UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE COMPUTACIÓN

DESARROLLO DEL PLAN DE CONTINUIDAD DE NEGOCIO DE ACUERDO A LOS ESTÁNDARES VIGENTES, PARA EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN, DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTOR: MATEO SEBASTIAN SANTOS ROCHA

TUTOR: JORGE ENRIQUE LÓPEZ LOGACHO

Quito - Ecuador
2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Mateo Sebastian Santos Rocha con documento de identificación N° 1723726475 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 22 de julio del año 2024

Atentamente,

Mateo Sebastian Santos Rocha

1723726475

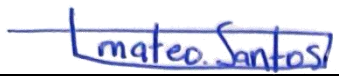
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Mateo Sebastian Santos Rocha con documento de identificación No. 1723726475, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto Técnico: "Desarrollo del plan de continuidad de negocio de acuerdo a los estándares vigentes, para el data center de la carrera de computación, de la Universidad Politécnica Salesiana, Sede Quito", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 22 de julio del año 2024

Atentamente,



Mateo Sebastian Santos Rocha

1723726475

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Jorge Enrique López Logacho con documento de identificación N° 1712082484, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DESARROLLO DEL PLAN DE CONTINUIDAD DE NEGOCIO DE ACUERDO A LOS ESTÁNDARES VIGENTES, PARA EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN, DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO, realizado por Mateo Sebastian Santos Rocha con documento de identificación N° 1723726475, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 22 de julio del año 2024

Atentamente,

Ing. Jorge Enrique López Logacho, MSc.

1712082484

DEDICATORIA

A mi madre, por brindarme los medios y recursos necesarios, por su amor incondicional, su inquebrantable apoyo en cada etapa de mi vida y por enseñarme los valores que ahora me definen y guían mi camino; a mis amigos, por estar presentes en cada situación y ser personas increíbles; y a mis profesores, por haber inculcado en mí un creciente interés por el aprendizaje.

AGRADECIMIENTO

Agradezco a mi madre por haber sido aquella persona que me guió por un camino difícil, por iluminar cada situación mala que nublaba mi progreso, y por impulsar con amor mi ánimo y espíritu. A mis abuelitos, por haber cuidado de mí y por estar siempre presentes. A mis amigos, que con risas y buenos momentos cambiaron el ambiente de los malos momentos y generaron recuerdos inolvidables. A todas las personas que conforman mi vida, por enseñarme cosas nuevas que, indirectamente, me guiaron al camino en el que hoy me encuentro, agradecido por haberlo experimentado.

ÍNDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

Desarrollo de un plan de continuidad de negocio (BCP) conforme a las normas ISO 22301, COBIT y ITIL, enfocado en el Data Center de la carrera de Computación de la Universidad Politécnica Salesiana. El BCP incluye un análisis de impacto al negocio (BIA) que detalla los incidentes ocurridos desde el periodo 54 hasta el 63, evaluando riesgos, vulnerabilidades y amenazas lógicas, físicas y factor humano mediante una escala de criticidad calculada matemáticamente. Esta evaluación facilita la valoración de activos críticos y la determinación de tiempos objetivo de recuperación (RTO) y punto objetivo de recuperación (RPO), asegurando así la preparación ante posibles incidentes.

Dentro del plan, se reconocen y documentan los roles y responsabilidades específicos de cada miembro del Data Center, estructurando las funciones necesarias para la ejecución efectiva del plan. Esto incluye la asignación de tareas según la metodología RACI, asegurando una distribución equitativa de responsabilidades y garantizando la coordinación durante incidentes.

Adicionalmente, se establece un programa de mantenimiento regular para los planes de BCP, DRP y CP, con el fin de identificar y corregir áreas que puedan requerir ajustes o mejoras, para fortalecer la resiliencia del Data Center, además optimiza la respuesta ante incidentes, minimizando así el impacto operativo y la disponibilidad de los servicios de virtualización y almacenamiento.

Palabras clave: plan de continuidad de negocio, análisis de impacto al negocio, tiempo objetivo de recuperación.

ABSTRACT

Development of a business continuity plan (BCP) in accordance with ISO 22301, COBIT and ITIL standards, focused on the Data Center of the Computing degree at the Salesiana Polytechnic University. The BCP includes a business impact analysis (BIA) that details the incidents that occurred from period 54 to 63, evaluating risks, vulnerabilities and logical, physical and human factor threats using a mathematically calculated criticality scale. This evaluation facilitates the assessment of critical assets and the determination of recovery time objective (RTO) and recovery point objective (RPO), thus ensuring preparation for possible incidents.

Within the plan, the specific roles and responsibilities of each member of the Data Center are recognized and documented, structuring the functions necessary for the effective execution of the plan. This includes assigning tasks according to the RACI methodology, ensuring equitable distribution of responsibilities and ensuring coordination during incidents.

Additionally, a regular maintenance program is established for the BCP, DRP and CP plans, in order to identify and correct areas that may require adjustments or improvements, to strengthen the resilience of the Data Center, also optimizes the response to incidents, minimizing thus the operational impact and availability of virtualization and storage services.

Keywords: business continuity plan, business impact analysis, objective recovery time.

CAPITULO I

ANTECEDENTES Y GENERALIDADES

1.1 INTRODUCCIÓN

El Data Center de la Universidad Politécnica Salesiana, Campus Sur, ubicado en Quito, Ecuador, brinda servicios de almacenamiento y virtualización para actividades académicas e investigativas. Con el fin de proveer una continuidad operativa y proteger la información, se implementará un plan de continuidad de negocio (BCP) que incluye la evaluación de activos, el análisis de impacto del negocio (BIA), el desarrollo de planes de recuperación de desastres (DRP), el desarrollo de un plan de contingencia (CP), con el fin de proteger los dispositivos y servicios, y la salvaguarda de datos. Este proceso permitirá al Data Center estar preparado para enfrentar incidentes.

