Propuesta de un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE

Chicaiza Yugcha, Katherine Ibeth y Velasco Guanoluisa, Karen Alejandra

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de integración curricular, previo a la obtención del título de Ingeniería en Tecnologías de la Información

Ing. Jerez Villota, Eleana Inés, Msc.

Sangolquí 23 de febrero del 2024

Copyleaks

Plagiarism and AI Content Detection Report

6. Tesis Chicaiza Velasco WORD.pdf

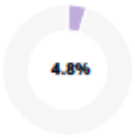
Scan details

Scan time:	Total Pages:	Total Words:
May 15th, 2024 at 17:26 UTC	34	8299

Plagiarism Detection

Types of plagiarism		Words
Identical	0.1%	8
Minor Changes	0%	0
Paraphrased	1%	87
Omitted Words	19.5%	1615

AI Content Detection



Text coverage		Words
AI text	4.8%	240
Human text	95.2%	6444

Learn more

Plagiarism Results: (5)

Plan de Recuperación de Desastres (DRP) y Continuidad de Negocio (BCP)... 0.7%

https://cerounosoftware.com.mx/plan-de-recuperacion-de-desastres-drp-y-continuidad-de-negocio-bcp/

...

Propuesta para el diseño del plan de recuperación de desastres. Caso Uni... 0.5%

https://repository.ucatolica.edu.co/items/f86cd1e2-1e40-49fc-88eb-93eea543b70c

Menu Inicio Comunidades Estadísticas Navegar Español English Iniciar sesión Correo electrónicoContraseña Iniciar s...

Crea un Plan de recuperación de desastres (DRP) en SAP 0.5%

https://www.tesselar.mx/blog/crea-un-plan-de-recuperacion-de-desastres-drp-en-sap

Ramiro Landa

...

5 claves para la continuidad de negocio - Tecsens - Seguridad TI 0.3%

https://www.tecsens.com/5-claves-para-la-continuidad-de-negocio/

twitter Linkedin Español Català English Deutsch Servicios Cloud Cloud privado Cloud backup Disaste...

ELEANA INES JEREZ VILLOTA

Firmado digitalmente por ELEANA INES JEREZ VILLOTA
Fecha: 2024.05.15 12:47:36 -05'00'

Ing. Eleana Inés Jerez Villota, MSc.

CC. 1717225039

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que en el trabajo de integración curricular: **"Propuesta de un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE"**, fue realizado por las señoritas **Chicaiza Yugcha, Katherine Ibeth y Velasco Guanoluisa, Karen Alejandra;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 28 de marzo de 2024

ELEANA INES JEREZ VILLOTA

Ing. Eleana Inés Jerez Villota, MSc.
C.C 1717225039

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Nosotras, **Chicaiza Yugcha, Katherine Ibeth,** con cédula de ciudadanía **Nº** 1726153784 **y Velasco Guanoluisa, Karen Alejandra,** con cédula de ciudadanía Nº 1725984080, declaramos que el contenido, ideasy criterios de trabajo de integración curricular: **"Propuesta de un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE"**, es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 28 de marzo de 2024

.....
Chicaiza Yugcha, Katherine Ibeth
C.C 1726153784

.....
Velasco Guanoluisa, Karen Alejandra
C.C 1725984080

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Nosotras, **Chicaiza Yugcha, Katherine Ibeth**, con cédula de ciudadanía Nº 1726153784 y **Velasco Guanoluisa, Karen Alejandra**, con cédula de ciudadanía Nº 1725984080, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Título: "Propuesta de un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE"**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 28 de marzo de 2024

.....

Chicaiza Yugcha, Katherine Ibeth
C.C 1726153784

.....

Velasco Guanoluisa, Karen Alejandra
C.C 1725984080

Dedicatoria

Dedico este trabajo a mis amados padres, Fernando Velasco y Piedad Guanoluisa, quienes han sido mis pilares y fuente de inspiración. Su amor incondicional y su sabia guía han sido fundamentales en cada paso de este camino académico. A mi querido hermano, Steven Velasco, cuya presencia ha llenado mi vida de alegría y ha sido mi mayor fortaleza. Además, dedico este trabajo a una persona especial mi novio Henry Llanes cuyo amor y apoyo constante y su ánimo han sido un regalo invaluable en este viaje hacia el éxito.

Karen Alejandra Velasco Guanoluisa

Dedicatoria

Dedico este trabajo de Titulación con profundo amor y gratitud a mis amados padres, José Chicaiza y Patricia Yugcha. Su apoyo incondicional a lo largo de este arduo camino académico ha sido mi mayor fortaleza, inspirándome a perseverar y nunca rendirme. A mis hermanos, Cristian y Alexis Chicaiza, les agradezco por su apoyo emocional. Sus palabras de ánimo han sido un refugio en mis momentos difíciles, impulsándome a seguir adelante con determinación.

Y a mi amado hijo, Nicolás, quien ha sido mi luz y mi razón para esforzarme cada día. Tu presencia en mi vida ha sido mi mayor motivación, y este logro es también para ti. Que sepas que todo lo que hago es pensando en un futuro mejor para ambos. Este logro no habría sido posible sin su apoyo.

Katherine Ibeth Chicaiza Yugcha

Agradecimiento

En este momento de celebración y gratitud, quiero expresar mi más sincero agradecimiento a las personas que han sido fundamentales en este viaje de trabajo y estudio. A mi querida mamá, Piedad, le agradezco profundamente por su incansable dedicación, sus madrugadas, sus mimos y esos deliciosos almuerzos que me preparó durante este último semestre, mientras trabajaba y estudiaba al mismo tiempo. Su sacrificio y amor incondicional han sido el sostén de mi fuerza y determinación. A mi amado papá, Fernando, le agradezco por haberme infundido desde el inicio de este camino la confianza y la seguridad de que podría lograrlo. Su fe en mí ha sido un gran impulso en cada paso que he dado. A mi hermano Steven, por cada noche en la que llegaba agotada, pero él siempre estaba ahí para animarme y recordarme que su hermana mayor lo lograría. Su apoyo incondicional y sus palabras de aliento han significado mucho para mí. A mi novio, Henry, le agradezco por levantar mi ánimo, por confiar en mí y por su amor constante que llena mi vida de alegría y motivación. Su presencia ha sido un faro de luz en los momentos más desafiantes. A mi mejor amiga, Mishell, le agradezco por estar conmigo día a día, dándome fuerzas y abrazos cuando más los necesitaba. Su lealtad y compañerismo durante esta trayectoria académica han sido un regalo invaluable que nunca olvidaré. A la Universidad de las Fuerzas Armadas ESPE, también quiero expresar mi profundo agradecimiento por brindarme las herramientas necesarias para mi formación académica y personal.

A cada uno de ustedes, les debo mi éxito y les estaré eternamente agradecido por su amor, apoyo y presencia constante en mi vida.

Karen Alejandra Velasco Guanoluisa

Agradecimiento

Quiero agradecer a mis padres por nunca dejar de apoyarme junto con mis hermanos, ya que gracias a todo su apoyo emocional y comprensión durante este semestre he logrado culminar con éxito esta etapa de mi vida.

Además, quiero agradecer a nuestra tutora la Ing. Jerez Villota, Eleana Inés, quien nos ha guiado con su sabiduría y todos sus consejos fuero fundamentales para el desarrollo y la culminación de este proyecto de titulación.

Este logro es el resultado del esfuerzo y el apoyo de muchos, y por eso estoy profundamente agradecido con cada uno de ustedes.

Katherine Ibeth Chicaiza Yugcha

Índice de Contenidos

Índice de tablas

Índice de figuras

Resumen

La presente investigación propone el desarrollo de un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, con el objetivo de fortalecer la capacidad de adaptación ante posibles fallos o ataques cibernéticos. Se realizará una revisión de literatura de marcos de referencia, metodologías, normas y estándares relacionados con la gestión de la seguridad de la información. Se seleccionarán aquellos que se utilizarán como guías para la propuesta del DRP. Además, se llevará a cabo la detección de activos críticos y procesos fundamentales para la implementación de los tiempos de recuperación objetivo (RTO) y de trabajo (RWT).

El alcance del proyecto abarca la implementación de medidas para fortalecer la capacidad de recuperación frente a posibles fallos, minimizando el riesgo de interrupciones en las operaciones. En la actualidad, dada la creciente dependencia de las organizaciones en la tecnología de la información, un DRP se vuelve de vital importancia para garantizar la continuidad del negocio y proteger los datos críticos frente a amenazas.

La implementación exitosa del plan permitirá elaborar estrategias más sólidas para la protección y recuperación de datos, mejorando la capacidad de respuesta y facilitando una pronta recuperación de datos. Se busca optimizar continuamente el plan para garantizar una mayor preparación ante posibles desastres y asegurar la integridad y disponibilidad de los recursos críticos de los laboratorios.

Palabras claves: Plan de recuperación de desastres, Plan de continuidad del negocio, análisis de riesgos, departamento de informática, infraestructura IT.

Abstract

This research proposes the development of a Disaster Recovery Plan (DRP) for the Computer Laboratories of the ESPE Armed Forces University, with the objective of strengthening the capacity to adapt to possible failures or cyber attacks. An exhaustive literature review of reference frameworks, methodologies, norms and standards related to information security management will be carried out. Those will be selected to be used as guides for the DRP proposal. In addition, the detection of critical assets and fundamental processes will be carried out for the implementation of the objective recovery times (RTO) and work times (RWT).

The scope of the project covers the implementation of measures to strengthen recovery capacity against possible failures, minimizing the risk of interruptions in operations. Today, given the increasing dependence of organizations on information technology, a DRP becomes vitally important to ensure business continuity and protect critical data from threats.

The successful implementation of the plan will allow the development of more solid strategies for data protection and recovery, improving response capacity and facilitating prompt data recovery, improving response capacity and facilitating prompt recovery from adverse situations. It seeks to continually optimize the plan to ensure greater preparedness for possible disasters and ensure the integrity and availability of critical laboratory resources.

Keywords: Disaster recovery Plan, bussiness continuity plan, risk análisis, computer science departamento, IT infraestructura.

Capítulo I

Introducción

Antecedentes

En las últimas décadas, el mundo ha experimentado una transformación significativa en la gestión de la información y los recursos tecnológicos. Desde la era pre-digital hasta la actualidad, las organizaciones han evolucionado en su enfoque hacia la protección de datos y la continuidad operativa, especialmente en el contexto de desastres naturales, que por lo general no pueden ser controlados, ciberataques y otros eventos disruptivos. Este cambio se ha reflejado en la creciente importancia de los Planes de Recuperación de Desastres (DRP) como una medida esencial para que nos ayude a garantizar la resiliencia de las operaciones.

La planificación de la recuperación de desastres se ha convertido en una preocupación crucial, ya que, con el inicio de la era digital, las organizaciones empezaron a recolectar y almacenar grandes cantidades de datos, lo cual complicó diseñar planes de recuperación de desastres efectivos. Sin embargo, la llegada de la computación en la nube proporcionó una solución al permitir la tercerización de los planes de recuperación a través de servicios como la Recuperación de Desastres como Servicio (DRaaS).

Para preservar la continuidad del negocio y minimizar las pérdidas que puedan ocasionar los desastres, se debe contar con un plan de recuperación, así poder otorgar seguridad a la empresa en su flujo normal de trabajo y maximizar las posibilidades de restablecer las operaciones.

Los laboratorios del Departamento de Ciencias de Computación de la Universidad de Las Fuerzas Armadas ESPE, cuentan con una infraestructura tecnológica que alberga información y datos que son considerados como activos digitales, por lo tanto, la presente investigación planteará un plan de recuperación de desastres tomando en cuenta estos activos digitales.

Planteamiento del problema

Justificación

Debido a que los planes de recuperación de desastres en la actualidad son de vital importancia y en su mayoría, las organizaciones no están debidamente preparadas para hacer frente a situaciones críticas, surge la necesidad de desarrollar un Plan de Recuperación ante Desastres para los Laboratorios de Computación de la Universidad de las Fuerzas Armadas ESPE, con el objetivo de reducir las posibles vulnerabilidades.

Esta investigación propone generar un plan de recuperación de desastres para asegurar el adecuado funcionamiento de los servicios digitales de los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE. Este plan formará parte integral del sistema de gestión de la seguridad de la información de la institución, donde se identificarán los activos y procesos críticos de la institución.

Basándonos en esta información, se desarrollarán estrategias y acciones específicas en distintos niveles para fortalecer la capacidad de adaptación ante posibles fallos o incluso ataques cibernéticos. Además de determinar los tiempos de recuperación objetivo (RTO), los cuales son fundamentales para establecer metas y plazos de recuperación en caso de desastres informáticos.

Objetivos

Objetivo General

Proponer un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación.

Objetivos Específicos

- Realizar la revisión de literatura de los marcos de referencia; las metodologías; las normas y los estándares; que se utilizan como guías y enfoques para proponer un Plan de Recuperación de Desastres (DRP).
- Seleccionar los marcos de referencia; las metodologías; las normas y los estándares;

que se utilizarán como guías y enfoques para proponer un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación.

- Realizar un análisis de la situación actual de la Infraestructura Tecnológica de los Laboratorios del Departamento de Ciencias de la Computación.
- Establecer los tiempos de recuperación de la infraestructura Tecnológica de los Laboratorios de Departamento de Ciencias de la Computación.
- Analizar los riesgos, amenazas y vulnerabilidades de la Infraestructura Tecnológica de los laboratorios del Departamento de Ciencias de la Computación.
- Definir las estrategias de recuperación de los servicios de TI de los Laboratorios del Departamento de Ciencias de la Computación.
- Diseñar e implementar pruebas basadas en las estrategias de recuperación de los servicios de TI de los Laboratorios del Departamento de Ciencias de la Computación.
- Diseñar un plan de capacitación al personal de los Laboratorios del Departamento de Ciencias de la Computación sobre las nuevas estrategias de recuperación y cómo aplicarlas en caso de una interrupción real.

Alcance

En el Sistemas de Gestión de Seguridad de la Información aplicada a los laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, se considera una parte fundamental la implementación de un Plan de Recuperación de Desastres. Aplicando los indicadores de RPO (Recovery Point Objetive) y RTO (Recovery Time Objetive) se identificarán los activos y procesos críticos para la implementación de medidas a distintos niveles con el fin de fortalecer la capacidad de recuperación frente a posibles fallas, reduciendo al mínimo el riesgo de interrupciones en las operaciones que se realiza en los laboratorios.

Además, la implementación exitosa de este plan permitirá a los laboratoristas elaborar estrategias más sólidas para la protección y recuperación de datos. Se pretende establecer un camino claro y eficiente para gestionar incidentes, mejorando la capacidad de respuesta y facilitando una pronta recuperación de datos en situaciones adversas. En este contexto, la

optimización continua del plan garantizará una mayor preparación ante posibles desastres, minimizando las molestias y asegurando la integridad y disponibilidad de los recursos críticos de los laboratorios del departamento de Computación.

Capítulo II

Revisión de Literatura

El presente capítulo tiene como objetivo analizar el estado del arte dentro del contexto de implementaciones de Plan de Recuperación de Desastres (DRP) para infraestructuras tecnológicas y de las normas, estándares, metodologías y mejores prácticas que las guían.

Preguntas de investigación

En el proceso de revisión de literatura, se han elaborado Preguntas de Investigación (PI) que funcionan como directrices para la búsqueda de información en los artículos pertinentes, a continuación, se detallan las preguntas de investigación formuladas:

- **PI1:** ¿Cuál es el estado del arte, relacionado con el diseño DRP?
- **PI2:** ¿Cuáles son las normas que las instituciones usan en un DRP?
- **PI3:** ¿Cuáles son las estrategias de recuperación en las instituciones?
- **PI4:** ¿Cuáles son las mejores prácticas para mantener y utilizar regularmente el DRP?
- **PI5:** ¿Cuáles son las metodologías de evaluación que utilizan en los estudios para evaluar el impacto del DRP en la continuidad operativa?

Cadena de búsqueda

Definimos un conjunto de palabras clave para construir una cadena de búsqueda óptima. Esta cadena fue implementada con el propósito de localizar artículos relevantes. La formulación final de la cadena de búsqueda fue la siguiente:

(“disaster recovery plan” OR DRP OR “business continuity plan” OR BCP OR “risk analysis” OR RA) AND “computer science department” AND “IT infrastructure”

Proceso de búsqueda

Durante el proceso de búsqueda obtuvimos artículos en cada base de datos científica, se obtuvo un total de 195 trabajos relacionados, antes de aplicar los criterios de inclusión y

exclusión. En la Tabla 1 se presenta el desglose del número de artículos obtenidos por cada base de datos digital.

Tabla 1

Resultados de la cadena de búsqueda en las distintas bases digitales

Bases digitales	Cantidad de artículos
Science Direct	65
Google Schoolar	130

Nota. En esta tabla se visualizan los resultados obtenidos por cada base digital. Fuente propia.

Criterios de Inclusión y Exclusión

La cantidad inicial de artículos recuperados no refleja la cantidad de materiales efectivamente utilizados en este trabajo de titulación, ya que podría haber duplicaciones o la inclusión de documentos poco relevantes al tema. Con el propósito de refinar y seleccionar de manera más precisa, se establecieron los siguientes criterios:

Criterios de inclusión

- Trabajos publicados en el periodo de 2019 a 2023.
- Trabajos que reportan implementaciones de DRP en el titulo o resumen.
- Trabajos donde el titulo o el resumen reportan implementaciones de DRP de infraestructuras TI en Departamento de Ciencias de la Computación.

Criterios de exclusión

- Trabajos que no reporten la aplicación de normas o estándares internacionales para la implementación del DRP.

Luego de aplicar los criterios de inclusión y exclusión obtuvimos un total de 18 trabajos relevantes.

Resultados de la revisión

En esta sección responderemos a cada una de las preguntas de investigación planteadas en este trabajo.

- **PI1: ¿Cuál es el estado del arte, relacionado con el diseño DRP?**

  El estado del arte relacionado con el diseño de Planes de Recuperación de Desastres (DRP) abarca diversas normativas, estrategias y metodologías que se han consolidado en el ámbito de la gestión de la continuidad del negocio y la seguridad de la información.

  ISO 2230, COBIT 5, ISO 27001, ISO 27002, IRAM/ISO/IEC 17799: Estas normativas proporcionan un marco sólido para el diseño de DRP, abordando aspectos como respaldo, replicación de servidores, acuerdos interinstitucionales y gestión de riesgos (Nieto, 2015).

  ISO 27031, ISO/IEC 31000: Se destaca el análisis de riesgos cualitativos y cuantitativos, considerando elementos como la probabilidad, impacto y la criticidad para obtener niveles de riesgo (Maravi et al., 2015), (Lopez et al., 2018).

  ISO 31000, MAGERIT, IDO/IEC 27031:2011: Estas normas y metodologías proporcionan herramientas para gestionar riesgos, realizar análisis de vulnerabilidades y definir estrategias de continuidad del negocio (Maravi et al., 2015)

  ISO 20071, ISO 27031: La implementación de un Sistema de Gestión de Calidad Normalizada (SGCN) basado en la gestión de riesgos se destaca como una estrategia integral (Maravi et al., 2015)

  Evaluar, Dirigir y Monitorear (EDM): De acuerdo a Cobit significa evaluar, dirigir y monitorear las estrategias de gestión de la continuidad del negoci (Castaño y Garzón, 2015) o

  Metodología PMI, NIST, Metodología DRI: Estas metodologías proporcionan marcos de trabajo para la planificación y gestión de la recuperación de desastres (Romero, 2014).

ISO 27001, Método SoVI: Se destaca la importancia de la investigación aplicada para la identificación de procesos críticos y el uso del método SoVI.

El estado del arte muestra una convergencia en el uso de normativas reconocidas, estrategias de respaldo y recuperación, análisis de riesgos y metodologías específicas para diseñar Planes de Recuperación de Desastres robustos y alineados con las mejores prácticas de la industria (Anggraini et al., 2019).

- **PI2: ¿Cuáles son las normas que las instituciones usan en un DRP?**

1. ISO 22301 – Socios de Negocios y Sistemas de Gestión de la Continuidad del Negocio: Proporciona un marco general para establecer, implementar, mantener y mejorar sistemas de gestión de la continuidad del negocio (Vásquez, 2017).
2. ISO 27001: Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información: Se centra en la seguridad de la información y aborda aspectos relevantes para garantizar la disponibilidad y la integridad de los datos (Vásquez, 2017).
3. COBIT 5 – Control Objetives for Information and Relates Technologies: Ofrece un marco de referencia para la gestión y gobierno de la tecnología de la información, incluyendo elementos clave para la continuidad del negocio (Castaño y Garzón, 2015).
4. ISO 27002 – Tecnologías de la Información – Tecnologías de Seguridad – Código de Práctica para la Gestión de la Seguridad de la Información: Proporciona pautas detalladas para implementar controles de seguridad de la información, siendo relevante para el DRP (Vásquez, 2017).
5. NIST 800-34 – Contingency Planning Guide for Information Technology Systems: Desarrollado por el Instituto Nacional de Estandares y Tecnología de EE.UU., proporciona orientación específica para la planificación de contingencias en sistemas de tecnología de la información (Gordon y Salazar, 2020).

