento y la explicación minuciosa de las condiciones presentes del laboratorio, así como la seguridad física de los aparatos informáticos, fue crucial porque, antes de sugerir soluciones, se analiza la situación real del laboratorio (por ejemplo, su infraestructura).

3.3 Métodos de investigación

3.3.1 Método Analítico – Sintético

El método analítico-sintético permite estudiar un fenómeno al dividirlo en sus partes fundamentales para examinarlas por separado y luego integrarlas nuevamente, destacando las conexiones entre los elementos y el conjunto. Facilitando una visión global y profunda del tema. (Guanoluisa Almache, Bosquez Remache, Esparza Pijal, &

Benavides, 2023). Este método fue clave porque permitió analizar las causas de los daños a los equipos y se identificaron los factores físicos, humanos o técnicos involucrados, para examinarlos individualmente. Luego, mediante síntesis, se integraron las soluciones en un plan unificado, articulando estrategias, protocolos y recursos. Así, el proyecto no solo identificó riesgos aislados, sino que propuso una estrategia estructurada para la recuperación ante desastres.

3.3.2 Método Inductivo – Deductivo

Esta metodología combina la inducción, que consiste en observar de manera directa la realidad para formular a partir de ahí teorías y conceptos más abstractos. Por otro lado, el razonamiento deductivo se basa en proposiciones o conceptos teóricos que determinan conexiones lógicas entre ideas. Se pretende, con base en esta concepción teórica, comparar los resultados con evidencia tangible y observable. En otras palabras, se pasa de la teoría a la práctica confirmando conceptos con datos empíricos. (Neuman, 2020).

Fue apropiado porque posibilitó iniciar desde situaciones específicas (como incidentes sucedidos, encuestas) hasta llegar a conclusiones generales acerca de la seguridad física del laboratorio 1. Posteriormente, utilizando lógica de deducción, se adaptaron esas normas al contexto particular de la ULEAM Extensión El Carmen. Esto aseguró que el plan no se basará en teorías, sino en experiencias y prácticas más efectivas.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias

3.4.1.1 Encuesta

Esta técnica utiliza cuestionarios estructurados para recabar información directa de personas sobre sus puntos de vista, comportamientos o actitudes. Mediante preguntas estructuradas, ofrece resultados cualitativos y cuantitativos. (Mohamed, Carranza, Meza, León, & Gonzáles, 2023). La encuesta se llevó a cabo en la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, y fue hecha concretamente a 138 estudiantes y 12 profesores que emplean el Laboratorio 1 de Ingeniería en Software. Obtuvieron cuantificables que resultaron esenciales para el diagnóstico, ya que aportaron evidencia concreta y organizada sobre la situación del laboratorio.

3.4.1.2 Entrevista

La entrevista es un método sistemático de recolección de información que utiliza un cuestionario prediseñado con preguntas cerradas y ordenadas lógicamente, permitiendo respuestas precisas y comparables. Su aplicación facilita la cuantificación de resultados mediante la codificación numérica de las respuestas, permitiendo un análisis estadístico. (Gonzáles, 2021). La entrevista se dirigió a 1 miembro del personal técnico del Laboratorio 1 de la carrera de Ingeniería en Software, con el objetivo de profundizar en aspectos que no podían ser completamente abordados mediante la encuesta. Este instrumento permitió conocer de forma más detallada las experiencias relacionadas con fallos en la seguridad física, condiciones de infraestructura y prácticas de mantenimiento.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población y muestra

3.4.1.3 Población

Población se refiere al total de individuos o elementos que poseen las características relevantes para un estudio, las cuales se encuentran en cierta ubicación y tiempo determinado y estas pueden ser familias, universidades, profesores, entre otros. También se conoce como universo o colectivo. (Aguirre, Ortiz, & Sainz, 2021). En este proyecto la población es una población finita que está conformada de docentes, estudiantes y personal técnico que interactúa con el objeto de investigación que es el Laboratorio 1 de la ULEAM Extensión El Carmen. Los cuales son un total de 244 individuos, divididos en 15 docentes, 159 estudiantes de ingeniería de software y 69 de Tics y 1 técnico.

3.4.1.4 Muestra

La muestra es una parte seleccionada de la población que permite realizar estudios, cuyos resultados pueden generalizarse al grupo completo. Es decir, la muestra representa a la población. (Grau, 2020). La muestra obtenida para esta investigación fue de 149 individuos. La cual fue obtenida bajo la fórmula de población finita extraída de (Aguirre, Ortiz, & Sainz, 2021). La cual servirá como enfoque para la aplicación de las herramientas (encuestas y entrevista) y posterior análisis.

3.4.1.4.1 Obtención de Muestra

- n: Tamaño de la muestra
- N: Tamaño de la población
- Z: Valor de la distribución normal estándar (Z-score) según el nivel de confianza
  - 90% → 1.645
  - 95% → 1.96
  - 99% → 2.576
- p: Proporción esperada de éxito (si no se conoce, se usa 0.5 para máxima variabilidad)
- q = (1− p): Proporción esperada de fracaso.
- e: Margen de error tolerado (por ejemplo, 0.05 para 5%)

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

$$n = \frac{244 * (1.96)^2 * 0.5 * (1-0.5)}{(0.05)^2 * (244-1) + (1.96)^2 * 0.5 * (1-0.5)}$$

$$n = \frac{244 * (1.96)^2 * 0.5 * (0.5)}{(0.05)^2 * (243) + (1.96)^2 * 0.5 * (0.5)}$$

$$n = \frac{244 * 3.84 * 0.25}{0.0025 * (243) + 3.84 * 0.25}$$

$$n = \frac{234.24}{0.607 + 0.96}$$

$$n = \frac{234.24}{1.567}$$

$$n = 149.48$$

$$n = 149 \ \ MUESTRA$$

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.4.1.1 Encuesta

Se diseñó una encuesta mediante Google Forms, compuesta por 149 individuos resultado de la muestra obtenida de la población, se aplicaron preguntas cerradas de selección múltiple con 4 opciones distintas, dirigida a docentes y estudiantes que

interactúan en el ambiente del Laboratorio 1 en la Uleam El Carmen, el cuestionario se enfocó Recolectar información sobre la percepción y experiencias de estudiantes y docentes en relación con los riesgos físicos, fallos técnicos y medidas de seguridad existentes en el Laboratorio.

3.4.1.2 Entrevista.

Se realizó una entrevista con preguntas abiertas al técnico encargado del Laboratorio de Cómputo 1 de la Uleam El Carmen, esta entrevista tuvo como objetivo obtener información técnica detallada sobre las condiciones actuales de seguridad física, mantenimiento, infraestructura y procedimientos de contingencia del Laboratorio 1, a partir de la experiencia directa del personal técnico, para sustentar el diseño de un Plan de Recuperación de Desastres enfocado en minimizar riesgos y pérdidas.

3.5.2.2 Estructura de los instrumentos de recolección de datos aplicados

La encuesta y la entrevista están compuestas por 10 preguntas interrelacionadas y redactadas para cada técnica. En la encuesta, las preguntas tienden a ser cerradas, para así obtener datos cuantitativos y poderlos analizar numéricamente. En cambio, las preguntas de la entrevista son abiertas, lo que permite obtener información más rica y profunda. Los formatos de ambos instrumentos se adjuntan como anexos a este documento.

3.4.1.3 ENCUESTA

Encuestado:	Fecha:
Objetivo: Recolectar información sobre la percepción y experiencias de estudiantes y docentes en relación con los riesgos físicos, fallos técnicos y medidas de seguridad existentes en el Laboratorio 1 de la carrera de Ingeniería en Software de la ULEAM Extensión El Carmen, con el fin de identificar debilidades y oportunidades de mejora en la gestión de desastres y protección de equipos informáticos.	

1. ¿Con qué frecuencia se presentan fallos eléctricos durante el uso del laboratorio?

- Nunca
- Rara vez
- Frecuentemente
- Siempre

2. ¿Considera que el laboratorio está preparado para enfrentar desastres naturales (inundaciones, incendios, sismos)?

- Totalmente preparado
- Medianamente preparado
- Poco preparado
- Nada preparado

3. ¿Se siente seguro frente a posibles robos o actos vandálicos dentro del laboratorio?

- Muy seguro
- Algo seguro
- Poco seguro
- Nada seguro

4. ¿Los equipos cuentan con sistemas de protección eléctrica visibles (UPS o reguladores)?

- Sí, en todos los equipos
- En algunos equipos
- No se observan
- No lo sé

5. ¿Hay control sobre quién entra al laboratorio fuera de clases?

- Siempre
- A veces
- Casi nunca
- Nunca

6. ¿Ha participado usted en actividades de preparación ante emergencias en el laboratorio (simulacros o capacitaciones)?

- Sí, más de una vez
- Sí, una vez
- Solo charla informativa
- Nunca

7. ¿Considera que la infraestructura del laboratorio es adecuada para proteger los equipos?

- Muy adecuada
- Adecuada
- Poco adecuada
- Inadecuada

8. ¿Ha notado que algunos equipos no funcionan correctamente por falta de mantenimiento?

- Sí, varios
- Algunos
- Muy pocos
- Todos funcionan bien

9. ¿Ha perdido información o archivos durante su trabajo por apagones?

- Varias veces
- Una vez
- Nunca
- No aplica

10. ¿Está de acuerdo en implementar un Plan de Recuperación de Desastres en el laboratorio?

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

3.4.1.4 ENTREVISTA

Entrevistado:	Fecha:
Objetivo: Obtener información detallada sobre las condiciones actuales de seguridad física, mantenimiento, infraestructura y procedimientos de contingencia del Laboratorio 1, a partir de la experiencia directa del personal técnico, para sustentar el diseño de un Plan de Recuperación de Desastres enfocado en minimizar riesgos y pérdidas.	

1. ¿Ha tenido que enfrentar situaciones de fallos eléctricos en el laboratorio? ¿Cómo se gestionaron?
2. ¿Qué medidas de protección existen actualmente frente a desastres naturales como inundaciones o sismos?
3. ¿Ha ocurrido algún incidente de robo, vandalismo o ingreso no autorizado al laboratorio? ¿Qué acciones se tomaron?
4. ¿Qué tipo de sistemas de respaldo eléctrico (UPS, reguladores) están instalados en el laboratorio? ¿Funcionan correctamente?
5. ¿Con qué frecuencia se presentan fallas o daños en los equipos informáticos del laboratorio? ¿A qué cree usted que se deben principalmente estos problemas? Además, ¿cada cuánto tiempo se realiza la revisión o mantenimiento de estos equipos?
6. ¿Existe algún procedimiento técnico o guía para actuar en caso de una emergencia en el laboratorio?
7. ¿Considera que el laboratorio tiene puntos críticos de vulnerabilidad? ¿Cuáles serían los más urgentes a atender?
8. ¿Cómo describiría el estado de la infraestructura física del laboratorio en cuanto a su resistencia frente a amenazas externas?
9. ¿Se ha producido pérdida de información importante por apagones, daños o errores técnicos? ¿Cómo se resolvió?
10. ¿Qué acciones considera prioritarias para mejorar la gestión ante riesgos y amenazas en el laboratorio?

3.5.3 Plan de recolección de datos

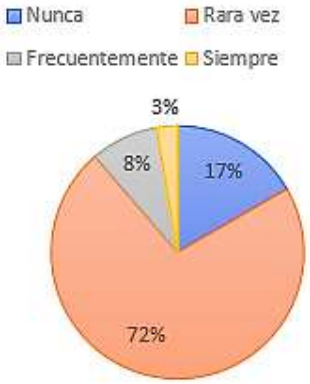
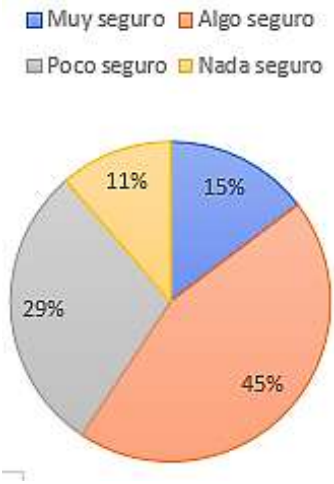
El plan de recolección de datos busca garantizar la seguridad física de los equipos informáticos en el Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM, Extensión El Carmen, mediante un plan de recuperación de desastres. Se recopilará información sobre riesgos, estado de los equipos y medidas de seguridad actuales. Se utilizarán encuestas y entrevistas como instrumentos principales. Este enfoque combinado permitirá una evaluación integral. Los datos se recolectarán en dos semanas, asegurando confidencialidad. Los resultados orientarán estrategias efectivas de prevención y respuesta.

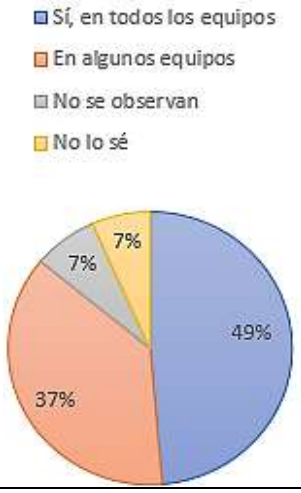
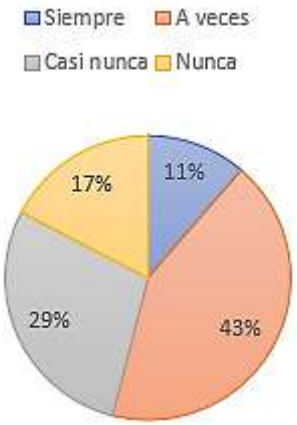
Individuos	**Actividad**	**Fecha**
150 individuos de la población entre estudiantes y docentes.	Las encuestas fueron realizadas de manera virtual, la recolección se realizó en un periodo de dos semanas. Se identificarán vulnerabilidades del laboratorio frente a desastres naturales o humanos.	27/07/2025 - 04/08/2025
1 técnico de mantenimiento del laboratorio 1.	La entrevista fue de manera presencial, la entrevista se realizó en un tiempo de 20 min. Con esta herramienta se buscó tener información más precisa y detallada basada en experiencia que la obtenida en la encuesta	04/08/2025

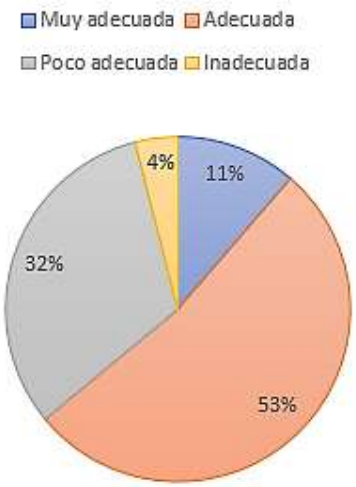
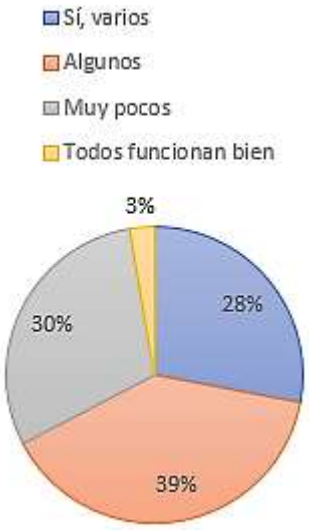
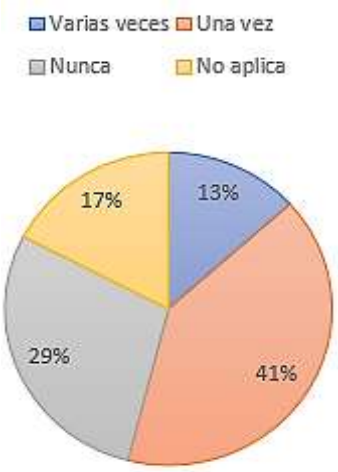
Tabla 3. Plan de recopilación de datos

3.6 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos

Pregunta	Gráfica	Análisis
1. ¿Con qué frecuencia se presentan fallos eléctricos durante el uso del laboratorio?		La gran mayoría de los encuestados respondió con un 72% indicó que rara vez se presentan fallos eléctricos Mientras tanto un 17% afirma que nunca hay fallos eléctricos, por otra parte 8% considera que los fallos eléctricos ocurren con frecuencia y a su vez el 3% indica que siempre se presenta.
2. ¿Considera que el laboratorio está preparado para enfrentar desastres naturales (inundaciones, incendios, sismos)?		Un poco menos de la mitad de los encuestados correspondiente al 45% piensan que esta poco preparado por otra parte un 27% opinan que están medianamente preparado, mientras que un 21% señalan que no está nada preparado y un 7% considera que están totalmente preparados
3. ¿Se siente seguro frente a posibles robos o actos vandálicos dentro del laboratorio?		Los resultados muestran que el 45% de los estudiantes manifiesta sentirse algo seguro frente a posibles robos o actos vandálicos dentro del laboratorio, mientras que un 29% indica sentirse poco seguro por otro lado, únicamente un 15% afirma sentirse muy seguro

Pregunta	Gráfica	Análisis
		y un 11% declara que nada seguro.
4. ¿Los equipos cuentan con sistemas de protección eléctrica visibles (UPS o reguladores)?		Observamos que el 49% de los encuestados afirman que los equipos cuentan con un sistema de protección, por otro lado, el 37% señalan que solo en algunos equipos, Por otro lado, un 7% no observan ningún tipo de protección además un 7% no tiene conocimiento al respecto.
5. ¿Hay control sobre quién entra al laboratorio fuera de clases?		Un poco menos de la mitad que corresponde al 43%, nos dice que solo a veces hay control mientras que un 29% indica que ocurre ocasionalmente, en cambio un 17 % afirma que nuca hay supervisión, y un 11% indica que siempre se realiza control.
6. ¿Ha participado usted en actividades de preparación ante emergencias en el laboratorio (simulacros o capacitaciones)?		Se puede evidenciar que un 37% nunca ha participado en estos tipos de actividades, mientras que un 32 % únicamente ha asistido a charla informática, en cambio un 20% ha participado una vez y un 11% ha participado más de una ocasión.