1.2 PROBLEMA DE ESTUDIO

La Carrera de Computación de la Universidad Politécnica Salesiana en Quito, Campus Sur, enfrenta una serie de desafíos que comprometen la operatividad eficiente del Data Center, una infraestructura vital para el apoyo de actividades académicas e investigativas, La vulnerabilidad ante ciberataques plantea un riesgo significativo para la integridad y seguridad de los datos almacenados en el data center. Sin medidas de seguridad adecuadas, la institución está expuesta a accesos no autorizados, alteración o eliminación de datos por parte de actores maliciosos. Un Plan de Continuidad de Negocio (BCP) ayudaría a establecer protocolos de seguridad sólidos, tales como sistemas de respaldo, para prevenir y mitigar los impactos de posibles ciberataques, garantizando así la confidencialidad y disponibilidad de la información crítica, El riesgo de eventos naturales como terremotos, inundaciones o incendios representa una amenaza física para la infraestructura del Data Center y los equipos de TI. Un BCP permitiría implementar medidas preventivas y de mitigación, como el diseño de instalaciones resistentes a desastres naturales, la ubicación estratégica de equipos críticos y la

implementación de sistemas de respaldo de energía, para asegurar la continuidad operativa del Data Center incluso en situaciones adversas, Los problemas en dispositivos de almacenamiento como 3PAR y MSA pueden afectar la disponibilidad y la integridad de los datos almacenados en el data center. Mediante un BCP, se podrían establecer procedimientos de monitoreo y mantenimiento preventivo de estos dispositivos, así como protocolos de respaldo y recuperación de datos, para garantizar la continuidad de los servicios y la protección de la información crítica en caso de fallas técnicas, La crisis energética en Ecuador, especialmente los cortes de energía eléctrica durante los fines de semana, representa otro desafío para el funcionamiento del Data Center. Un BCP permitiría implementar soluciones de redundancia y respaldo energético, como generadores de emergencia y sistemas UPS (Fuente de alimentación ininterrumpida), para garantizar la disponibilidad de energía y la continuidad de los servicios durante períodos de crisis energética.

1.2.1 Antecedentes

La infraestructura del Data Center enfrenta múltiples desafíos que comprometen la disponibilidad de servicio. Entre estos desafíos se presenta las amenazas latentes ciberataques, eventos naturales, problemas técnicos en dispositivos de almacenamiento, falta de capacitaciones al área de NOC y la crisis energética en Ecuador que provoca cortes de energía eléctrica, han pasado seis años desde la última actualización del Plan de Continuidad de Negocio (BCP).

1.2.2 Importancia y alcance

El Data Center brindando los servicios de almacenamiento y virtualización para actividades académicas e investigativas. La ausencia de medidas de seguridad y protocolos adecuados lo expone a riesgos graves que pueden dañar la infraestructura y los equipos de TI. La proximidad a una quebrada aumenta la vulnerabilidad a inundaciones, lo que representa un riesgo significativo para la infraestructura del Data Center.

La crisis energética en Ecuador, con frecuentes cortes de energía, también amenaza la continuidad operativa del Data Center. La pérdida de servicio de almacenamiento y virtualización interrumpiría significativamente las prácticas de estudiantes que dependen de máquinas virtuales para materias como Administración y Gestión de Redes y Fundamentos de Sistemas Operativos. Además, los avances en el área de investigación se verían afectados.

1.2.3 Delimitación

La delimitación geográfica se extiende a las instalaciones y equipos situados dentro del Campus Sur, considerando las particularidades del entorno local. Entre los inconvenientes adicionales que podrían surgir se encuentran la proximidad a una quebrada, lo que aumenta el riesgo de inundaciones, y la ubicación en una zona sísmica, que eleva la probabilidad de daños por terremotos. Además, la infraestructura del campus puede estar sujeta a cortes de energía frecuentes debido a la crisis energética nacional, y a limitaciones en la conectividad de red, que pueden afectar la disponibilidad de servicios externos. Otro factor para considerar es la posible caída de ceniza volcánica, que puede afectar la operatividad de los equipos de TI y la calidad del aire, generando problemas adicionales para el mantenimiento y funcionamiento del Data Center.

1.3 JUSTIFICACIÓN

La implementación de un Plan de Continuidad del Negocio (BCP) para el Data Center de la Carrera de Computación de la Universidad Politécnica Salesiana en Quito, Campus Sur, es imprescindible para garantizar la continuidad de las actividades académicas e investigativas y mitigar los riesgos de interrupciones operativas. El Data Center desempeña un papel crítico en el respaldo de estas actividades, y cualquier interrupción podría tener repercusiones significativas en la productividad estudiantil y el avance de la investigación, Los estándares reconocidos como COBIT, ITIL y la norma ISO 22301 proporcionan directrices sólidas para identificar y abordar los riesgos asociados con la interrupción de las operaciones del Data

Center. Sin un BCP efectivo, la universidad enfrentaría desafíos significativos en la recuperación de datos, la gestión de la crisis y la restauración de servicios críticos, lo que podría afectar negativamente la reputación institucional, los servicios y los costos.

Se llevará a cabo un Análisis de Impacto en el Negocio (BIA) para identificar los sistemas, procesos y recursos críticos del Data Center, así como evaluar el impacto financiero y operativo de su interrupción. Este análisis permitirá identificar los riesgos específicos que podrían afectar la operatividad del Data Center, como ciberataques, eventos naturales y problemas en dispositivos de almacenamiento, A través del BCP, se desarrollarán e implementarán estrategias específicas de mitigación de riesgos, incluyendo la redundancia de sistemas críticos, la implementación de medidas de seguridad cibernética mejoradas y la capacitación del personal en la gestión de crisis. Estas medidas fortalecerán la resiliencia del Data Center y minimizarán el impacto de posibles interrupciones en las actividades académicas e investigativas.

1.4 OBJETIVO GENERAL

Este objetivo implica la creación de un marco integral que aborde los riesgos y contingencias potenciales que podrían afectar la operatividad del Data Center. El diseño del BCP involucrará una evaluación exhaustiva de los riesgos específicos que enfrenta el centro de datos, considerando tanto amenazas internas como externas. Esto incluirá la identificación de posibles desastres naturales como terremotos, inundaciones o incendios, así como la evaluación de riesgos relacionados con ciberataques, fallos en dispositivos de almacenamiento y crisis energéticas, como cortes de suministro eléctrico, El BCP se centrará en garantizar la disponibilidad de los servicios críticos para los estudiantes, docentes y personal, priorizando la continuidad de las actividades académicas e investigativas. Esto implicará la implementación de medidas de redundancia y respaldo para los sistemas y datos críticos, así como la adopción de estrategias de recuperación rápida para minimizar el tiempo de inactividad en caso de un

desastre.