6. BS 25999 – British Standard for Business Continuity Management: Ofrece un enfoque estructurado para la gestión de la continuidad del negocio, que incluye aspectos relacionados con el DRP (Lopez et al., 2018).
7. ISO/IEC 31000 - Gestión de Riesgos: Principios y Directrices: Proporciona principios generales y directrices para la gestión de riesgos, lo cual es esencial para el diseño efectivo de un DRP (Lopez at al., 2018).
8. ISO/IEC 27031 – Seguridad y Resiliencia: Sistemas de Tecnología de la Información – Guía para Recuperación: Se Centra en la recuperación de sistemas de tecnologías de la información, proporcionando directrices específicas para la gestión de la continuidad del negocio (Maravi et al., 2015).

- **PI3: ¿Cuáles son las estrategias de recuperación en las instituciones?**

  La mayoría de las alternativas analizadas cuentan con las estrategias a continuación:

  1. Backups y Restauración: Realizar copias de seguridad regulares de datos críticos y sistemas, tener procedimientos efectivos para restaurar la información en caso de pérdida (Arévalo et al., 2016).
  2. Recuperación en Línea (Online Recovery): Mantener servicios y sistemas en línea continuamente, a través de redundancias y replicación, para garantizar la disponibilidad constante incluso durante un evento disruptivo (Nieto, 2015).
  3. Recuperación Fuera de Línea (Offline Recovery): Almacenar copias de seguridad y recursos críticos fuera de línea, desconectados de la red principal, para protegerlos de amenazas cibernéticas y asegurar su integridad (Nieto, 2015).
  4. Recuperación Remota (Remote Recovery): Establecer procedimientos para recuperar sistemas y datos desde ubicaciones remotas o centros de datos alternativos en caso de que la ubicación principal sea inaccesible o afectada (Nieto, 2015).

5. Espejos de Sitios (Mirror Sites): Mantener réplicas exactas de sistemas y servicios en ubicaciones geográficas distintas para garantizar la continuidad operativa en caso de desastre (Castaño y Garzón, 2015).
6. Sitios Calientes, Tibios y Fríos: Disponer de sitios alternativos con diferentes niveles de preparación. Calientes tienen infraestructuras listas para su uso inmediato, tibios requieren configuración adicional y fríos necesitan instalación y configuración completa (Castaño y Garzón, 2015).
7. Acuerdos Institucionales: Establecer colaboraciones con otras instituciones para compartir recursos y capacidades en situaciones de emergencia, facilitando la recuperación conjunta (Maravi et al, 2015).
8. Respaldos de Base de Datos y Sistemas: Asegurar la integridad y disponibilidad de bases de datos y sistemas críticos mediante respaldos regulares y procedimientos eficientes de restauración (Barragán y Puentes, 2016).
9. Infraestructura de Respaldo: Contar con equipos y servicios redundantes que pueden entrar en funcionamiento rápidamente en caso de falla de la infraestructura principal.
10. Redundancia de Equipos: Implementar sistemas con redundancia, como servidores duplicados y sistemas de alimentación de energía, para minimizar el impacto de posibles fallas (Gordon y Salazar, 2020).
11. RTO (Recovery Time Objective) y RPO (Recovery Point Objective): Definir los objetivos de tiempo y puntos de recuperación para determinar cuánto tiempo y cuantos datos pueden perderse sin afectar significativamente las operaciones (Arévalo et al., 2016)

- **PI4: ¿Cuáles son las mejores prácticas para mantener y utilizar regularmente el DRP?**

1. Revisión y Actualización Periódica: Programa revisiones regulares del DRP para reflejar cambios en la infraestructura, personal, procesos y tecnologías (Herrada, 2018).
2. Simulacros y Ejercicios Prácticos: Realizar simulacros periódicos para poner a prueba el DRP en situaciones simuladas. Estos ejercicios identifican áreas de mejora, familiarizan al personal con los procedimientos y mejoran la capacidad de respuesta (Vásquez, 2017).
3. Involucramiento del Personal: Capacitar al personal regularmente sobre los procedimientos del DRP y su papel en la implementación. Mantener a todos los involucrados informados y comprometidos con el plan (Castaño y Garzón, 2015).
4. Documentación detallada: El DRP debe estar de manera clara y detallada. Incluye instrucciones paso a paso para facilitar su implementación rápida y efectiva (Maravi et al., 2015).
5. Respuesta a incidentes en Tiempo Real: Implementar un sistema de respuesta a incidentes que permita a los equipos tomar medidas inmediatas en caso de una amenaza o incidente. Esto puede incluir una cadena de comunicación clara y protocolos de actuación (Dhanujati y Suganda , 2018).
6. Revisión Post-Evento: Después de un evento real o simulado, realizar revisiones exhaustivas para evaluar la efectividad del DRP. Identificar lecciones aprendidas y áreas de mejora (Anggraini et al., 2019).
7. Actualización de Contactos de Emergencia: Mantener actualizada la lista de contactos de proveedores, garantías y mantenimiento (Rivas & Salazar, 2019).
8. Gestión de cambios Controlada: Implementar un proceso controlado para gestionar cambios en el DRP. Cualquier actualización debe ser revisada y aprobada antes de su implementación (Rivas & Salazar, 2019).

9. Almacenamiento Seguro y Accesible: Se debe a que el DRP esté almacenado de forma segura, pero es accesible para aquellos que necesitan implementarlo. Utiliza soluciones de almacenamiento en la nube o copias físicas seguras (Castaño y Garzón, 2015).
10. Comunicación Clara y Consistente: Establecer canales claros y procedimientos de comunicación en caso de una emergencia. Todos los involucrados deben tener claro como comunicarse y recibir actualizaciones (Maravi et al., 2015).
11. Mantenimiento de Equipos y Recursos de Respaldo: Realizar mantenimiento regular en los equipos y recursos de respaldo para garantizar que estén operativos cuando se necesiten. Actualizar software y firmware según sea necesario (Vásquez, 2017).
12. Revisión de Tendencias y Amenazas: Mantener al tanto de las tendencias en desafíos que puedan surgir (Nieto, 2015).
13. Informe y Auditoría Interna: Implementa procesos de informe y auditoría interna para evaluar la conformidad con el DRP y garantizar que todos los aspectos sean manejados adecuadamente (Lopez et al., 2018).

- **PI5: ¿Cuáles son las metodologías de evaluación que utilizan en los estudios para evaluar el impacto del DRP en la continuidad operativa?**
    1. Simulacros y Ejercicios de Recuperación: Programar simulacros regulares que involucren los elementos clave del DRP, evaluando la efectividad de las estrategias de respaldo, recuperación y las respuestas a incidentes (Maravi et al., 2015).
    2. Indicadores Clave de Rendimiento (KPIs): Establecer KPIs específicos, como el tiempo de recuperación, la precisión de la restauración y la efectividad de los procedimientos de respuesta. Monitorear y analizar estos KPIs regularmente.
    3. Revisión Post-Evento: Llevar a cabo revisiones detalladas después de eventos simulados o reales para identificar lecciones aprendidas, áreas de mejora y ajustar el DRP según sea necesario (Sanabria, 2020).

4. Análisis de Vulnerabilidades y Riesgos: Realizar análisis continuos de vulnerabilidades y riesgos, utilizando enfoques cualitativos y cuantitativos para evaluar la efectividad del DRP en abordar posibles amenazas (Lopez, Cubillos, y Casas, 2018).
5. Pruebas de Estrés: Someter el DRP a pruebas de estrés para evaluar su resistencia y capacidad de respuesta en situaciones extremas. Identificar debilidades y fortalezas del plan (Arévalo et al., 2016).
6. Encuestas y Entrevistas: Realizar encuestas y entrevistas con particiones clave para obtener retroalimentación sobre la percepción de la efectividad del DRP y sugerencias de mejora (Castaño y Garzón, 2015)
7. Pruebas de Recuperación de tecnología de la Información: Implementar pruebas específicas de recuperación de sistemas de tecnología de la información, evaluando la restauración de datos, aplicaciones y servicios críticos (Arévalo et al., 2016).
8. Seguimiento Continuo y Actualización: Establecer un proceso de seguimiento continuo para monitorear la efectividad del DRP. Actualizar el plan según cambios en la infraestructura, tecnología o procesos (Romero, 2014).
9. Pruebas de Continuidad del Negocio: Integrar pruebas de continuidad del negocio que involucren a múltiples departamentos, evaluando la coordinación y la sinergia entre las estrategias de recuperación (Dhanujati y Suganda , 2018).
10. Método PDCA: Aplicar el ciclo PDCA (Planear, Hacer, Verificar, Actuar) para garantizar la mejora continua del DRP en función de la retroalimentación y los resultados obtenidos (Herrada, 2018).
11. Investigación Aplicada y Método SoVI: Integrar la investigación aplicada para identificar procesos críticos y aplicar el método SoVI para evaluar la viabilidad operativa en caso de interrupciones (Anggraini et al., 2019).

Capítulo III

Desarrollo

En un mundo empresarial cada vez más interconectado, la implementación efectiva del Plan de Recuperación de Desastres (DRP) se erige como una piedra angular para la continuidad operativa. Internacionalmente, se siguen estándares rigurosos como ISO/IEC 22301, que guían desde la evaluación de riesgos hasta la aplicación de estrategias avanzadas, como Online Recovery y Remote Recovery. Esta visión global, sin embargo, debe adaptarse a las realidades locales (Ati, 2018).

En Ecuador, la implementación del DRP se ve moldeada por desafíos y oportunidades únicas. Desde amenazas sísmicas hasta consideraciones de ciberseguridad, las organizaciones ecuatorianas deben personalizar estrategias, aprovechando estándares internacionales mientras abordan preocupaciones específicas. Con conciencia y colaboración, las empresas en Ecuador pueden fortalecer su capacidad de respuesta, enfrentando riesgos con resiliencia y garantizando la continuidad en cualquier circunstancia. Este análisis introductorio sienta las bases para explorar más profundamente las estrategias específicas y desafíos inherentes a este proceso vital.

Infraestructura TI de Instituciones de Educación Superior

Definición

La infraestructura de Tecnologías de la Información (TI) en instituciones educativas constituye el conjunto integral de recursos tecnológicos diseñados para respaldar eficazmente las actividades académicas y administrativas. Incluye elementos clave como redes de comunicación, estaciones de trabajo, servidores, software especializado y medidas de seguridad (Romero, 2014).

Los servidores, fundamentales en la gestión de datos, se despliegan con estrategias de respaldo y replicación, garantizando la disponibilidad y confiabilidad de la información académica

y administrativa (Barragán y Puentes, 2016). El software especializado y las plataformas de gestión educativa optimiza la creación, distribución y evaluación de contenidos académicos.

La seguridad de esta infraestructura se aborda mediante medidas como la autenticación segura, firewalls y protocolos de seguridad, salvaguardando datos sensibles y protegiendo contra amenazas cibernéticas (Vásquez, 2017).

El soporte técnico, respaldado por programas de mantenimiento preventivo, asegura el funcionamiento continuo de la infraestructura, mientras que la planificación de la continuidad académica, con objetivos de recuperación y estrategias de respaldo definidos, minimiza interrupciones en situaciones adversas (Barragán y Puentes, 2016).

La colaboración entre docente y estudiantes se facilita a través de plataformas interactivas y herramientas de comunicación, contribuyendo a un entorno educativo dinámico y participativo.

Elementos clave de la infraestructura TI para soportar las operaciones académicas

- Las redes de comunicación proporcionan acceso a recursos digitales, estaciones de trabajo equipadas facilitan actividades académicas, y servidores gestionan datos con estrategias de respaldo (Castaño y Garzón, 2015).
- El software especializado y plataformas educativas optimizan procesos, mientras medidas de seguridad protegen datos sensibles.
- El soporte técnico asegura funcionamiento continuo, y la planificación de la continuidad académica minimiza interrupciones (Barragán y Puentes, 2016).
- La colaboración digital mejora interacción, y la adaptación a innovaciones tecnológicas garantiza relevancia continua.

En conjunto, estos elementos forman una infraestructura ágil y eficaz para el entorno educativo.

Tecnología de la Información y Comunicación

El análisis de las Tecnologías de la Información y Comunicación (TIC) en instituciones educativas revela integración estratégica de herramientas digitales para potenciar el proceso educativo. Estas tecnologías abarcan desde la infraestructura de red hasta aplicaciones y plataformas específicas (Anggraini et al., 2019).

En términos de infraestructura, se implementan redes robustas para facilitar el acceso a recursos en línea, y se utilizan estaciones de trabajo actualizadas para optimizar la experiencia del usuario (Maravi et al., 2015). Los servidores desempeñan un papel clave en la gestión eficiente de datos académicos y administrativos.

En el ámbito del software y las plataformas educativas, se observa la adopción de herramientas especializadas que facilitan la creación, distribución y evaluación de contenidos académicos. Estas soluciones no solo agilizan los procesos, sino que también fomentan métodos de enseñanza más interactivos.

La seguridad de las TIC es una prioridad, con medidas como la autenticación segura y firewalls para proteger la integridad de los datos y la privacidad de los usuarios. El soporte técnico asegura el funcionamiento continuo, mientras que la planificación de la continuidad académica mitiga posibles interrupciones (Barragán y Puentes, 2016).

Rol de las Tecnologías en el Entorno Académico

Las Tecnologías de la Información y Comunicación (TIC) desempeñan un papel fundamental en el entorno académico, aportando significativamente a diversos aspectos de la enseñanza, el aprendizaje y la gestión institucional. Algunos de los roles clave de estas tecnologías incluyen (Barragán y Puentes, 2016):

- Facilitación del Aprendizaje:

  Contenidos Interactivos: Las TIC permiten la creación y distribución de contenidos interactivos, mejorando la participación y comprensión de los estudiantes.

Plataformas Educativas: Facilitan la entrega de materiales, tareas y evaluaciones en línea, ofreciendo un entorno de aprendizaje virtual.

- Acceso a Recursos Educativos:

  Internet y Bibliotecas Virtuales: Proporcionan acceso a una amplia gama de recursos educativos en línea, fomentando la investigación y el autoaprendizaje.

- Colaboración y Comunicación:

  Herramientas de Colaboración: Facilitan la colaboración entre estudiantes y docentes, incluso a distancia, a través de herramientas como videoconferencias y plataformas de trabajo colaborativo.

  Comunicación Institucional: Mejoran la comunicación entre la institución, docentes, estudiantes y padres a través de correos electrónicos, mensajes y portales en línea.

- Administración y Gestión Institucional:

  Sistemas de Gestión Escolar: Simplifican procesos administrativos como la inscripción, calificación y seguimiento académico.

  Gestión de Recursos: Ayudan en la asignación eficiente de recursos, como aulas y personal.

- Entorno Personalizado de Aprendizaje:

  Adaptabilidad: Permiten la personalización de la enseñanza según las necesidades individuales de los estudiantes, utilizando plataformas que se adaptan a diferentes estilos de aprendizaje.

- Seguridad y Protección de Datos:

  Seguridad en Línea: Garantiza la seguridad de la información y la privacidad de los estudiantes y docentes mediante medidas de seguridad en línea.

- Innovación Pedagógica:

Integración de Nuevas Tecnologías: Apoyan la implementación de enfoques pedagógicos innovadores, como el aprendizaje basado en proyectos y la gamificación.

- Desarrollo de Competencias Digitales:

  Preparación para el Futuro: Ayudan a los estudiantes a desarrollar habilidades digitales esenciales para su participación en la sociedad actual y futura.

Marco Legal y Regulatorio

En el contexto del Marco Legal y Regulatorio para la gestión de la infraestructura TI en instituciones educativas, es crucial considerar las leyes y regulaciones pertinentes (Maravi et al., 2015). La revisión de la literatura proporciona una comprensión de varios aspectos clave:

Normativas y estándares Internacionales

- ISO/IEC 27001: Enfoque en la seguridad de la información, aplicable para garantizar la integridad, confidencialidad y disponibilidad de los datos en instituciones educativas (Maravi et al., 2015).
- ISO/IEC 22301. Norma para la gestión de la continuidad del negocio, fundamental para asegurar la disponibilidad de los servicios educativos ante posibles interrupciones (Budiman, 2020).

Regulaciones de Seguridad y Continuidad del Negocio

- COBIT 5: Marco de gobierno y gestión de TI que aborda aspectos como la alineación estratégica, la entrega de valor y la gestión de riesgos (Vásquez, 2017), esencial para la gestión efectiva de la infraestructura TI educativa.
- COBIT (Cobit 2019). Enfocado en evaluar, dirigir y monitorear procesos, proporcionando directrices para garantizar la alineación de la infraestructura TI con los objetivos organizativos (Jaime y Barata, 2023).

Normativas Nacionales y Sectoriales

- Leyes de Protección de Datos: Se explora cómo las instituciones educativas se adecúan a leyes clave, como la Ley Orgánica de Protección de Datos Personales en Ecuador, para garantizar la privacidad de la información de estudiantes y personal.
- Normativas Locales de Continuidad del Negocio: Las regulaciones específicas en las jurisdicciones locales ecuatorianas que impactan directamente en la gestión de la infraestructura TI de instituciones educativas. Estas regulaciones podrían provenir de organismos como el Ministerio de Educación del Ecuador y otras entidades gubernamentales que supervisen la continuidad del negocio en el contexto educativo.

Buenas Prácticas de Seguridad y Riesgos

- NIST: Aunque no se menciona directamente en los artículos, el Instituto Nacional de Estándares y Tecnología (NIST) y sus estándares, como el NIST 800-34 (Rosado et al., 2021), ofrecen pautas valiosas para la gestión de riesgos y la planificación de la continuidad del negocio.

Metodologías de Gestión de Riesgos:

- ISO/IEC 31000: Marco para la gestión de riesgos que puede ser aplicado en instituciones educativas para identificar, evaluar y mitigar riesgos en la infraestructura TI (Lopez et al., 2018).

Contraloría General del Estado

La norma 410 04 se centra principalmente en establecer políticas y procedimientos relacionados con la gestión de la tecnología de la Información (TI) en una organización. Estas políticas y procedimientos abordan aspectos clave como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, legalidad del software, entre otros, y están alineados con las leyes y estándares de TI.

Ahora, en cuanto a la relación con el Plan de Recuperación ante Desastres, hay algunas conexiones potenciales:

1. Gestión de Riesgos: La norma menciona la incorporación de controles y sistemas de gestión de riesgos en las operaciones de TI. Esta gestión de riesgos es esencial para el DRP, ya que implica identificar posibles amenazas y establecer medidas para mitigar su impacto.
2. Supervisión y Medición del Cumplimiento: El establecimiento de procedimientos de supervisión y medición del cumplimiento también es relevante para el DRP. La supervisión constante ayuda a garantizar que las medidas de recuperación estén actualizadas y sean efectivas.
3. Convenios y Colaboraciones: La promoción de convenios con otras organizaciones para el intercambio de información puede ser crucial en un plan de recuperación ante desastres. La colaboración con otras entidades puede facilitar la recuperación y la continuidad de las operaciones después de un evento adverso.
4. Actualización Permanente: La norma destaca la importancia de actualizar permanentemente las políticas y procedimientos en tecnología de la información. Esto se relaciona con el DRP, ya que las amenazas y tecnologías cambian con el tiempo, y el plan debe mantenerse al día.
5. Controles Internos y confidencialidad: La norma menciona la importancia de controles internos, seguridad y confidencialidad, aspectos fundamentales en un DRP para garantizar la integridad y seguridad de la información durante y después de un desastre.

La norma aborda elementos que son esenciales para la preparación y la resistencia de los sistemas de TI frente a eventos adversos. En general, la gestión de la tecnología de la Información y el DRP están interrelacionados en la medida en que ambos contribuyen a la continuidad y la resiliencia de las operaciones de una organización (Contreras, 2020).

La Norma ISO/IEC 24762:2008

La norma ISO/IEC 24762:2008 proporciona directrices detalladas sobre la prestación de servicios de recuperación de desastres de tecnologías de la información y las comunicaciones (RD TIC) como parte integral de la gestión de la continuidad del negocio. Estas directrices son aplicables tanto a los proveedores de servicios de DR TIC “internos” como a los “subcontratados”, incluyendo instalaciones físicas y servicios.

Los aspectos clave abordados por la norma ISO/IEC 24762:2008 incluyen:

1. Requisitos para la implementación, operación, monitoreo y mantenimiento de servicios e instalaciones de DR TIC: Establece los estándares y las prácticas que deben seguirse para garantizar la efectividad y la confiabilidad de los servicios de recuperación de desastres de tecnologías de la información y las comunicaciones.
2. Capacidades y prácticas para los proveedores de servicios de DR TIC subcontratados: Define las capacidades necesarias que deben tener los proveedores de servicios de DR TIC subcontratados para garantizar entornos operativos seguros y facilitar los esfuerzos de recuperación de las organizaciones.
3. Orientación para la selección del sitio de recuperación: Ofrece criterios y recomendaciones para la selección de ubicaciones de recuperación adecuadas que sean seguras y estratégicamente ubicadas para garantizar una recuperación efectiva en caso de desastre.
4. Guía para la mejora continua de los servicios de RD TIC: Proporciona pautas para que los proveedores de servicios de recuperación de desastres de tecnologías de la información y las comunicaciones mejoren constantemente sus servicios, asegurando así su eficacia a lo largo del tiempo.