Pregunta	Gráfica	Análisis
7. ¿Considera que la infraestructura del laboratorio es adecuada para proteger los equipos?		La mitad de los encuestados que corresponde al 53% piensa que, si está adecuada la infraestructura, mientras que un 32% señala que es poco adecuada para proteger los equipos, en cambio un11% indica que es muy adecuada y un 4% califica que es inadecuada.
8. ¿Ha notado que algunos equipos no funcionan correctamente por falta de mantenimiento?		Más de la mitad de los encuestados con un 67% opinan que los equipos no funcionan correctamente, mientras que un 30% señalan que son muy pocos los equipos que no funcionan y una minoría de 3% piensan que todos funcionan bien.
9. ¿Ha perdido información o archivos durante su trabajo por apagones?		Los resultados indica que más de la mitad de los encuestado, es decir que el 54% ha perdido archivo por apagones ya sea una vez o por varias veces, mientras que un 29% respondió que nunca a tenido problemas y un 17% de los encuestado respondió que no aplica en su caso.

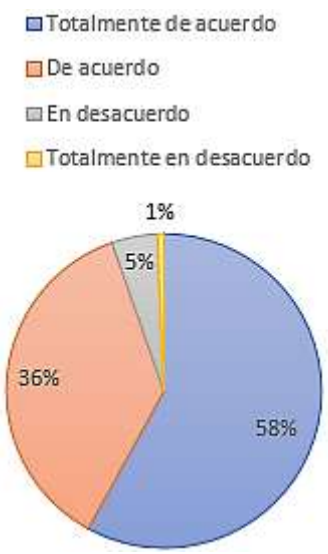
Pregunta	Gráfica	Análisis
10. ¿Está de acuerdo en implementar un Plan de Recuperación de Desastres en el laboratorio?		Los resultados indican que la mayor parte de las personas encuestadas están a favor de un Plan de Recuperación de Desastres en el laboratorio, el 36% estuvo de acuerdo y el 58% completamente de acuerdo, por otra parte solamente un 5% manifestó que están en desacuerdo y solo el 1% señaló estar totalmente en desacuerdo.

Tabla 4. Análisis de encuesta

Pregunta	Respuesta	Análisis
1. ¿Ha tenido que enfrentar situaciones de fallos eléctricos en el laboratorio? ¿Cómo se gestionaron?	*"sí, tuvimos un inconveniente como hace casi año, en ese falló, fallaron las instalaciones eléctricas ahí se quemaron unos ups ahí lo que se procedió hacer fue informar a Manta para que ellos vinieran a solucionar"*	Se puede concluir con la entrevista que, si existen eventos de fallos eléctricos, y que existen problemas en el cableado, lo que tuvo consecuencias como quemar dispositivos.
2. ¿Qué medidas de protección existen actualmente frente a desastres naturales como inundaciones o sismos?	*"medidas de protección como tal, no, no cuenta la extensión con eso."*	Se evidencia la inexistencia de un plan ante desastres naturales. Y medidas de protección ante estos casos.
3. ¿Se ha producido algo evento de vandalismos, robo o acceso no autorizados a las instalaciones de laboratorio?.¿Qué medidas se ¿implementaron?	*"sí, el semestre anterior a este, se robaron mouse, teclados, se robaron cables HDMI, les arrancaban el conector USB y lo que se procedió hacer fue hacer una reunión con los docentes y decirles que era responsabilidad suya lo que pasara durante esas horas de clase, entonces ahí ellos ya hablaron con los estudiantes, incluso se hizo que no desconectaran los dispositivos en las computadoras, se habló un poco con los estudiantes*	Los problemas por robos se dan y son poco predecibles y muy difíciles de controlar, por la respuesta se puede notar que no se cuenta con un plan de acción en estos casos.

Pregunta	Respuesta	Análisis
	sobre ese tema y ya ha disminuido esto"	
4. ¿Qué tipo de sistemas de respaldo eléctrico (UPS, reguladores) están instalados en el laboratorio? ¿Funcionan correctamente?	*"Están instalados, pero no sirven."*	Nos comenta el técnico que los UPS y reguladores de corriente en su gran mayoría están en mal estado o no sirven, lo que lleva a consecuencias más grande en los laboratorios, como daño en los dispositivos.
5. ¿Con qué frecuencia se presentan fallas o daños en los equipos informáticos del laboratorio? ¿A qué cree usted que se deben principalmente estos problemas? Además, ¿cada cuánto tiempo se realiza la revisión o mantenimiento de estos equipos?	*"A ver, lo que pasa es que el laboratorio sufrió una remodelación en la carrera de software y antes de eso los fallos eran recurrentes, pero después que ya hubo tema de la remodelación de máquinas y todo casi no hemos tenido problemas sobre eso, y el mantenimiento se lo realiza cada tres o cuatro meses, cada inicio de semestre"*	En conclusión, se dice que el laboratorio sufrió una actualización de equipos y que antes eran más comunes los problemas, pero actualmente debido a ser nuevos equipos los problemas son menores y que el mantenimiento se hace por semestre.
6. ¿Existe algún procedimiento técnico o guía para actuar en caso de una emergencia en el laboratorio?	*"no"*	En esta pregunta se aclara que no existen guías o procedimientos en caso de una emergencia.
7. ¿Considera que el laboratorio tiene puntos críticos de vulnerabilidad? ¿Cuáles serían los más urgentes a atender?	*"Si el ingreso, porque no es segura, cualquiera puede abrir las puertas,"*	Nos aclara que no existe ningún tipo de control o seguridad al ingresar a los laboratorios, lo que puede desencadenas más problemas.

Pregunta	Respuesta	Análisis
8. ¿Cómo describiría el estado de la infraestructura física del laboratorio en cuanto a su resistencia frente a amenazas externas?	*"regular."*	La infraestructura física de los laboratorios se nota regular en palabras del entrevistado en cuanto a resistencia a amenazas externas.
9. ¿Se ha producido pérdida de información importante por apagones, daños o errores técnicos? ¿Cómo se resolvió?	*"Estos errores técnicos sí hubo, bueno cuando había el tema de los apagones, tuvimos estos problemas en las computadoras, en los monitores he incluso hasta hubo discos m2 SCD que se dañaron por esos apagones. Entonces lo que se hizo también informar a Manta, que se llevaron las computadoras a garantía y nos supieron ayudar con eso"*	Nos supo explicar que este tema de fallos eléctricos con los apagones de inicio de año, eran un tema muy regular, pero actualmente también son un problema, pero menos común, debido a las conexiones en mal estado.
10. ¿Qué medidas estima que son prioritarias para optimizar el control ante amenazas y peligros en el laboratorio?	*"lo principal seria cambiar todo el tema de los ups dentro de los laboratorios. Segundo este cambiar toda la instalación eléctrica"*	En acciones recomendadas, nos recomienda hacer un cambio en las instalaciones eléctricas y en la renovación de los UPS.

Tabla 5. Análisis entrevista

3.6.2 Análisis y presentación de los resultados alcanzados

El propósito de esta investigación fue analizar la gestión de desastres e identificar problemas, vulnerabilidades, amenazas relacionadas con los equipos, infraestructura y seguridad del Laboratorio de Cómputo 1 de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, y proponer como solución un plan de recuperación ante desastres.

En la pregunta 3 tanto de la encuesta como de la entrevista nos habla de posibles robos o actos vandálicos dentro del laboratorio 1, en esta ocasión nuevamente los encuestados y el entrevistado coincidieron en las respuestas mostrando así que, si existen o son muy frecuentes estos actos vandálicos en el Laboratorio 1, siendo una acción muy perjudicial para estudiantes y la institución como tal, indispensable en corregir o prevenir.

En la pregunta 5 de la encuesta y la pregunta 7 de la entrevista que habla sobre el control que existe sobre quién entra al laboratorio fuera de horarios de clases y vulnerabilidades que se ven en el mismo, en este caso los encuestados nos dicen que a veces ahí control y otras veces no, y el entrevistado nos dice que no hay control en absoluto cualquiera puede abrir las puertas.

La pregunta 8 de la encuesta y la pregunta 5 de la entrevista con el tema de si existen algunos equipos que no funcionan correctamente por falta de mantenimiento. Los encuestados en cantidad considerable piensa que si hay algunos equipos que no funcionan por falta de mantenimiento, y el entrevistado nos da un dato de que se actualizaron los equipos y al ser nuevos se ve con menos frecuencia.

La pregunta 10 de la encuesta y de la entrevista sobre si se está de acuerdo en implementar un Plan de Recuperación de Desastres en el laboratorio. En ambos casos consideran necesario el tomar acciones preventivas y ven viable el uso de un DRP, ya que si necesitan cambios y medidas preventivas urgentes.

3.6.3 Informe final del análisis de los datos

La situación crítica en el Laboratorio 1 de la Carrera de Ingeniería en Software de la ULEAM Extensión El Carmen, que se detalla en el análisis de datos de este capítulo, es principalmente consecuencia de vulnerabilidades serias en la seguridad física del equipo informático y la ausencia de preparación tanto del alumnado como del equipo técnico frente a catástrofes. Los problemas existentes fueron confirmados con mayor profundidad a través de las encuestas aplicadas a 149 personas (alumnos y maestros) y la entrevista realizada al técnico responsable del laboratorio, lo que hizo evidente la urgencia de establecer un Plan de Recuperación de Desastres (DRP). Los hallazgos destacan la atención de control de acceso, protección eléctrica, infraestructura y preparación para situaciones de emergencia. Además, hay un consenso general sobre lo esencial que es aplicar medidas preventivas.

Respecto a la frecuencia de fallas eléctricas, el 89 % indicó que son infrecuentes porque ocurren nunca o pocas veces, el ingeniero entrevistado, sin embargo reportó errores graves, como una falla eléctrica que impacto a los equipos y las unidades de alimentación ininterrumpida (UPS), esto quería decir que las eléctricas estaban experimentando fallas. Estas diferentes perspectivas muestran que, a pesar de que los alumnos no consideran que los fallos sean comunes, su existencia tiene un impacto demostrar la necesidad de renovar los sistemas de protección eléctrica mediante la actualización de reguladores y UPS.

Un 66% de las personas encuestadas cree que el laboratorio está "poco" o "nada preparado" para situaciones de emergencia debido a desastres naturales, y el técnico también opina que no hay protocolos establecidos para afrontar catástrofes naturales como terremotos o inundaciones. Esto revela una vulnerabilidad importante, sobre todo si se tiene en cuenta el clima de El Carmen, que puede sufrir daños por humedad debido a fuertes lluvias. Si no se cuenta con planes de contingencia, la probabilidad de que se generen interrupciones operativas y daños irreparables a los equipos se incrementa.

El 40% de las personas se siente poco o nada segura frente a robos y actos vandálicos, y el técnico ha corroborado que han existido robos previos (de teclados, ratones y cables HDMI). La ausencia de control de acceso es una señal de un grave problema en la seguridad física, dado que el 46 % de los encuestados sostiene que nunca o a veces se supervisa quién tiene acceso al laboratorio y que el técnico asegura que cualquiera puede abrir las puertas, dado que esto incrementa la posibilidad de sufrir robos y sabotajes, las medidas para controlar el acceso y la vigilancia son imprescindibles.

Lo que se refiere a protección eléctrica y mantenimiento, a pesar de que el 86% de los participantes en la encuesta dijo que los equipos tienen sistemas de protección eléctrica (UPS o reguladores), el técnico fue honesto al admitir que la mayor parte de estos aparatos no operan adecuadamente, lo cual concuerda con informes sobre averías en dispositivos debido a cortes de energía. El 67% de los participantes en la encuesta también manifestó que algunos equipos no funcionan debido a la falta de mantenimiento, pero el técnico afirmó que han disminuido las dificultades después de una renovación reciente de los equipos esto nos indica que, a pesar de los avances, la falta de mantenimiento periódico y la obsolescencia de los sistemas de respaldo eléctrico siguen siendo un problema.

En cuanto a la capacitación y el entrenamiento para circunstancias de emergencia, el 69 % de los encuestados garantizo no haber tomado parte en simulacros o entrenamientos, a la vez que el técnico corroboró que no hay protocolos o pautas determinadas para emergencias, los encuestados afirmaron que no habían tomado parte en simulaciones o capacitaciones, y el técnico corroboró que no había protocolos ni directrices de emergencia. La ausencia de preparación incrementa el riesgo de que se pierdan los datos y haya daños físicos, ya que se limita la capacidad de reaccionar ante incidentes, un 54% de los encuestados ha informado que existen pérdida de información a causa de cortes de energía, lo que demuestra la necesidad de contar con protocolos de emergencia y sistemas robustos con el fin de responder.

Para resumir, los datos indican que el Laboratorio 1 está expuesto a riesgos importantes a causa de fallos eléctricos, falta de preparación frente a desastres naturales, control de acceso inadecuado, mantenimiento irregular, infraestructura deficiente y la falta de protocolos para situaciones de emergencia. Se apoya en gran medida la implementación de un DRP y se le considera fundamental para reducir estos riesgos, salvar los equipos informáticos y asegurar que las actividades académicas sigan su curso. Las sugerencias incluyen la implementación de controles de acceso rigurosos, la ejecución de simulacros y capacitaciones regulares, el establecimiento de sistemas eléctricos funcionales para protegerse, y la creación de un plan documentado que incluya todas las etapas del manejo de riesgos, desde la prevención hasta la recuperación.

Capítulo IV

4 Marco propositivo

4.1 Introducción

El capítulo actual se enfoca en el diseño de un Plan de Recuperación de Desastres (DRP) que busque proteger principalmente los equipos informáticos del Laboratorio 1 de Ingeniería en Software en la ULEAM Extensión, El Carmen. El propósito es asegurar la operatividad continua y salvar los recursos tecnológicos ante amenazas como cortes de electricidad, incendios, inundaciones o accesos no permitidos. Para esto, se utilizará la metodología NIST SP 800-34, que define maneras de detectar riesgos, analizar vulnerabilidades y elaborar estrategias para la recuperación. El objetivo de este análisis es identificar las brechas en la seguridad actual y sugerir un plan de acción para reducir el impacto de los incidentes en los servicios académicos.

4.2 Descripción de la propuesta

La presente propuesta corresponde a un Plan de recuperación de desastre para la seguridad física de los equipos informáticos del Laboratorio 1 de Ingeniería en Software en la ULEAM Extensión, El Carmen. Surge de la necesidad de salvar los equipos informáticos y asegurar que las actividades académicas continúen a pesar de sucesos como cortes eléctricos, incendios, inundaciones o accesos no autorizados. Para lograr esto, empleé el método NIST SP 800-34, que posibilitó la identificación de riesgos, la evaluación de debilidades y la formulación de estrategias para recuperarse. Mi intención con esta propuesta es reforzar la seguridad física y garantizar que el laboratorio siga funcionando a pesar de las circunstancias desfavorables.

4.3 Determinación de recursos

4.4 Humanos

Esta tabla ofrece detalles acerca de los participantes en mi proyecto, su rol y las actividades que realizaron, esto ayuda a entender cómo se repartirán las obligaciones y la cooperación necesaria para finalizar el trabajo.

Cant	Colaborador	Rol	Descripción
	Ing. Clara Pozo Hernández	Tutora	Participo como guía durante el desarrollo de mi proyecto
	Ing. Jean Carlos	Encargado del laboratorio	Intervino como responsable de los laboratorios, brindando la información necesaria durante la entrevista aportando respuestas clave para obtener el diagnostico.
150	Estudiantes	Estudiantes de la carrera de Software	Participaron en la encuesta realizada con el fin de recopilar información para el análisis del capítulo III.
	Angie Moreira	Investigadora	Realizo el proyecto integrador

Tabla 6 Recursos Humanos

4.4.1 Tecnológicos

Esta taba nos detalla todos los recursos tecnológicos y conjunto de herramientas informáticas que nos facilitaron la ejecución de los procesos necesarios para este proyecto.