1.4.1 Objetivos específicos

- Generar un Análisis de impacto en el negocio (BIA) para el data center y cuantifica el impacto de los riesgos en los procesos y servicios críticos.
- Identificar los riesgos que pueden afectar al Data Center y su impacto en la carrera de Computación.
- Crear un registro de riesgos detallando la probabilidad de ocurrencia, impacto y medidas de control para cada riesgo.
- Analizar los requisitos del BCP para el data center, considerando los protocolos vigentes del Data Center.
- Diseñar un BCP efectivo y eficiente para el centro de datos, implementando los recursos disponibles, evaluando su eficacia con simulacros de desastres, análisis de tiempos de recuperación, monitorización continua de la disponibilidad
- Implementar el BCP en el data center en base a un análisis de dispositivos y recursos más importantes o comprometedores, estimando los tiempos de inactividad en caso de presentar un desastre, aprovechando los dispositivos y recursos del Data Center para continuar con sus actividades.

CAPITULO II

MARCO TEÓRICO

2.1 FUNDAMENTOS

2.1.1 Fundamento teórico

2.1.1.1 ***Plan de continuidad de negocio (BCP).*** Según (Mauricio Olivari Tavera & Ramírez Coll, 2013), "El Plan de Continuidad de Negocio es un plan proactivo que busca asegurar que los productos o servicios continúen siendo entregados durante una interrupción no planeada." (Párrafo siete)

Un Plan de Continuidad de Negocio (BCP) para un Data Center es un conjunto organizado de estrategias y procedimientos diseñados para asegurar que los servicios más importantes de tecnología de la información sigan funcionando sin problemas, incluso en situaciones adversas. Este plan se adapta específicamente al Data Center, teniendo en cuenta la infraestructura física, los recursos y los servicios esenciales. Además, el BCP crea medidas preventivas para evitar problemas en las operaciones, como problemas de software, fallos de hardware y desastres naturales, garantizando resultados positivos. Estos resultados incluyen una disminución significativa del tiempo sin servicio, una mayor capacidad de recuperación del Data Center ante problemas inesperados y la capacidad de recuperarse rápidamente de situaciones difíciles, lo que asegura la satisfacción del cliente.

2.1.1.2 ***Análisis de Impacto al Negocio (BIA).*** Según (Moreno & Galeano Sánchez, 2013): Un determina las funciones o procesos de negocios críticos necesarios, sus dependencias o recursos, e identifica aplicaciones informáticas claves para el negocio. estima el impacto financiero y operacional de una interrupción y el marco de tiempo de recuperación necesario para las funciones

críticas del negocio. El BIA proporciona a la organización las bases para desarrollar un plan de continuidad de negocio. (p.1)

El Análisis de Impacto en el Negocio (BIA) es un proceso esencial en la gestión de la continuidad operativa de un Data Center. Su objetivo primordial es evaluar y entender cómo una interrupción no planificada puede afectar las operaciones críticas del Data Center. Esto implica determinar los recursos necesarios para recuperarse y el tiempo estimado para restablecer estas funciones esenciales, este analiza sus dependencias y recursos asociados. Esto implica identificar los sistemas informáticos, aplicaciones, datos, personal clave y otros recursos necesarios para llevar a cabo estas funciones de manera efectiva, también se encarga de medir el impacto financiero y operacional de una interrupción en estas funciones críticas. Esto incluye evaluar los costos asociados con la pérdida de ingresos, el tiempo de inactividad, la disminución de la productividad, los costos de recuperación y cualquier otro impacto financiero directo o indirecto. También se evalúan los efectos en la operación del Data Center, como el deterioro de la reputación, la reducción en la satisfacción de los clientes y el no cumplimiento de los acuerdos de nivel de servicio.

2.1.1.1 Plan de Recuperación ante Desastres (DRP).

"Es un documento detallado que describe cómo una organización responderá eficazmente a un incidente no planificado y reanudará las operaciones comerciales." (IBM, 2023, Párrafo uno)

"Los DRP ayudan a garantizar que las empresas estén preparadas para enfrentar muchos tipos diferentes de desastres, incluidos cortes de energía, ataques de ransomware y malware, desastres naturales y mucho más". (IBM, 2023, Párrafo dos)

Un Plan de Recuperación de Desastres (DRP) Asegurar la rápida y eficaz restauración de los servicios críticos de tecnología de la información alojados en este entorno vital. Este DRP se centra en mitigar los efectos adversos de interrupciones graves, Las ventajas de un DRP bien

diseñado incluyen una reducción significativa del tiempo de inactividad, una mayor resiliencia del Data Center ante situaciones de crisis y una rápida recuperación de los servicios esenciales.

2.1.1.4 ***Los Planes de Contingencia (CP).*** Ayudan a las organizaciones a recuperarse tras una interrupción. Tanto si se preparan para la propagación mundial de un virus mortal, como para la gestión de una crisis en torno a una filtración de datos o simplemente para la pérdida de un cliente importante, los planes de contingencia ayudan a las organizaciones a volver a ponerse en pie tras un acontecimiento negativo. (IBM, 2023, Párrafo uno)

Un Plan de Contingencia (CP) es un conjunto de procedimientos y protocolos diseñados para guiar a una organización en la gestión y recuperación de eventos inesperados o crisis que puedan afectar sus operaciones normales

CAPÍTULO III

METODOLOGÍA

3.1 CONTEXTO DE LA ORGANIZACIÓN

El Data Center opera bajo la norma ISO 22301:2019 y se rige por los marcos COBIT e ITIL. Proporciona servicios de virtualización y almacenamiento, con máquinas virtuales utilizadas por estudiantes de pregrado y postgrado, así como por docentes. Se clasifica como un Data Center TIER 1, pero este presenta todos los componentes necesarios para ser considerado un TIER 2 a excepción de un componente.