La norma ISO/IEC 24762:2008 ofrece pautas esenciales para establecer y mantener servicios de recuperación de desastres (RD) en el ámbito de las tecnologías de la información y las comunicaciones (TIC). Estas pautas son fundamentales para garantizar la continuidad del

negocio y proteger las operaciones en caso de interrupciones. La norma aborda aspectos como la selección del sitio de recuperación, los requisitos para proveedores de servicios internos y subcontratados, y la mejora continua de los servicios de RD TIC. Su aplicación no solo asegura la eficacia de los servicios de recuperación, sino que también fortalece la resiliencia organizacional en un entorno empresarial dinámico.

Seguridad de la Información y Ciberseguridad

Seguridad de la Información

La seguridad de la información en instituciones educativas se fundamenta en conceptos esenciales extraídos de normativas y estrategias específicas, destacando la importancia de salvaguardar la integridad, confidencial y disponibilidad de los datos. A continuación, se presentan los conceptos clave:

- Gestión Integral de la Seguridad de la Información (SGSI): Implementar un SGSI basado en normativas como ISO/IEC 27001 permite estructurar políticas, procesos y controles para garantizar la seguridad de la información en todos los niveles de la institución educativa (Khairur y Benfano , 2022).
- Identificación y Valoración de Activos de Información: Reconocer y evaluar los activos de información críticos, como datos académicos, administrativos y de investigación, para priorizar medidas de protección y asignar recursos de manera eficiente.
- Políticas de Acceso y Control de Usuarios: Establecer políticas claras para la gestión de accesos, asignación de roles y privilegios, asegurando que únicamente personal autorizado acceda a la información sensible.
- Concientización y Formación en Seguridad: Promover la concientización y capacitación continua en seguridad de la información entre estudiantes, docentes y personal administrativo para fomentar buenas prácticas y reducir riesgos de seguridad.

- Protección contra Amenazas y Ataques Cibernéticos: Implementar medidas de protección activa, como firewalls, sistemas de detección de intrusiones y actualizaciones de seguridad, para prevenir y mitigar amenazas cibernéticas (Khairur y Benfano , 2022).
- Gestión de Incidentes de Seguridad: Establecer procedimientos claros para la detección, reporte y respuesta a incidentes de seguridad, permitiendo una gestión efectiva en situaciones de vulnerabilidad (Sanabria, 2020).
- Auditorías y Evaluaciones de Seguridad: Realizar auditorías periódicas y evaluaciones de seguridad para garantizar el cumplimiento de políticas, identificar posibles vulnerabilidades y ajustar las estrategias de seguridad de manera proactiva.
- Seguridad en Procesos de Continuidad Educativa: Integrar prácticas de seguridad en la planificación de la continuidad académica, asegurando la disponibilidad de sistemas y datos críticos en situaciones de contingencia.
- Cultura de Seguridad: Fomentar una cultura de seguridad en la comunidad educativa, donde la protección de la información sea responsabilidad de todos, fortaleciendo la postura de seguridad de la institución.
- Adaptabilidad a Estándares Internaciones: Alinear las prácticas de seguridad con estándares internacionales, como ISO/IEC 27001, para garantizar la implementación de mejores prácticas reconocidas a nivel global (Lopez et al., 2018).

Estos conceptos conforman un marco integral de seguridad de la información adaptado al contexto educativo, proporcionando una guía sólida para la protección efectiva de los activos de información en instituciones educativas.

Ciberseguridad

La ciberseguridad en el ámbito educativo se refiere a las medidas y prácticas implementadas para salvaguardar la infraestructura tecnológica, datos y sistemas informáticos utilizados en instituciones educativas. Su objetivo principal es garantizar la confidencialidad,

integridad y disponibilidad de la información, así como proteger contra amenaza cibernéticas específicas asociadas con el entorno académico (Khairur y Benfano , 2022).

Amenazas y Desafíos Específicos en el Entorno Académico

- Phishing Educativo: Campañas diseñadas para engañar a estudiantes, profesores y personal administrativo, comprometiendo credenciales de acceso y propagando malware.
- Ataques a Plataformas de Aprendizaje en Línea: Amenazas dirigidas a sistemas de gestión de aprendizaje y plataformas en línea, buscando interrumpir clases, acceder a datos estudiantiles o alterar contenido.
- Vulnerabilidades en Dispositivos Móviles: Puntos de vulnerabilidad asociados con el uso extendido de dispositivos móviles en entornos educativos, especialmente si no se implementan medidas de seguridad adecuadas.
- Fuga de Información de Investigaciones: Riesgos relacionados con la pérdida no autorizada de resultados de investigaciones o datos confidenciales, afectando la propiedad intelectual y la reputación institucional.
- Acoso Cibernético: La ciberseguridad aborda el acoso cibernético en el ámbito educativo, protegiendo a estudiantes contra posibles ataques o intimidaciones en línea.

Estos aspectos resumen los aspectos clave de la ciberseguridad en instituciones educativas, abordando amenazas específicas que podrían afectar la integridad y la seguridad de la información en el entorno académico (Rodríguez, 2011).

Planificación de la Continuidad del Negocio (BCP) y Plan de Recuperación de Desastres (DRP)

Plan de Continuidad de Negocio (BCP)

Un Plan de Continuidad de Negocios (BCP) es una guía detallada que busca identificar y salvaguardar los procesos críticos de una empresa. Su propósito es desarrollar políticas, planes y procedimientos para asegurar la continuidad operativa en situaciones imprevistas. La

responsabilidad principal recae en la alta gerencia, quienes, por su profundo conocimiento del negocio, pueden identificar con precisión los procesos cruciales y establecer planes de respaldo. Este enfoque se basa en políticas y objetivos empresariales para mantener la productividad y la presencia en el mercado, evitando interrupciones significativas.

Objetivos del BCP

- Minimizar Pérdidas: Reducir al máximo las pérdidas económicas derivadas de incidentes inesperados.
- Alta Disponibilidad del Servicio: Garantizar un alto porcentaje de disponibilidad de servicios para los clientes.
- Mitigación de Efectos Negativos: Disminuir los impactos adversos de incidentes, como el cierre de operaciones o la caída en el mercado.

El BCP abarca proyectos específicos como el Plan de Continuidad TIC (PCTIC), centrado en la tecnología, y el Plan de Recuperación ante Desastres (DRP), que es el enfoque central de este trabajo. Ambos proyectos proporcionan una visión integral de los elementos críticos del negocio en diversas áreas y cómo las operaciones podrían verse afectadas por eventos no controlados adecuadamente (Ati, 2018).

Plan de Recuperación de Desastres (DRP)

Un Plan de Recuperación de Desastres (Disaster Recovery Planning, DRP), también conocido como Plan de Continuidad de Negocio para TI, es un proceso crítico en el cual se evalúan los riesgos a los que una organización puede estar expuesta. Su objetivo principal es documentar, implementar, probar y mantener procedimientos que permitan a la organización retomar sus operaciones de manera eficiente y minimizar las pérdidas derivadas de un desastre (Pitta, 2018).

La responsabilidad principal de la creación y ejecución de un DRP recae en el departamento de Tecnología de la Información (TI) de la organización. Este plan se enfoca en

restablecer las operaciones de los sistemas informáticos críticos, por lo que es esencial que el DRP considere la estrategia general de la organización y el nivel de criticidad de sus activos. Idealmente, el DRP debe ser efectivo y adaptarse a las necesidades específicas de la organización.

El desarrollo del DRP debe tener en cuenta diversos factores, incluida la estrategia organizacional y la criticidad de los activos. Además, debe diseñarse con el objetivo principal de garantizar la continuidad del negocio. Por lo tanto, el plan debe incorporar un conjunto integral de medidas preventivas, detectivas y correctivas frente a posibles desastres. La efectividad del DRP se mide por su capacidad para mantener la continuidad operativa y minimizar el impacto adverso en la organización (Gamboa y Giraldo, 2016).

Desastre Informático

Un Desastre Informático se refiere a situaciones críticas que afectan la infraestructura tecnológica y la integridad de los datos en una organización. Estos desastres pueden surgir de diversas fuentes, como fallas en hardware, software, ciberataques, pérdida accidental de datos, entre otros. La gestión de un Desastre Informático implica la implementación de medidas preventivas y correctivas para minimizar el impacto y garantizar la recuperación eficiente de la infraestructura y los datos afectados.

Fases de un Desastre

Las fases de un desastre se pueden describir generalmente en cuatro etapas: mitigación, preparación, respuesta y recuperación. Cada fase desempeña un papel crucial en la gestión integral de desastres y busca reducir al mínimo los impactos negativos y facilitar una recuperación efectiva. A continuación, se describen brevemente estas fases:

1. **Mitigación**: Reducir o prevenir el impacto negativo de un desastre.
    - Identificación y evaluación de riesgos.
    - Implementación de medidas preventivas.

- Desarrollo de códigos de construcción y regulaciones.
- Creación de infraestructuras resistentes.

2. **Preparación:**
    - Desarrollo de planes de emergencia y evacuación.
    - Realización de simulacros y entrenamientos.
    - Almacenamiento de suministros de emergencia.
    - Establecimiento de sistemas de alerta temprana.

3. **Respuesta:**
    - Activación de planes de emergencia.
    - Evacuación y rescate de personas afectadas
    - Proporcionar asistencia médica y refugio.
    - Coordinación de recurso y servicios de emergencia.

4. **Recuperación:**
    - Evaluación de daños y necesidades.
    - Restablecimiento de servicios esenciales.
    - Asistencia a la comunidad para la reconstrucción.
    - Revisión y actualización de planes y políticas.

Es importante destacar que estas fases no siempre ocurren de manera lineal ni tienen límites estrictos entre sí. Además, las actividades de mitigación y preparación a menudo se llevan a cabo de manera continua, y la respuesta y la recuperación pueden superponerse durante el desarrollo del evento. La gestión efectiva de desastres implica una planificación integral que abarque todas las fases y promueve la resiliencia de las comunidades frente a eventos adversos (Gamboa y Giraldo, 2016).

Gestión de Riesgos y Normativas

Análisis de Riesgo

El análisis de riesgo es un proceso sistemático que implica la evaluación y cuantificación de los riesgos potenciales asociados con una actividad, proyecto o situación. Su objetivo principal es proporcionar información valiosa para tomar decisiones informadas sobre cómo gestionar o mitigar esos riesgos. Aquí hay una descripción general de los elementos clave del análisis de riesgo:

1. Identificación de Riesgos
2. Evaluación de Riesgos
3. Análisis Cuantitativo y Cualitativo
4. Mitigación de Riesgos
5. Monitoreo y Revisión Continua

El análisis de riesgo es una parte integral de la gestión de proyectos, la toma de decisiones empresariales y la planificación estratégica. Proporciona una base sólida para abordar los desafíos potenciales y tomar medidas proactivas para garantizar la seguridad y el éxito en diversas situaciones (Rodríguez, 2011).

Análisis de Impacto del Negocio (BIA)

El Análisis del Impacto del Negocio (BIA, por sus siglas en inglés, Bussines Impact Analysis) es un proceso crucial dentro del ámbito de la gestión de la continuidad del negocio. Su objetivo principal es evaluar y comprender el impacto potencial que tendrían las interrupciones en las operaciones comerciales. Aquí se describen los elementos clave del BIA:

1. Identificación de Procesos Críticos: Identificación de los procesos y funciones comerciales que son esenciales para la operación continua de la organización.
2. Determinación de Requisitos de Recuperación: Establecimiento de los objetivos de tiempo de recuperación (RTO) y los puntos de recuperación (RPO) para cada proceso crítico.

3. Evaluación de Impacto Financiero y Operativo: Evaluación de las pérdidas financieras y operativas que podrían surgir debido a la interrupción de procesos críticos.
4. Priorización de Recursos y Actividades: Identificación de los recursos y actividades clave necesarios para la recuperación de procesos críticos.
5. Documentación de Resultados y Recomendaciones: Documentación de los resultados del BIA, incluidas las prioridades de recuperación y las recomendaciones para mejorar la resiliencia.

El BIA es esencial para la planificación efectiva de la continuidad del negocio, ya que proporciona una comprensión clara de las prioridades de recuperación y ayuda a asignar recursos de manera eficiente. Los resultados del BIA sirven como base para el desarrollo de planes de continuidad del negocio y estrategias de recuperación ante desastres (Castaño y Garzón, 2015).

Punto de Recuperación Objetivo (RPO) y Tiempo de Objetivo (RTO)

Punto de Recuperación Objetivo (RPO). Se refiere al intervalo de tiempo tolerable para la pérdida de datos durante un evento disruptivo antes de que se vuelva inaceptable para la organización.

- **Importancia:** Determina la frecuencia con la que se deben realizar copias de seguridad para garantizar que, en caso de incidente, la cantidad de datos perdidos sea aceptable.

Tiempo de Objetivo (RTO). Establece el periodo máximo de tiempo en el que se espera que se restauren los servicios y las operaciones comerciales normales después de un evento disruptivo.

- **Importancia:** Indica el tiempo máximo que una organización puede permitirse estar inactiva antes de que se produzcan consecuencias significativas.

Relación entre RPO y RTO.

- **Interconexión:** El RPO y el RTO están interrelacionados; el RPO afecta directamente la cantidad de datos perdidos durante un incidente, y el RTO establece la ventana de tiempo para la recuperación.
- **Balance:** Es esencial equilibrar el RPO y el RTO en función de las necesidades comerciales y la tolerancia al riesgo.
- **Estrategia:** Una estrategia efectiva de continuidad del negocio considera ambos elementos para garantizar una recuperación eficiente y acorde con los objetivos comerciales.

Establecer el RPO y el RTO adecuados implica una comprensión profunda de las operaciones comerciales, la tecnología subyacente y las expectativas de los interesados. Estos parámetros son esenciales para desarrollar planes de recuperación efectivos y garantizar la resiliencia de la organización frente a eventos disruptivos (Maravi et al., 2015).

Tratamiento de Riesgo y Estrategias

Tratamiento de Riesgo. El tratamiento de riesgos es un componente esencial en la gestión integral de riesgos de una organización. Se refiere al conjunto de acciones planificadas y sistemáticas que una entidad implementa para abordar y gestionar los riesgos identificados durante el proceso de análisis de riesgos. El objetivo principal del tratamiento de riesgos es reducir la probabilidad de que ocurran eventos no deseados y minimizar el impacto en caso de que se materialicen (Ati, 2018).

Estrategia de Tratamiento de Riesgos. La estrategia de tratamiento de riesgos es un marco organizado y planificado que guían a una entidad en la gestión de los riesgos identificados. Consiste en la implementación de acciones específicas destinadas a mitigar, transferir, aceptar o evitar los riesgos, con el objetivo de optimizar los resultados y preservar la integridad y continuidad de las operaciones empresariales. A continuación, se describen las opciones para el tratamiento de riesgos:

1. Mitigación: Implica la implementación de medidas proactivas para reducir la probabilidad de que ocurra un riesgo o disminuir su impacto. Esto podría incluir la mejora de procesos, la seguridad física, la capacitación del personal o la implementación de tecnologías de seguridad.
2. Transferencia: Consiste en compartir el riesgo con otra entidad, como una aseguradora. Al comprar seguros, la organización transfiere parte o la totalidad de la responsabilidad financiera asociada con ciertos riesgos a la aseguradora.
3. Evitación: En este enfoque, la organización reorganiza sus operaciones o decisiones para eliminar por completar la exposición al riesgo. Esto podría implicar la interrupción de ciertas actividades comerciales o la renuncia a ciertos proyectos.
4. Aceptación**:** Algunas organizaciones optan por aceptar ciertos riesgos cuando los costos asociados con su tratamiento superan los beneficios esperados. Esto suele

ser una opción consciente y se lleva a cabo cuando los riesgos son considerados aceptables.

5. Diversificación: Se refiere a la distribución de los riesgos en diferentes áreas o activos para reducir el impacto de un riesgo específico en una parte particular de la organización. Esto es común en inversiones financieras.
6. Controles y Planes de Contingencia: Implica la implementación de medidas de seguridad y la creación de planes de contingencia para responder de manera efectiva en caso de que ocurra un riesgo. Esto puede incluir protocolos de seguridad, copias de seguridad de datos, sistemas de recuperación de desastres.

Una estrategia de tratamiento de riesgos bien desarrollada no solo ayuda a preservar la estabilidad operativa, sino que también contribuye al logro de metas estratégicas y a la resiliencia a largo plazo de la organización (Ati, 2018).

CAPITULO IV

Solución propuesta

El Plan de Recuperación de Desastres (DRP) desempeña un papel fundamental en la gestión y sostenimiento de los sistemas de los Laboratorios del Departamento de Ciencias de la Computación (DCCO) de la Universidad de las Fuerzas Armadas “ESPE”. La crítica importancia del DRP en este contexto radica en la naturaleza específica de las actividades y los recursos involucrados en estos espacios especializados.

Al contar con un DRP robusto, la Universidad se garantiza la capacidad de recuperación rápida de los Laboratorios del DCCO, mitigando de manera efectiva los impactos negativos en caso de eventos inesperados. En este contexto, el DRP no solo se concibe como una salvaguardia técnica, sino como un elemento esencial para preservar la continuidad operativa y la integridad de los recursos informáticos que respaldan la educación y las operaciones diarias en los Laboratorios del DCCO.

Diagnóstico de la Situación actual

Los laboratorios del DCCO son entornos dedicados a actividades informáticas avanzadas y al uso intensivo de recursos tecnológicos. Ante la posibilidad de eventos catastróficos como fallas de infraestructura, cortes de energía, incendios, inundaciones o ataques cibernéticos, el DRP se erige como una estrategia esencial. Este plan comprende un conjunto meticuloso de procedimientos, protocolos y directrices diseñados para minimizar el impacto de tales desastres.

El objetivo principal del DRP en los Laboratorios del DCCO es asegurar la pronta recuperación de las operaciones esenciales, minimizando al máximo la pérdida de datos y recursos valiosos. Dada la naturaleza crítica de estas operaciones para la imagen, educación y las actividades diarias de la Universidad de las Fuerzas Armadas “ESPE”, la implementación y mantenimiento de un DRP sólido son cruciales.

Misión

Disponer de talento humano calificado, así como de infraestructura moderna en hardware y software, que permita tanto a docentes como a estudiantes de la Universidad de las Fuerzas Armadas ESPE, desarrollar habilidades analíticas y funcionales de capacitación en las áreas de Ciencias de la Computación, generando conocimiento transferible para contribuir al progreso de la Universidad.

Visión

Contar con talento humano y laboratorios de docencia de excelencia, posicionados a nivel nacional e internacional en las áreas de Ciencias de la Computación, siendo reconocidos como referente institucional por su contribución en ámbitos académicos.

Objetivos estratégicos de los laboratorios

Minimizar el impacto de situaciones de emergencia y asegurar la continuidad de las operaciones, priorizando la seguridad de las personas y los bienes. Este objetivo se abordará a través de un plan de seguridad integral que contempla las siguientes etapas:

Identificación de Riesgos

- Identificar de manera exhaustiva los posibles eventos que podrían afectar los laboratorios, como incendios, terremotos, cortes de energía, entre otros.
- Evaluar el nivel de riesgo asociado a cada evento identificado para priorizar y enfocar los recursos de manera eficiente.

Planificación

- Diseñar estrategias y procedimientos específicos para hacer frente a los eventos identificados, considerando las características y necesidades particulares de los laboratorios.
- Asignar y garantizar los recursos necesarios, tales como equipos de seguridad, protocolos de evacuación y sistemas de respaldo de energía.

Implementación

- Llevar a cabo acciones concretas para implementar el plan de seguridad, asegurando que todos los procedimientos y recursos estén en su lugar y sean conocidos por el personal.
- Realizar simulacros y entrenamientos periódicos para mejorar la preparación del personal y evaluar la efectividad del plan.

Monitoreo y Evaluación

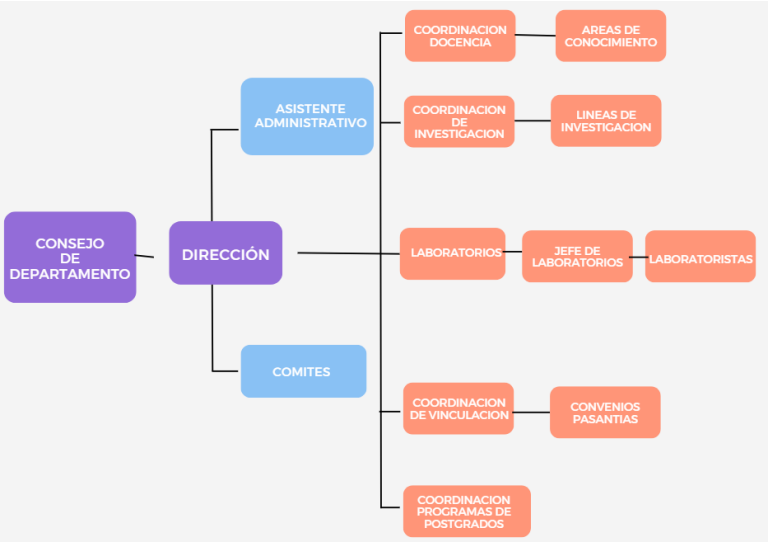
- Realizar revisiones periódicas del plan de seguridad para evaluar su eficacia y realizar ajustes según sea necesario.
- Establecer un sistema continuo de monitoreo de riesgos y actualización de procedimientos en respuesta a cambios en la infraestructura o en la naturaleza de los riesgos.