Cant	**Recursos**	**Descripción**
1	Computadora hp intel core i5 de 8,00 GB	Herramienta clave para procesar, analizar y almacenar información durante el proyecto
1	Teléfono Infinity HOT 50i	Dispositivo portátil que posibilita la comunicación, el registro de información en tiempo real, la captura de fotografías como evidencia etc.
1	Impresora	Dispositivo que se utilizó para realizar las debidas impresiones y documento final.
10 meses	Internet	Recurso indispensable ya que me ayudo a la busque y recopilación de información necesaria y confiables.
	Microsoft Forms	Herramienta en línea fundamental para aplicar la encuesta a los estudiantes.
	Microsoft office	Instrumento que se emplea para compilar datos y redactar la documentación de la investigación.

Tabla 7. Recursos Tecnológicos

4.4.2 Económicos

A continuación, se detalla los recursos económicos utilizados para la elaboración del proyecto, indicando la cantidad costo unitario y valor total.

Cantidad	Descripción	Costo Unitario	Sub total
40	Viáticos para trasladarme a la institución	$1,50	$60
1	Computadora hp intel core i5 de 8,00 GB de RAM	$590	$590
1	Teléfono Infinity HOT 50i	$160	$160
1	Impresora	$250	$250
10 meses	Internet	$18	$180
1	Kits de materiales de trabajo (Hojas, bolígrafo, etc.)	$25	25
		Valor Total	1,265

Tabla 8. Recursos Económicos

4.5 Etapas de acción para el desarrollo de la propuesta

4.5.1 Programa para la elaboración del plan de recuperación ante desastres en el laboratorio 1.

PROGRAMA PARA LA ELABORACIÓN DEL PLAN DE RECUPERACIÓN ANTE DESASTRES EN EL LABORATORIO 1.		
Objetivo • Identificar los riesgos de seguridad física que afectan a los equipos informáticos del Laboratorio 1 de la carrera de Ingeniería en Software de la ULEAM Extensión El Carmen. • Desarrollar un Plan de Recuperación de Desastres fundamentado en la técnica de la metodología **NIST SP 800-34 Rev.1**, que asegure la continuidad de las operaciones del laboratorio si ocurren incidentes.		
Técnicas y Procedimientos	**Ref. a Papel**	**Fecha**
1. Identificación de riesgos • Identificar de los activos • Valorar activos • Diseño de instrumentos • Aplicación de instrumentos • Matriz de riesgo (probabilidad x Impacto)	4.5.1.3 4.5.1.3.1 4.5.1.3.2 4.5.1.3.3 4.5.1.3.4 4.5.1.3.6	1. 03/10/2025 04/10/2025 05/10/2025 06/10/2025 08/10/2025 10/10/2025 - 12/10/2025
2. Desarrollar política de planificación de contingencia • Documento Política de Contingencia	5.1.4.2	2. 13/10/2025- 15/10/2025
3. Análisis de impacto de negocio (BIA) • Identificar funciones críticas • Resultados Formularios RTO, RPO, MTD	5.1.4.3 5.1.4.3.1 5.1.4.3.2	3. 16/10/2025- 18/10/2025

4. Identificar controles preventivos • Identificación de salvaguardas existentes • Identificar el estado de sistemas	5.1.4.4 5.1.4.4.1 5.1.4.4.2	4. 20/10/2025-25/10/2025
5. Diseño de estrategias de contingencia • Identificación de salvaguardas existentes • Manejo de Backups y almacenamiento • Costos estimados • Tiempo de recuperación	5.1.4.5 5.1.4.5.1 5.1.4.5.2 5.1.4.5.3 5.1.4.5.4	5. 01/11/2025-10/11/2025

Tabla 9. Programa de auditoría

4.5.1.1 Repaso de la Metodología

4.5.1.1.1 Metodología de elaboración de DRP basada en NIST

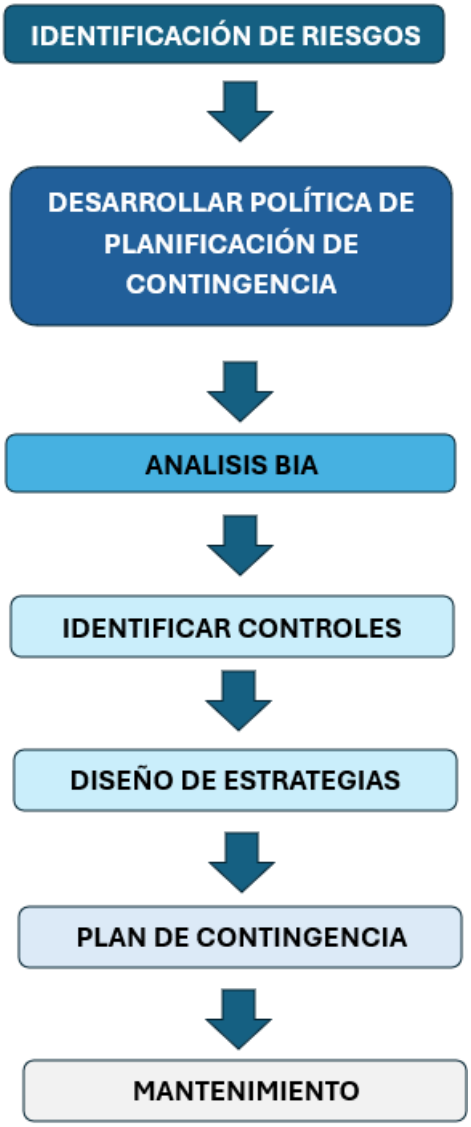


Ilustración 8. Metodología DRP. Elaboración Propia

Esta metodología se basa en el documento de nombre "NIST Special Publication 800-34 Rev. 1" creado por el NIST que es el Instituto Nacional de Estándares y Tecnología de Estados Unidos, se trata de una guía con una metodología de siete fases para desarrollar un plan de contingencia que en nuestro caso es un plan de recuperación ante desastres (DRP), con esta metodología se busca una gestión controlada para minimizar el impacto de interrupciones en sistemas críticos, asegurando la continuidad del negocio y la recuperación rápida ante interrupciones. La metodología planteada cuenta con una pre etapa que se aumentó a la planteada por el NIST, la fase es la de identificación de riesgos. (Marianne, Pauline, Wohl, Dean, & David, 2010).

4.5.1.2 Definición del alcance y objetivos del proyecto

4.5.1.2.1 Descripción de proyecto

Este proyecto tiene como enfoque crear un plan de recuperación ante desastres en el laboratorio 1 de la ULEAM extensión el Carmen, el plan se centrará en garantizar la continuidad operativa del laboratorio mediante procedimientos estructurados a seguir para restaurar de manera eficiente los sistemas tratando de que sea en el menor tiempo posible después de un incidente. El documento contara con: lista de contactos de emergencia (personal encargado, técnico de mantenimiento, decanato, policía, bomberos), inventario de activos críticos (hardware, software, programas), procedimientos detallados de respaldo y recuperación, procedimientos de declaración de desastre y activación del plan, Plan de comunicación para durante y después del incidente.

La ejecución del proyecto se llevará a cabo en 7 fases interconectadas que siguen un ciclo de vida de la planificación de contingencias publicado por el NIST. Donde inicialmente, se tomará el tiempo de identificar activos y a su vez los riesgos y amenazas a los que están expuestos los mismos. Luego, se establecerán las bases del proyecto, definiendo los roles y responsabilidades de las personas encargadas del laboratorio y el marco de trabajo general. A continuación, se realizará un análisis de impacto en el negocio, usado para identificar los activos más importantes del laboratorio y evaluar las consecuencias que trae si alguno de estos llega a fallar.

Una vez que se hayan identificado los riesgos, el siguiente paso es identificar que controles preventivos tener para reducir la probabilidad de que se desencadene un desastre. Después, se crearán métodos de contingencia para llevar a cabo planes de acción ante cualquier evento no pronosticado. Con todo lo demás hecho se procederá a desarrollar un plan documental contra desastres detallado paso a paso, junto con las listas de verificación y los contactos de emergencia. Por último, el proyecto incluirá una fase de mantenimiento para garantizar que el plan se revise y actualice constantemente.

4.5.1.3 IDENTIFICACIÓN DE RIESGOS

4.5.1.3.1 Identificar de los activos

4.5.1.3.1.1 *Activos físicos*

Id	Código	Nombre de Activo	Descripción Técnicas	Periféricos Asociados	Marca	Modelo
A01	074213	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Teclado genérico y	LG	9EN336
A02	074504	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A03	074507	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor Dell, Teclado y Mouse	Dell	E1913FS
A04	074497	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A05	074385	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A06	074381	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Mouse y	ASUS	VP228
A07	074494	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A08	074479	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Mouse y Sin Teclado	LG	VP228
A09	074506	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Teclado y Mouse	LG	20MK400H-B

Id	Código	Nombre de Activo	Descripción Técnicas	Periféricos Asociados	Marca	Modelo
A10	074496	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A11	074501	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado	ASUS	VP228
A12	074500	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A13	074503	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado	ASUS	VP228
A14	074502	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Mouse	ASUS	VP228
A15	074499	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A16	074405	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado	ASUS	VP228
A17	074534	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor LG, Mouse Genius y	LG	W1742ST
A18	072002	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor BENQ, Teclado y	BENQ	ET-002-B
A19	074397	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado Y	ASUS	VP228
A20	074095	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado	ASUS	VP228

Id	Código	Nombre de Activo	Descripción Técnicas	Periféricos Asociados	Marca	Modelo
A21	074079	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Mouse Genius y Teclado	ASUS	VP228
A22	074408	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y Mouse Genius	ASUS	VP228
A23	074412	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Monitor ASUS, Teclado y	ASUS	VP228
A24	074498	Computadora de Escritorio	Procesador Intel i7, Ram 16MG.	Teclado y Mouse Genius	ASUS	VP228
A25	073816	Rack	Estructura metálica para organizar equipos de TI (servidores, red).	Switches, Routers y Cableado	Microtk	Crs326-24g-24s+rm
A26	077184	Aire Acondicionado	Controla la temperatura lo que protege a los equipos	Filtros de Aire	Green Air	Lmvc060cc201
A27		Proyector	Proyección de imágenes o video desde la computadora	Control	Epson	EX9240

Tabla 10: Activos Físicos

4.5.1.3.1.2 *Activos lógicos*

ID	Activos	Marca	Descripción	Modelo	Estado	Categoría
A0001 - H0001	Sistema Operativo	Windows	64 bits	11	Operativo	Software
A0002 - H0002	Office	Microsoft	64 bits	2019	Operativo	Software
A0003 - H0003	Visual Studio Code	Microsoft	64 bits	17.14	Operativo	Software
A0004 - H0004	Android Studio	Google	64 bits	2025.1.3.8	Operativo	Software
A0005 - H0005	NetBeans	Apache	64 bits	25	Operativo	Software
A0006 - H0006	MySQL/postgreSQL	Oracle	64 bits	8.4	Operativo	Software

Tabla 11: Activos lógicos

4.5.1.3.2 Valorar Activos

VA	Valor de Activo	Descripción
1	**Muy Bajo**	Activo con valor mínimo dentro del inventario. Su pérdida no afecta las operaciones.
2	**Bajo**	Activo tiene poca importancia, su afectación genera molestia menor sin comprometer las actividades.
3	**Medio**	El activo es necesario para ciertas funciones. Su pérdida puede afectar temporalmente algunos servicios.
4	**Alto**	Activo importante para operaciones críticas. Su falla interrumpe actividades clave.
5	**Muy Alto**	Activo esencial cuya pérdida detiene las operaciones o compromete gravemente la seguridad o el desempeño académico.

Tabla 12. Valor de activos. Elaboración propia

Posteriormente, cada activo fue evaluado de acuerdo con los niveles establecidos en la Tabla 9, como se detalla en la Tabla 10

Tipos de Activos	Valor			
	D	**I**	**C**	**V.A**
Computadoras de Escritorio	5	3	4	5
Rack	4	4	3	3.6
Aire Acondicionado	5	4	3	4
Proyectores	1	3	4	2.6

Tabla 13. Identificación de amenazas. Elaboración propia

4.5.1.3.3 Diseño de instrumentos

Se elaboró un cuestionario que a su vez se implementó con el fin de detectar las amenazas existentes en el laboratorio y saber las salvaguardas actuales implementadas en el mismo, se aplicaron 6 encuestas sobre: malware, robo, inundaciones, daño, incendio; cada una con 25 preguntas, las cuales fueron aplicadas al encargado del laboratorio.

Cuestionario para Analizar Riesgos			CI 2-5
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:	**Observación**		
Fecha:	**Revisado por:**		

Tabla 14. Cuestionario para Analizar Riesgos

4.5.1.3.4 Aplicación de instrumentos

Para poder responder los instrumentos propuestos se llevó a cabo una revisión minuciosa de las instalaciones de los laboratorios para verificar su estado actual y comprobar cómo se encuentran la infraestructura, el mobiliario y los equipos.

Ilustración 9. Revisión de procesador de maquinas

Ilustración 10. Revisión del estado de las maquinas

Además, el ingeniero Jean Carlos, encargado del laboratorio de TI y Software, contribuyó activamente al responder las preguntas de los cuestionarios, su colaboración fue esencial para obtener información exacta acerca de las condiciones actuales en los laboratorios, los protocolos de mantenimiento y las acciones de seguridad que se han puesto en marcha.

Ilustración 11. Encuesta al encargado del laboratorio

Se muestran los cuestionarios que ya han sido respondidos, los cuales se refieren a la evaluación de riesgos y tratan sobre amenazas como el robo, el fuego, las inundaciones, el daño y el malware. Cada cuestionario cuenta con 25 preguntas enfocadas en su respectivo asunto, lo que posibilitó la recolección de información exacta y minuciosa acerca de los incidentes que podrían perjudicar al laboratorio.

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

Realizado por: Angie Elizabeth Moreira Huerta

Observación:

Fecha: 20/10/2025

Revisado por: Ing. Clara Guadalupe Poso Hernández

Ilustración 12. Cuestionario de análisis de Riesgos

4.5.1.3.5 Tabulación de Datos

Posterior a la aplicación de los cuestionarios mediante una plantilla creada en Microsoft Excel, que fue usada para registrar las preguntas y respuestas que se obtuvieron a lo largo del proceso de evaluación de manera organizada. En esta hoja, los datos se dispusieron en columnas con el fin de distinguir cada pregunta y su respectiva respuesta con la siguiente escala:

0	Riesgo
1	Seguridad
2	No aplica

Tabla 15. Escala de riesgo. Elaboración propia

RIESGO MALWARE	
PREGUNTA	**RESPUESTA**
1. ¿Existe una política de seguridad definida para la protección contra malware?	0
2. ¿Se cuenta con un software antivirus actualizado en los equipos del laboratorio?	0
3. ¿Los usuarios tienen restricciones para la instalación de software no autorizado?	0
4. ¿Se realizan análisis periódicos para detectar posibles infecciones?	1
5. ¿Existen medidas para prevenir ataques de phishing dentro de la red del laboratorio?	0
6. ¿Se cuenta con control de acceso para evitar el uso no autorizado de los dispositivos?	0
7. ¿Los sistemas operativos están actualizados con parches de seguridad?	1
8. ¿Se han identificado incidentes previos de malware en el laboratorio?	1
9. ¿Los estudiantes reciben capacitación sobre buenas prácticas de seguridad informática?	2
10. ¿Las redes Wi-Fi cuentan con medidas de protección contra accesos no autorizados?	1
11. ¿Se utilizan herramientas de monitoreo para detectar comportamiento sospechoso en los equipos?	1
12. ¿Existe un procedimiento de respuesta en caso de infección por malware?	1
13. ¿Se aplican filtros de contenido para prevenir el acceso a sitios maliciosos?	1
14. ¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?	0
15. ¿El tráfico de red es monitoreado para detectar actividad sospechosa?	1
16. ¿Los dispositivos USB están restringidos para evitar infecciones?	0
17. ¿Los archivos de descarga son verificados antes de su uso?	1
18. ¿Se han realizado auditorías previas que detecten vulnerabilidades en la lógica de seguridad?	0
19. ¿Existen políticas de gestión de actualizaciones para reducir riesgos de infección?	0
20. ¿Se implementan registros de actividad para identificar intentos de acceso sospechosos?	0
21. ¿Los accesos a cuentas institucionales están protegidos con autenticación de múltiples factores?	1
22. ¿Los servidores del laboratorio tienen protecciones específicas contra ataques externos?	0
23. ¿Se han documentado procedimientos de limpieza y eliminación de malware en los equipos?	1
24. ¿Se cuenta con herramientas de análisis forense para detectar el origen de una infección?	2
25. ¿Las medidas de seguridad actuales han sido probadas mediante pruebas de penetración?	0
TOTAL CONTROLES NO APLICADOS:	2
TOTAL DE CONTROLES EVALUADOS	23
TOTAL CONTROLES SEGURIDAD:	11
TOTAL CONTROLES RIESGO:	12
PORCENTAJE SEGURIDAD	48%
PORCENTAJE RIESGO	52%

Tabla 16. Tabulación Elaboración Propia

Con los resultados de porcentaje de riesgo de los cuestionarios se puede medir el nivel de riesgo que genera el peligro identificado en cuestión y se puede calcular la probabilidad basándonos en la siguiente escala:

NIVEL DE APARICIÓN (PROBABILIDAD)		
1	**MAS BAJO**	1%-10%
2	**BAJO**	10%-30%
3	**MEDIO**	30%-50%
4	**ALTO**	50%-75%
5	**MÁS ALTO**	75%-100%

Tabla 17. Nivel de aparición (probabilidad). Elaboración Propia

Luego para calcular el impacto, se consideró la siguiente escala:

Valor De Impacto	Descripción
1	**Mínimo/Muy baja:** Las actividades no se ven interrumpidas y son fluidas
2	**Bajo:** Ocasiona un impacto menor en las actividades, pero no reducen el flujo de las mismas.
3	**Moderado/ Medio:** Causa pausas momentáneas en las actividades, permite el flujo limitado de las actividades
4	**Alto:** genera daños notables y causa un plantón temporal en las actividades.
5	**Grave/ Muy alta:** causa medidas catastróficas, una detención total de las actividades y no fluye el flujo de trabajo.