3.2 OBJETIVOS DE CONTINUIDAD DE NEGOCIO

Garantizar la disponibilidad continua de los servicios de virtualización para satisfacer las necesidades de los usuarios, minimizando el impacto de las interrupciones en las actividades académicas y administrativas. Asegurar la integridad y confidencialidad de los datos almacenados en las máquinas virtuales y mantener la reputación del Data Center como proveedor confiable de servicios de TI.

3.3 EVALUACIÓN DEL IMPACTO DE NEGOCIO

Las interrupciones en el sistema de climatización, valoración de activos que indican el nivel de criticidad, aspectos que podrían afectar negativamente el rendimiento del servicio de virtualización y almacenamiento. Esto podría resultar en una pérdida de productividad para los usuarios y dañar la reputación del Data Center.

3.4 EVALUACIÓN DE RIESGOS

Se requiere realizar una clasificación de los riesgos, amenazas y vulnerabilidades que enfrenta el Data Center. Es importante llevar a cabo esta evaluación utilizando métricas de Tiempo Objetivo de Recuperación (RTO) y Punto Objetivo de Recuperación (RPO) para

identificar los activos que se encuentran en riesgo y analizar el impacto potencial en los servicios proporcionados. Este análisis debe incluir la identificación de fallos específicos relacionados con los riesgos identificados. Las interrupciones no planificadas en los servicios de virtualización y almacenamiento, derivando en pérdidas financieras significativas y daños a la reputación institucional.

3.5 ESTRATEGIAS Y SOLUCIONES DE CONTINUIDAD DE NEGOCIO

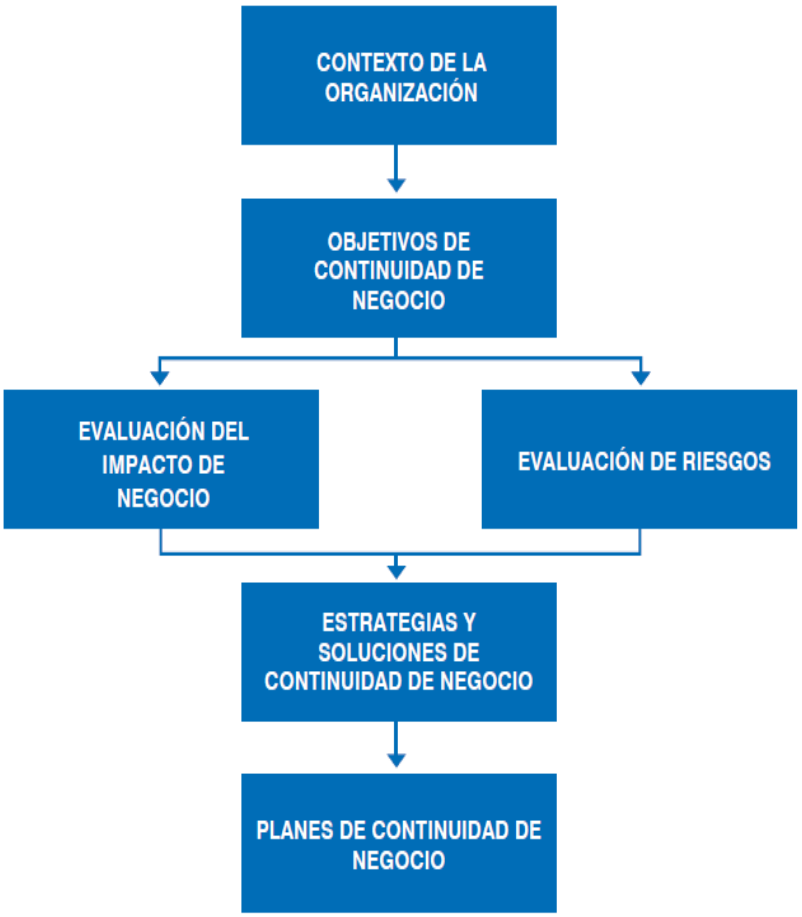
Implementar medidas correctivas para mejorar la redundancia en el sistema de refrigeración, como la instalación de sistemas de respaldo o la actualización de equipos existentes. Desarrollar y mantener procedimientos de respuesta a emergencias para mitigar los impactos de las interrupciones en el servicio y garantizar una recuperación rápida y efectiva.

3.6 PLANES DE CONTINUIDAD DE NEGOCIO

Se implementa estrategias específicas de mitigación de riesgos. Esto incluirá la asignación de responsabilidades en base a la normativa COBIT, la definición de procedimientos de respuesta a emergencias y la programación de ejercicios de

simulacro para probar la efectividad del BCP actualizado.

Figura 1
Conceptos de la norma ISO 22301:2019



Nota. Metodología de BCP en base a norma ISO 22301:2019. Elaborado por: Bevan (2019).

Las razones por las cuales es importante el cumplir con ITIL, COBIT, ISO 22301:2019, son demostradas en la Figura No.2, Indicándonos paso a paso como es que estas se adaptan al margen del marco común, pasando con la flexibilidad que la empresa cuenta, seguido de base de conocimientos los cuales llegan a ser colectivos, es decir de cada uno de los empleados en la empresa, finalmente los niveles de servicio nos permite el identificar el propósito y finalmente una adaptabilidad a siguientes tecnologías y futuros proyectos.

Figura 2

Razones para cumplir con normativas como ISO, COBIT e ITL

Nota. Beneficios de uso de normativas ISO, COBIT e ITL, Elaborado por: Tech-Blog (2023).

3.7 SELECCIÓN DE HERRAMIENTAS DE RIESGOS ÓPTIMA

3.7.1 Análisis de fmea

"El Análisis de Modo y Efecto de Fallas es un recurso analítico diseñado para evaluar y medir los posibles efectos que una falla técnica o procesal puede tener lugar en la operatividad de una empresa" (Terreros, 2023, Parrafo tres).

3.7.2 Análisis de hazop:

El Estudio de Peligros y Operatividad, "Se basa en la premisa de que los accidentes o problemas de operativa se producen como consecuencia de la desviación de las variables del proceso con respecto a los parámetros normales de operación" (HAZOP, s.f., Párrafo segundo).