Para la realización de estos objetivos se tomó en cuenta el Plan de Contingencia y Recuperación de Desastres de TIC's de la Universidad de las Fuerzas Armadas ESPE.

Estructura organizacional

Figura 1

Organigrama del DCCO y Laboratorios



Nota. El organigrama representa la estructura del Consejo de Departamento de Ciencias de la Computación. Fuente propia.

Normativa de seguridad para el uso de los laboratorios de Computación

La seguridad en el entorno de los Laboratorios de Computación es un componente crítico para salvaguardar la integridad de personas, recursos y datos. El desarrollo e implementación de normativas específicas garantiza un ambiente de trabajo seguro, confiable y eficiente. A continuación, se detalla las normativas de seguridad que rigen el uso de los Laboratorios de Computación en la Universidad de las Fuerzas Armadas “ESPE”.

Seguridad Física

- **Control de Acceso:** Se implementan cerraduras electrónicas basadas en tags con códigos de identificación para registrar y controlar el acceso al laboratorio.
- **Vigilancia Activa:** La presencia de cámaras de seguridad y sistemas de control de movimiento proporciona una vigilancia constante, disuadiendo posibles accesos no autorizados.
- **Control de Visitantes:** Se regula el acceso de estudiantes y visitantes, garantizando que solo el personal autorizado y estudiantes cumpliendo con las normas ingresen al laboratorio.
- **Prohibición de Consumo:** Se prohíbe la ingestión de alimentos o bebidas dentro de los laboratorios para mantener la limpieza y orden.

Seguridad de Datos

- **Acceso Exclusivo a Servidores:** El acceso a los servidores es exclusivo para personal autorizado con credenciales de red, limitando las modificaciones y garantizando la seguridad de los datos.

- **Prohibición de Almacenamiento:** Se prohíbe el almacenamiento de información importante en las computadoras del laboratorio, asegurando la confidencialidad y la integridad de los datos.

Seguridad Eléctrica

- **Inspecciones Regulares:** Se realizan inspecciones periódicas de las instalaciones eléctricas para garantizar el cumplimiento de normativas y estándares de seguridad.
- **Dispositivos de Protección:** Se utilizan reguladores de voltaje y Sistemas de Alimentación Ininterrumpida (UPS) para prevenir daños por sobrecargas y cortocircuitos.

Seguridad del Hardware

- **Mantenimiento Preventivo:** Se establece la importancia del mantenimiento adecuado de equipos para prevenir posibles fallas y garantizar un funcionamiento confiable.
- **Prohibición de Manipulación:** Queda prohibida la manipulación, desconexión o remoción de equipos por parte de usuarios finales.

Seguridad de Software

- **Actualización Regular:** Se establece un proceso regular de instalación de actualizaciones para todo el software utilizado en el laboratorio.
- **Restricciones de Instalación:** Se prohíbe la instalación de software sin licencia y no autorizado por el Departamento de Ciencias de la Computación.
- **Firewall y Antivirus:** Se implementa un firewall y antivirus en todos los equipos para bloquear el acceso no autorizado y detectar amenazas en tiempo real.

Seguridad Medioambiental Ante Desastres

- **Manual de Seguridad ante Desastres:** Se hace referencia a un manual específico que proporciona recomendaciones para situaciones de emergencia, como la erupción del Cotopaxi.

Estas normativas forman un marco integral que garantiza la seguridad en todos los aspectos, desde el acceso físico hasta la protección de datos y la prevención de desastres. Su implementación contribuye significativamente a la continuidad operativa y al resguardo de la integridad de los usuarios y recursos de los Laboratorios de Computación en la Universidad de las Fuerzas Armadas “ESPE”. Para la realización de estas normativas se tomó en cuenta el Manual de Seguridad para los Laboratorios Generales de Computación.

Análisis de Impacto en el Negocio (BIA)

El enfoque del Análisis de Impacto en el Negocio (BIA) se orienta a comprender la capacidad de respuesta del negocio frente a posibles interrupciones, poniendo especial atención en la identificación de los procesos críticos y su influencia en el funcionamiento global de la organización. El BIA es una metodología que clasifica sistemáticamente los procesos de la organización, para establecer una estrategia efectiva que permita su pronta recuperación en disrupción.

En el desarrollo del BIA, los procesos organizacionales son desglosados y categorizados, lo que posibilita la definición de una estrategia de recuperación adaptada y eficaz. Esta estrategia se construye teniendo en cuenta factores esenciales como la tolerancia del negocio y el impacto potencial en caso de interrupciones.

Una herramienta fundamental en este proceso es el mapeo detallado de los procesos críticos, junto con la identificación de las herramientas utilizadas para su ejecución. Este enfoque facilita la comprensión profunda de la infraestructura operativa, permitiendo determinar puntos clave para la pronta recuperación y minimización de impactos en el caso de eventos disruptivos (Pin, 2018).

Figura 2

Metodología BIA

Nota. El diagrama representa todos los procesos que incluye la Metodología BIA. Fuente Propia

Alcance del Plan

Identificación de los procesos organizacionales

La identificación de los procesos organizacionales en el Departamento de Ciencias de la Computación (DCCO) de la Universidad de las Fuerzas Armadas “ESPE” es un componente fundamental en el desarrollo del Plan de Recuperación de Desastres (DRP) para los laboratorios. A continuación, se presenta una descripción más detallada de los procesos clave identificados:

Tabla 2

Gestión de procesos del Laboratorio del DCCO

	Objetivo	Procedimiento
Gestión de Mantenimiento de Equipos de Laboratorio	• Garantizar la disponibilidad y el rendimiento óptimo de los equipos.	• Identificación de procesos de mantenimiento preventivo y correctivo, especificando las acciones necesarias para mantener la operatividad de los equipos y minimizar las interrupciones.
Gestión de Registro y Monitoreo para Reservas de Laboratorio	• Coordinar eficientemente el uso de espacios y recursos en los laboratorios.	• Detallar cómo se registra y monitorea la reserva de los laboratorios, asegurando la asignación eficaz de recursos y evitando conflictos de uso.
Gestión de Sistema de Vigilancia	• Garantizar la seguridad de los laboratorios mediante un sistema de vigilancia.	• Describir la instalación, mantenimiento y acceso a las grabaciones del sistema de vigilancia, detallando protocolos de seguridad asociados.
Gestión de Control de Acceso	• Controlar el acceso a los laboratorios y sus recursos, permitiendo solo la entrada de personal autorizado.	• Identificar roles y responsabilidades en la gestión del control de acceso, especificando medidas para mantener la seguridad y proteger la integridad de los espacios y equipos.
Gestión del Centro de Datos (Data Center)	• Garantizar la disponibilidad, integridad y seguridad de la infraestructura del Data Center para respaldar las operaciones críticas.	• Asegurar la disponibilidad y el rendimiento óptimo de la infraestructura tecnológica. El procedimiento asociado implica la planificación e implementación de actividades de mantenimiento preventivo y correctivo. Esto incluye la identificación de procesos específicos, detallando las acciones necesarias para mantener la operatividad de los

Objetivo	Procedimiento
	equipos y minimizar las interrupciones en el funcionamiento del Data Center. Este proceso garantiza que la infraestructura tecnológica crítica se mantenga en condiciones óptimas para respaldar las operaciones de la organización.

Nota. Cada fila de la tabla describe un proceso con sus objetivos y procedimientos detallados para lograrlos.

La identificación detallada de estos procesos proporciona una comprensión profunda de las operaciones en los laboratorios del DCCO. Esta información es esencial para desarrollar un DRP sólido, ya que permite establecer claramente los elementos críticos que deben protegerse y restaurarse en caso de un desastre. Los flujogramas de los procesos se encuentran en el Apéndice 1.

Matriz de Holmes

La matriz de Holmes es una herramienta valiosa que permite priorizar parámetros con características similares de manera sistemática. Su principal función radica en la comparación y clasificación de estos parámetros según su importancia relativa (Rivadeneira, 2013). Los pasos para crear la matriz de Holmes son los siguientes:

1. Organización de criterios: Los criterios se disponen tanto en filas como en columnas de la matriz.
2. Diagonal principal: En la diagonal principal, no se omite la puntuación, ya que representa la comparación de un criterio consigo mismo.
3. Asignación de valores: En cada casilla fuera de la diagonal principal, se asignan valores de la siguiente manera:

- Si el criterio de la fila es más importante que el de la columna, se asigna el valor 1; de lo contrario, se asigna 0.
- Si el criterio de la columna es más importante que el de la fila, se asigna el valor 1; de lo contrario, se asigna 0.
- Si los criterios tienen igual importancia, se asigna el valor 0.5

4. Cálculo de totales por filas: Se suman los valores de cada fila para obtener el total.
5. Suma total de los totales por filas: Se suman los totales de todas las filas para obtener un total general.
6. Determinación del peso de cada criterio: Se calcula dividiendo el total de cada fila entre la suma total de todos los totales por filas. Esto proporciona una medida relativa de la importancia de cada criterio en el contexto general de la matriz.

   La aplicación sistemática de estos pasos garantiza una evaluación objetiva y fundamentada en la priorización de parámetros, lo que facilita la toma de decisiones informadas en diversos contextos de análisis y planificación (Abad, 2019).

Tabla 3

Matriz de priorización de Holmes

No	¿Cuál es el proceso más prioritario?	A	B	C	D	E	Total	Orden
A	Gestión de Mantenimiento de Equipos de Laboratorio		**0**	**1**	**0.5**	**0**	**1.5**	**4**
B	Gestión de Registro y Monitoreo para Reservas de Laboratorio	**1**		**1**	**0.5**	**0**	**2.5**	**2**
C	Gestión de Sistema de Vigilancia	**0**	**0**		**0**	**1**	**1**	**5**

No	¿Cuál es el proceso más prioritario?	A	B	C	D	E	Total	Orden
D	Gestión de Control de Acceso	**0.5**	**0.5**	**1**		**0**	**2**	**3**
E	Gestión del Centro de Datos (Data Center)	**1**	**1**	**0**	**1**		**3**	**1**

Nota. La tabla representa la evaluación de los procesos según su prioridad.

Tabla 4

Criterios de Puntuación

Criterios de puntuación	
Si es mejor que otro curso	1
Si es igual	0,5
Si es peor	0

Nota. La tabla muestra el valor de asignación según si criterio

Tabla 5

Priorización de los Procesos Críticos

Proceso	Orden de Prioridad
Gestión del Centro de Datos (Data Center)	1
Gestión de Riesgo y Monitoreo para Reservas de Laboratorio	2
Gestión de Control de Acceso	3
Gestión de Mantenimiento de Equipos de Laboratorio	4

Proceso	Orden de Prioridad
Gestión de Sistema de Vigilancia	5

Nota. La Tabla muestra el orden de los procesos según su criticidad, identificando el proceso de Gestión del Centro de Datos (Data Center) como el proceso prioritario.

Identificación de los procesos críticos

La identificación de los procesos críticos es una fase clave en el marco del Análisis de Impacto en el Negocio (BIA). Para llevar a cabo esta tarea de manera sistemática y precisa, se empleará una tabla de calificaciones como herramienta fundamental en este proceso estratégico.

En esta etapa, se someterá a análisis un macroproceso y sus componentes, compuestos en total por cinco procesos distintos. Tras una evaluación detallada, se ha determinado que tres de estos procesos merecen una calificación de criticidad debido a su importancia esencial para el funcionamiento continuo y efectivo de la organización.

La identificación de estos procesos críticos se erige como un paso fundamental en la formulación de la estrategia de recuperación. Al concentrarse en estos procesos de alta prioridad, se asegura que los recursos y las medidas de recuperación se implementen de manera eficiente y efectiva. Esto, a su vez, contribuye a minimizar los tiempos de inactividad y los impactos negativos en el negocio en caso de interrupciones, garantizando así una pronta y educativa recuperación.

Tabla 6

Tabla del primer proceso

Macroproceso	Proceso	Subproceso	Responsable
Gestión de Laboratorios del DCCO	Gestión de Mantenimiento	Mantener un alista actualizada de todos los equipos de laboratorio y su documentación técnica.	**Laboratoristas del DCCO**

	de Equipos de Laboratorio	Identificar los riesgos potenciales para la operación de los equipos, incluyendo factores ambientales, uso intensivo, etc.	**Laboratoristas del DCCO**
		Establecer planes de mantenimiento preventivo y correctivo para cada equipo, considerando intervalos y procedimientos específicos.	**Laboratoristas del DCCO**
		Realizar copias de seguridad regulares de las configuraciones y datos críticos de los equipos, como ajustes de calibración y parámetros de funcionamiento.	**Laboratoristas del DCCO**
		Mantener una lista de inventario para mantenimiento y recursos necesarios para llevar a cabo reparaciones.	**Laboratoristas del DCCO**
		Realizar simulaciones de posibles fallos y sus efectos en la operación del laboratorio para estar preparado ante situaciones inesperadas.	**Laboratoristas del DCCO**

Nota. La tabla detalla los subprocesos de la gestión de mantenimiento de Equipos bajo el macroproceso de la gestión de laboratorios del DCCO.

Tabla 7

Tabla del segundo proceso

Macroproceso	Proceso	Subproceso	Responsable
Gestión de Laboratorios del DCCO	Gestión de Registro y Monitoreo para Reservas de Laboratorio	Gestionar un sistema de respaldo para los datos de las reservas, incluyendo registros de solicitudes, programas y todo tipo de documentación.	Laboratoristas del DCCO
		Realizar copias de seguridad regulares de las bitácoras y registros generados, asegurando su integridad.	Laboratoristas del DCCO
		Gestionar los canales de comunicación para notificar a los usuarios sobre interrupciones y cambios en las reservas planificadas.	Laboratoristas del DCCO

Macroproceso	Proceso	Subproceso	Responsable
		Entrenar al personal en los procedimientos de reserva manual en caso de que el sistema automatizado no esté disponible.	Laboratoristas del DCCO

Nota. Esta tabla detalla los subprocesos del proceso de gestión de riesgo y monitoreo para reservas de laboratorio dentro del macroproceso de gestión de laboratorios del DCCO.

Tabla 8

Tabla del tercer proceso

Macroproceso	Proceso	Subproceso	Responsable
Gestión de Laboratorios del DCCO	Gestión de Sistema de Vigilancia	Almacenar un respaldo para las imágenes y datos capturados por el sistema de vigilancia.	**Laboratoristas del DCCO**
		Realizar copias de seguridad de las configuraciones de cámaras y sistemas de monitoreo para una rápida restauración	**Laboratoristas del DCCO**

Nota. La tabla detalla los subprocesos del proceso de gestión de sistemas de vigilancia dentro *del macroproceso gestión de laboratorios del DCCO.*

Tabla 9

Tabla del cuarto proceso

Macroproceso	Proceso	Subproceso	Responsable
Gestión de Laboratorios del DCCO	Gestión de Control de Acceso	Enumerar y documentar todos los puntos de acceso a los laboratorios, ya sea ingreso manual o mediante servidores con tags.	Laboratoristas del DCCO
		Mantener un registro detallado de los sistemas de control de acceso utilizados, incluyendo hardware, software y configuraciones.	Laboratoristas del DCCO
		Establecer niveles de acceso según roles específicos, definiendo qué áreas pueden ser accesibles para cada grupo de usuarios.	Laboratoristas del DCCO

Macroproceso	Proceso	Subproceso	Responsable
		Realizar copias de seguridad regulares de las configuraciones del sistema de control de acceso para facilitar la restauración.	Laboratoristas del DCCO
		En caso de fallo del sistema automatizado, establecer procedimientos de acceso manual, incluyendo el registro y seguimiento	Laboratoristas del DCCO
		Mantener una lista actualizada de contactos de emergencia que puedan ser notificados en caso de interrupciones del control de acceso	Laboratoristas del DCCO

Nota. La tabla detalla los subprocesos de gestión de control de acceso dentro del macroproceso gestión de laboratorios del DCCO.

Tabla 10

Tabla del Quinto Proceso

	Proceso	Subproceso	Responsable
Gestión de Laboratorios del DCCO	Gestión del Centro de Datos (Data Center)	Mantener un registro actualizado de todos los equipos y servidores en el Data Center, incluyendo su documentación técnica.	**Laboratoristas del DCCO**
		Identificar los riesgos potenciales para la operación del Data Center, considerando factores ambientales, demanda de recursos, etc.	**Laboratoristas del DCCO**
		Establecer planes de mantenimiento preventivo y correctivo para cada componente del Data Center, definiendo intervalos y procedimientos específicos.	**Laboratoristas del DCCO**
		Realizar copias de seguridad regulares de las configuraciones y datos críticos almacenados en el Data Center, como configuraciones de red y bases de datos.	**Laboratoristas del DCCO**
		Mantener una lista de inventario para el mantenimiento y los recursos necesarios para llevar a cabo reparaciones en el Data Center.	**Laboratoristas del DCCO**

Proceso	Subproceso	Responsable
	Realizar simulaciones de posibles fallos y evaluar sus efectos en la operación del Data Center para estar preparado ante situaciones inesperadas.	**Laboratoristas del DCCO**

Nota. Esta tabla detalla los subprocesos del proyecto de gestión del centro de datos

En las tablas previamente expuestas, se identifican los diversos procesos y subprocesos inherentes a los laboratorios del DCCO. A partir de esta información, se desarrolla la tabla de calificación, la cual constituye una herramienta fundamental para evaluar la criticidad de dichos procesos. Esta evaluación se logra mediante la aplicación de cinco aspectos esenciales cuidadosamente seleccionados, los cuales desempeñan un papel crucial en el proceso de calificación.

- Mantenimiento de Equipos: La gestión de mantenimiento de los equipos de laboratorio es esencial para garantizar un entorno seguro y un funcionamiento eficiente. Cualquier fallo en el mantenimiento preventivo o correctivo puede afectar la seguridad de los usuarios y la calidad de los resultados. La falta de respaldo de datos y configuraciones críticas también puede tener consecuencias graves en caso de pérdida.
- Disponibilidad de Laboratorios y Reservas: La gestión integral de monitoreo y registro para reservas de laboratorios incide directamente en la disponibilidad de recursos para investigaciones y experimentos. Interrupciones en el sistema de reserva automatizado o en la gestión de datos de reserva podrían afectar la programación y eficiencia de las actividades del laboratorio.
- Vigilancia y Seguridad: Un sistema de vigilancia efectivo es crucial para garantizar la seguridad de las instalaciones y prevenir incidentes. La pérdida de imágenes o datos capturados, junto con la incapacidad para restaurar rápidamente el sistema en caso de

fallos, podría tener consecuencias en la seguridad y capacidad de respuesta ante amenazas.

- Control de Acceso y Seguridad Física: La gestión de control de acceso es esencial para proteger los recursos y mantener la integridad de las áreas restringidas. La falta de control adecuado en el acceso a los laboratorios podría poner en riesgo la confidencialidad de los proyectos y la seguridad general de las instalaciones.
- Cumplimiento Normativo y Regulatorio: La necesidad de cumplir con políticas internas y regulaciones externas es un factor crítico para la operación de los laboratorios. La falta de cumplimiento podría conllevar sanciones legales, pérdida de fondos o problemas de reputación.

Para la generación de las calificaciones, se asigna un puntaje del uno al cinco, donde: muy elevada (5), elevada (4), media (3), baja (2), muy baja (1), y se calcula el promedio para definir la criticidad de cada aspecto evaluado.

Tabla 11

Tabla de calificaciones

Calificación	Clasificación	Significado
20 - 25	Crítico	• Las aplicaciones no pueden ejecutarse y deben ser reemplazadas con otras funciones. • No se reemplazan con funciones manuales. • El costo de interrupciones es muy elevado. • No tolera interrupciones.
16 - 19	Vital	• Las funciones pueden ser manejadas manualmente durante un corto plazo. • El costo de interrupciones no es muy alto si es en un periodo de 5 días. • Tolera interrupciones.
5 - 15	Deseable	• Las funciones pueden ser manejadas manualmente durante un largo plazo.

Calificación	Clasificación	Significado
		• El costo de interrupciones es muy bajo.

Nota. Esta tabla muestra el rango de criticidad que se asignó a cada aspecto evaluado

Tabla 12

Primer proceso calificado

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Mantenimiento de equipos	Disponibilidad de Laboratorios y Reservas	Vigilancia y seguridad	Control de Acceso y Seguridad Física	Cumplimiento Normativo y Regulatorio		
Gestión de Laboratorios del DCCO	Gestión de Mantenimiento de Equipos de Laboratorio	Mantener un alista actualizada de todos los equipos de laboratorio y su documentación técnica.	Laboratoristas del DCCO	5	5	3	3	5	21	Crítico
		Identificar los riesgos potenciales para la operación de los equipos, incluyendo factores ambientales, uso intensivo, etc.	Laboratoristas del DCCO	2	4	2	5	5	18	Vital
		Gestionar los canales de comunicación para notificar a los usuarios sobre interrupciones y cambios en las reservas planificadas.	Laboratoristas del DCCO	5	5	3	2	5	20	Crítico
		Realizar copias de seguridad regulares de las configuraciones y datos críticos de los equipos, como ajustes de calibración y parámetros de funcionamiento.	Laboratoristas del DCCO	5	2	3	4	5	19	Vital
		Mantener una lista de inventario para mantenimiento y recursos necesarios para llevar a cabo reparaciones.	Laboratoristas del DCCO	5	5	3	4	5	22	Crítico
		Realizar simulaciones de posibles fallos y sus efectos en la operación del laboratorio para estar preparado ante situaciones inesperadas.	Laboratoristas del DCCO	2	2	2	2	5	13	Deseable

Nota. Esta tabla muestra los subprocesos más críticos del proceso de Gestión de Mantenimiento de Equipos de Laboratorio.