Tabla 18. Nivel de impacto. Elaboración propia

Teniendo la escala de nivel de impacto establecido tocaba medir el mismo en los riesgos que se está identificando como son: malware, incendio, daño, inundación y robo. Para lo cual se tomó en cuenta tres dimensiones a evaluar como son:

- Confidencialidad: Se trata de asegurar que la información solo sea accesible por aquellos que están autorizados.
- Disponibilidad: Garantiza que los sistemas y los datos sean alcanzables y permanezcan a disposición de los usuarios habilitados cuando se requiera.
- Integridad; que garantiza que la información este completa, precisa y no haya sido alterada de manera no autorizada

RIESGOS	CONFIDENCIALIDAD	DISPONIBILDAD	INTEGRIDAD	PROMEDIO
MALWARE	5	5	5	5,0
ROBO	4	4	3	3,7
INCENDIO	2	5	5	4,0
DAÑO	1	3	4	2,7
INUNDACION	1	5	5	3,7

Tabla 19. Gravedad (Impacto). Elaboración propia

4.5.1.3.6 Matriz de Riesgo (Impacto x Probabilidad)

Finalmente, para obtener el nivel de riesgo en la matriz de riesgo debemos multiplicar el impacto por la probabilidad como se mostró al inicio, con esto sabemos cuáles son los riegos que necesitan atención urgente en caso de una catástrofe.

LEYENDA		PROBABILIDAD				
		1 MARGINAL	2 APRECIABLE	3 IMPORTANTE	4 GRAVE	5 MUY GRAVE
IMPACTO	5 MUY GRAVE	5	10	15	20	25
	4 GRAVE	4	8	12	16	20
	3 IMPORTANTE	3	6	9	12	15
	2 APRECIABLE	2	4	6	8	10
	1 MARGINAL	1	2	3	4	5

Tabla 20. Valor de riesgo (impacto x probabilidad). Elaboración propia

1 MUY BAJO	**Riesgo Muy Bajo:** Riesgo mínimo, solo requiere vigilancia sin medidas preventivas iniciales.
2 BAJO	**Riesgo Bajo:** Riesgo reducido, se monitorea sin necesidad de medidas preventivas de inicio.
3 MEDIO	**Riesgo Medio:** Riesgo moderado, evaluar económicamente medidas preventivas; si no es viable, controlar variables.
4 ALTO	**Riesgo Alto:** Riesgo elevado, exige medidas preventivas obligatorias y control estricto de variables.
5 MUY ALTO	**Riesgo Muy Alto:** Riesgo crítico, requiere medidas preventivas urgentes; no iniciar proyecto sin reducir y controlar el riesgo.

Tabla 21. Nivel de Gravedad. Elaboración propia

Finalmente uniendo los datos obtenidos de las tablas anteriores (probabilidad e impacto) y sumado al cálculo del nivel de riesgos, se completa la matriz de riesgos. Y permite observar y concluir que los riesgos que necesitan medidas preventivas urgentes son: malware e incendio. Sin dejar a un lado los otros que tienen cifras bastantes altas.

MATRIZ DE RIESGOS				
RIESGO	**Aparición (probabilidad)**	**Gravedad (Impacto)**	**Valor de Riesgo**	**Nivel de riesgo**
MALWARE	4	5	20	MUY GRAVE
ROBO	3	4	11	GRAVE
INCENDIO	4	4	16	MUY GRAVE
DAÑO	3	3	8	IMPORTANTE
INUNDACION	4	4	15	GRAVE

Tabla 22. Matriz de Riesgos. Elaboración propia

CAPITULO V

5 Auditoria

5.1 Informe de Auditoria

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

5.1.1 Objetivo:

- Identificar los riesgos de seguridad física que afectan a los equipos informáticos del Laboratorio 1 de la carrera de Ingeniería en Software de la ULEAM Extensión El Carmen.
- Elaborar un Plan de Recuperación de Desastres basado en la metodología **NIST SP 800-34 Rev.1**, que garantice la continuidad operativa del laboratorio en caso de incidentes.

5.1.2 Personal Involucrado:

- Encargado del laboratorio
- Estudiantes de la carrera de Software
- Docentes de la carrera de Software

5.1.3 Alcance:

Este proyecto tiene como enfoque crear un plan de recuperación ante desastres en el laboratorio 1 de la ULEAM extensión el Carmen, el plan se centrará en garantizar la continuidad operativa del laboratorio mediante procedimientos estructurados a seguir para restaurar de manera eficiente los sistemas tratando de que sea en el menor tiempo posible después de un incidente.

6. **Identificación de riesgos**
    - Identificar de los activos
    - Valorar activos
    - Diseño de instrumentos
    - Aplicación de instrumentos
    - Matriz de riesgo (probabilidad x Impacto)
7. **Desarrollar política de planificación de contingencia**
    - Documento Política de Contingencia
8. **Análisis de impacto de negocio (bia)**

- Identificar funciones críticas
- Resultados Formularios RTO, RPO, MTD

9. **Identificar controles preventivos**

   - Identificación de salvaguardas existentes
   - Determinar el estado de sistemas

10. **Diseño de estrategias de contingencia**

    - Identificar cada salvaguardas existentes
    - Manejo de Backups y almacenamiento
    - Costos estimados
    - Tiempo de recuperación
    - Kit de recuperación

5.1.4 Hallazgos

Al finalizar la evaluación de los riesgos se obtuvieron los siguientes hallazgos.

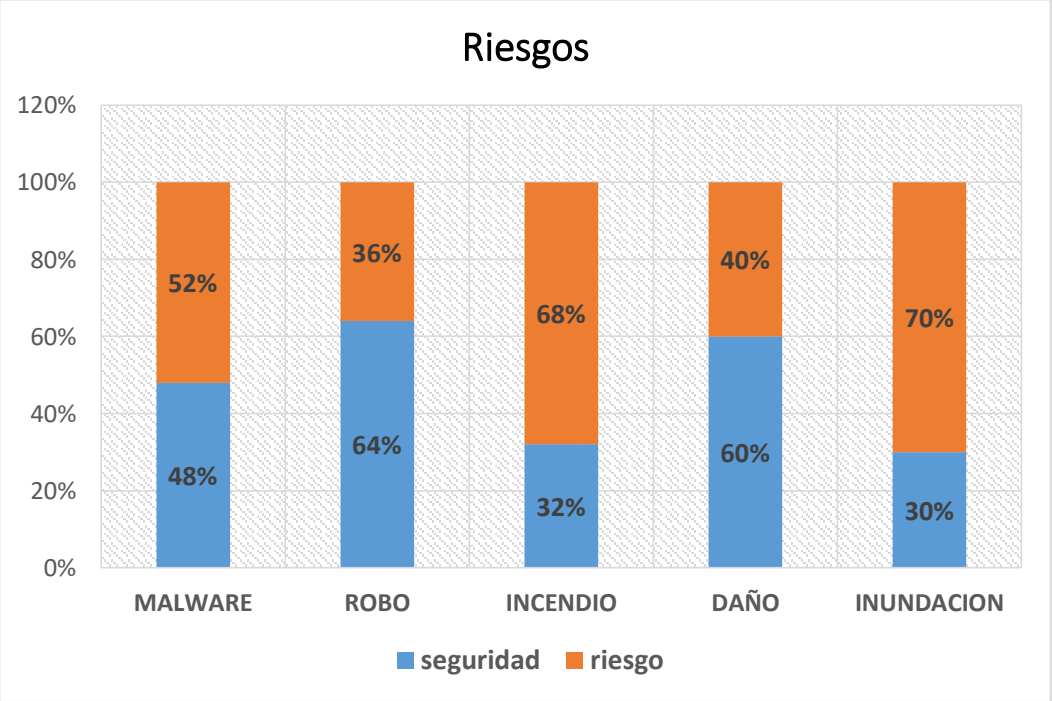
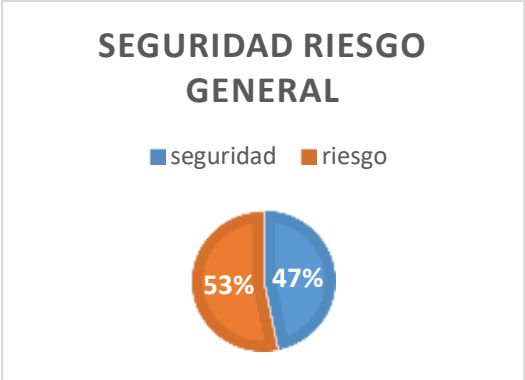
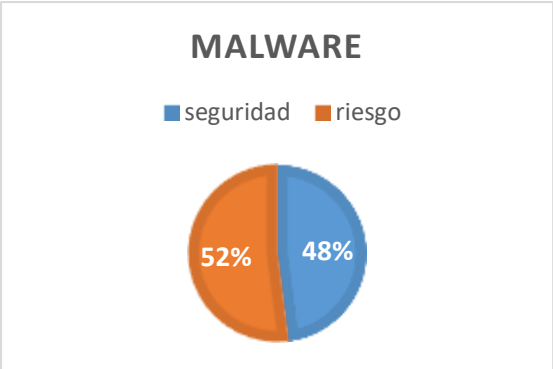
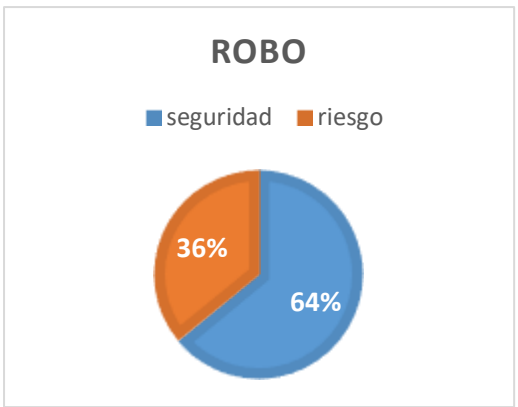
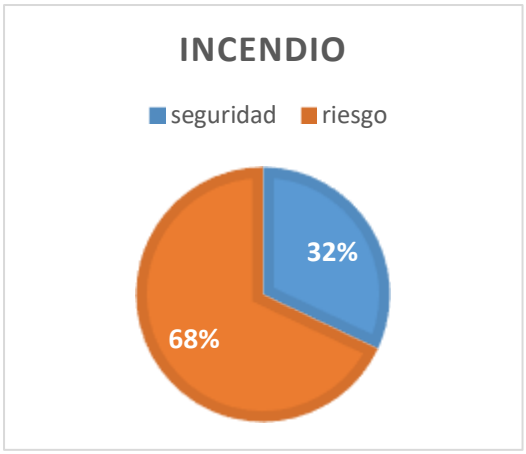
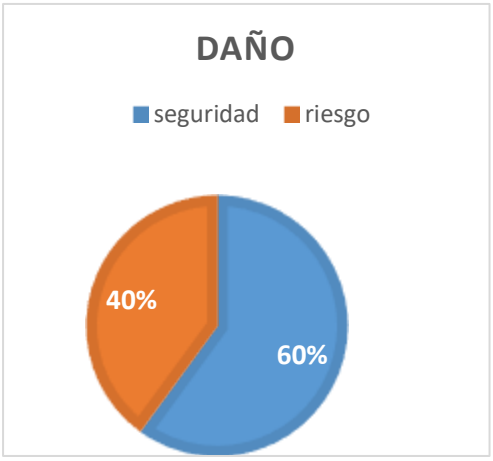


Ilustración 13. Hallazgos

<table>
<tr><td> 
</td><td>Los resultados generales obtenidos de los cuestionarios nos indican que el nivel de seguridad es menor al riesgo. Lo que aumenta las probabilidades de que exista un accidente de no llegar a tomar medidas precautelares.</td></tr>
<tr><td> 
</td><td>Malware debido a:
-No existe una política de seguridad.
-No existe un antivirus completo.
-No tienen restricciones para la instalación de software no autorizado
-No existen medidas de seguridad ante este riesgo
-No hay un control de los dispositivos periféricos conectados en los computadores.</td></tr>
<tr><td colspan="2">Es considerado un riesgo muy grave según el cuestionario aplicado, ya que el laboratorio está muy vulnerable a este tipo de ataques y la seguridad aplicada actualmente es más baja que el riesgo.</td></tr>
<tr><td> 
</td><td>Robo debido a:
-No existen control de acceso
-No están identificado los equipos.
-No firman un registro antes de ingresar
-No cuenta con sistema de alarma
No Hay dispositivos de rastreo
-No existen protocolos de incidentes</td></tr>
<tr><td colspan="2">Este riesgo es uno de los pocos donde la seguridad es mayor al riesgo, pero aún tiene riesgo considerable a tomar en cuenta y un nivel grave, por la situación de inseguridad que se vive es uno d ellos puntos a reforzar igualmente.</td></tr>
</table>

<table>
<tr><td> 
</td><td>Incendio debido a:
-No existen detectores de humo
-No existen rutas de evacuación.
-No se ha realizado simulacros.
-No son seguras la conexiones
-No se ha realizados inspecciones técnicas
-No están en buen estado las instalaciones
-No se verifica el vencimiento de los extintores</td></tr>
<tr><td colspan="2">Igual que el malware es considerado un riesgo muy grave debido al mal estado de la infraestructura eléctrica y los apagones comunes en el país. Es unos de los riesgos con más elevado porcentaje de riesgo y menor seguridad.</td></tr>
<tr><td> 
</td><td>Daño debido a:
-No presenta uso inadecuado de los equipos
-No cuenta con protección contra sobrecarga
-No tienen los equipos bien asegurados correctamente.
-No han implementado procedimientos para reportar daños
-No son revisadas las conexiones
-No cuenta con protección ante alteración de voltaje.</td></tr>
<tr><td colspan="2">El cuestionario dio como resultado mayor seguridad que riesgo, cuenta con un nivel de riesgo importante y aunque es el de menor nivel, no toca desestimarlo y es importante reducir su nivel de riesgo.</td></tr>
</table>

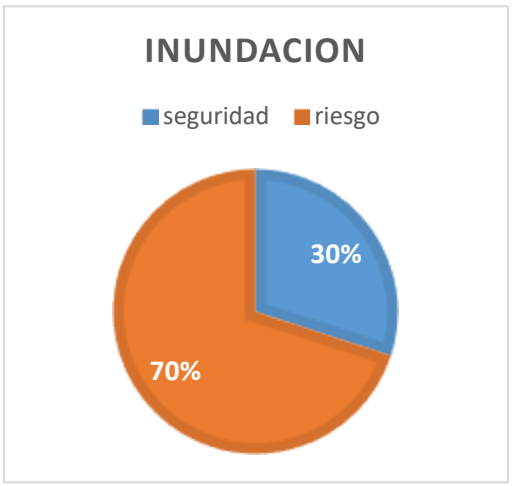
<table>
<tr>
<td> 
</td>
<td>Inundación debido a:
-No tiene sistemas de alerta para detectar acumulación de agua
-No cuanta con un protocolo de emergencia
-No tiene protección contra cortocircuitos por humedad
-No se ha identificado vías seguras de evacuación
-No están almacenados documentos físicos en áreas protegidas
-No se ha revisado estructuras para prevenir filtraciones
-No se han realizado auditorías previas</td>
</tr>
<tr>
<td colspan="2">Es uno de los riegos que registro menos nivel de seguridad en el cuestionario y tiene un nivel grave de riesgo, debido a que la infraestructura está muy antigua y necesita renovación.</td>
</tr>
</table>

Tabla 23. Hallazgos

5.1.4.1 Opinión

Los principales riesgos identificados son el robo, daño físico, incendio, inundación y malware. Al analizar el impacto de cada uno, se concluyó que el incendio, la inundación y el malware son los que requieren medidas urgentes, como se observa a continuación:

RIESGO	Nivel de riesgo
MALWARE	MUY GRAVE
ROBO	GRAVE
INCENDIO	MUY GRAVE
DAÑO	IMPORTANTE
INUNDACION	GRAVE

Tabla 24. Nivel de Riesgos

5.1.4.1.1 Recomendaciones

Por los datos obtenidos hasta ahora y viendo los riegos que se pueden ocasionar de no tomar medidas preventivas a tiempo y por evitar posibles amenazas a futuro se recomienda la implementación de un plan de recuperación

5.1.4.2 Plan de recuperación

Se creó una política de contingencia sobre el plan de recuperación ante desastres del Laboratorio 1 en la ULEAM extensión el Carmen, que consta con el propósito, objetivo, resumen de los riesgos y salvaguardas a plantear, identificación de escenarios, roles y documentos de respaldo en caso de emergencias. Con el objetivo de resumir el plan y presentarlo para que sea probado posteriormente.