3.7.3 Análisis de Raci

"Es una herramienta gráfica que organiza las responsabilidades y sigue las tareas de los trabajos colaborativos" (Santos, 2024, Parrafo quinto).

3.7.4 Ventajas y Desventajas

En la Tabla No.1 se analizarán las ventajas que presentan cada una de las herramientas.

Tabla 1
Tabla comparativa de ventajas de herramientas de análisis de riesgos

VENTAJAS DE HERRAMIENTAS		
FMEA	**HAZOP**	**RACI**
Permite prevenir fallos que se puedan presentar.	Permite detectar y prevenir accidentes y otros incidentes no deseados.	Ayuda a no cometer confusiones y duplicar tareas en un proceso.
Detecta y genera una escala de prioridad de riesgos.	Contribuye a reducir los costos asociados a fallos y paradas no planificadas.	Encarga y delega cargos promoviendo la responsabilidad de cada integrante.
Puede generar una mejorar de seguridad y calidad de servicios.	Puede generar una operación continua y fiable	RACI permite detectar los cuellos de botella en el proceso de trabajo.

Nota. La siguiente tabla compara las herramientas planteadas, analizando cada ventaja existente. Elaborado por: El Autor.

La Tabla No. 2 presenta un análisis de las limitaciones de las herramientas propuestas en relación con la problemática del Data Center. Este análisis se realizó tomando en consideración el tamaño de la organización, la adecuación de las herramientas al personal del área de NOC, y su capacidad para abordar proyectos

Tabla 2
Tabla comparativa de limitaciones de herramientas de análisis de riesgos

LIMITACIONES DE HERRAMIENTAS		
FMEA	**HAZOP**	**RACI**
Puede ser subjetivo, dependiendo del ambiente donde se planea enfocar un FMEA No asegura una detección de todos los fallos potenciales	Requiere una inversión significativa de tiempo y recursos. No detectar todos los riesgos potenciales Tiende a ser compleja	Puede ser inflexible No es adecuada para proyectos pequeños.

Nota. La siguiente tabla compara las herramientas planteadas, analizando limitaciones ventaja que estas presentan. Elaborado por: El Autor.

3.7.5 Comparación de Herramientas

El Análisis de Modo y Efecto de Fallas (FMEA) analiza posibles fallos en procesos y sistemas, mejorando la seguridad y calidad de los servicios. Sin embargo, su eficacia puede verse limitada por la subjetividad del entorno y no siempre detecta todos los fallos potenciales. En un Data Center, FMEA puede ayudar a prevenir riesgos técnicos.

Estudio de Peligros y Operatividad (HAZOP) identifica anomalías en procesos para prevenir accidentes y problemas de operatividad. HAZOP es apropiado para reducir costos asociados a fallos, pero su eficacia depende de la experiencia del personal junto con una gran inversión de tiempo y fuentes de ingresos, En un Data Center, HAZOP puede generar operaciones fiables.

La matriz RACI organiza responsabilidades y tareas, evitando confusiones y duplicaciones de procesos o trabajos. Es útil para delegar responsabilidades y detectar cuellos de botella. En un Data Center, RACI proporciona una estructura clara para la gestión de la continuidad del negocio, asegurando que cada miembro conozca su papel y responsabilidad

3.7.6 Justificación de implementación de herramienta de análisis de riesgos

La matriz RACI es la mejor opción a comparación de las otras herramientas analizadas, ya en base a la necesidad de un Plan de Continuidad de Negocio (BCP) su capacidad para organizar y delegar responsabilidades de manera distribuida logra enfocar cada riesgo a una persona la cual debe encargarse de solucionar o notificar dicho percance. Esta herramienta evita confusiones y duplicaciones de tareas, lo que es apropiado en un entorno el cual requiere de una supervisión constante. RACI facilita las responsabilidades y permite identificar rápidamente los cuellos de botella en los procesos, Aunque puede ser vista como inflexible y no adecuada para proyectos pequeños, su estructura clara y su enfoque en la responsabilidad individual la hacen ideal para este caso.

CAPITULO IV

RESULTADOS

4.1 DESARROLLO DE BCP

En el presente documento se desarrollará un Plan de Continuidad del Negocio (BCP) basado en la metodología planteada conforme a la norma ISO 22301:2019, así como en los marcos COBIT e ITIL.

Dicha metodología consta de seis pasos, de los cuales se unirán el paso 3 que corresponden a la Evaluación del Impacto de Negocio en el apartado 3.3 y la Evaluación de Riesgos que corresponde al apartado 3.4 para generar un Análisis de Impacto en el Negocio (BIA). Esta integración permitirá una comprensión más estructurada, manteniendo el principio de dicha metodología.

4.1.1 Contexto de la organización

4.1.1.1 ***Evaluación Integral del Data Center.*** El Data Center de la Universidad Politécnica Salesiana, Campus Sur, ubicado en la Av. Rumichaca Ñan s/n, Quito 170146, latitud: 0°16'57.66"S y longitud: 78°33'2.61"O, se encuentra en el laboratorio de IHM, en el segundo piso del bloque D. Comenzó sus operaciones en febrero del 2018, dedicado a brinda dos servicios: almacenamiento y virtualización.

El almacenamiento se refiere a la gestión de datos, utilizando discos duros (HDD) y unidades de estado sólido (SSD). La virtualización permite crear versiones virtuales de recursos informáticos mediante hipervisores como VMware, que gestionan máquinas virtuales (VM). Todos los componentes y dispositivos de almacenamiento cuentan con redundancia, excepto el

sistema de aire acondicionado, clasificando este Data Center como TIER 1. A pesar de esta limitación, el Data Center continúa operando y brindando servicios hasta el periodo 64, actualmente en curso.