Tabla 13

Segundo proceso calificado

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Mantenimiento de equipos	Disponibilidad de Laboratorios y Reservas	Vigilancia y seguridad	Control de Acceso y Seguridad Física	Cumplimiento Normativo y Regulatorio		
Gestión de Laboratorios del DCCO	Gestión de Riesgo y Monitoreo para Reservas de Laboratorio	Gestionar un sistema de respaldo para los datos de las reservas, incluyendo registros de solicitudes, programas y todo tipo de documentación.	Laboratoristas del DCCO	3	5	2	3	5	18	Vital
		Realizar copias de seguridad regulares de las bitácoras y registros generados, asegurando su integridad.	Laboratoristas del DCCO	4	3	3	4	5	19	Vital
		Gestionar los canales de comunicación para notificar a los usuarios sobre interrupciones y cambios en las reservas planificadas.	Laboratoristas del DCCO	4	5	2	5	5	21	Crítico
		Entrenar al personal en los procedimientos de reserva manual en caso de que el sistema automatizado no esté disponible.	Laboratoristas del DCCO	5	5	2	4	5	21	Crítico

Nota. Esta tabla muestra los subprocesos más críticos del proceso de Gestión de Riesgo y Monitoreo para Reservas de Laboratorio.

Tabla 14

Tercer proceso calificado

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Mantenimiento de equipos	Disponibilidad de Laboratorios y Reservas	Vigilancia y seguridad	Control de Acceso y Seguridad Física	Cumplimiento Normativo y Regulatorio		
Gestión de Laboratorios del DCCO	Gestión de Sistema de Vigilancia	Almacenar un respaldo para las imágenes y datos capturados por el sistema de vigilancia.	Laboratoristas del DCCO	2	2	5	2	4	15	Deseable
		Realizar copias de seguridad de las configuraciones de cámaras y sistemas de monitoreo para una rápida restauración.	Laboratoristas del DCCO	2	2	5	3	4	16	Vital

Nota. Esta tabla muestra los subprocesos más críticos del proceso de Gestión de Sistema de Vigilancia.

Tabla 15

Cuarto proceso calificado

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Mantenimiento de equipos	Disponibilidad de Laboratorios y Reservas	Vigilancia y seguridad	Control de Acceso y Seguridad Física	Cumplimiento Normativo y Regulatorio		
Gestión de Laboratorios del DCCO	Gestión de Control de Acceso	Enumerar y documentar todos los puntos de acceso a los laboratorios, ya sea ingreso manual o mediante servidores con tags.	Laboratoristas del DCCO	2	5	2	5	5	19	Vital
		Mantener un registro detallado de los sistemas de control de acceso utilizados incluyendo hardware, software y configuraciones.	Laboratoristas del DCCO	4	4	2	4	5	19	Vital
		Establecer niveles de acceso según roles específicos, definiendo qué áreas pueden ser accesibles para cada grupo de usuarios.	Laboratoristas del DCCO	1	5	2	5	5	18	Vital
		Realizar copias de seguridad regulares de las configuraciones del sistema de control de acceso para facilitar la restauración.	Laboratoristas del DCCO	3	2	2	3	4	14	Deseable
		En caso de fallo del sistema automatizado, establecer procedimientos de acceso manual, incluyendo el registro y seguimiento.	Laboratoristas del DCCO	1	4	2	5	5	17	Vital
		Mantener una lista actualizada de contactos de emergencia que puedan ser notificados en caso de interrupciones del control de acceso	Laboratoristas del DCCO	1	5	4	5	5	20	Crítico

Nota. Esta tabla muestra los subprocesos más críticos del proceso de Gestión de Control de Acceso.

Tabla 16

Quinto proceso calificado

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Mantenimiento de equipos	Disponibilidad de Laboratorios y Reservas	Vigilancia y seguridad	Control de Acceso y Seguridad Física	Cumplimiento Normativo y Regulatorio		
Gestión de Laboratorios del DCCO	Gestión del Centro de Datos (Data Center)	Mantener un registro actualizado de todos los equipos y servidores en el Data Center, incluyendo su documentación técnica.	Laboratoristas del DCCO	3	5	4	4	5	21	Crítico
		Identificar los riesgos potenciales para la operación del Data Center, considerando factores ambientales, demanda de recursos, etc.	Laboratoristas del DCCO	4	3	4	3	4	18	Vital
		Establecer planes de mantenimiento preventivo y correctivo para cada componente del Data Center, definiendo intervalos y procedimientos específicos.	Laboratoristas del DCCO	4	3	4	3	4	18	Vital
		Realizar copias de seguridad regulares de las configuraciones y datos críticos almacenados en	Laboratoristas del DCCO	5	3	3	4	4	19	Vital

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Mantenimiento de equipos	Disponibilidad de Laboratorios y Reservas	Vigilancia y seguridad	Control de Acceso y Seguridad Física	Cumplimiento Normativo y Regulatorio		
		el Data Center, como configuraciones de red y bases de datos.								
		Mantener una lista de inventario para el mantenimiento y los recursos necesarios para llevar a cabo reparaciones en el Data Center.	**Laboratoristas del DCCO**	5	3	4	5	4	21	Crítico
		Realizar simulaciones de posibles fallos y evaluar sus defectos en la operación del Data Center para estar preparado ante situaciones inesperadas.	**Laboratoristas del DCCO**	5	3	4	4	5	21	Crítico

Nota. Esta tabla muestra los subprocesos más críticos del proceso de Gestión del Centro de Datos.

Identificación de servicios e infraestructura tecnológica de soporte para procesos críticos

Una vez identificado los procesos críticos y vitales, se determina los recursos de TI para la ejecución de los mismos.

Tabla 17

Recursos TI primer proceso

PROCESO	SUBPROCESOS						RECURSOS TI
	GMELS P1	GMELS P2	GMELS P3	GMELS P4	GMELS P5	GMELS P6	
Gestión de Mantenimiento de Equipos de Laboratorio	X	X	X	X	X	X	Intranet
	X	X	X	X	X	X	Internet
			X	X		X	Equipos de Usuarios Finales
	X	X	X	X	X	X	Energía Eléctrica
							Sistema Soyal
	X	X	X	X	X	X	Hojas de Cálculo
	X		X	X			Sistema Acronis

Nota: GMELSP1: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 1.
GMELSP2: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 2.
GMELSP3: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 3.
GMELSP4: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 4.

GMELSP5: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 5.
GMELSP6: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 6.

Tabla 18

Recursos TI primer proceso

PROCESO	SUBPROCESOS						RECURSOS TI
	GMELS P1	GMELS P2	GMELS P3	GMELS P4	GMELS P5	GMELS P6	
Gestión de Mantenimiento de Equipos de Laboratorio	X	X	X	X	X	X	Intranet
	X	X	X	X	X	X	Internet
			X	X		X	Equipos de Usuarios Finales
	X	X	X	X	X	X	Energía Eléctrica
							Sistema Soyal
	X	X	X	X	X	X	Hojas de Cálculo
	X		X	X			Sistema Acronis

Nota: GMELSP1: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 1.
GMELSP2: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 2.
GMELSP3: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 3.
GMELSP4: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 4.
GMELSP5: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 5.
GMELSP6: Gestión de Mantenimiento de Equipos de Laboratorios Subproceso 6.

Tabla 19

Recursos TI segundo proceso

PROCESO	SUBPROCESOS				RECURSOS TI
	GRMRLSP1	GRMRLSP2	GRMRLSP3	GRMRLSP4	
Gestión de Registro y Monitoreo para Reservas de Laboratorios	X	X	X	X	Intranet
	X	X	X	X	Internet
			X	X	Equipos de Usuarios Finales
	X	X	X	X	Energía Eléctrica
					Sistema Soyal
	X	X			Hojas de Cálculo
	X			X	Sistema Acronis

Nota: GRMRLSP1: Gestión de Registro y Monitoreo para Reservas de Laboratorios Subproceso 1.
GRMRLSP2: Gestión de Registro y Monitoreo para Reservas de Laboratorios Subproceso 2.
GRMRLSP3: Gestión de Registro y Monitoreo para Reservas de Laboratorios Subproceso 3.
GRMRLSP4: Gestión de Registro y Monitoreo para Reservas de Laboratorios Subproceso 4.

Tabla 20

Recursos TI tercer proceso

PROCESO	SUBPROCESOS		RECURSOS TI
	GSVSP1	GSVSP2	
	X	X	Intranet
	X	X	Internet
Gestión de Sistema de Vigilancia			Equipos de Usuarios Finales
	X	X	Energía Eléctrica
	X		Sistema Soyal
		X	Hojas de Cálculo
			Sistema Acronis

Nota: GSVSP1: Gestión de Sistema de Vigilancia Subproceso 1.
GSVSP 2: Gestión de Sistema de Vigilancia Subproceso 2.

Tabla 21

Recursos TI cuarto proceso

PROCESO	SUBPROCESOS						RECURSOS TI
	GCASP1	GCASP2	GCASP3	GCASP4	GCASP5	GCASP6	
	X	X	X	X	X	X	Intranet
	X	X	X	X	X	X	Internet
Gestión de Control de Acceso							Equipos de Usuarios Finales
	X	X	X	X	X	X	Energía Eléctrica
	X	X	X	X	X	X	Sistema Soyal
	X	X	X	X	X		Hojas de Cálculo
							Sistema Acronis

Nota: GCASP1: Gestión de Control de Acceso Subproceso 1.
GCASP2: Gestión de Control de Acceso Subproceso 2.
GCASP3: Gestión de Control de Acceso Subproceso 3.
GCASP4: Gestión de Control de Acceso Subproceso 4.
GCASP5: Gestión de Control de Acceso Subproceso 5.
GCASP6: Gestión de Control de Acceso Subproceso 6.

Tabla 22

Recursos TI quinto proceso

PROCESO	SUBPROCESOS						RECURSOS TI
	GCD1	GCD2	GCD3	GCD4	GCD5	GCD6	
Gestión del Centro de Datos	X	X	X	X	X	X	Intranet
	X	X	X	X	X	X	Internet
		X	X		X	X	Equipos de Usuarios Finales
	X	X	X	X	X	X	Energía Eléctrica
	X	X	X		X	X	Sistema Soyal
	X	X	X		X	X	Hojas de Cálculo
	X	X		X	X	X	Sistema Acronis

Nota: GCCD1: Gestión del Centro de Datos1.
GCCD2: Gestión del Centro de Datos2.
GCCD3: Gestión del Centro de Datos3.
GCCD4: Gestión del Centro de Datos4.
GCCD5: Gestión del Centro de Datos5.
GCCD6: Gestión del Centro de Datos6.

Impactos en los procesos críticos de los laboratorios del DCCO

Los efectos negativos pueden surgir en situaciones de interrupciones, fallos o desastres que impactan directamente las operaciones esenciales de una organización. En el contexto de los laboratorios del Departamento de Ciencias de la Computación (DCCO), los procesos críticos se definen como aquellas actividades y funciones vitales para el funcionamiento continuo y exitoso de la organización. La comprometida ejecución de estos procesos podría acarrear consecuencias significativas para los laboratorios.

La evaluación del impacto se realiza en el momento más crucial de cada proceso, considerando específicamente los tipos de impacto operacional y de imagen, como se puede observar en las encuestas realizadas del Apéndice 3. Esta evaluación busca determinar las consecuencias en toda la organización en caso de interrupción de un proceso específico en los laboratorios del DCCO.

Dada la complejidad inherente de los procesos del negocio, se ha optado por especificar los valores de impacto de manera cualitativa. A continuación, se presenta la clasificación detallada de impacto:

- Impacto Nulo (0): No se observa un impacto significativo en la operatividad ni en la imagen de la organización.
- Impacto Leve (1): Se identifican consecuencias mínimas, con un impacto ligero en las operaciones y la imagen.
- Impacto Medio (2): Se reconocen efectos moderados, con cierta afectación en la operatividad y una percepción media en la imagen institucional.
- Impacto Grave (3): Se constatan consecuencias serias, con un impacto significativo en las operaciones y una afectación considerable en la imagen.
- Impacto Catastrófico (4): Se evidencian consecuencias devastadoras, con un impacto crítico en las operaciones y una afectación severa en la imagen, comprometiendo la integridad y continuidad de la organización.

Esta categorización cualitativa proporciona una base integral para la comprensión de las posibles repercusiones en la operatividad y la imagen de la organización ante situaciones críticas en los laboratorios del DCCO.

La pauta que se utilizará para la calificación del impacto se resume de manera clara en la siguiente tabla:

Tabla 23

Tipos de impacto

Tipos de Impacto	**Criterios y evaluación**			
	Leve	**Medio**	**Grave**	**Catastrófico**
Operacional	Produce retrasos en procesos no vitales	Produce retrasos en procesos vitales	Produce retrasos graves en procesos críticos	Produce interrupción inmediata de procesos vitales

Tipos de Impacto	Criterios y evaluación			
	Leve	**Medio**	**Grave**	**Catastrófico**
De Imagen	Parte de la percepción que brindan los laboratorios disminuye	Genera un declive en la imagen de los laboratorios para la Universidad	Afecta la confianza de estudiantes, profesores y la comunidad universitaria	Mala reputación por las funciones que deberían brindar los laboratorios

Nota: Esta tabla permite una rápida visualización y comprensión de cómo diferentes niveles de impacto pueden influir en la operación, la imagen y la estabilidad económica de los laboratorios del DCCO.

Tabla 24

Resultados del primer proceso

Gestión de Mantenimiento de Equipos de Laboratorio					
	Gravedad				
Impacto	2 horas	6 horas	1 día	2 días	1 semana
Operacional	0	1	2	3	4
De Imagen	0	1	1	2	3

Nota. La tabla nos proporciona una evaluación de la gravedad del impacto en la Gestión del mantenimiento de equipos de Laboratorio.

Tabla 25

Resultados del segundo proceso

Gestión de Registro y Monitoreo para Reservas de Laboratorio					
	Gravedad				
Impacto	2 horas	6 horas	1 día	2 días	1 semana
Operacional	0	1	1	2	3
De Imagen	0	1	1	2	2

Nota: La tabla nos proporciona una evaluación de la gravedad del impacto en la Gestión de Registro y Monitoreo para Reservas de Laboratorio.

Tabla 26

Resultados del tercer proceso

Gestión de Sistema de Vigilancia					
	Gravedad				
Impacto	2 horas	6 horas	1 día	2 días	1 semana
Operacional	0	1	1	2	2
De Imagen	0	1	1	2	3

Nota: La tabla nos proporciona una evaluación de la gravedad del impacto en la Gestión de Registro y Monitoreo para Reservas de Laboratorio.

Tabla 27

Resultados del cuarto proceso

Gestión de Control de Acceso					
	Gravedad				
Impacto	2 horas	6 horas	1 día	2 días	1 semana
Operacional	1	2	2	3	4
De Imagen	1	2	3	4	4

Nota: La tabla nos proporciona una evaluación de la gravedad del impacto en la Gestión de Control de Acceso.

Tabla 28

Resultados del quinto proceso

Gestión de Centro de Datos (Data Center)					
	Gravedad				
Impacto	2 horas	6 horas	1 día	2 días	1 semana
Operacional	0	2	3	4	4
De Imagen	0	1	2	3	4

Nota: La tabla nos proporciona una evaluación de la gravedad del impacto en la Gestión de Centro de Datos.

Determinación del RTO y WRT

La Determinación del RTO (Objetivo de tiempo de recuperación) y WRT (Tiempo de recuperación real) es esencial para planificar y gestionar la recuperación ante desastres. El RTO

representa el tiempo máximo que una organización se fija como objetivo para recuperar sus sistemas y servicios después de un incidente catastrófico. Es el período durante el cual la organización aspira a restaurar sus operaciones críticas a un estado funcional normal tras un evento adverso.

Por otro lado, el WRT es el tiempo real que realmente se tarda en recuperar los sistemas y servicios. Comparar el RTO planificado con el WRT permite evaluar la efectividad del plan de recuperación y ajustar estrategias si es necesario. Ambos elementos son fundamentales para garantizar una recuperación eficiente y minimizar los impactos en las operaciones críticas de la organización.

Tabla 29

Resultados de RTO y WRT

Proceso	Servicio	RTO	WRT
Gestión de Mantenimiento de Equipos de Laboratorio	Intranet	2 horas	1 hora
	Internet	2 hora	1 hora
	Equipos de Usuarios Finales	3 horas	2 horas
	Energía Eléctrica	1 hora	10 minutos
	Hojas de Cálculo	3 horas	30 minutos
	Sistema Acronis	2 horas	1 hora
Gestión de Registro y Monitoreo para Reservas de Laboratorio	Intranet	2 horas	1 hora
	Internet	2 horas	1 hora
	Equipos de Usuarios Finales	3 horas	2 horas
	Energía Eléctrica	1 hora	10 minutos
	Hojas de Cálculo	3 horas	1 hora
	Sistema Acronis	2 horas	1 hora
Gestión de Sistema de Vigilancia	Intranet	2 horas	1 hora
	Internet	2 horas	1 hora
	Equipos de Usuarios Finales	3 horas	2 horas
	Energía Eléctrica	1 hora	10 minutos
Gestión de Control de Acceso	Intranet	2 horas	1 hora
	Internet	2 hora	1 hora
	Equipos de Usuarios Finales	3 horas	2 horas
	Energía Eléctrica	1 hora	10 minutos
	Hojas de Cálculo	3 horas	30 minutos
	Sistema Soyal	1 hora	30 minutos

Nota: RTO determina la cantidad máxima de tiempo tolerable necesario para que todos los procesos críticos vuelvan a sus actividades. WRT determina la cantidad máxima de tiempo tolerable que se necesita para que el proceso vuelva a operar.

Determinación del MTD

La Determinación del MTD (Tiempo de inactividad máximo tolerable) es crucial para establecer el periodo máximo durante el cual una organización puede soportar que sus sistemas o servicios estén inactivos debido a un incidente catastrófico. En el contexto del Plan de Recuperación de Desastres (DRP), se determina antes de que se produzcan impactos significativos en la operación y en los objetivos de la empresa.

Es una medida crítica que define cuánto tiempo máximo puede permitirse una organización estar fuera de línea antes de que los efectos negativos resulten intolerables. En esencia, el MTD establece el límite temporal dentro del cual la organización debe recuperarse y volver a estar operativa después de un evento adverso.

Tabla 30

Resultados del MTD

Procesos de Negocio	MTD
Gestión de Mantenimiento de Equipos de Laboratorio	1 día
Gestión de Registro y Monitoreo para Reservas de Laboratorio	2 días
Gestión de Sistema de Vigilancia	6 horas
Gestión de Control de Acceso	2 horas
Gestión de Centro de Datos	1 hora

Notas. Opinión del jefe de laboratorios del DCCO

Tabla 31

Resultados del MTD

Procesos de Negocio	MTD
Gestión de Mantenimiento de Equipos de Laboratorio	18 horas y 40 minutos

Procesos de Negocio	MTD
Gestión de Registro y Monitoreo para Reservas de Laboratorio	19 horas y 10 minutos
Gestión de Sistema de Vigilancia	12 horas 10 minutos
Gestión de Control de Acceso	17 horas y 10 minutos
Gestión de Centro de Datos	15 horas y 10 minutos

Nota. Calculo Generado = RTO + WRT

MTD: Define la cantidad total de un tiempo en el cual un proceso puede interrumpirse

Determinación del RPO

El RPO (Objetivo del punto de recuperación) es el punto en el tiempo hasta el cual una organización está dispuesta a recuperar sus datos después de un incidente catastrófico. Representa el intervalo de tiempo máximo en el que los datos pueden perderse o no estar disponibles antes de que la recuperación sea considerada aceptable para la organización. En términos sencillos, el RPO define cuánta información una organización puede permitirse perder en caso de un desastre antes de que la recuperación se complete satisfactoriamente. Establecer un RPO claro es crucial para orientar la estrategia de recuperación y garantizar que la pérdida de datos se mantenga dentro de límites aceptables para la operación continúa y efectiva de la organización.

Tabla 32

Resultados del RPO

Servicio	RPO
Intranet	1 día
Internet	3 horas
Equipos de Usuarios Finales	1 día
Energía Eléctrica	10 minutos
Hojas de Cálculo	1 día
Sistema Acronis	6 horas
Sistema Soyal	2 horas

Nota: Esta tabla representa la cantidad máxima aceptable de pérdida de datos que los laboratorios pueden permitir.