DOCUMENTO DE POLÍTICA DE CONTINGENCIA PARA EL PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) DEL LABORATORIO DE LA ULEAM EL CARMEN

Versión: 1.0

Fecha de Elaboración: noviembre 04, 2025

Elaborado por: Angie Moreira

Revisado Por: Clara Poso

Aprovado por:

Revisión Programada: Anual o tras cualquier incidente significativo

Introducción

Propósito

Este documento presenta una política de contingencia como parte del plan de recuperación ante desastres del Laboratorio 1 en la ULEAM extensión el Carmen, cuyo enfoque principal es permitir la continuidad de las funciones cotidianas de los estudiantes y maestros en el laboratorio y a su vez definir procedimientos para responder de manera adecuada a cualquier incidente que vulnere la seguridad física de los activos. Con estas directrices se busca minimizar los impactos ante los riegos con más probabilidad presente y tomar medidas antes de que ocurra algo no previsto.

Alcance

Esta política es válidas para todos los ya sean activos físicos y lógicos:

- Equipos de computación (servidores, ordenadores, redes).
- Infraestructura física (Almacenamiento, electricidad y redes).
- Infraestrutura del laboratorio.
- Programas informáticos y aplicaciones laborales.
- Procesos de operación (Mantenimiento, Claves prácticas).
- Información crucial (Proyectos, investigaciones, bases de datos y tesis).
- Contingencias identificadas en la fase de riesgos, tales como: fallos técnicos, eventos naturales, daños humanos, malware.

OBJETIVOS ESPECÍFICOS

- Actualizar activamente la lista de riesgos existentes.
- Implementar salvaguardas específicas para los riegos identificados
- Permitir tener tiempos de recuperación reducidos para que las actividades no se vean afectadas y en funciones criticas tener un estimado de 72 horas.
- Proteger la integridad de los datos y la permanencia de los mismos.

RECONOCIMIENTO DE ESCENARIOS

En base a la etapa anterior de riesgos, dar prioridad a situaciones como las siguientes:

- Malware (alta probabilidad, impacto muy significativo).
- Robo (incidencia alta y probabilidad media).
- Incendio (probabilidad alta, impacto alto).
- Daño (probabilidad media, impacto medio).
- Inundación (probabilidad alta, impacto alto).

RIESGOS IDENTIFICADOS Y SALVAGUARDAS

Riesgos	Salvaguardas
MALWARE	• Instalar aplicaciones antimalware gratuitas (ej. Malware Bytes) • Instalar antivirus gratuitos de buena reputación • Limitar acceso a páginas de no seguras con el corta fuegos.
ROBO	• Asegurar bien los periféricos de las computadoras con binchas. • Revisión del laboratorio antes y después de cada clase. • Implementar cámaras de seguridad.
INCENDIO	• Verificar el estado de las instalaciones eléctricas • Remplazar los dispositivos ups averiados • Tener un kit contra incendios en el laboratorio.
DAÑO	• Incentivar a los alumnos a un buen uso de las instalaciones. • Establecer protocolos de conducta en los laboratorios.

	• Buscar una entra y salida del laboratorio ordenada.
INUNDACION	• Revisar el estado de las ventanas, para evitar filtración de agua. • Revisar el estado del techado de la universidad para evitar goteras. • Elevar las computadoras del suelo y paredes, para evitar humedad

Tabla 25. Riesgos Identificados

ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Encargado del Laboratorio	• Asignar recursos • Respaldar el plan • Declarar los estados de contingencia
Personal que usa del laboratorio	• Conocer sobre el plan de contingencia • Reportar accidentes
Equipo de Respuesta a Incidentes	• Monitorean riesgos • Informan riesgos • Ejecutan el plan ante desastres
Departamento de TI	• Soporte para respaldos • Soporte para recuperación de datos • Mantenimientos

Tabla 26. Roles y responsabilidades

COMUNICACIÓN

El plan de contingencia para la recuperación ante desastres estará disponible físicamente y digitalmente, además:

- Se establecerán canales de comunicación alternativos.
- Contará con lista de contactos de emergencia actualizada trimestralmente.
- Lista de contactos para servicios fuera de TI como mantenimiento del aire acondicionado.

MONITOREO Y ACTUALIZACIÓN

- Revisión semestral de la política de contingencia
- Actualización del plan después de cada accidente real

- Evaluación de efectividad anual
- Modificación según cambios que ocurren con el tiempo como: equipos, procesos o personal

RECURSOS

Recursos necesarios para:

- Asignar herramientas de respaldo y mantenimientos.
- Software de respaldo y recuperación de datos
- kits de emergencia (extintores, botiquines)
- Documentación adicional
- Protectores de energía
- Comunicación

OBJETIVOS DE RECUPERACIÓN

- **RTO:** < 72 horas para processos críticos
- **RPO:** < 24 horas para datos críticos
- **MTD:** Establecer

CRONOGRAMA DE ENTREGABLES

- Fase 2 Riesgos: 30/10/2025
- Fase 3 (BIA):
- Fase 4 (Controles):
- Fase 5 (Estrategias):
- Fase 6 (Plan de contingencia):
- Fase 7 (Mantenimiento):

DOCUMENTOS DE REFERENCIA

- Manual de Procedimientos del Laboratorio
  Link: https://www.uleam.edu.ec/wp-content/uploads/2016/11/REGLAMENTO-PARA-EL-USO-DE-LABORATORIOS-DE-LA-UNIVERSIDAD.pdf
- Reglamento de la ULEAM
  Link: https://www.uleam.edu.ec/reglamentos/

- Lista detallada de riesgos identificados.
  Riesgos identificados se muestran en la Tabla. 12

- Reporte de Incidentes previos.
  Se muestra en la ilustración 21 y 22
- Contactos de Emergencia.
  Link: https://departamentos.uleam.edu.ec/diit/contactenos/

FIRMAS DE APROBACIÓN:

Elaborado por:

_____

Angie Moreira (Creadora del plan)

04/11/2025

Revisado por:

_____

Clara Poso (tutora)

04/11/2025

Aprobado por:

_____

Encargado del laboratorio

04/11/2025

Distribución: Todos los miembros del laboratorio y autoridades correspondientes.

5.1.4.3 ANALISIS DE IMPACTO DE NEGOCIO (BIA)

5.1.4.3.1 Identificar funciones críticas

Para la identificación de las funciones críticas del laboratorio se hizo una visita técnica con el encargado del departamento TI, donde se implementó un formulario de identificación (anexo E), que busca obtener datos como dependencias, los tiempos MTD (Máximo Tolerable), RTO (Objetivo de Recuperación), RPO (Punto de Recuperación) e impacto económico y prioridad.

Puntos a tomar en cuenta:	Escala para detectar una función:
• RPO ≤ RTO.	• Crítico: MTD < 8h • Medio: MTD > 24h • Bajo: MTD > 72h
• RTO ≤ MTD	

Ilustración 14. Pautas del estudio

5.1.4.3.2 Resultados formularios (RTO, RPO, MTD)

De la aplicación del formulario de identificación de funciones criticas (anexo E) se terminaron detectando 4 funciones basadas en los principales riesgos encontrados, estas son: el suministro de energía, conectividad de red, servidor académico, mantenimiento, seguridad física, recuperación malware.

ID	Funciones	Prioridad	MTD	RTO	RPO	Pérdida (72h)	Impacto (72h)	Consecuencias (72h)
FC-01	Suministro de Energía	1	8h	2h	1h	$500	Crítico	Retraso académico grave
FC-02	Conectividad de Red	1	8h	4h	1h	$400	Crítico	Cancelaciones prácticas en línea
FC-03	Internet y disponibilidad	1	24h	8h	4h	$700	Alto	Detención labores académicas
FC-04	Mantenimiento	3	72h	24h	12h	$100	Bajo	No se pueden hacer prácticas
FC-05	Seguridad Física	2	24h	8h	8h	$800	Alto	No se pueden hacer prácticas
FC-06	Recuperación Malware	1	24h	8h	4h	$600	Alto	Pérdida de información

Tabla 27. Análisis BIA

Con los datos obtenidos del estudio pudimos identificar que las funciones críticas en el Laboratorio 1 de la ULEAM extensión el Carmen son: el suministro de energía y la conectividad a la red ya que su máximo tolerable es muy bajo, y las funciones de alta prioridad son el servidor académico seguridad física del laboratorio y ataques malware con un máximo tolerable de 24 horas y función de nivel bajo es el mantenimiento por su tiempo tolerable que es alto.

5.1.4.4 IDENTIFICAR CONTROLES PREVENTIVOS

5.1.4.4.1 Identificar el estado de sistemas

Se realizó 5 preguntas por cada función critica identificada, para con ello a consiguiente se pueda obtener las salvaguardas actuales del laboratorio. Este formulario se observa en el Anexo F y los resultados se muestran a continuación.

5.1.4.4.2 Identificación de salvaguardas existentes

Partiendo de la visita técnica al laboratorio y los datos obtenidos de campo, se pudieron identificar 11 salvaguardas salidas de las funciones criticas identificadas, que son las que ya existen actualmente y están funcionales, pueden ser algo deficientes, pero son con las que se maneja el equipo técnico.

#	Área	Salvaguardas actuales detectadas	Detalles
1	Suministro de Energía	Conexión a tierra física verificada	Existe y está implementada en el laboratorio
2		Capacidad eléctrica adecuada	Soporta la carga total sin sobrecalentamiento detectado
3		Reguladores de voltaje en algunos equipos	Protegen parte de los equipos contra variaciones de voltaje
4	Conectividad de Red	Cableado estructurado (conexión cableada)	Todo el laboratorio usa cableado estructurado
5		Velocidad y estabilidad de red local aceptable	Conexión por cable buena, solo con fallos técnicos temporales
6	Internet y Disponibilidad	Conexión a Internet razonablemente estable	Caídas no muy frecuentes
7	Mantenimiento	Mantenimiento preventivo básico anual	Se realiza normalmente cada año (limpieza y revisión)
8		Inventario de hardware actualizado	Existe principalmente hardware y se mantiene
9	Seguridad Física	Cableado de red organizado	Evita riesgos de tropiezos y daños

10	Recuperación y Malware	Antivirus activo en todos los equipos	Microsoft defender activo y actualizado
11		Firewall centralizado configurado desde matriz	Bloquea sitios no permitidos y protege la red

Tabla 28. Salvaguardas existentes

5.1.4.5 DISEÑO DE ESTRATEGIAS DE CONTINGENCIA

5.1.4.5.1 Identificación de salvaguardas ante riesgos

Con los datos obtenidos anteriormente y sabiendo que salvaguardas existen, se puede recomendar la implementación de nuevas salvaguardas para mejorar la seguridad ante riesgos.

Riesgo	Salvaguarda Actual	Salvaguarda Recomendada	Nivel de seguridad actual	Nivel de seguridad esperado	Acción Requerida	Costo Promedio
Malware	Microsoft Defender activo	Cambiar a antivirus empresarial	Bajo	Medio o Alto	Implementar las 4 mejoras lógicas	600-800
	Firewall centralizado	Desactivar admin local (usar cuentas estándar + LAPS)				
		Activar WDAC o AppLocker				
		Habilitar BitLocker en todos los discos				
Robo	Ninguna medida física efectiva	Anclar CPUs y monitores	Bajo	Medio o Alto	Instalación física + sistema de video	1800-3000
	Cableado organizado	Sistema de Control de acceso Completo				
	Control de acceso medio	4 Cámaras IP + NVR con alarma				
Incendio	Extintor	Recarga e inspección anual	Bajo	Medio	Mantenimiento +	200-300

	Sin detección automática	3 o 4 Detectores de humo autónomos			instalación de sensores	
Daño electrico	Puesta a tierra OK	UPS para todos los equipos	Medio	Alto	Compra e instalación de infraestructura UPS	1800-2500
	UPS en una que otra PC	Supresores de picos en todos los puestos				
Inundacion	Ninguna medida actual	Elevar equipos +15cm del suelo	Bajo	Medio	Obra civil menor + sensores	200-500
		Sensores de agua y mejor filtrado en suelo				
		Sellado de techos y tuberías				
					TOTAL	4,600$-7,100$

Tabla 29. Salvaguardas recomendadas

5.1.4.5.2 Manejo de Backups y almacenamiento

Basándose en el análisis BIA anterior donde robo y ataques malware son riesgos entre críticos y altos. Y dado que las funciones criticas tienen un RPO de 1 a 4 y la probabilidad FC-06 de malware es alta por ello el diseño de backups debe ser robusto y rápido.

5.1.4.5.2.1 Estrategia de Copia de Seguridad

La estrategia se basará en la regla 3-2-1 modificada, usando discos duros y USB como los medios removibles que rotarán dentro y fuera del laboratorio que consiste en tener 3 copias de seguridad y mantener el dato original los PC del laboratorio, una copia en el disco duro de Backup A (en el laboratorio), y una tercera copia en el disco duro B (Fuera del laboratorio). Además, toca tener, 2 medios: que son en los discos duros externos removibles y unidad USB C de gran capacidad. Y, por último, 1 sitio externo al laboratorio: que cuente con un juego de discos duros/USB debe ser transportado diariamente a una ubicación física alterna segura, esto protege al laboratorio de la pérdida total de datos ante desastres locales como Incendio, robo o Inundación.

- Frecuencia de las copias de seguridad (cumpliendo el RPO): Se realizarán backups incrementales cada 1 a 4 horas según la criticidad de la función, directamente a un disco duro externo dedicado que actúa como el almacenamiento de backup local.
- Etiquetar y almacenar: Los recursos tienen que estar conservados en un recipiente robusto y etiquetados de forma precisa con la fecha y hora de la última copia.
- Juego de discos: Para garantizar que al menos una copia esté siempre segura, se aconseja disponer de un mínimo de 5 o 7 unidades para facilitar una rotación eficiente sin sobrescribir las copias más actual.
- Vida útil: Los discos duros externos son propensos a sufrir fallos físicos y tienen una vida útil corta, es necesario que sean sustituidos cada tres a cinco años de manera preventiva, y su estado de salud debe ser supervisados ininterrumpidamente a través del software.Protocolo de Protección Anti-Malware

Este protocolo es crítico al usar medios físicos de conexión directa como USB o SATA y es esencial para cumplir el RTO de 8 horas para la Recuperación Malware como se especifica en la FC-06.

Etapa	Acción	Justificación
Inicio del Backup	El disco duro de respaldo solo debe conectarse cuando inicie la copia	Reducir la ventana de exposición al Malware en la red.
Durante el Backup	El software debe ejecutar la copia automáticamente y luego validar la integridad.	Asegurar la fiabilidad de la copia.
Fin del Backup (CRÍTICO)	Desconexión Física Inmediata: Una vez que se haya terminado la copia es necesario desenchufar básicamente el USB o el disco duro del servidor	Debe establecer un Air Gap(división lógica y física con el fin de prevenir que el ransomware pueda cifrar o perjudicar la copia de seguridad
Almacenamiento Local	Los discos desconectados que permanezcan en el sitio deben ser guardados en una Caja Fuerte o Gabinete Ignífugo con acceso restringido.	Protege los medios contra Robo e Incendio mientras esperan la rotación.

Tabla 30. Protocolo de Backup

5.1.4.5.3 Costos estimados

Componente	Estimación de Costo	Justificación y Función Crítica Asociada
Múltiples Discos Duros Externos/USB	$500 - $800 USD	Adquisición de medios para la rotación off-site (3-2-1).
Caja Fuerte / Armario Ignífugo	$100 - $300 USD	Conservación segura de discos de respaldo para evitar el robo o incendio.
Sistemas de Alimentación Ininterrumpida (UPS)	$100 - $300 USD	Vital para proteger la FC-01 Suministro de Energía y la integridad del backup.
Software de Backup y Restauración	$20 - $50 USD	Instrumento para automatizar la copia incremental y respetar el RTO.
Malwarebytes Free	$0 USD	Herramienta de desinfección esencial para la Recuperación Malware FC-06.
Tiempo de Personal / Implementación	$200 USD (Tiempo de IT)	Costo asociado a la instalación, configuración y creación de protocolos de uso de las herramientas gratuitas.
Total, Estimado	$920 - $1750 USD	

Tabla 31. Costos estimados

De contar con el presupuesto se aumentaría la replicación automatizada en la nube. En lugar de rotar discos físicos, se aplicarán políticas de retención automatizadas en la consola de la nube, eliminando así el desgaste físico de puertos USB y la necesidad de monitorear la salud física de múltiples discos externos. Las configuraciones a cambiar en caso de implementar serian:

- **Configuración previa:** primero activar inmutabilidad configurando el repositorio en la nube para que los archivos subidos no puedan ser modificados ni borrados por un periodo definido de 7 o más días.