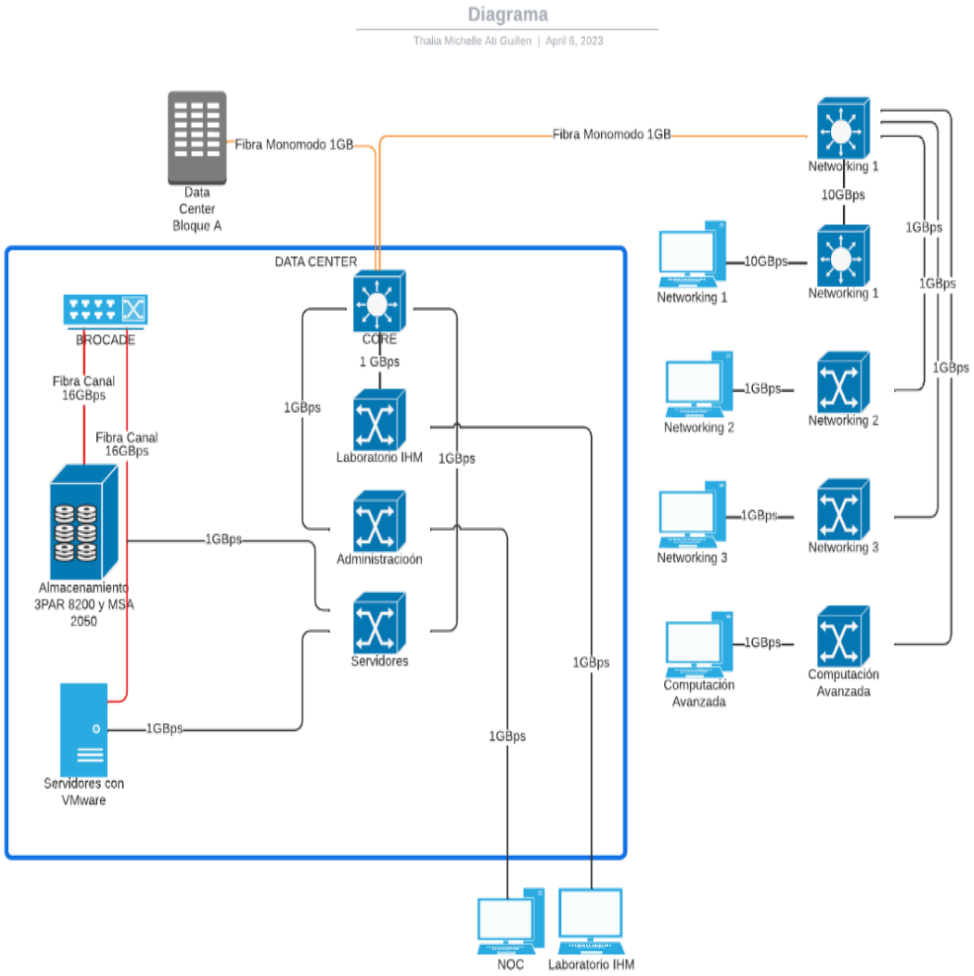
Además, el Data Center cuenta con la ISO 22301 y estándares de COBIT e ITIL para la gestión de las tecnologías de la información.

El Data Center está permanentemente supervisado por personal administrativo que monitorea el comportamiento y desarrollo de la infraestructura. Este equipo es responsable de detectar fallas de software, hardware y cualquier comportamiento inusual que pueda afectar su funcionamiento. La vigilancia constante permite generar registros detallados de incidentes o fallas.

4.1.1.2 ***Análisis de topología Data Center.*** El Data Center, opera una estructura distribuida en el segundo piso, En el laboratorio de IHM, donde se encuentran el centro de procesamiento y almacenamiento de datos. Los componentes que procesamiento que lo constituyen son HPE XL230A, HPE XL190R Gen10, HPE XL250a y dispositivos de almacenamiento HPE 3PAR 8200 y MSA2050, brindando el servicio de virtualización a estudiantes y distribuyéndolo a diferentes laboratorios como IHM, Networking 1, Networking 2, Networking 3, Computación Avanzada.

Dicha topología se encuentra detalla de manera más extensa en la Figura No.3

Figura 3
Diagrama de topología de Data Center



Nota. Topología del Data Center Elaborado por: Guillen (2023).

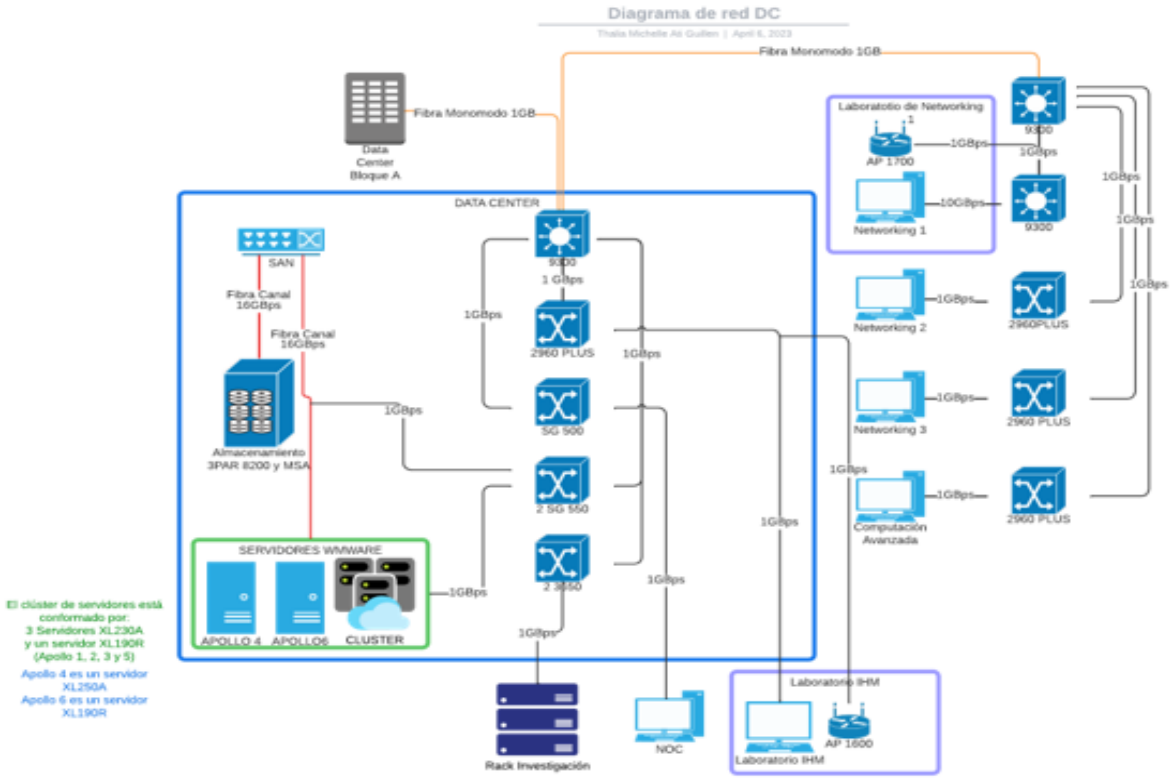
4.1.1.3 ***Infraestructura de Red.*** La estructura de red en el Data Center de la Carrera de Computación de la Universidad Politécnica Salesiana, Campus Sur, está equipada con una conectividad Cisco, contando con dispositivos de almacenamiento y procesamiento de datos. Los sistemas de almacenamiento