Análisis de Riesgo (RA)

El Análisis de Riesgo (RA) es un proceso integral que se lleva a cabo para identificar, evaluar y priorizar los posibles riesgos que podrían afectar a los laboratoristas y sus sistemas en el Departamento de Ciencias de la Computación (DCCO). Su objetivo primordial es proporcionar una comprensión profunda de las amenazas y sus impactos, permitiendo tomar decisiones informadas en la implementación de medidas de mitigación y en el desarrollo del Plan de Recuperación de Desastres (DRP). Para lograr este objetivo, se siguieron los siguientes pasos específicos dentro de los Laboratorios del DCCO:

- **Identificación de Amenazas:** El RA se enfoca en identificar amenazas potenciales que podrían generar interrupciones en los laboratorios. Estas amenazas pueden incluir eventos naturales, errores técnicos, acciones no autorizadas y la pérdida de servicios esenciales.
- **Evaluación de Vulnerabilidades:** Se lleva a cabo una evaluación minuciosa de las vulnerabilidades presentes en los sistemas y recursos ante las amenazas identificadas. Este análisis abarca desde las debilidades en la infraestructura hasta los sistemas de TI, la seguridad física y los procedimientos operativos.
- **Estimación de Impactos:** Se determina el posible impacto de cada amenaza, considerando aspectos como la interrupción de servicios, pérdida de datos, daños financieros y reputacionales. Esta evaluación proporciona una visión clara de las consecuencias potenciales de cada escenario de riesgo.
- **Cálculo de Probabilidades:** Se cuantifica la probabilidad de materialización de cada amenaza, tomando en cuenta factores históricos, geográficos, técnicos y operativos. Este paso permite asignar valores específicos a la posibilidad de ocurrencia de cada riesgo.

- **Desarrollo de Estrategias de Mitigación:** Con base en los resultados del análisis, se proponen estrategias efectivas para mitigar o reducir los riesgos identificados. Estas estrategias pueden abarcar desde medidas de seguridad física hasta la implementación de redundancias en sistemas y respaldo de datos.

Es esencial destacar que cada actividad realizada por el personal de los laboratorios del DCCO se registra y documenta meticulosamente, permitiendo así conocer el nivel de riesgo que podría afectar la prestación de servicios a los estudiantes. Este enfoque proactivo garantiza la seguridad y continuidad operativa de los laboratorios en todo momento.

Tabla 33

Actividades de los procesos

Procesos	Actividades
Gestión de Mantenimiento de Equipos de Laboratorio	Crear un inventario completo de equipos de laboratorio. Definir calendario y plan de mantenimiento preventivo. Realizar inspecciones regulares de equipos. Registrar y documentar solicitudes de mantenimiento. Asignar tareas de mantenimiento a técnicos. Realizar mantenimiento correctivo cuando se detectan problemas. Registrar y mantener historiales de mantenimiento. Verificar la calibración y funcionamiento de los equipos después del mantenimiento. Actualizar registros y documentación después de cada actividad de mantenimiento.
Gestión de Registro y Monitoreo para Reservas de Laboratorio	Configurar equipos mediante un disco espejo. Registrar y mantener un calendario de disponibilidad de laboratorios. Recopilar información de reserva por carrera. Supervisar el uso y la ocupación de los laboratorios. Generar bitácoras sobre el uso y la demanda de los laboratorios. Administrar y resolver conflictos de horarios de reserva.
Gestión de Sistema de Vigilancia	Diseñar y planificar la ubicación de cámaras de vigilancia. Instalar cámaras y sistemas de grabación. Configurar la infraestructura de red para la transmisión. Monitorear las imágenes en tiempo real desde un centro de control. Analizar y revisar grabaciones de video en busca de eventos

Procesos	Actividades
	relevantes. Responder a alertas y notificaciones de eventos sospechosos.
Gestión de Control de Acceso	Implementar sistemas de control de acceso físico, como tarjetas de identificación o biométricos. Configurar perfiles de acceso para docentes. Registrar las entradas y salidas de la comunidad universitaria. Responder a solicitudes de acceso temporal o excepcional. Gestionar y mantener sistemas de bloqueo y desbloqueo remoto.
Gestión de Centro de Datos	Monitoreo y vigilancia constante de los sistemas y equipos. Gestión de la Seguridad física y lógica del Data Center. Realización de copias de seguridad regulares y aseguramiento de la integridad de los datos. Cumplimiento normativo y aplicación de estándares de seguridad. Planificación estratégica para la mejora continua de la infraestructura y los procesos.

Nota. En esta tabla podemos ver las actividades por proceso para una mejor comprensión de las responsabilidades involucradas en cada área de gestión.

La valoración de activos es fundamental para la gestión integral de riesgos. Los criterios de valoración de activos dentro de los laboratorios del DCCO se definen considerando su importancia y dependencia en los procesos operativos. La categorización utilizada para esta evaluación se detalla a continuación:

- Bajo = 1: Se asigna a activos con una importancia mínima o una dependencia limitada en los procesos de los laboratorios. Su impacto en las operaciones es relativamente bajo.
- Moderado = 2: Se otorga a activos que poseen una importancia y dependencia moderada en los procesos. Su impacto en las operaciones es significativo, pero no crítico.
- Alto = 3: Se asigna a activos con una importancia considerable y una dependencia significativa en los procesos de los laboratorios. Su impacto en las operaciones es sustancial.

- Crítico = 4: Se reserva para activos de vital importancia y con una dependencia absoluta en los procesos de los laboratorios. Su impacto en las operaciones es crucial y su pérdida tendría consecuencias graves.

Esta categorización proporciona una guía clara para priorizar la protección y la asignación de recursos en función de la criticidad de cada activo. La valoración de activos contribuye significativamente a la toma de decisiones informada en la implementación de medidas de seguridad y en la formulación de estrategias de gestión de riesgos para garantizar la continuidad operativa de los laboratorios del DCCO.

Tabla 34

Niveles de atributos

Atributos	**Criterios y Evaluación**			
	Bajo	**Moderado**	**Medio**	**Crítico**
Dependencia	Ningún otro activo depende de este para entregar servicios a usuarios.	Pocos activos dependen de este para entregar servicio a usuarios.	Una gran cantidad de activos dependen de este para entregar servicios a usuarios	Todos los activos dependen de este para entregar servicios a usuarios
Funcionalidad	Activos con capacidades tecnológicas muy limitadas	Activo con capacidades tecnológicas limitadas	Activo con capacidades tecnológicas avanzadas	Activo con capacidades tecnológicas de última generación
Confidencialidad, Integridad y Disponibilidad	La divulgación, modificación y no disponibilidad del activo puede afectar de forma insignificante la entrega de servicios a usuarios.	La divulgación, modificación y no disponibilidad del activo puede afectar en parte la entrega de servicios a usuarios.	La divulgación, modificación y no disponibilidad del activo puede afectar significativamente en la entrega de servicios a usuarios.	La divulgación, modificación y no disponibilidad del activo puede afectar totalmente la entrega de servicios a usuarios.

Nota: En la tabla se detallan las pautas de evaluación para la valoración de activos.

Tabla 35

Atributos de los procesos

Activos	Atributos			
	Dependencia	Funcionalidad	Confidencialidad, Integridad y Disponibilidad	Valoración
Red de Datos	3	3	3	27
Internet	4	3	4	48
Equipos de Usuarios Finales	3	2	3	18
Energía Eléctrica	4	4	4	64
Hojas de Cálculo	1	1	2	2
Sistema Acronis	2	3	3	18
Sistema Soyal	2	3	4	24

Nota: Resultados de atributos de los procesos

Identificación de Riesgos

La identificación de riesgos es el procedimiento destinado a reconocer y categorizar posibles situaciones, eventos o circunstancias que podrían generar un impacto adverso en un sistema, proyecto, operación o entidad.

Cuando se trata del desarrollo de un Plan de Recuperación ante Desastres (DRP), este proceso implica la identificación de amenazas potenciales que podrían ocasionar interrupciones, daños o pérdidas en la infraestructura tecnológica y operativa de una organización.

Estimación de Riesgo

Se trata del proceso de evaluación y cuantificación de los posibles riesgos que podrían impactar la capacidad de una organización para recuperarse tras un desastre. Este procedimiento implica la identificación de riesgos potenciales que podrían interrumpir las operaciones normales, evaluando su probabilidad de ocurrencia y determinando el impacto que tendrían en la organización. La estimación de riesgo es un Plan de Recuperación ante Desastres (DRP) resulta fundamental para:

- Identificar las amenazas más significativas y sus posibles consecuencias.

- Priorizar las medidas de mitigación y planificación según la gravedad de los riesgos.
- Establecer recursos y estrategias adecuados para abordar los riesgos identificados.
- Tomar decisiones informadas sobre la asignación de recursos y la implementación de medidas de contingencia.

En la última instancia, la estimación de riesgo en un DRP ayuda a la organización a estar mejor preparada para enfrentar situaciones de desastre al identificar los riesgos clave y desarrollar estrategias efectivas para minimizar su impacto en las operaciones.

Evaluación de Riesgo

La evaluación de riesgos engloba la identificación, evaluación y priorización de las posibles amenazas y riesgos que podrían afectar la infraestructura tecnológica, datos y procesos críticos de una organización en caso de un desastre. Este proceso comprende:

- **Identificación de riesgos:** Reconocimiento de amenazas potenciales, como incendios, inundaciones, fallos de hardware, ataques cibernéticos, entre otros, que podrían causar interrupciones en las operaciones.
- **Evaluación de impacto:** Valoración del posible impacto de cada riesgo identificado en términos de pérdida de datos, tiempo de inactividad, costos financieros, reputación de la organización, etc.
- **Priorización:** Clasificación de los riesgos según su gravedad y probabilidad de ocurrencia, permitiendo a la organización focalizarse en los riesgos más críticos y tomar medidas para mitigarlos.
- **Estrategias de mitigación:** Desarrollo de estrategias y planes para reducir los riesgos identificados, que pueden incluir medidas preventivas, procedimientos de respaldo, implementación de sistemas redundantes, entre otros.
- **Documentación:** Registro detallado de los riesgos identificados, su evaluación, estrategias de mitigación y planes de respuesta correspondientes en el Plan de Recuperación ante Desastres (DRP).

La evaluación de riesgos resulta fundamental para diseñar un DRP efectivo que permita a una organización estar preparada para responder a situaciones de desastre y minimizar el impacto en sus operaciones.

Tabla 36

Tabla de Identificación, estimación y evaluación de riesgos

Procesos	Identificación de Riesgos	Estimación del Riesgo	Evaluación del Riesgo
Gestión de Mantenimiento de Equipos de Laboratorio	• Fallos inesperados de equipos de laboratorio. • Retrasos en la programación de mantenimiento preventivo. • Incumplimiento de configuración y verificación. • Insuficiente documentación de historiales de mantenimiento.	•Calcular la probabilidad de fallos de equipos en función de su vida útil y frecuencia de uso. •Evaluar la posible repercusión operativa de la interrupción de equipos críticos.	• Priorizar equipos críticos en función de su importancia en el proceso educativo y científico. • Evaluar el impacto de la falta de mantenimiento preventivo y correctivo en la calidad y seguridad de las operaciones. • Determinar la frecuencia y alcance de las inspecciones y el mantenimiento para reducir el riesgo de fallos.
Gestión de Registro y Monitoreo para Reservas de Laboratorio	• Problemas en la disponibilidad. Dificultades en la generación de bitácoras de uso.	•Calcular el impacto de posibles conflictos en franjas horarias para el uso de los laboratorios	• Establecer procedimientos que resuelvan rápidamente conflictos de horarios y mejorar la eficiencia en la asignación de recursos.
Gestión de Sistema de Vigilancia	• Monitoreo insuficiente de áreas críticas. • Incapacidad para identificar eventos relevantes en tiempo real. • Brechas en la seguridad y acceso no autorizado a las grabaciones.	• Evaluar la probabilidad de problemas técnicos en el sistema de vigilancia según su infraestructura. Calcular el impacto de posibles problemas de monitoreo en la seguridad y respuesta ante incidentes.	• Implementar procedimientos para una supervisión constante del sistema de vigilancia. Definir protocolos para la revisión periódica de grabaciones y la notificación de eventos sospechosos.

Procesos	Identificación de Riesgos	Estimación del Riesgo	Evaluación del Riesgo
Gestión de Control de Acceso	• Fallos en los sistemas de control de acceso. • Errores en la asignación de perfiles. • Falta de supervisión y revisión de registros de acceso.	• Evaluar la probabilidad de problemas técnicos en los sistemas de control de acceso. Calcular el impacto de posibles accesos no autorizados a áreas restringidas.	• Implementar procedimientos para el mantenimiento y monitoreo constante de los sistemas de control de acceso. Definir protocolos para la revisión de registros de acceso y la actualización de la base de datos de usuarios.
Gestión del Data Center	• Interrupción del suministro eléctrico. • Fallos en los sistemas de refrigeración. • Pérdida de conectividad de red. • Amenazas físicas como incendios, inundaciones o terremotos. • Fallos en los sistemas de respaldo y recuperación de datos. • Amenazas cibernéticas como ataques de hackers, malware o ransomware.	• Evaluar la probabilidad de cada uno de los riesgos identificados y su posible impacto en las operaciones del data center. • Calcular el tiempo de inactividad tolerable para cada servicio o aplicación alojada en el centro de datos.	• Priorizar los riesgos identificados según su probabilidad e impacto. • Realizar un análisis de coste-beneficio para determinar qué medidas de mitigación son más efectivas y rentables. • Establecer estrategias de contingencia y planes de recuperación ante posibles escenarios de riesgo.

Nota. Esta tabla organiza las actividades relacionadas con la identificación, estimación y evaluación de riesgos para cada uno de los procesos mencionados.

Una vez establecida la dependencia de los activos en los procesos críticos de los laboratorios del DCCO, es esencial identificar las vulnerabilidades que estos activos puedan presentar, así como las amenazas asociadas.

La vulnerabilidad se define como “una debilidad susceptible de ser aprovechada por una amenaza”, mientras que una amenaza se considera “cualquier factor que podría explotar una vulnerabilidad, siendo cualquier causa potencial de un incidente considerada una amenaza”. Las amenazas pueden surgir de diversas fuentes, ya sea de origen natural o humano, y pueden ser tanto accidentales como intencionales (Ati, 2018).

Tabla 37

Tabla de Tipos de Riesgos

Riesgos		
Eventos Naturales	Erupción Volcánica	Una erupción volcánica puede causar daños significativos a la infraestructura debido a la emisión de cenizas, lava y flujo piroclástico. Además, las interrupciones en las comunicaciones y el transporte pueden dificultar el acceso y la operación de los laboratorios.
	Fenómenos Sísmicos	Los sismos representan un riesgo importante, ya que pueden causar daños en los equipos y la infraestructura, además de interrupciones en los servicios de energía y comunicaciones. Los laboratorios deben estar preparados para afrontar los efectos de temblores y posibles réplicas.
	Inundaciones por Condiciones Climáticas	Las inundaciones pueden dañar los equipos y las instalaciones de los laboratorios, además de interrumpir el suministro de energía y las comunicaciones. La pérdida de documentos y datos también podría ser una consecuencia. Se deben establecer medidas para prevenir y mitigar los efectos de las inundaciones.
Errores Técnicos	Incendios Inducidos por Acciones Humanas	Los incendios causados por errores humanos pueden destruir equipos, documentos y espacios físicos. Es esencial tener sistemas de detección y extinción de incendios, así como capacitar al personal en prácticas de seguridad y prevención.
Acciones No Autorizadas	Fallos Operativos Internos	Los fallos operativos internos, como la mala configuración de sistemas, pueden llevar a interrupciones y pérdida de datos. La capacitación constante del personal y la implementación de controles de calidad son fundamentales.
	Seguridad Cibernética	Los ciberataques pueden comprometer la seguridad de los sistemas, la integridad de los datos y la privacidad de la información. Implementar medidas de seguridad cibernética robustas, como firewalls, cifrado y sistemas de detección de intrusiones, es esencial para mitigar este riesgo.
Pérdida de Servicios Esenciales	Pérdida de Suministro de Energía	La interrupción del suministro eléctrico puede afectar gravemente la operación de los laboratorios. Se deben tener sistemas de respaldo, como generadores, para garantizar la continuidad de los servicios críticos durante cortes de energía.

Nota. Esta tabla organiza los riesgos identificados junto con sus descripciones correspondientes para una mejor comprensión de las amenazas potenciales que pueden afectar a los laboratorios.

Estrategias de recuperación de servicios e infraestructura tecnológica de soporte para proceso críticos

Estas estrategias son fundamentales para asegurar la continuidad del negocio ante posibles interrupciones o desastres que puedan afectar los sistemas y servicios tecnológicos.

La recuperación de servicios e infraestructura tecnológica de soporte para procesos críticos se refiere a un conjunto de métodos planificados y evaluados destinados a mantener o restablecer rápidamente las operaciones esenciales de una organización en caso de interrupciones graves, ya sean causadas por desastres naturales, fallas de sistemas, ciberataques u otras contingencias imprevistas. Estas estrategias buscan reducir el impacto de las interrupciones y garantizar la continuidad de los servicios esenciales para clientes y usuarios.

En el contexto de los procesos, estas estrategias se centran en la restauración de sistemas y datos después de eventos catastróficos como incendios o eventos sísmicos, entre otros. Implican la implementación de planes, infraestructuras y procedimientos que permitan una recuperación rápida de sistemas y aplicaciones esenciales.

Es importante destacar que la Recuperación de la Continuidad del Negocio (BCP) se encarga de mantener las operaciones esenciales en marcha durante y después de eventos disruptivos, abarcando no solo la tecnología, sino también la gestión de recursos humanos, comunicación, instalaciones y procesos.

Adicionalmente, el Punto de Recuperación Objetivo, mencionado previamente, se refiere al periodo máximo en el que se pueden perder datos durante una interrupción antes de que el impacto sea inaceptable. Esto nos permite definir dónde deben ubicarse los respaldos y la frecuencia de las copias de seguridad.

Tabla 38

Estrategias en Riesgos de Pérdida de Información

Pérdida de Información	Riesgo	Estrategias de Recuperación
En forma total	Eventos Naturales	Copia de Seguridad en Ubicación Remota: Mantener copias de seguridad periódicas de los datos en un lugar geográficamente separado de los laboratorios. Esto asegura que los datos estén protegidos incluso si ocurre un desastre localizado. Almacenamiento en la Nube: Utilizar servicios de almacenamiento en la nube para respaldar los datos críticos. Los proveedores de la nube generalmente cuentan con redundancia y medidas de seguridad que protegen los datos de pérdidas físicas. Soluciones de Replicación de Datos: Implementar soluciones de replicación de datos en tiempo real para mantener copias actualizadas de los datos en ubicaciones alternas. Restauración por Prioridad: Establecer una estrategia de restauración por prioridad, recuperando primero los datos más críticos para la continuidad de las operaciones.
	Errores Técnicos	Respaldo Fuera del Sitio: Mantener copias de seguridad en un lugar externo a los laboratorios para prevenir la pérdida de datos en caso de incendio en el lugar principal. Seguridad Física Mejorada: Implementar medidas de seguridad física, como sistemas de detección de incendios avanzados, extintores y sistemas de supresión de incendios, para minimizar el riesgo de incendios provocados por humanos. Seguridad de Acceso: Reforzar las políticas de seguridad de acceso a las instalaciones para reducir la posibilidad de acciones maliciosas. Registro de Actividades: Mantener registros detallados de las actividades de los usuarios y los sistemas para detectar y prevenir cualquier comportamiento anómalo. Pruebas de Recuperación: Realizar pruebas periódicas de recuperación de datos para garantizar que los procedimientos sean efectivos y que el personal esté capacitado para llevarlos a cabo.
En forma parcial	Acciones No Autorizadas	Sistemas de Monitorización y Detección de Intrusiones: Implementar soluciones de monitorización y detección de intrusos que alerten sobre actividades inusuales o no autorizadas en los sistemas y redes. Restauración Selectiva: Desarrollar procedimientos para la restauración selectiva de datos afectados por acciones no autorizadas, con el objetivo de minimizar el impacto y restaurar solo los componentes necesarios.

Pérdida de Información	Riesgo	Estrategias de Recuperación
		Cambio de Contraseñas y Restablecimiento de Credenciales: En caso de una violación de seguridad, cambiar contraseñas y restablecer credenciales para prevenir futuros accesos no autorizados. Actualizaciones de Seguridad: Mantener actualizados los sistemas y aplicaciones con parches de seguridad para mitigar vulnerabilidades conocidas.
	Pérdida de Servicios Esenciales	Generadores de Energía de Respaldo: Instalar generadores de energía de respaldo que puedan mantener los sistemas críticos en funcionamiento durante cortes de energía. Sistemas de UPS (Sistemas de Alimentación Ininterrumpida): Utilizar sistemas de UPS para proporcionar energía temporal a los equipos críticos en caso de cortes de energía. Planificación de Cargas de Energía: Establecer un plan para priorizar los sistemas y equipos críticos que necesitan energía durante un corte, asegurando que los recursos disponibles se utilicen de manera efectiva. Distribución de Energía Redundante: Implementar distribución de energía redundante para reducir la dependencia de una única fuente de energía. Respuesta ante Emergencias: Entrenar al personal en procedimientos de respuesta ante emergencias relacionadas con la pérdida de energía y cómo actuar para minimizar los impactos. Políticas de Ahorro de Energía: Implementar políticas de ahorro de energía en equipos y sistemas no esenciales para reducir la carga durante períodos de alta demanda.

Nota: Esta tabla detalla los riesgos de pérdida de información junto con las estrategias de recuperación correspondientes.