- **Inicio del Backup:** Verificación de conexión segura y encriptada (VPN o SSL/TLS) hacia el proveedor de nube. Esto asegura que los datos viajen cifrados desde el laboratorio hasta la nube sin intercepciones.
- **Durante del Backup:** Antes de salir del servidor, el software cifra con AES-256 la copia local y la réplica en el internet, esto es para asegurar que los datos guardados en la nube no puedan leerse sin la clave de des encriptación.
- **Fin del Backup:** Informar el éxito y valida la credibilidad de modo automático por correo electrónico.
- **Aislamiento local:** La unidad de backup local debe tener credenciales distintas a las del dominio principal y acceso restringido.

Esto aumentaría la seguridad y protección de la información, pero aumentaría súbitamente los costos de implementación.

5.1.4.5.4 Tiempo de recuperación

El plan de recuperación está diseñado para cumplir con los siguientes RTO:

ID	Función Crítica	Impacto (72h)	RTO Objetivo
FC-01	Suministro de Energía	Crítico	2 horas
FC-02	Conectividad de Red	Crítico	4 horas
FC-03	Internet y disponibilidad	Alto	8 horas
FC-06	Recuperación Malware	Alto	8 horas
FC-05	Seguridad Física	Alto	8 horas
FC-04	Mantenimiento	Bajo	24 horas

Tabla 32. Tiempos de recuperación

5.1.4.5.5 Kit de recuperación

Ítem	Descripción	Dónde Comprar	Precio	Cantidad	Total
Maleta plástica hermética 50 cm (roja)	Que proteja al Kit de humedad o daños	Ferretería “Kiwi”	$18.00	1	$18
Extintor CO_2 2 kg (recargado)	Para alertas de fuego	Ferretería “Kiwi”	$31.16	1	$31.16
Manta ignífuga apaga fuego 1×1 m (fibra de vidrio)	Para alertas de fuego	Mercado libre ec	$10.50	3	$31.50
Candado ideal para uso en exteriores de 48 mm – CERMAX + cable flexible 3/16" acero 7x19 recubierto PVC, 75 m – FIERO 25 m	Para asegurar computadoras os dispositivos o puertas como la de los swich.	Ferretería “Kiwi”	$5+ $1.18 x m	1+20m	$28.60
Linterna recargable de 1200lm - TRUPER	En caso de un apagón masivo o fallas eléctricas	Ferretería “Kiwi”	$23.19	1	$23.19
UPS de 4 tomas de 600VA / 360W - 120VAC + RJ45. - EPCOM	Ante problemas eléctricos o remplazo de uno averiado	Computron	$65.69	1	$65.69
Disco Duro Externo 2tb Adata Hd710 Pro Ahd710p-2tu31 + USB 16gb adata.	Estos contaran con: -El ultimo respaldo -Sistemas operativos booteable -antivirus, antimalware	Computrom	$140.00	1+1	$140
Gel sílice (bolsas de 500 g)	Para extraer el exceso de humedad de dispositivos en caso de inundación	Mercado libre ec	$17.00	3	$51
Kit herramientas mantenimiento equipos.	–juego de destornilladores de precisión 58 en 1	Mercado libre ec	$24.35	1	$24.35

Ítem	Descripción	Dónde Comprar	Precio	Cantidad	Total
	– Cuchillo para uso general. – Correa antiestática. – Pinzas antiestáticas. – Pin expulsor de tarjeta SIM, ventosa LCD. – Plectro triangular. – Reglas de acero inoxidable, espátula de metal y espátula de plástico				
Cinta aislante + bridas	Para garantizar la seguridad de los dispositivos o preparar el cableado	Ferretería	$8.00	2+1	$8
TOTAL					**$421.56**.

Tabla 33. Costos Kit Recuperación

Capítulo VI

6 Conclusiones y recomendaciones

6.1 Conclusiones

- La detección de las problemáticas que comprometen la integridad y la seguridad física de los equipos tecnológicos del Laboratorio 1 del programa de Ingeniería en Software de la ULEAM Extensión El Carmen posibilitó el hallazgo de las vulnerabilidades más relevantes. Esto se considera un pilar esencial para decidir acciones enfocadas en proteger el equipo informático y prevenir daños.
- El análisis de fuentes bibliográficas confiables permitió que la investigación tuviera una base teórica, estableciendo un vínculo claro entre el programa de recuperación ante desastres y la seguridad física del equipo informático. Las entrevistas y encuestas realizadas a estudiantes, maestros y personal técnico brindaron información valiosa acerca de la condición actual del laboratorio, lo que permitió entender cómo los usuarios perciben el laboratorio y respaldar la toma de decisiones para aumentar la seguridad.
- La detección de amenazas ambientales y físicos, como el robo o la obsolescencia de las redes eléctricas de respaldo, confirma que la seguridad del equipo está directamente relacionada con la presencia de protocolos formales con el fin actuar y vigilar continuamente.
- El establecimiento de protocolos para actuar en emergencias permitió que el personal del Laboratorio 1 tuviera roles y responsabilidades definidas, lo que ayudó a responder de manera ordenada y puntual ante situaciones imprevistas. Esto contribuye a disminuir los riesgos y atenuar las consecuencias de eventos adversos.
- La documentación del Plan de Recuperación de Desastres posibilitó que se recopile la información requerida para su implementación adecuada, lo cual favoreció la distribución de copias al personal encargado del mantenimiento y a los responsables de utilizar el laboratorio. Esto refuerza la continuidad en las operaciones y el manejo apropiado de los recursos tecnológicos

6.2 Recomendaciones

- A la universidad (Extensión El Carmen de ULEAM), se aconseja que la universidad asigna recursos técnicos y financieros para implementar y mantener el plan de recuperación de desastres, asegurando así la protección de los equipos informáticos y la continuidad de las actividades académicas en el Laboratorio 1.
- Al coordinador de la carrera de ingeniería en software: se recomienda que el coordinador de la carrera supervise y fomente la implementación del plan de recuperación ante desastres, además de que actualice con regularidad los protocolos de seguridad física, en función de las necesidades efectivas del laboratorio.
- Al personal docente y técnico del laboratorio: se sugiere que el personal se capacite de manera constante en cómo manejar correctamente los equipos informáticos y qué procedimientos seguir en situaciones de emergencia, para así disminuir los riesgos. Y actuar de forma eficaz frente a cualquier eventualidad.
- A los alumnos se les recomienda emplear los equipos de manera responsable y observar las reglas de seguridad que rigen en el laboratorio, ayudando de esta manera a preservar los recursos tecnológicos y evitar incidentes.

7 Bibliografía

Aguirre, A. Á., Ortiz, E. G., & Sainz, J. L. (2021). *Metodología de la Investigación en Enfermería.* D.R. © Edicione. Obtenido de https://www.researchgate.net/publication/379197457_Descripcion_de_poblacion_muestra_y_muestreo

Alban, G. P., Arguello, A. E., & Molina, N. E. (2020). Metodologías de investigación educativa. *RECIMUNDO*. doi:10.26820/recimundo/4.(3).julio.2020.163-173

Almagro, L. (2019). *CIBERSEGURIDAD MARCO NIST.* OEA. Obtenido de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Amaya, G. D., & Ángel, R. A. (2023). *Diseño y elaboración del plan de recuperación de desastres para el área TI de la Escuela Colombiana de Ingeniería Julio Garavito.* UNIVERSIDAD PILOTO DE COLOMBIA. Obtenido de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12501/Dise%C3%B1o%20y%20Elaboracion%20del%20DRP%20para%20el%20area%20de%20TI%20de%20la%20ECI.pdf?sequence=1&isAllowed=n

ANT. (2021). *PLAN DE RECUPERACION ANTE DESASTRES.* agencia nacional de tierras. Obtenido de https://www.ant.gov.co/sites/default/files/2024-06/documentos/archivos/GINFO-Plan-001.pdf

Antonio, P. G., Rosaura, H. T., Hans, C. C., & Amanda, O. V. (2023). *Fortalecimiento Metodológico de la Seguridad Informática en Posgrados: Análisis y Estrategias de Mejora.* Comité Editorial del Grupo AEA. Obtenido de https://www.editorialgrupo-aea.com/index.php/EditorialGrupoAEA/catalog/book/56

Atiku, M., Garba, A. A., & Bade, A. M. (2021). A Brief Analysis on the Existing Disaster Recovery Phases and Activities Plans. *iJournals: International Journal of Software & Hardware Research in Engineering (IJSHRE)*, 10. Obtenido de https://www.researchgate.net/publication/349522421_A_Brief_Analysis_on_the_Existing_Disaster_Recovery_Phases_and_Activities_Plans

Awasthi, A. (2020). ROLE OF TEAM MEMBERS IN DISASTER RECOVERY PLANNING. *recentscientific*, 5. Obtenido de https://www.researchgate.net/publication/339130860_Role_of_Team_Members_in_Disaster_Recovery_Planning

Bacula Systems S.A. (2023). *IT Disaster Recovery plan.* Bacula Systems S.A. Obtenido de https://www.baculasystems.com/wp-content/uploads/2023/02/dr-guide.pdf

Belapurkar, R. (2022). Evolution of Security and Perimeter-Based Approach. *rutvik*. Obtenido de https://www.rutvik.uk/zt-1?

Benítez, J. M. (2021). *DISEÑO DE UNA SOLUCIÓN INTEGRAL DE BACKUP Y DISASTER RECOVERY.* Catalunya: Universitat Oberta de Catalunya. Obtenido de https://openaccess.uoc.edu/bitstream/10609/132629/6/josemhbTFG0621memoria.pdf

Bhat, A. K. (2025). RECUPERACIÓN DE DESASTRES EN LA ERA DIGITAL: UNA TRANSFORMACIÓN TECNOLÓGICA. *IAEME*, 17. Obtenido de https://www.researchgate.net/publication/390398726_DISASTER_RECOVERY_IN_THE_DIGITAL_AGE_A_TECHNOLOGICAL_TRANSFORMATION

Bigelow, S. J. (2025). *¿Qué es un plan de recuperación ante desastres (DRP)?* TechTarget. Obtenido de https://www-techtarget-com.translate.goog/searchdisasterrecovery/definition/disaster-recovery-plan?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Borrego, S., & Vivar, I. (2022). *Gestión de riesgos para la prevención y mitigación de desastres en el patrimonio documental. El plan de reducción de riesgo de desastre.* Archivo Nacional de la República de Cuba. Obtenido de https://www.researchgate.net/publication/368116508_Gestion_de_riesgos_para_la_prevencion_y_mitigacion_de_desastres_en_el_patrimonio_documental_El_plan_de_reduccion_de_riesgo_de_desastre

Briceño, E. V. (2021). *SEGURIDAD DE LA INFORMACIÓN.* Editorial Área de Innovación y Desarrollo,S.L. Obtenido de https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

B-safe. (2020). *Protección de hardware y software.* B-SAFE. Obtenido de https://lms.project-bsafe.eu/wp-content/uploads/2018/05/4-Content-Unit-Hardware-and-software_ES-1.pdf

Carazas, R. R., Huiza, D. M., Martínez, M. d., Barrios, S. T., & Quispe, M. L. (2024). *Método de investigación científica.* nstituto de Investigación y Capacitación © 4Profesional del Pacífico para su sello editorial IDICAP PACÍFICO. Obtenido de idicap.com/ojs/index.php/editorialeip/article/view/285/303

Chávez, J. D. (2021). *Fundamentos de Auditoría Informática.* Venezuela: IEASS, Editores. Obtenido de https://www.academia.edu/45170544/Fundamentos_de_Auditor%C3%ADa_Inform%C3%A1tica?nav_from=3eaf804b-e084-4ac1-ad13-89ea1f349e07

CIAT. (2024). *Guía para el diseño de un plan de continuidad de negocio para administraciones tributarias.* ciat.org. doi:978-9962-722-63-2

Connor, T. (2023). *Una descripción general de las publicaciones especiales del NIST 800-34, 800-61, 800-63 y 800-218.* Google. Obtenido de https://www-schellman-com.translate.goog/blog/federal-compliance/overview-nist-800-series-special-publications?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Council. (2020). *Disaster Preparedness and recovery plan.* Community Foundation Leadership Team. Obtenido de https://cloudian-com.translate.goog/guides/disaster-recovery/4-disaster-recovery-plan-examples-and-10-essential-plan-items/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Dearniwati, E., Nurlette, G. A., Anwar, S., & Purwanto, H. (2025). Preparation of IT Disaster Recovery Plan (DRP) using NIST SP 800-34 Framework (Case Study: PT Pamapersada Nusantara, Jakarta). *Eduvest – Journal of Universal Studies,* 9. Obtenido de https://www.researchgate.net/publication/388781234_Preparation_of_IT_Disaster_Recovery_Plan_DRP_using_NIST_SP_800-34_Framework_Case_Study_PT_Pamapersada_Nusantara_Jakarta

Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 2700.* Universidad Nacional de Colombia. Obtenido de https://repositorio.unal.edu.co/bitstream/handle/unal/80158/9789587946017.pdf?sequence=2&isAllowed=y

Duque, F. J. (2022). *Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 27000.* Bogota: Editorial Universidad Nacional de Colombia. Obtenido de

https://repositorio.unal.edu.co/bitstream/handle/unal/80158/9789587946017.pdf?sequence=2&isAllowed=y

Duque, F. J., Echeverry, C. E., & Trujillo, M. L. (2024). *Modelos y marcos de referencia de gestión de riesgos en entornos digitales.* Manzinales: Universidad Nacional de Colombia. Obtenido de https://repositorio.unal.edu.co/bitstream/handle/unal/86596/Libro_Digital_Modelosymarcosdereferencia.pdf?sequence=2&isAllowed=y

EAR/PILAR. (2025). *Manual de Continuidad.* PIlar. Obtenido de https://www.ar-tools.com/doc/manual_bcm_es_2025.pdf

Gonzáles, J. L. (2021). *DISEÑO Y METODOLOGÍA DE LA INVESTIGACIÓN.* ENFOQUES CONSULTING EIRL. Obtenido de https://www.researchgate.net/publication/352157132_DISENO_Y_METODOLOGIA_DE_LA_INVESTIGACION

González, J. (2021). *Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario* (Vol. 171). Castilla: Ediciones de la Universidad de Castilla La Mancha. Obtenido de https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/8728928.pdf&ved=2ahUKEwjB3bet8K-OAxXomrAFHe18ADsQFnoECBEQAQ&usg=AOvVaw3LvewxG-2IcaiDSW4RXPHl

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

Guanoluisa Almache, F., Bosquez Remache, J., Esparza Pijal, S., & Benavides. (2023). APUNTES SOBRE LOS MÉTODOS DE INVESTIGACIÓN Y TÉCNICAS DE RECOLECCIÓN DE DATOS UTILIZADAS EN LA INVESTIGACIÓN JURÍDICA. *Bibliotecas. Anales de Investigacion*, 17. Obtenido de https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://dialnet.unirioja.es/descarga/articulo/9285926.pdf&ved=2ahUKEwj9sdn0ubCOAxUfRDABHdOKA8gQFnoECBgQAQ&usg=AOvVaw268IfeM_Sm_PF2zGviYKvg

GUILLEN, T. M. (2018). *DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO BASADO EN COBIT, ITIL Y DE ACUERDO A LA NORMA ISO 2230 PARA EL CPD.* Quito: UNIVERSIDAD POLITÉCNICA SALESIANA. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/15904/1/UPS-ST003686.pdf

Herbane, B. (2010). The Evolution of Business Continuity Management: A Historical Review of Practices and Drivers. *Routledge*, 26. Obtenido de www.researchgate.net/publication/227608980_The_Evolution_of_Business_Continuity_Management_A_Historical_Review_of_Practices_and_Drivers

Hodgson, Q. E., Clark-Ginsberg, A., Haldeman, Z., Lauland, A., & Mitch, I. (2022). *Managing Response to Significant Cyber Incidents.* Santa Monica: © RAND Corporation. Obtenido de https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1265-4/RAND_RRA1265-4.pdf

INCIBE. (2020). *CONTINGENCIA DE CONTINUIDAD DE NEGOCIO.* Madrid: Incibe. Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Isniah, S., Purba, H. H., & Debora, F. (2020). Plan do check action (PDCA) method: literature review. 11. Obtenido de https://www.researchgate.net/publication/343384691_Plan_do_check_action_PDCA_method_literature_review_and_research_issues

ISO.org. (2005). ISO/IEC 27001:2005. 41. Obtenido de https://mmujica.wordpress.com/wp-content/uploads/2007/07/iso-27001-2005-espanol.pdf

ITA. (2020). *Disaster Recovery Plan Template.* Obtenido de https://fsmsdc.org/wp-content/uploads/2020/03/DisasterRecoveryPlanTemplate.pdf

Lara, E. G. (2023). *Seguridad en la Infraestructura de Redes: Desafíos y Estrategias de Protección.* VICTEC. Obtenido de https://portal.amelica.org/ameli/journal/572/5724522015/5724522015.pdf

Ludy, H., & Raúl, G. (2010). ANALISIS DE IMPACTO AL NEGOCIO. *Universidad Piloto de Colombia.*, 4.