3PAR 8200 y MSA se conectan mediante un switch SAN con conexiones de fibra canal de 16 Gbps. Este switch SAN se conecta a los servidores VMware, que incluyen 3 servidores HPE XL230A, 2 servidores HPE XL190R Gen10 y 1 servidor HPE XL250a, todos con una conexión de fibra óptica de 1 Gbps.

El rack de investigación y el área de NOC (Centro de Operación de Red) también tienen conexiones de fibra óptica de 1 Gbps, permitiendo monitorizar el estado del Data Center en todo momento. Adicionalmente, el Data Center se comunica con el laboratorio de IHM mediante fibra óptica de 1 Gbps y con el laboratorio de Networking 1 y el bloque A a través de una conexión de fibra monomodo de 1 Gbps.

Figura 4

Diagrama de red del Data Center



Nota. topología de red del Data Center Elaborado por: Guillen (2023).

4.1.1.4 ***Sistemas de Almacenamiento.*** El sistema de almacenamiento en el Data Center de la Carrera de Computación de la Universidad Politécnica Salesiana, Campus Sur. Está compuesto por dos principales dispositivos: el HPE 3PAR 8200 y el MSA2050. El HPE 3PAR 8200 cuenta con dos configuraciones: un 3PAR Master de 50 TB con RAID 6, que incluye 26 discos SSD y 14 discos FC, y un 3PAR UPS de 20 TB con RAID 5, que contiene 10 discos SSD y 14 discos FC. El sistema MSA2050 dispone de 50 TB de almacenamiento, compuesto por 24 discos SAS, y opera en modo espejo.

Tabla 3
Sistema de almacenamiento Data Center

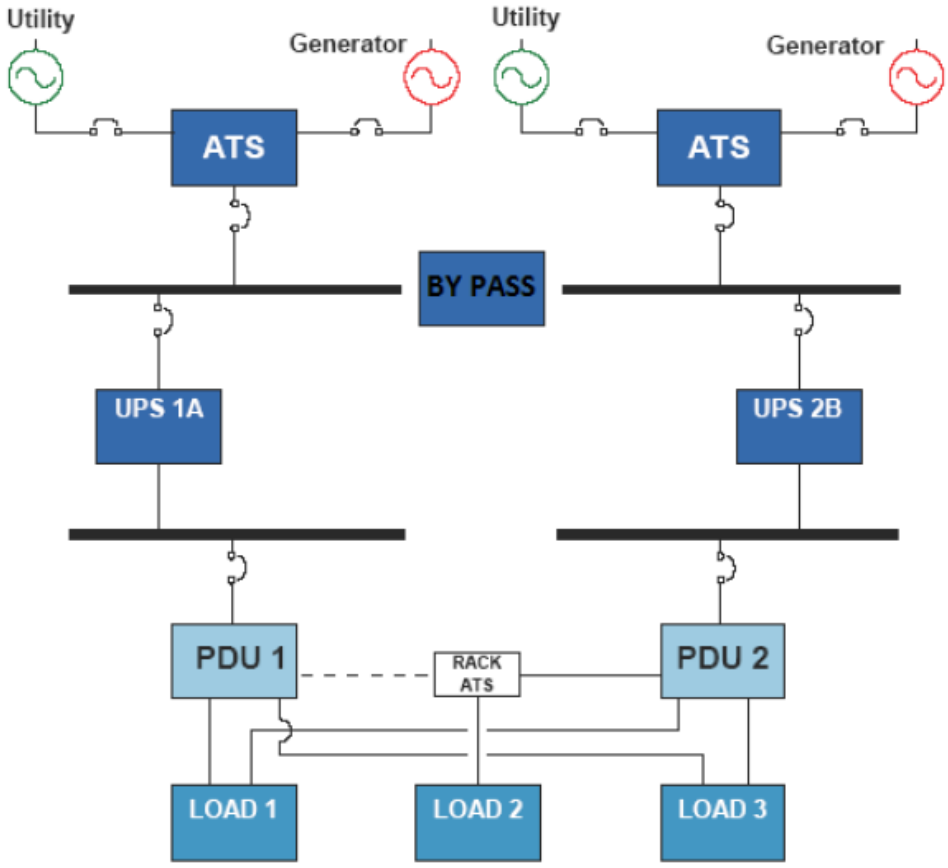
Almacenamiento	**Número Discos SSD**	**Número Discos FC**	**Número Discos SAS**	**Capacidad Total (TB)**
HPE 3PAR 8200 Master	26	14	N/A	50
HPE 3PAR 8200	10	14	N/A	20
MSA2050	N/A	N/A	24	50
TOTAL	36	28	24	120

Nota. Representación de componentes de almacenamiento del Data Center en el periodo 64.

Elaborado por: El Autor.

4.1.1.5 ***Sistema Eléctrico.*** En el siguiente grafico se muestra el esquema eléctrico de la data center.

Figura 5
Diagrama eléctrico del Data Center



Nota. Diagrama Eléctrico del Data Center. Elaborado por: Plagecons (2017).

El alimentador que proviene del TTA ubicado cerca de la guardianía (LADO A) se compone de un conductor calibre #1/0 AWG SUPERFLEX por cada fase, un conductor calibre #2 AWG SUPERFLEX para el neutro y un cable calibre #4 AWG para la conexión de tierra.