Tabla 39

Estrategias en riesgos de pérdida de servicios o recursos TI

Recursos Críticos	Riesgo	Estrategia de Recuperación
Intranet	Eventos Naturales	Mantener configuraciones de red documentadas y actualizadas en un lugar seguro. En caso de daños a la infraestructura, utilizar la documentación para reconfigurar rápidamente los dispositivos de red.
	Errores Técnicos	Implementar sistemas de respaldo de configuraciones de red y tener procedimientos para la restauración rápida de estas configuraciones en caso de cambios no autorizados o fallas.
	Acciones No Autorizadas	Implementar controles de acceso estrictos a los dispositivos de red. Utilizar sistemas de detección de intrusiones para identificar y responder a intentos de acceso no autorizados.

Recursos Críticos	Riesgo	Estrategia de Recuperación
Internet	Pérdida de Servicios Esenciales	Diseñar un plan de conmutación a redes de respaldo en caso de pérdida de energía eléctrica. Establecer políticas de priorización de tráfico para mantener la conectividad esencial.
	Eventos Naturales	Diversificar las conexiones a proveedores de Internet para asegurar redundancia en caso de interrupciones. Mantener una conexión de respaldo, como un proveedor móvil, para garantizar la continuidad.
	Errores Técnicos	Mantener equipos de red y sistemas de enrutamiento actualizados para minimizar las interrupciones debido a fallos técnicos. Tener contactos y contratos de soporte con los proveedores de servicios de Internet.
	Acciones No Autorizadas	Implementar sistemas de detección y prevención de intrusiones en la red para evitar ataques que puedan afectar la conectividad a Internet.
Equipos de Usuarios Finales	Pérdida de Servicios Esenciales	Establecer protocolos de conmutación automática a una conexión de respaldo (por ejemplo, un enlace móvil) en caso de pérdida de la conexión principal.
	Eventos Naturales	Mantener inventario actualizado de equipos y mantener copias de seguridad de las imágenes de sistema. Establecer procedimientos para la recuperación rápida en equipos de reemplazo.
	Errores Técnicos	Fomentar el almacenamiento de datos en servidores o sistemas compartidos en lugar de dispositivos individuales para minimizar la pérdida en caso de fallos. Implementar políticas de respaldo automatizado.
	Acciones No Autorizadas	Implementar soluciones de seguridad de endpoints que incluyan antivirus, antimalware y sistemas de detección de intrusiones. Restringir la instalación de software no autorizado.
Energía Eléctrica	Pérdida de Servicios Esenciales	Proporcionar sistemas de alimentación ininterrumpida (UPS) a equipos críticos. Establecer procedimientos de respuesta para el uso de dispositivos móviles en caso de cortes prolongados.
	Eventos Naturales	Mantener generadores de energía de respaldo y sistemas de alimentación ininterrumpida (UPS) para mantener activos los equipos y sistemas críticos durante cortes prolongados.
	Errores Técnicos	Realizar mantenimiento preventivo de sistemas eléctricos y equipos. Mantener documentación actualizada de los sistemas de energía para una restauración eficiente.
	Acciones No Autorizadas	Limitar el acceso físico a sistemas eléctricos solo al personal autorizado. Implementar sistemas de monitorización para detectar manipulaciones no autorizadas.
	Pérdida de Servicios Esenciales	Diseñar planes de respuesta para activar generadores y sistemas de UPS en caso de pérdida prolongada de energía. Establecer procedimientos para mantener equipos esenciales en funcionamiento.
	Eventos Naturales	Mantener copias actualizadas de las configuraciones del sistema y los datos de acceso. Establecer protocolos para restaurar rápidamente las configuraciones en caso de pérdida o daño.

Recursos Críticos	Riesgo	Estrategia de Recuperación
Sistema Soyal	Errores Técnicos	Mantener un respaldo de la base de datos del sistema en un servidor seguro. Realizar pruebas periódicas de restauración de datos para garantizar la recuperación efectiva.
	Acciones No Autorizadas	Implementar políticas de control de acceso y autenticación sólidas. Mantener registros de auditoría de actividades para rastrear cualquier acceso no autorizado.
	Pérdida de Servicios Esenciales	Alimentar el sistema Soyal con sistemas de UPS para mantener su funcionamiento en caso de cortes de energía. Tener un plan de respuesta para conmutar a modos de operación alternativos si es necesario.
	Eventos Naturales	Almacenar hojas de cálculo en sistemas de almacenamiento compartido o en la nube para minimizar la pérdida en caso de daño local. Establecer procedimientos para la restauración en nuevas ubicaciones.
Hojas de Cálculo	Errores Técnicos	Implementar sistemas de respaldo automático y frecuente de las hojas de cálculo. Educación sobre las prácticas de almacenamiento y respaldo de datos entre los usuarios.
	Acciones No Autorizadas	Controlar el acceso a hojas de cálculo mediante sistemas de autenticación y permisos. Mantener un registro de las ediciones y accesos a las hojas de cálculo.
	Pérdida de Servicios Esenciales	Utilizar sistemas de almacenamiento compartido o en la nube para permitir el acceso desde diferentes ubicaciones en caso de pérdida de energía eléctrica.
	Eventos Naturales	Mantener una copia de seguridad actualizada del sistema Acronis en un lugar seguro fuera de las instalaciones. Implementar políticas para la recuperación rápida del sistema en caso de desastre.
Sistema Acronis	Errores Técnicos	Establecer procedimientos para la reinstalación y configuración del sistema Acronis en caso de falla. Mantener una copia de las configuraciones y políticas personalizadas.
	Acciones No Autorizadas	Implementar medidas de seguridad para prevenir el acceso no autorizado al sistema Acronis. Mantener registros de actividades para identificar cambios no autorizados.
	Pérdida de Servicios Esenciales	Mantener el sistema Acronis en sistemas de alimentación ininterrumpida (UPS) para asegurar la continuidad de las operaciones.

Nota: La tabla detalla los recursos críticos, los riesgos asociados a cada uno de estos recursos y las estrategias de recuperación correspondientes.

Planificación Integral:

- Desarrollar un plan de recuperación detallado que abarque todos los aspectos clave de las operaciones, desde la tecnología hasta los recursos humanos y la comunicación.

- Identificar los procesos críticos y los sistemas que los respaldan para establecer prioridades claras en caso de interrupción.

Respaldos y Réplicas:

- Realizar respaldos regulares de datos y sistemas para asegurar una copia actualizada y segura disponible en caso de fallo.
- Implementar réplicas de sistemas y datos en ubicaciones fuera del sitio para garantizar la disponibilidad y reducir los tiempos de recuperación.

Infraestructura Redundante:

- Utilizar sistemas y servicios redundantes para minimizar el impacto de las interrupciones, incluyendo servidores en espejo y fuentes de energía alternativas.

Virtualización y Nube:

- La virtualización y la adopción de servicios en la nube permiten una rápida migración de sistemas y aplicaciones en caso de fallos, ya que pueden implementarse en diferentes ubicaciones con facilidad.

Pruebas y Simulacros:

- Realizar pruebas regulares de tus planes de recuperación para identificar debilidades y mejorar la eficiencia de los procedimientos.
- Organizar simulacros de interrupciones para entrenar al personal en la ejecución de las estrategias de recuperación.

Equipos de Respuesta a Incidentes:

- Establecer equipos específicos encargados de gestionar la recuperación en caso de interrupciones, definiendo roles y responsabilidades claras para cada laboratorista.

Seguridad y Protección:

- Incorporar medidas de seguridad sólidas para proteger los sistemas y los datos durante y después de una interrupción, como detección de intrusiones, cortafuegos y análisis de vulnerabilidades.

Monitorización Continua:

- Implementar herramientas de monitorización que te permitan supervisar constantemente la salud de tus sistemas y detectar cualquier signo de problemas antes de que se conviertan en interrupciones mayores.

Capacitación del Personal:

- Asegura que tu equipo esté capacitado en los procedimientos de recuperación y sepa cómo actuar en caso de una interrupción.

Es crucial revisar y actualizar periódicamente las estrategias de recuperación para reflejar cambios en la infraestructura tecnológica, procesos y riesgos emergentes. Estas estrategias involucran una combinación de tecnología, planificación y acción coordinada para minimizar los tiempos de inactividad y los impactos negativos en el negocio.

Pruebas y Capacitaciones

Durante las pruebas realizadas en el laboratorio DCCO para la gestión y mantenimiento de equipos, se realizaron actividades para evaluar la efectividad y la adecuación de los procedimientos establecidos en el manual. Este análisis proporciona información valiosa sobre los tiempos de ejecución actuales y destaca áreas que pueden beneficiarse de mejoras para aumentar la eficacia de los procesos y, por ende, fortalecer el Plan de Recuperación ante Desastres (DRP). A continuación, se presenta un análisis de estas pruebas:

Tabla 40

Estrategias de Recuperación para la Gestión de Mantenimiento de Equipos de Laboratorio

Gestión de Mantenimiento de Equipos de Laboratorio				
Estrategia	**Riesgos**	**Objetivos**	**Pasos**	**Resultados**
ER1/ER2	Pérdida de información en los equipos de laboratorio.	1. Validar la efectividad de los procedimientos de mantenimiento preventivo y correctivo para garantizar la integridad y disponibilidad de los datos almacenados en los equipos de laboratorio. 2. Validar la eficacia de los procedimientos de mantenimiento para asegurar la disponibilidad y	1. Realizar un recorrido para identificar y documentar todos los equipos informáticos en cada bloque. 2. Registrar los detalles importantes de cada equipo, como marca, modelo y estado. 3. Mantener un registro de todas las partes recibidas para mantenimiento correctivo. 4. Asegurarse de mantener actualizada la información sobre las piezas utilizadas en cada intervención. 5. Identificar y determinar si los equipos no utilizados deben ser dados de baja o reasignados. 6. Crear tickets de soporte para problemas que requieran la intervención de la Unidad de Tecnologías de la Información y Comunicaciones (UTICs).	1. Se verificó el inventario detallado de los equipos informáticos por bloque, asegurando un seguimiento preciso de su estado y ubicación. 2. Se gestionaron eficientemente las partes y piezas para el mantenimiento correctivo, con una adecuada documentación de los recursos utilizados. Se identificaron los tiempos de mantenimiento y se llevaron registros tanto de cada equipo como de los equipos por bloques. 3. Se generaron tickets de soporte para problemas específicos, garantizando una respuesta rápida ante incidencias.

Gestión de Mantenimiento de Equipos de Laboratorio				
Estrategia	**Riesgos**	**Objetivos**	**Pasos**	**Resultados**
		funcionamiento óptimo de los servicios y recursos tecnológicos en los laboratorios.	7. Inspeccionar y corregir problemas de conectividad o rendimiento en la red de datos. 8. Verificar el funcionamiento correcto de los equipos. 9. Realizar la limpieza y pruebas de encendido. 10. Preparar los equipos para el período académico mediante clonación de discos duros. 11. Documentar todas las actividades de mantenimiento realizadas. 12. Reportar fallas eléctricas a la unidad de desarrollo físico si es necesario.	4. Se realizó el mantenimiento preventivo según normas establecidas, asegurando el correcto funcionamiento de los equipos. 5. Se documentaron exhaustivamente todas las actividades realizadas durante el proceso. 6. Estos resultados demuestran el compromiso con la continuidad operativa de los laboratorios y el óptimo rendimiento de los equipos.

Nota. Las pruebas realizadas permitieron validar la efectividad y la adecuación de los procedimientos establecidos en el manual de gestión y mantenimiento de equipos en los laboratorios del DCCO. Se identificaron áreas de mejora y se tomaron acciones para garantizar un proceso eficiente y confiable en el mantenimiento de la infraestructura tecnológica.

Figura 3

Prueba de Gestión de Mantenimiento de Equipos

Nota. La imagen muestra el proceso de la gestión de mantenimiento de quipos del laboratorio. Fuente propia.

Tabla 41

Estrategias de recuperación para la Gestión de Registro y Monitoreo para Reservas de Laboratorio

Gestión de Registro y Monitoreo para Reservas de Laboratorio	
Aspecto	**Descripción**
Objetivo	Garantizar la asignación eficiente de los espacios de laboratorios mediante un sistema de reserva basado en una plataforma web accesible.
Fundamento	Basado en un proyecto de titulación previamente desarrollado.
Estado actual	En proceso de implementación.
Responsable	Jefe de Laboratorios del Departamento de Ciencias de la Computación (DCCO).
Acceso al sistema	A través de un navegador web.
Funcionalidad	Visualizar la disponibilidad de los laboratorios en tiempo real y realizar reservas según necesidades académicas.
Requisitos	Obligatorio contar con el carnet de identificación del estudiante que incluya su ID y cédula de identidad para efectuar una reserva.

Nota. La tabla describe varios aspectos relacionados con la implementación de la plataforma para la gestión de registro y monitoreo para reservas de laboratorio

Tabla 42

Estrategias de recuperación para la Gestión de Control de Acceso

Gestión de Control de Acceso				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
ER1	Pérdida de Información	1. Garantizar la integridad y seguridad del control de acceso durante eventos de desastre. 2. Identificar posibles vulnerabilidades en el sistema que puedan afectar la capacidad de recuperación del laboratorio ante un desastre.	1. Verificar la disponibilidad y adecuación de los recursos necesarios. 2. Acceder al sistema servidor y cliente utilizando el programa 701Client. 3. Editar, crear o modificar puertas y grupos de puertas según la necesidad. 4. Crear usuarios, asignando IDs únicos y configurando sus permisos de acceso. 5. Enviar la información de los usuarios a los relojes biométricos. 6. Acceder al servidor 701 y realizar las configuraciones necesarias.	1. Se confirma que el sistema es capaz de preservar la integridad de la información durante eventos críticos, cumpliendo así con el objetivo de garantizar la seguridad del control de acceso. 2. La prueba exitosa indica una fortaleza del sistema en términos de preservar la información durante eventos críticos. 3. No se identifican vulnerabilidades significativas en el sistema que comprometan su capacidad de recuperación ante desastres, lo que sugiere una adecuada preparación y robustez del sistema de control de acceso.

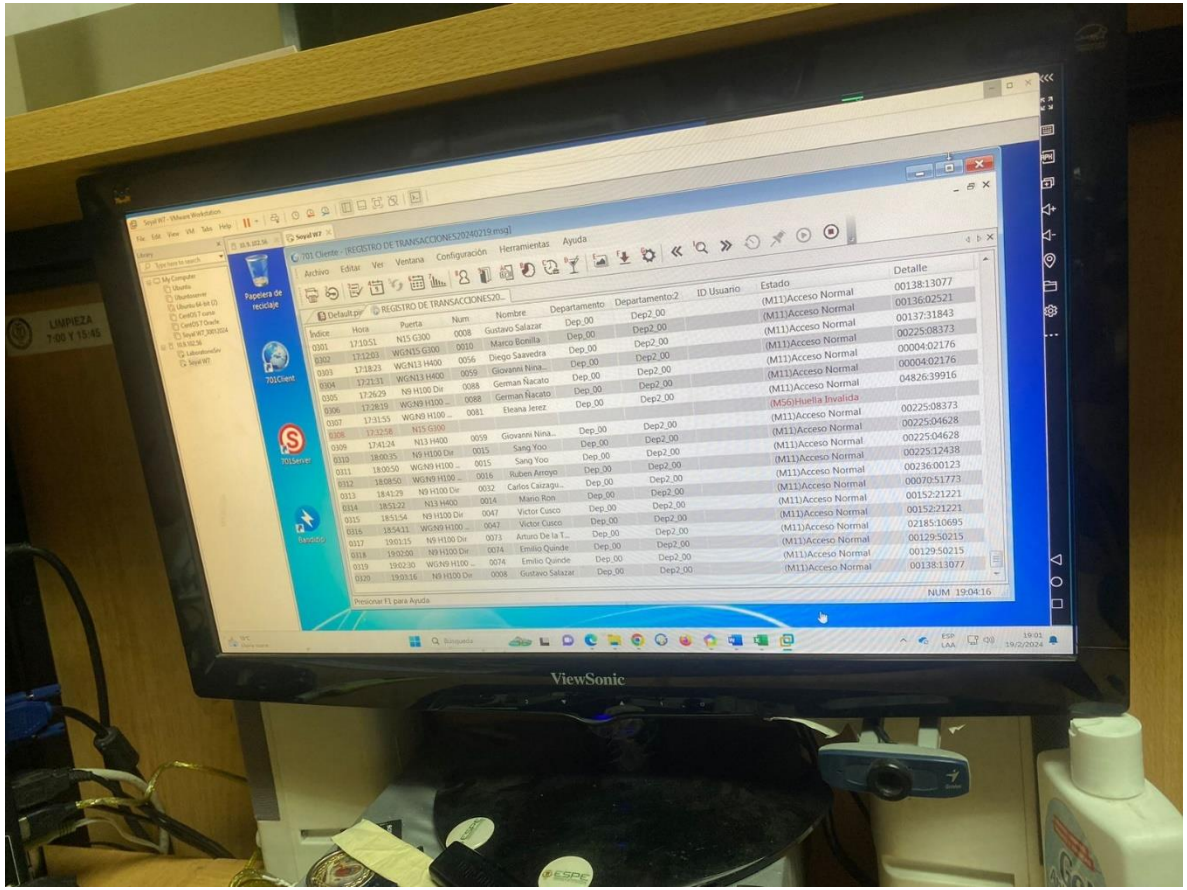
Gestión de Control de Acceso				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
			7. Verificar el estado de los nodos y biométricos para asegurar su correcto funcionamiento. 8. Registrar el ingreso utilizando tarjetas o TAGs biométricos en los lectores correspondientes. 9. Verificar que el registro de acceso se realice sin inconvenientes. 10. Confirmar que los datos se registren correctamente en el sistema.	
ER2	Pérdida de Servicios o Recursos TI	1. Evaluar la capacidad del sistema Soyal para mantener la integridad y seguridad del control de acceso en situaciones adversas.	1. Verificar el estado de los equipos tras la baja de energía. 2. Restablecer el suministro eléctrico. 3. Encender los equipos afectados. 4. Reiniciar el sistema. 5. Comprobar la integridad de los registros de acceso.	1. Se verificó el estado de los equipos afectados y se procedió a restablecer el suministro eléctrico. Posteriormente, se encendieron los equipos y se reinició el sistema para asegurar su correcto funcionamiento. Se comprobó la integridad de los registros de acceso y se realizaron pruebas para registrar el acceso al

Gestión de Control de Acceso				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
			6. Realizar pruebas de acceso y registrar con normalidad un acceso al laboratorio. 7. Registrar cualquier incidente relacionado con la baja de energía.	laboratorio, confirmando que el sistema estaba operativo. 2. En caso de futuras situaciones similares, es importante mantener un protocolo claro para manejar eventos de baja de energía de manera eficiente y minimizar cualquier impacto en las operaciones del laboratorio.

Nota. Los resultados de las pruebas realizadas en el proceso de Gestión de Control de Acceso en el Laboratorio DCCO permitieron confirmar la efectividad y fiabilidad del sistema Soyal en la gestión del control de acceso, tanto en la preservación de la integridad de la información como en la continuidad de los servicios y recursos de tecnología de la información.

Figura 4

Prueba de Gestión de Control de Acceso



Nota. La imagen muestra el sistema Soyal utilizado para la gestión de Control de Acceso de los Laboratorios. Fuente propia

Tabla 43

Estrategias de recuperación para la Gestión del Sistema de Vigilancia.