Marianne, S., Pauline, B., Wohl, P. A., Dean, G., & David, L. (2010). *Contingency Planning Guide for Federal Information Systems.* Nist. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Mena, E. A., & Ordóñez, J. A. (2021). *Fundamentos de seguridad informática.* Quevedo: Editorial Grupo Compás. Obtenido de https://www.researchgate.net/publication/354054517_Libro_Fundamentos_de_seguridad_informatica

Ministerio de turismo Kenia. (2023). *Plan disaster recovery.* Obtenido de https://www.tpf.go.ke/sites/default/files/reports/Disaster%20Recovery%20Plan%20website%202023.pdf

Mitnick, k., & Simon, W. (2020). *El Arte de la Intrucion.* Wiley Publishing, Inc. Obtenido de https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Intrusion.pdf

Mohamed, M. M., Carranza, C. P., Meza, F. T., León, C. R., & Gonzáles, J. L. (2023). *Metodología de la investigación: Guía para el proyecto de tesis.* Puno, Peru: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C. Obtenido de https://editorial.inudi.edu.pe/index.php/editorialinudi/catalog/view/82/124/149

Morales, J. L. (2021). *PROPUESTA DE UN PLAN DE CONTINGENCIA Y DE RECUPERACIÓN DE DESASTRES FRENTE A LOS RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE TICS.* QUITO: UNIVERSIDAD POLITÉCNICA SALESIANA. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/21298/1/UPS%20-%20TTS534.pdf

National Institute of Standards and Technology. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.* Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

Neuman, W. L. (2020). *Social Research Methods: Qualitative and Quantitative Approaches* (Vol. 8th). Pearson. Obtenido de https://letrunghieutvu.yolasite.com/resources/w-lawrence-neuman-social-research-methods_-qualitative-and-quantitative-approaches-pearson-education-limited-2013.pdf

Nikolovski, S., Milenkovski, B., Petreska, A., & Slavkovska, D. (2024). Cloud services modeling for long-term intellectual capital protection. *AIIT*, 8. Obtenido de

https://eprints.uklo.edu.mk/id/eprint/10533/1/Cloud%20services%20modeling%20for%20long-term%20intellectual%20capital.pdf

NQA. (2022). *ISO 27001:2022*. NQA. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

ORELLANA, A. E. (2017). *Evaluación de riesgos y Desarrollo de un plan de recuperación ante desastres informáticos aplicado al Centro de Datos y Comunicaciones de la UPSE.* SANTA ELENA: UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA. Obtenido de https://repositorio.upse.edu.ec/bitstream/46000/3978/1/UPSE-TIN-2017-0005.pdf

Pamungkas, E. D., Fatonah, S., Akbar, H., & Firmansyah, G. (2023). Análisis del plan de recuperación ante desastres basado en el marco NIST SP 800-34. *JISS*. Obtenido de https://www.researchgate.net/publication/375554163_Disaster_Recovery_Plan_Analysis_Based_on_the_NIST_SP_800-34_Framework_Case_Study_PT_Wijaya_Karya_Persero_Tbk

Pinchao, R. S., Hernández, C. G., & Minaya Macías, R. W. (2024). *Fundamentos de Seguridad Informática y Ciberseguridad.* El Carmen, Manabí, Ecuador: Ediciones Gesicap. Obtenido de https://www.researchgate.net/publication/389395515_Fundamentos_de_Seguridad_Informatica_y_Ciberseguridad

Preston, W. C. (2021). *Modern Data Protection.* O'Reilly Media. Obtenido de https://dokumen.pub/modern-data-protection-ensuring-recoverability-of-all-modern-workloads-1nbsped-1492094056-9781492094050.html

PRIA. (2020). Asset Management – The Foundation of DRP. *PROPERTY RECORDS INDUSTRY ASSOCIATION*, 15. Obtenido de https://member.pria.us/files/resource_library_files/Archival_Backup_and_Disaster_Recovery/Disaster_Preparedness_Asset_Management_2020-04-27_cf.pdf

Rađenović, T., & Živković, S. (2022). THE EFFECTIVENESS OF BUSINESS CONTINUITY MANAGEMENT SYSTEM IN ENTERPRISES. *RESEARCHGATE*, 7. Obtenido de

https://www.researchgate.net/publication/366946784_The_Effectiveness_of_Business_Continuity_Management_System_in_Enterprises

Ramiro, R. (13 de 06 de 2020). *Conceptos básicos de Plan de Continuidad de Negocio (RPO, RTO, WRT, MTD…)*. Obtenido de ciberseguridad.blog: https://ciberseguridad.blog/conceptos-basicos-de-plan-de-continuidad-de-negocio-rpo-rto-wrt-mtd/

Reaño, R. E., Miñán, V. A., Saavedra, C. L., & Castillo, N. A. (2023). *Amenaza, riesgo y respuesta. Metodologías de evaluación de riesgos informáticos.* Quito: Atik Editorial. Obtenido de https://www.researchgate.net/publication/373645636_Amenaza_riesgo_y_respuesta_Metodologias_de_evaluacion_de_riesgos_informaticos#pf2a

red.tic. (2021). *Recomendaciones para el almacenamiento de información.* UNAM. Obtenido de https://www.red-tic.unam.mx/recursos/2021/2021_Recomendaciones_RedResponsablesTIC_02.pdf

Rene, K. (2024). *Information Technology DRP*. NWF. Obtenido de https://nwfhealth.org/wp-content/uploads/2024/05/900-921-x-1-IT-Disaster-Recovery-Plan-FY-23-24-April-24.pdf

Rios, E. M. (2020). *DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS PARA EL CENTRO DE DATOS DE LA GOBERNACIÓN DEL DEPARTAMENTO DEL CHOCÓ.* CHOCÓ: UNIVERSIDAD PONTIFICIA BOLIVARIANA. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/6049/DISE%C3%91O_PLAN_RECUPERACI%C3%93N_DESASTRES_INFORM%C3%81TICOS.pdf

Rivas, P., & Luna, M. L. (2014). *El método de proyectos.* Marea verde. Obtenido de https://www.apuntesmareaverde.org.es/grupos/tec/loe/3eso/metodo_proyectos.pdf

Robalino, A. P., Chávez, W. G., & Lunavictoria, J. K. (2023). *Auditoría Informática.* Riobamba: La Caracola Editores. Obtenido de http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2023-09-27-175154-2.%20LIBRO_AUDITORIA%20INFORMA%CC%81TICA%20digital.pdf

Rocío, B. A., Richard, B. M., Hernando, C. C., & Janeth, O. C. (2021). Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio. *Universidad*

Santo Tomás, 32. Obtenido de https://www.redalyc.org/journal/5604/560468688007/560468688007.pdf

Saeed, S. (2020). Disaster Recovery Planning: Best Practices for Ensuring Operational Continuity. *Mehran University of Engineering and Technology*, 20. Obtenido de https://www.researchgate.net/publication/383360303_Disaster_Recovery_Planning_Best_Practices_for_Ensuring_Operational_Continuity

SafetyCulture. (2024). *SafetyCulture*. Obtenido de SafetyCulture: https://safetyculture.com/es/temas/ciclo-pdca/

Seco, A., Martins, W., & Netto, G. (2024). Plan de Continuidad de Negocios: importancia creciente para las Administraciones Tributarias. *Centro Interamericano de Administraciones Tributarias - CIAT*, 39. Obtenido de https://www.ciat.org/Biblioteca/DocumentosdeTrabajo/2024/DT-03-24-seco-netto-martins.pdf

Smith, E. (2021). ¿Qué es una ranura de seguridad Kensington y por qué probablemente tu ordenador la tenga? ¿Y qué tan bien funciona? *Tedium*. Obtenido de https://tedium.co/2021/07/14/kensington-security-slot-history/

Stephen, M. (2023). Data Backup Strategies in Disaster Recovery: Ensuring Minimal Downtime. *IEEE Transactions on Cloud Computing*, 40. Obtenido de https://www.researchgate.net/publication/383276577_Data_Backup_Strategies_in_Disaster_Recovery_Ensuring_Minimal_Downtime

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems.* NIST. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems.* NIST Special Publication 800-34 Rev. 1. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Taarup, J. (2020). THE BUSINESS IMPACT ANALYSIS. *University College Copenhagen*, 22. Obtenido de https://www.researchgate.net/publication/371789651_THE_BUSINESS_IMPACT_ANALYSIS

Torres, R. A., & Tapia, J. P. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. *Dominio de las ciencias*, 14. doi:http://dx.doi.org/10.23857/dc.v7i4.2425

Watters, J. (2020). *Disaster Recovery, Crisis response and business continuity.* Apress. Obtenido de https://ndl.ethernet.edu.et/bitstream/123456789/49643/1/18.pdf.pdf

Yagual, D. I. (2015). *DESARROLLO DEL ESQUEMA DE SEGURIDAD, PLAN DE RECUPERACIÓN ANTE DESASTRES INFORMÁTICOS Y SOLUCIÓN PARA EL NIVEL DE EXPOSICIÓN DE AMENAZAS Y VULNERABILIDADES APLICADA A LOS SERVIDORES Y EQUIPOS DE COMUNICACIÓN DEL CENTRO DE DATOS.* ESCUELA SUPERIOR POLITECNICA DEL LITORAL. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/30025/1/T-84693%20QUIRUMBAY%20YAGUAL.pdf

Anexo

Anexo A . Aprobación de tema

Anexo B. Aceptación o aprobación de la empresa (de ser el caso)

Anexo C. Instrumento entrevista (de ser el caso)

Anexo D. Instrumento encuesta (de ser el caso)

Anexo E. Formulario de identificación de funciones criticas

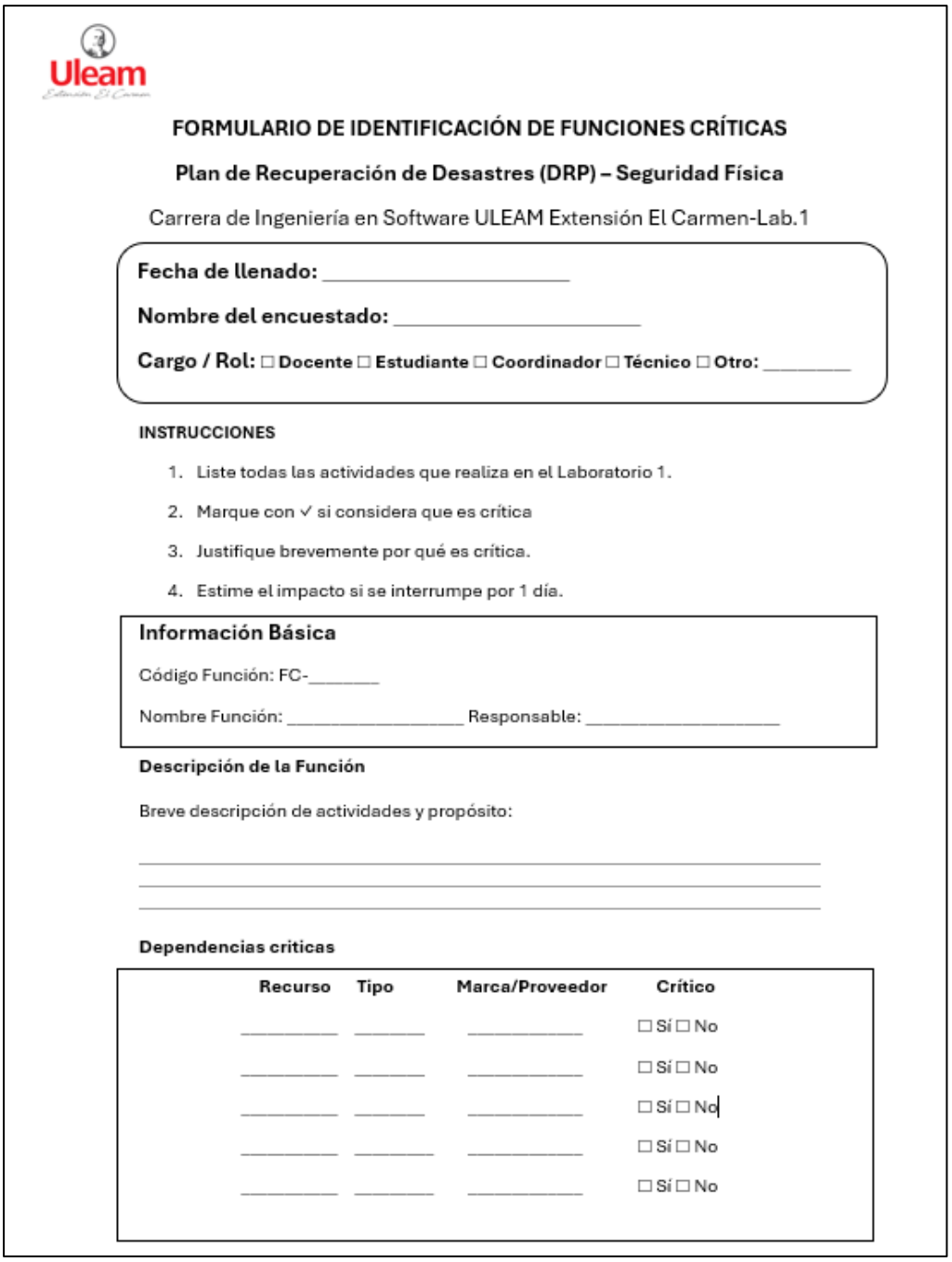
Anexo F. Identificar Salvaguardas

Área de Enfoque	Pregunta de Evaluación	Sí	No	Observaciones
1. Suministro de Energía	1¿Todos los equipos críticos (servidor, switches) están conectados a un sistema UPS (Batería de Respaldo)?		x	Solo hay UPS para en servidor principal de la Extensión, no en laboratorios
	2¿Existe una toma de tierra adecuada y verificada para todo el cableado eléctrico del laboratorio?	x		Existe la conexión a tierra
	3¿El sistema eléctrico del laboratorio soporta la carga total de todos los equipos sin sobrecalentamiento?	x		No se han detectado sobre calentamiento
	4¿Se utiliza algún tipo de protector de sobretensión (supresor de picos) en la mayoría de los equipos?		x	En algunos casos hay reguladores de voltaje
	5¿Se ha realizado una auditoría eléctrica reciente para verificar el estado de los enchufes y el cableado?		x	Personalmente desconozco si departamento técnico de matriz ha realizado verificación
2. Conectividad de Red	6¿El laboratorio utiliza un sistema de cableado estructurado?	x		La conexión es cableada
	7¿Se hace una revisión semestral a los equipos de red y cableado de los mismos?	x		
	8¿La velocidad de la red es suficiente para las tareas académicas requeridas?	x		Por cable la conexión es buena, excepto por problemas técnicos temporales
	9¿Existe un monitoreo activo de la red para detectar y solucionar caídas o problemas de rendimiento?	x		
	10¿Están todos los puertos de red no utilizados deshabilitados para prevenir conexiones no autorizadas?		x	Todos los puertos de red son utilizados
3. Internet y disponibilidad	11¿Todos los ordenadores del laboratorio tienen conexión estable a Internet de buena velocidad?		x	
	12¿Están el 100% de los equipos encendidos y operativos durante todo el horario de apertura del laboratorio?		x	Hay estudiantes que traen sus laptops
	13¿Existe al menos una máquina en el laboratorio que aún utilice un sistema operativo que ya no soporte con actualizaciones de seguridad?		x	
	14¿Se han reportado caídas de Internet en el laboratorio frecuentemente?	x		No muy frecuente
	15¿Se ha confirma semanalmente que el firewall o sistema de seguridad de red está activo y actualizado?	x		

Ilustración 15. Visita técnica estado actual del laboratorio parte1.