Gestión del Sistema de Vigilancia				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
ER1	Pérdida de información debido a fallos en la vigilancia o registro de actividades.	1. Garantizar la trazabilidad y la seguridad de los espacios de laboratorio. 2. Mantener un registro preciso de las actividades realizadas.	1. Conexión al procesador de señal: Se establece la conexión al procesador de señal desde el cuarto de comunicaciones hacia un monitor en la oficina para la visualización de las cámaras de seguridad. 2. Revisión de conexiones y canales: Se revisan las conexiones existentes, incluyendo los canales de las aulas de cada piso, donde se muestra la fecha y hora de cada evento o escenario registrado. 3. Conexión por punto de red: Se intenta realizar la conexión mediante el punto de red correspondiente, dado que cada	1. Durante las pruebas, se constató que el sistema de video vigilancia basado en los DVRs de la serie DX4800 es confiable para el control de incidentes en los Laboratorios del Departamento de Computación. Los equipos están correctamente configurados y accesibles para cada bloque, permitiendo una supervisión efectiva de los eventos en diferentes franjas horarias. No se identificaron fallos significativos en su funcionamiento, demostrando así su eficacia en la gestión de la seguridad y el control de los Laboratorios Generales de Computación de la Universidad de las Fuerzas Armadas ESPE. 2. Además, es importante destacar que, durante la gestión de incidentes, se asegura que la información de las

Gestión del Sistema de Vigilancia				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
			bloque tiene una dirección IP asignada para la gestión de red.	grabaciones de las cámaras de seguridad no se pierda. En caso de necesidad, se puede acceder a las grabaciones a través del procesador de señal, lo que proporciona una herramienta adicional para la revisión y análisis de eventos pasados. Esto contribuye a mantener un registro completo de la actividad en los laboratorios y facilita la investigación de incidentes específicos.
ER2	Interrupción del servicio de vigilancia debido a fallos en los dispositivos o sistemas.	1. Mantener la continuidad del servicio de vigilancia de laboratorios ante posibles fallos o interrupciones.	1. Intento de acceso al navegador mediante la conexión IP: 2. Se intentó acceder al navegador utilizando la conexión IP estándar. 3. En caso de fallar el acceso, se activó el protocolo establecido para situaciones de este tipo.	1. Durante las pruebas realizadas, se confirmó que el sistema de vigilancia de los laboratorios está equipado con mecanismos de redundancia y respaldo efectivos. Esto asegura la continuidad del servicio incluso en situaciones de fallos en uno de los DVRs, demostrando la eficacia de los equipos de respaldo para mantener la funcionalidad del sistema. Este hallazgo respalda la

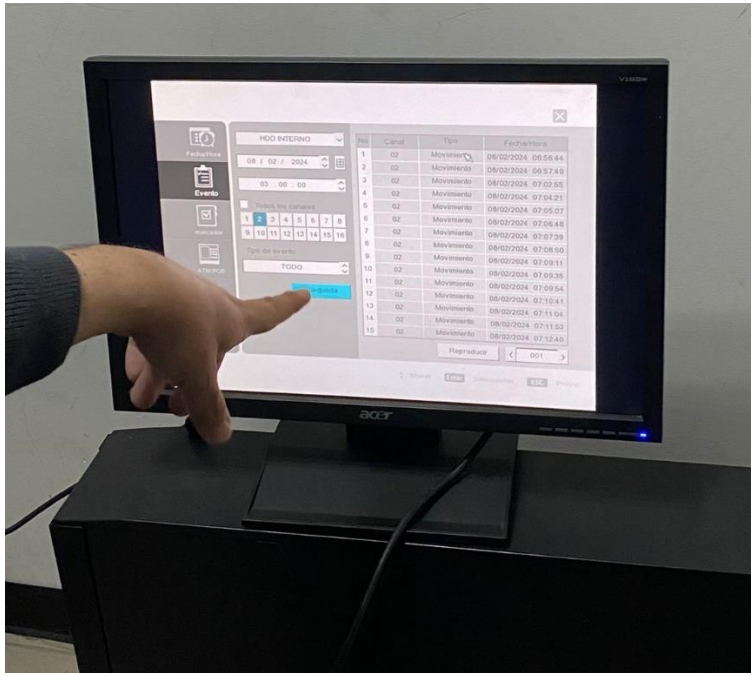
Gestión del Sistema de Vigilancia				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
			4. Se solicitó autorización al jefe de DCCO para realizar una revisión más detallada. 5. Ante la imposibilidad de acceder al navegador por este medio, se procedió con la siguiente acción. 6. En caso de cortes eléctricos, bajas de voltaje o variaciones, se identificaron inmediatamente. • Se procedió a desconectar y reconectar los equipos afectados para restablecer el suministro eléctrico. • Esta acción se realizó manualmente para asegurar una restauración segura del sistema.	garantía de seguridad y control en los Laboratorios Generales de Computación de la Universidad de las Fuerzas Armadas ESPE. 2. Además, se mantuvo una atención constante en asegurar la continuidad de la grabación de las cámaras de seguridad durante todo el proceso de gestión de incidentes. Se verificó que las grabaciones no se vieran afectadas por cortes de energía u otros fallos en el sistema. Esta medida estratégica aseguró que el servicio de vigilancia permaneciera operativo sin interrupciones significativas, proporcionando una cobertura continua de seguridad en los laboratorios.

Nota: Las pruebas realizadas para el Sistema de Gestión de Vigilancia de Laboratorios DCCO demostraron la efectividad y la fiabilidad del sistema en garantizar la trazabilidad, la seguridad y el control de los espacios de laboratorio. Tanto las estrategias para mitigar riesgos de pérdida de información como las de pérdida de servicios o recursos de TI resultaron satisfactorias, confirmando la adecuación de los procedimientos establecidos. La implementación de mecanismos de redundancia y respaldo garantizar la

continuidad del servicio incluso en situaciones adversas, lo que contribuye a mantener un entorno seguro y controlado en los Laboratorios Generales de Computación de la Universidad de las Fuerzas Armadas ESPE”.

Figura 5

Gestión del Sistema de Vigilancia.



Nota. Realización de la prueba de Gestión de Vigilancia. Fuente propia.

Tabla 44

Estrategias de recuperación para la Gestión del Centro de Datos (Data Center)

Gestión del Centro de Datos (Data Center)				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
ER1	Interrupción del suministro eléctrico	1. Validar la eficacia del protocolo de respuesta ante fallos de energía eléctrica.	1. Notificación de fallos de energía al departamento de Seguridad Física. 2. Evaluación inicial para determinar la causa del fallo (interna o externa). 3. Activación del protocolo para la corrección del fallo por parte del electricista designado. 4. Puesta en marcha del protocolo para activar la planta de energía si es necesario. 5. Notificación al proveedor de servicios de red en caso de problemas de conectividad. 6. Verificación del funcionamiento de sistemas y equipos tras la restauración del suministro eléctrico.	1. Validación de la eficacia del protocolo de respuesta ante fallos de energía eléctrica. 2. Garantía de la continuidad operativa de los sistemas críticos. 3. Minimización del impacto de las interrupciones en las actividades del DCCO.
ER2	Interrupción de la conectividad de red	1. Validar la eficacia del protocolo de respuesta ante problemas de conectividad.	1. Notificación de problemas de conectividad al Departamento de UTICS. 2. Contacto con el proveedor de servicios de red para diagnosticar y resolver el problema. 3. Verificación del restablecimiento de la conectividad de red.	1. Validación del protocolo de respuesta ante problemas de conectividad de red. 2. Rápida resolución de problemas de conectividad para minimizar el impacto

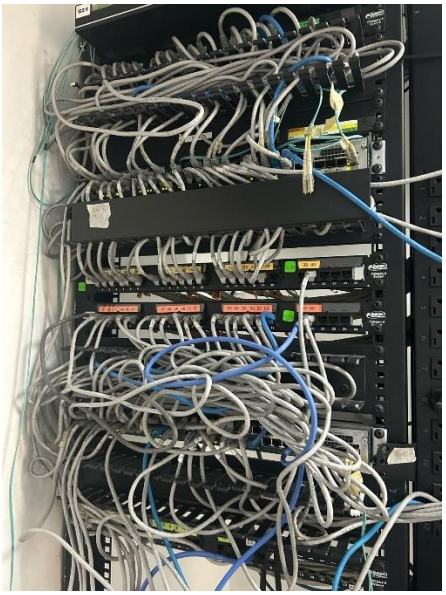
Gestión del Centro de Datos (Data Center)				
Estrategia	**Riesgo**	**Objetivos**	**Pasos**	**Resultados**
			4. Inspección detallada para detectar posibles daños o fallos causados por la interrupción eléctrica. 5. Restablecimiento del control de acceso a los laboratorios.	en las operaciones del Centro de Datos. 3. Garantía de la integridad y estabilidad de las operaciones del Data Center.

Nota. La prueba de gestión del Centro de Datos se centra en garantizar una respuesta eficaz y coordinada ante situaciones de fallo de energía eléctrica, con la colaboración activa del departamento de Seguridad Física y UTICS. Este proceso asegura la continuidad operativa de los sistemas críticos alojados en el Data Center y minimizar el impacto de las interrupciones en las actividades de los laboratorios del DCCO.

Se realizó el plan de capacitación que se encuentra en el Apéndice 4, dirigido a los Ingenieros Laboratoristas, donde se indicó todos los procesos del DRP y las estrategias de recuperación que se deben seguir en el caso de que ocurra algún incidente en los Laboratorios del Departamento de Ciencias de la Computación, el Jefe de Laboratorios, supo mencionar que se está trabajando en “Mi Bitácora” para la automatización de registros de asistencia y de ingreso a los laboratorios, también se esta llevando a cabo una reforma de mejora de la infraestructura de red para una mayor organización en cuanto al cableado, como se puede observar en la figura 6 y figura 7.

Figura 6

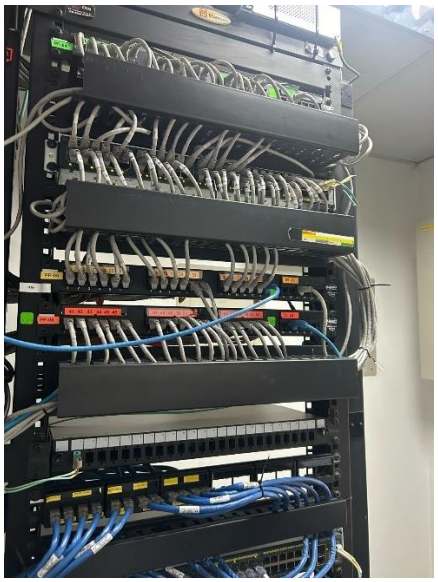
Infraestructura de red



Nota. La imagen muestra la infraestructura de red antes.

Figura 7

Infraestructura de red



Nota. La imagen muestra cómo se mejoró la infraestructura de red.

Vigencia

El Plan de Recuperación de Desastres (DRP) de los Laboratorios del Departamento de Ciencias de la Computación de Universidad de las Fuerzas Armadas “ESPE” se basa en las directrices de la norma ISO 24762, asegurando su vigencia y relevancia a lo largo del tiempo. Con una duración inicial de tres años desde su aprobación, este plan se activa inmediatamente después de ser aprobado.

Para garantizar su efectividad y capacidad de adaptación a los cambios en el entorno operativo, se realizan revisiones exhaustivas anuales durante todo el período de vigencia del plan. Estas revisiones incluyen una evaluación detallada de los procedimientos y protocolos establecidos, así como una valoración de la capacidad de respuestas ante distintos escenarios de desastre. También se verifica la disponibilidad de los recursos necesarios para la ejecución efectiva del plan.

En caso de detectarse cambios significativos en el entorno operativo o en los riesgos potenciales, se llevan a cabo evaluaciones adicionales fuera del período de revisión anual. Estas evaluaciones adicionales garantizan que los Laboratorios del DCCO estén preparados para enfrentar cualquier tipo de desastre, incluso si se producen cambios inesperados entre las revisiones programadas.

La combinación de una duración de tres años y revisiones anuales permite a los Laboratorios del DCCO mantener un nivel óptima de preparación ante posibles desastres. Esto asegura la protección de la continuidad de las operaciones y el adecuado desarrollo de las actividades educativas y científicas, proporcionando seguridad y tranquilidad a toda la comunidad universitaria.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

Después de finalizar esta investigación, podemos afirmar en términos generales que hemos logrado alcázar el objetivo principal que nos propusimos. Implementar un Plan de Recuperación ante Desastres (DRP) en los laboratorios del DCCO de la ESPE, adoptando la norma ISO 22301, ofreciendo beneficios sustanciales en la continuidad operativa. Al estandarizar los procesos de recuperación ante diversos escenarios, como fallos de hardware o cortes de energía, se asegura una respuesta ágil y eficaz. Esto minimiza cualquier impacto negativo en las actividades académicas, garantizando la disponibilidad constante de los recursos esenciales para los estudiantes.

La identificación de activos críticos y la implementación de medidas según la ISO 22301 aseguran la protección y preservación de los recursos académicos y científicos en los laboratorios de DCCO. Esta protección no solo abarca los activos materiales, como equipos y sistemas, sino también el conocimiento generado en estos entornos, lo que contribuye a la reputación y competitividad de la universidad.

El reconocimiento del papel crucial del personal en la respuesta ante desastres es fundamental. La participación activa de los ingenieros laboratoristas, con su experiencia y conocimiento, es esencial para ejecutar adecuadamente el plan de recuperación. Por lo tanto, la capacitación continua y el compromiso del personal son aspectos cruciales para fortalecer la resiliencia de los laboratorios del DCCO frente a desastres.

A través de la revisión periódica de procesos, pruebas y la identificación de áreas de mejora, se puede perfeccionar continuamente el DRP. Esta mentalidad de mejora continua garantiza que los laboratorios estén siempre preparados para enfrentar desafíos y mantener su funcionamiento óptimo en cualquier circunstancia.

Recomendaciones

Después de analizar detenidamente los resultados obtenidos en el proceso de investigación, se han formulado las siguientes recomendaciones para mejorar la preparación y la respuesta ante desastres en los laboratorios del Departamento de Ciencias de la Computación (DCCO) de la universidad de las Fuerzas Armadas “ESPE”:

- Es importante llevar a cabo una revisión y actualización regular del DRP para garantizar su relevancia y eficiencia frente a los cambios en la infraestructura, tecnología y procesos del DCCO. Esto incluye la incorporación de nuevas soluciones tecnológicas y la alineación con las necesidades actuales de los laboratorios.
- Implementar una estrategia de sensibilización y capacitación continua para todo el personal del DCCO sobre la importancia del DRP y su papel en la respuesta ante desastres. Esto asegurará que todos estén familiarizados con los procedimientos de emergencia y puedan actuar de manera efectiva en caso de una situación crítica.
- Es fundamental llevar a cabo simulacros y pruebas periódicas de recuperación ante desastres para evaluar la eficacia del DRP y el nivel de preparación del personal. Estas actividades permitirán identificar áreas de mejora y corregir posibles deficiencias en los procedimientos de respuesta.
- Se debe considerar la mejora de la infraestructura, como la implementación de soluciones de almacenamiento en la nube para el Data Center, y así garantizar la protección y recuperación segura de la información en caso de desastres.

Bibliografía

Abad, P. (2019). El Cuadro de Mando Integral Aplicado a la Planificación Estratégica de la Banca Privada. []. *Revista Ciencia UNEMI*, 20-35. doi:https://doi.org/10.29076/issn.2528-7737vol12iss29.2019pp20-35p

Anggraini, P., Kurniawan, R., Eko, R., Pardamean, B., Yuniarto, B., & Sukim. (2019). Biclustering Method to Capture the Spatial Pattern and to Identify the Causes of Social Vulnerability in Indonesia: A New Recommendation for Disaster Mitigation Policy. *ScienceDirect*, 31-37. Obtenido de https://www.sciencedirect.com/science/article/pii/S1877050919310567

Arévalo, L. P., Fernández, E. N., & Zambrano, Á. P. (2016). *Diseño del plan de recuperación de desastres (D.R.P.) para la Compañía Agencia de Aduanas Profesional nivel 1 SIAP sede Bogotá. [Trabajo de grado - Especialización. Universidad Católica de Colombia - RIUCaC].* Repositorio Institucional. Obtenido de http://hdl.handle.net/10983/13914

Ati, 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 22301, PARA EL CENTRO DE PROCESAMIENTO DE DATOS (CPD). [Trabajo de Titulación. Universidad Politécnica Salesiana Sede Quito].* Repositorio Institucional de la Universidad Politécnica Salesiana. Obtenido de https://dspace.ups.edu.ec/handle/123456789/15904

Barragán, L. F., & Puentes, Y. (2016). *Propuesta para el diseño del plan de recuperación de desastres. Caso Unidad Administrativa de Catastro Distrital UAECD. [Trabajo de grado - Especialización. Universidad Católica de Colombia - RIUCaC].* Repositorio Institucional. Obtenido de http://hdl.handle.net/10983/14044

Bonifaz, L. E., & Pomaquero, J. C. (2018). PLANIFICACIÓN ESTRATÉGICA Y GESTIÓN PÚBLICA POR OBJETIVOS: CASO DE ESTUDIO GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN PENIPE – CHIMBORAZO – ECUADOR. *Caribeña de Ciencias Sociales*.

Budiman, K. (2020). Disaster recovery planning with distributed replicated block. *ResearchGate*. doi:10.1088/1742-6596/1567/3/032023

Castaño, M. A., & Garzón, C. C. (2015). *DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES EN EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA FUNDACIÓN NEUMOLÓGICA COLOMBIANA [Proyecto de grado. Fundación Universitaria los Libertadores].* Repositorio institucional. Obtenido de http://hdl.handle.net/11371/309

Contreras, R. X. (2020). *Análisis comparativo de la norma 410 de control interno de la Contraloría General del Estado con COBIT5. [Trabajo de titulación. Universidad Catolica de Cuenca].* Repositorio institucional. Obtenido de https://dspace.ucacue.edu.ec/handle/ucacue/10284

Dhanujati, N., & Suganda , A. (2018). Data Center-Disaster Recovery Center (DC-DRC) for High Availability IT Service. *IEEE Xplore*. doi:10.1109/ICIMTech.2018.8528170

Gamboa, J. P., & Giraldo, E. H. (2016). *Plan de Recuperación de Desastres (DRP) Informáticos, en la Fase de Análisis de Impacto para una Empresa Petrolera. [Trabajo de grado. Universidad Piloto de Colombia].* Repositorio Institucional. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/2730

Gordon, A., & Salazar, G. (2020). DRP Analysis: Service Outage in Data Center due to Power Failures. [Proyecto de grado.]. *IEEE*. doi:10.1109/IEMCON51383.2020.9284920

Herrada, M. J. (2018). *Diseño y aplicación de un plan de recuperación ante desastres (DRP) en un centro de datos para empresas financieras basado en la norma ISO/IEC 22301. [Tesis de Maestria. Universidad Ricardo Palma].* Repositorio Institucional. Obtenido de https://hdl.handle.net/20.500.14138/1639

Jaime, L., & Barata, J. (2023). How can FLOSS Support COBIT 2019? Coverage Analysis and a Conceptual Framework. *ScienceDirect*, 680-687.

Khairur , R., & Benfano , S. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, 383-404. doi:https://doi.org/10.1016/j.eij.2022.03.001

Lopez, Á. V., Cubillos, E. R., & Casas, E. (2018). *Planeación para el diseño e implementación de un plan de recuperación de desastres (drp) para una entidad financiera. [Tesis de tercer nivel, Institución Universitaria Politécnico Grancolombiano].* Sistema NAcional de Bibliotecas SISNAB. Obtenido de http://hdl.handle.net/10823/1230

Maravi, G. R., Ñiquen, N. O., & Primo, J. P. (2015). *Diseño de un Plan De Recuperación Ante Desastres (DRP) para un centro de datos de una droguería [Tesis de Ingenieria, Universidad Periana de Ciencias Aplicadas.* Repositorio Institucional. Obtenido de http://hdl.handle.net/10757/668018

Nieto, B. V. (2015). *Análisis y evaluación para el diseño de un plan de recuperación ante desastres (DRP) aplicado en un centro de datos para empresas municipales basado en la norma ISO/IEC 24762:2008 [Proyecto de titulación. Universidad Politécnica Salesiana Sede Guayaquil].* Repositorio Institucional de la Universidad Politécnica Salesiana. Obtenido de https://dspace.ups.edu.ec/handle/123456789/10303

Pin, Y. I. (2018). *Análisis de procesos críticos para la elaboración de un BIA en la Empresa Mafelesa. [Trabajo de Titulación. Universidad de Guayaquil].* Repositorio institucional. Obtenido de http://repositorio.ug.edu.ec/handle/redug/36277

Pitta, S. T. (2018). *Diseño de un plan de contingencia informático basado en las normas ISO/IEC 22301 e ISO/IEC 27031 para la Ferretería Cesar S.A.S en la ciudad de Valledupar. [Tabajo de titulación. Universidad Nacional Abierta y a Distancia UNAD].* Repositorio de la institución. Obtenido de https://repository.unad.edu.co/handle/10596/21434

Rivas, K. S., & Salazar, G. D. (2019). Diseño de Plan de Recuperación de Desastres con base a la norma NIST 800-34 y al marco de PMBOK para una empresa aseguradora ecuatoriana. *Latin-American Journal of Computing*, 53-52.

Rodríguez, S. J. (2011). *Análisis y diseño de un plan de recuperación de desastres (DRP) para el centro de datos de la empresa promotora superior S.A. durante el segundo semestre del 2011. [Trabajo de grado - Pregrado. Universidad de la Costa].* Repositorio de la institución. Obtenido de http://hdl.handle.net/11323/1171

Romero, Y. A. (2014). *GUÍA GENERAL PARA LA ELABORACIÓN DE PLANES DE RECUPERACIÓN DE DESASTRES DESDE EL PMI EN LAS ÁREAS DE TECNOLOGÍA INFORMÁTICA DE LAS EMPRESAS PEQUEÑAS Y MEDIANAS EN BOGOTA D.C. [Tesis de Maestria. Universidad de la Salle].* Repositorio de la institución. Obtenido de https://ciencia.lasalle.edu.co/maest_ingenieria/10

Rosado , D., Moreno, J., Sanchez, L., Santos, A., Serrano, M., & Fernández, E. (2021). MARISMA-BiDa pattern: Integrated risk analysis for big data. *ScienceDirect*. doi:https://doi.org/10.1016/j.cose.2020.102155

Sanabria, C. (2020). *Diseño e implementación de un plan de recuperación de desastres para garantizar el funcionamiento de los servicios tecnológicos de la empresa CS&C Technology. [Trabajo de grado - Pregrado. Fundación Universitaria del Área Andina].* Repositorio Institucional Areandina. Obtenido de https://digitk.arandina.edu.co/handle/arandina/4418

Vásquez, W. M. (2017). *Propuesta de un método para elaborar un plan de recuperación de desastres (DRP) en el Área de tecnología de la información para Cooperativas de Ahorro y Crédito del Ecuador. [Tesis de Maestria. Escuela Superior Politécnica de Chimborazo].* Repositorio de la institución. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/6753

Apéndices