Área de Enfoque	Pregunta de Evaluación	Sí	No	Observaciones
4. Mantenimiento	16.¿Existe un programa de mantenimiento preventivo programado para el hardware (limpieza, revisión)?	x		Normalmente cada año
	17.¿Los equipos están utilizando la última versión estable del software y aplicaciones académicas?	x		
	18.¿Se documentan y registran todas las reparaciones y los problemas reportados de los equipos?		x	No en todos los casos
	19.¿El laboratorio dispone de un inventario actualizado de todo el hardware y software instalado?	x		Sobre todo, de hardware
	20.¿Se realizan purgas de archivos temporales y desfragmentación regularmente para optimizar el rendimiento?		x	
5. Seguridad Física	21.¿Las puertas del laboratorio tienen un sistema de acceso controlado (llave, tarjeta, código, biometria)?	x		
	22.¿Hay cámaras de seguridad que monitorean la entrada y el interior del laboratorio?	x		
	23.¿El cableado está organizado y asegurado para evitar riesgos de tropiezos o daños?	x		Sobre todo, el cableado de red
	24.¿Existe un extintor de incendios funcional y accesible dentro o justo al lado del laboratorio?		x	No se ha realizado la recarga
	25.¿Los equipos (CPU, monitores) están anclados o asegurados al mobiliario para prevenir robos?		x	No tienen anclaje
6. Recuperación y Malware	26.¿Todos los equipos tienen instalado y activo un software antivirus/antimalware actualizado?	x		Se posee, pero el mismo antivirus de Windows, Microsoft Defender
	27.¿El acceso a la configuración del sistema está restringido y protegido por contraseñas fuertes?		x	Los equipos se usan con el usuario administrador
	28.¿Hay una política que restringe a los usuarios la instalación de software no autorizado?	x		Existe, pero el sistema está abierto a instalación
	29.¿Se realizan pruebas de restauración de datos a partir de las copias de seguridad al menos anualmente?		x	No en equipos de laboratorio
	30.¿Existe una configuración firewall para evitar visitas a sitios no permitidos?	x		Configuración la realizan desde matriz

Ilustración 16. Visita técnica estado actual del laboratorio parte2.



FORMULARIO DE IDENTIFICACIÓN DE FUNCIONES CRÍTICAS

Plan de Recuperación de Desastres (DRP) – Seguridad Física

Carrera de Ingeniería en Software ULEAM Extensión El Carmen-Lab.1

Fecha de llenado: _____

Nombre del encuestado: _____

Cargo / Rol: ☐ Docente ☐ Estudiante ☐ Coordinador ☐ Técnico ☐ Otro: _____

INSTRUCCIONES

1. Liste todas las actividades que realiza en el Laboratorio 1.
2. Marque con ✓ si considera que es crítica
3. Justifique brevemente por qué es crítica.
4. Estime el impacto si se interrumpe por 1 día.

Información Básica

Código Función: FC-_____

Nombre Función: _____ Responsable: _____

Descripción de la Función

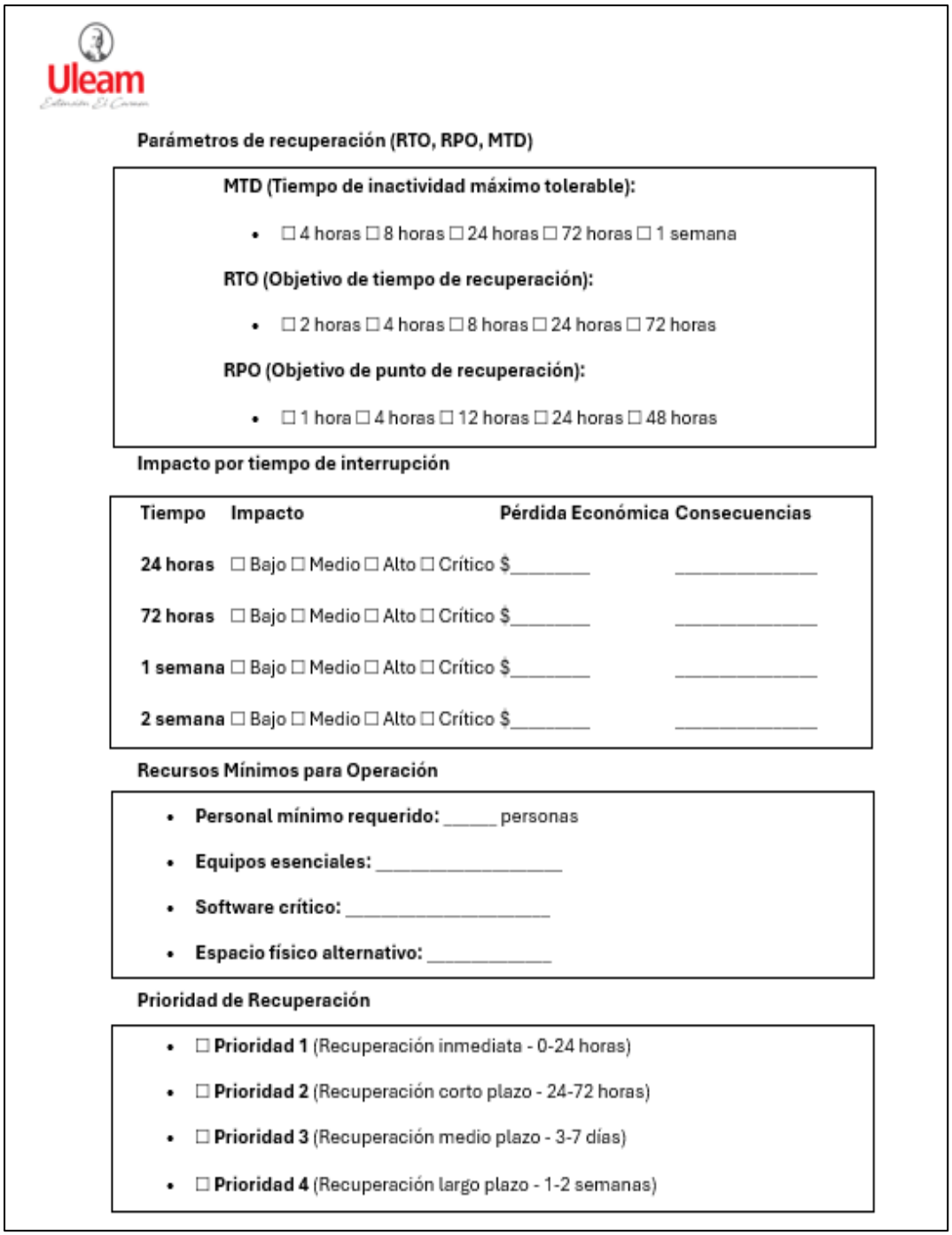
Breve descripción de actividades y propósito:

_____
_____
_____

Dependencias criticas

Recurso	Tipo	Marca/Proveedor	Crítico
_____	_____	_____	☐ Sí ☐ No
_____	_____	_____	☐ Sí ☐ No
_____	_____	_____	☐ Sí ☐ No
_____	_____	_____	☐ Sí ☐ No
_____	_____	_____	☐ Sí ☐ No

Ilustración 17. Anexo E, parte 1 formulario de identificación



Parámetros de recuperación (RTO, RPO, MTD)

MTD (Tiempo de inactividad máximo tolerable):

- ☐ 4 horas ☐ 8 horas ☐ 24 horas ☐ 72 horas ☐ 1 semana

RTO (Objetivo de tiempo de recuperación):

- ☐ 2 horas ☐ 4 horas ☐ 8 horas ☐ 24 horas ☐ 72 horas

RPO (Objetivo de punto de recuperación):

- ☐ 1 hora ☐ 4 horas ☐ 12 horas ☐ 24 horas ☐ 48 horas

Impacto por tiempo de interrupción

Tiempo	Impacto	Pérdida Económica	Consecuencias
24 horas	☐ Bajo ☐ Medio ☐ Alto ☐ Crítico	$_____	_____
72 horas	☐ Bajo ☐ Medio ☐ Alto ☐ Crítico	$_____	_____
1 semana	☐ Bajo ☐ Medio ☐ Alto ☐ Crítico	$_____	_____
2 semana	☐ Bajo ☐ Medio ☐ Alto ☐ Crítico	$_____	_____

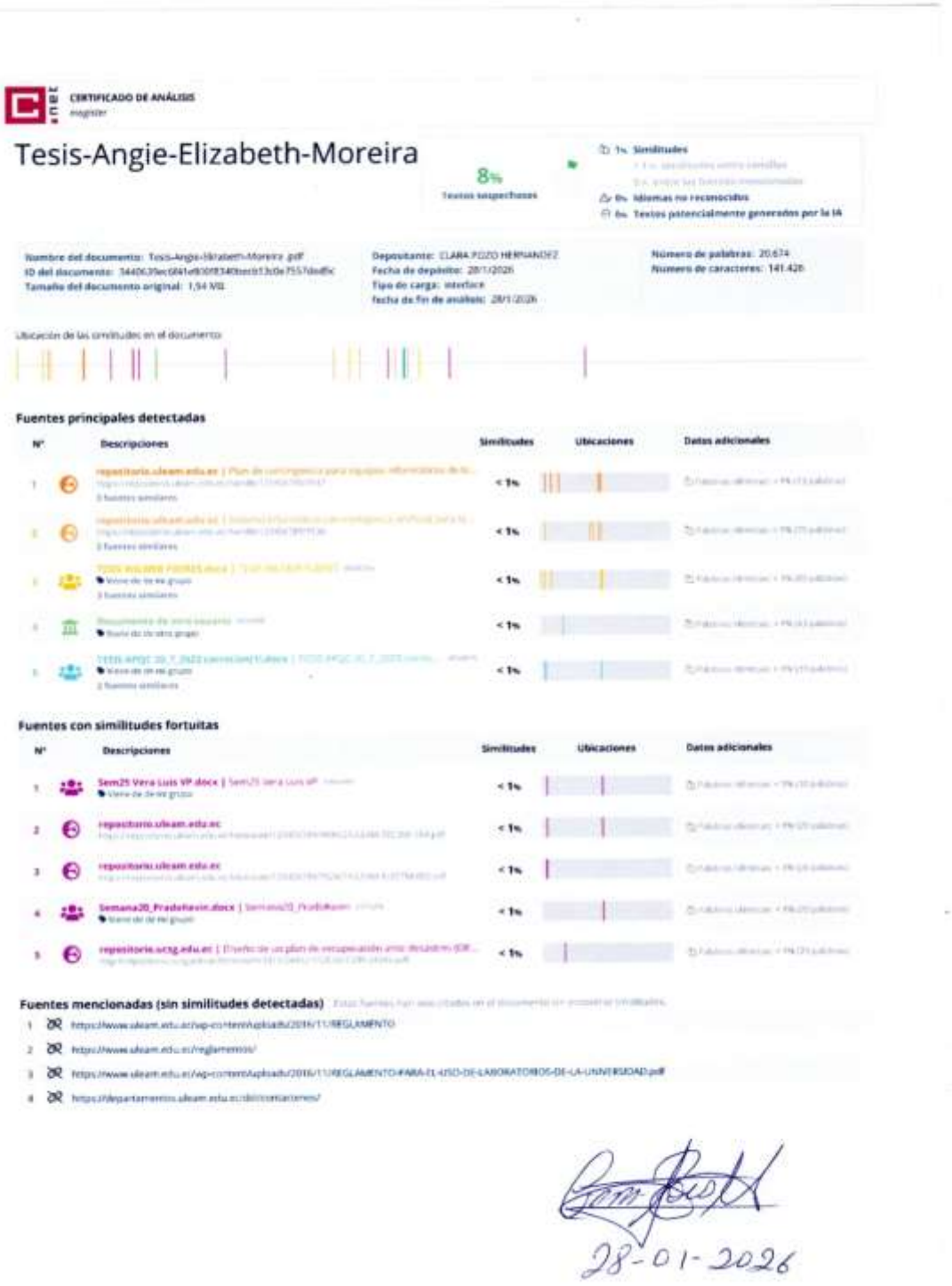
Recursos Mínimos para Operación

- **Personal mínimo requerido:** _____ personas
- **Equipos esenciales:** _____
- **Software crítico:** _____
- **Espacio físico alternativo:** _____

Prioridad de Recuperación

- ☐ **Prioridad 1** (Recuperación inmediata - 0-24 horas)
- ☐ **Prioridad 2** (Recuperación corto plazo - 24-72 horas)
- ☐ **Prioridad 3** (Recuperación medio plazo - 3-7 días)
- ☐ **Prioridad 4** (Recuperación largo plazo - 1-2 semanas)

Ilustración 18. Anexo E, parte 2 formulario de identificación



CERTIFICADO DE ANÁLISIS

Tesis-Angie-Elizabeth-Moreira

8%

Textos sospechosos

1% Similitudes

0% Idiomas no reconocidos

0% Textos potencialmente generados por la IA

Nombre del documento: Tesis-Angie-Elizabeth-Moreira .pdf

ID del documento: 3440639ec6841e8309f3408bec613c0e7557ddd9c

Tamaño del documento original: 1,94 MB

Depositante: CLARA POZO HERNANDEZ

Fecha de depósito: 28/1/2026

Tipo de carga: interface

fecha de fin de análisis: 28/1/2026

Número de palabras: 20.674

Número de caracteres: 141.420

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uleam.edu.ec | Plan de contingencia para equipos informáticos de la...	< 1%		
2	repositorio.uleam.edu.ec | Sistema informático para el control y gestión de...	< 1%		
3	TESIS WILMER PARRES.docx | Tesis de mi grupo	< 1%		
4	Documento de otro usuario | Tesis de otro grupo	< 1%		
5	TESIS APAZ 20_7_2022 correcciones1.docx | Tesis de mi grupo	< 1%		

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Sem25 Vera Luis VP.docx | Sem25 Vera Luis VP | Tesis de mi grupo	< 1%		
2	repositorio.uleam.edu.ec	< 1%		
3	repositorio.uleam.edu.ec	< 1%		
4	Semana20_Pradelavin.docx | Semana20_Pradelavin | Tesis de mi grupo	< 1%		
5	repositorio.ucsg.edu.ec | Diseño de un plan de recuperación ante desastres (DR...	< 1%		

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin coincidir con el texto.

1 https://www.uleam.edu.ec/wp-content/uploads/2019/11/REGLAMENTO

2 https://www.uleam.edu.ec/reglamentos/

3 https://www.uleam.edu.ec/wp-content/uploads/2019/11/REGLAMENTO-PARA-EL-USO-DE-LABORATORIOS-DE-LA-UNIVERSIDAD.pdf

4 https://departamentos.uleam.edu.ec/biblioteca/tesis/

28-01-2026

Anexo E Certificado de análisis

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

Anexo H. Certificado de coincidencia académica (emitido por tutor del sistema antiplagio)

Glosario

Exhaustiva: Que es completa, minuciosa y profunda, sin omitir nada.

Salvaguardas: Acciones de protección que se ejecutan para evitar perjuicios o disminuir los riesgos.

Contingencias: Circunstancias inesperadas que tienen el potencial de interferir con el funcionamiento normal de un sistema o actividad.

Restaurar: Reestablecer los servicios, datos o sistemas a su condición normal tras un incidente o una falla.

Catástrofes: Ocurrencias repentinas y serias que provocan un daño significativo a las personas, los bienes o el medio ambiente.

Desastres: Sucesos que provocan daños graves y sobrepasan la capacidad de reacción habitual de una entidad o comunidad.

Geofísicos: En relación con los procesos físicos de la Tierra, tales como: Terremotos, Erupciones volcánicas

Deterioro: Proceso de daño, desgaste o pérdida de calidad de algo con el tiempo.

Inoperativas: Que no funcionan o no pueden ser utilizadas.

Protocolos: Conjunto de normas, procedimientos o pasos establecidos que se deben seguir ante una situación específica.

Cibernética: Área relacionada con el control, comunicación y seguridad de sistemas informáticos y redes**.**

Desfavorables: Condiciones negativas o adversas que dificultan una actividad o proceso.

Infraestructura: Conjunto de instalaciones físicas y tecnológicas necesarias para el funcionamiento de una organización

Vulnerabilidad: Grado en el que un sistema, persona o infraestructura puede ser afectado por una amenaza o riesgo**.**

Estrategia: Conjunto de acciones planificadas con el fin de lograr un objetivo o manejar una circunstancia particular.

Ransomware: una clase de malware que requiere un pago para liberar sistemas o datos a los que ha bloqueado.

Confidencialidad: Se trata de asegurar que la información solo sea accesible por aquellos que están autorizados.

Disponibilidad: Asegura que los sistemas y la información sean accesibles y utilizables por los usuarios autorizados cuando se necesiten

Integridad: Que garantiza que la información este completa, precisa y no haya sido alterada de manera no autorizados.

Inmutabilidad: Propiedad que imposibilita la modificación o eliminación de datos después de haber sido almacenados.

Incidente: Suceso que amenaza o interrumpe la seguridad o el desempeño de un sistema.

Hardware: Partes físicas de un equipo informático, por ejemplo el monitor, el teclado o el disco duro.

Software: Aplicaciones y programas que hacen posible la operación del hardware.

Antivirus: Software que identifica, detiene y borra virus de computadora.

Auditorías: Métodos de inspección y evaluación para comprobar la observancia de reglas y controles.

Sobrecalentamiento: Elevación excesiva de la temperatura que tiene el potencial de perjudicar los dispositivos electrónicos.

Rehabilitación: Proceso de recuperación y restauración de una infraestructura o un sistema que ha sufrido daños.

Ininterrumpida: Que ópera de forma ininterrumpida, sin interrupciones ni descansos.

Eventualidades: Circunstancias inesperadas que pueden impactar el desarrollo normal de las actividades.

Interconectados: Que están interconectados o que unos dependen de otros.

Fenómenos: ocurren de forma natural o social.

Gobernadores: el gobierno o las entidades estatales.

Antimalware: Software creado para identificar y eliminar diversos tipos de software malicioso.