El alimentador que proviene del TTA ubicado en el bloque D se compone de un conductor calibre #4 AWG SUPERFLEX por cada fase, un conductor calibre #6 AWG SUPERFLEX para el neutro y un cable calibre #8 AWG para la conexión de tierra. En comparación con el LADO A, los conductores aquí son de menor calibre, es decir una menor

capacidad de corriente.

El TDCC (Tablero de Distribución General del Cuarto de Cómputo) es un gabinete metálico con dimensiones de 2000 x 1000 x 400 mm (alto x ancho x profundidad), equipado con puerta, doble fondo corredizo, base metálica para soporte sobre el piso y láminas de acrílico para cubrimiento de barras de cobre. Las acometidas eléctricas de ambos TTA llegan a breakers de protección de 125 A ubicados en la parte superior del TDCC. Desde allí, la energía se distribuye a los UPS, los sistemas de aire acondicionado y el centro de carga de distribución de energía normal

En el siguiente tabal se detallará de mejor manera como es que opera este sistema eléctrico, además se especificara en amperajes la capacidad que este mantiene, junto con el propósito.

Tabla 4
Sistema de distribución de energía TDCC

TABLERO DE DISTRIBUCION CENTRO DE COMPUTO TDCC		
Número de polos	**Capacidad (A)**	**PROPOSITO**
3PH	125	ENTRADA LADO A
3PH	100	ENTRADA UPS A
3PH	100	BYPASS UPS A
3PH	100	SALIDA UPS A
3PH	60	TVSS
3PH	125	ENTRADA LADO B
3PH	100	ENTRADA UPS B
3PH	100	BYPASS UPS B

3PH	100	SALIDA UPS B
3PH	60	TVSS

Nota. Tabla de capacidad, polos y propósitos del TDCC. Elaborado por: El Autor.

4.1.1.6 ***Servicios Brindados por Data Center.*** El Data Center de la Carrera de Computación de la Universidad Politécnica Salesiana, Campus Sur, brinda servicios de almacenamiento y virtualización. Utiliza discos duros y sólido. La virtualización, mediante VMware, permite a estudiantes y al área de investigación acceder a máquinas virtuales y gestionar entornos virtuales, beneficiando especialmente a materias como administración de sistemas operativos y gestión de redes. Aunque el Data Center, clasificado como TIER 1 por la falta de redundancia en el sistema de aire acondicionado, todos los componentes de almacenamiento tienen redundancia, asegurando la continuidad de sus servicios hasta el periodo 64, actualmente en curso.

4.1.2 Objetivos de continuidad de negocio

En el apartado 1.4.1 y 1.4.2, los objetivos planteados ya se encuentran detallados y estructurados de manera integral en el documento, en base al Data Center de la Universidad Politécnica Salesiana, incluyendo las normativas que este implica, en este caso ISO 22301, COBIT e ITIL.

4.1.3 Análisis de impacto de negocio (BIA)

4.1.3.1 ***Identificación de Procesos.*** Las funciones críticas del Data Center, es pertinente analizar su actividad a lo largo de los años de operación. Este análisis incluye revisar el historial de incidentes previamente gestionados para determinar los componentes que más frecuentemente presentan fallos, así como evaluar si estos incidentes han afectado la capacidad del Data Center para ofrecer servicios de manera efectiva.

En la siguiente tabla se detallará el lugar del incidente junto con una pequeña descripción del Data Center y el tiempo que este se ha presentado en el data center, desde el periodo 59 hasta el actual 64.

Tabla 5
Tabla de línea de tiempo de incidentes del Data Center

FECHA DEL REPORTE DE INCIDENTE	LUGAR DEL INCIDENTE	DESCRIPCIÓN	DURACION DEL INCIDENTE
	PERIODO 59		
martes, 22 de febrero de 2022	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo de un disco del 3PAR-MASTER	14 horas
	PERIODO 60		
miércoles, 27 de abril de 2022	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo en uno de los discos en el PAR MASTER	15 minutos

FECHA DEL REPORTE DE INCIDENTE	LUGAR DEL INCIDENTE	DESCRIPCIÓN	DURACION DEL INCIDENTE
miércoles, 27 de abril de 2022	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo del Service Processor del 3PAR MASTER	6 horas
miércoles, 27 de abril de 2022	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo del Service Processor del 3PAR UPS	6 horas
lunes, 20 de junio de 2022	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Perdida de conectividad de servidor Apollo 5	15 minutos
PERIODO 61			
lunes, 21 de noviembre de 2022	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el funcionamiento del UPS A	24 horas
martes, 31 de enero de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en Disco 16 del MSA	25 de marzo
jueves, 16 de febrero de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Perdida de conectividad de servidor Apollo 1	15 minutos
PERIODO 62			
jueves, 6 de abril de 2023	Universidad Politécnica Salesiana Campus Sur	Filtración de Agua en el Laboratorio de Netwoking 3	4 horas

FECHA DEL REPORTE DE INCIDENTE	LUGAR DEL INCIDENTE	DESCRIPCIÓN	DURACION DEL INCIDENTE
	Bloque D - Data Center ICC		
miércoles, 3 de mayo de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en Disco 12 del 3PAR-UPS	25 de marzo
miércoles, 17 de mayo de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Sobre carga de voltaje, en el tablero de distribución.	4 horas
jueves, 6 de julio de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Sobre Voltaje en el tablero de Distribución del DC ICC	6 horas
viernes, 7 de julio de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Caida Red del Data Center ICC	2 horas
lunes, 21 de agosto de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el servidor Apollo 4 - XL250	10 Minutos

FECHA DEL REPORTE DE INCIDENTE	LUGAR DEL INCIDENTE	DESCRIPCIÓN	DURACION DEL INCIDENTE
lunes, 21 de agosto de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el UPS 1, se perdio la funcionalidad de VOLTAJE INPUT	10 Minutos
PERIODO 63			
lunes, 4 de septiembre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el disco #5 del MSA	24 dias
martes, 3 de octubre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el disco #20 del MSA	30 Minutos
miércoles, 4 de octubre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el DRS, del servidor Apollo 3	12 horas
sábado, 28 de octubre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Apagado completo del Data Center	24 horas
lunes, 30 de octubre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo del UPS 1	2 horas

FECHA DEL REPORTE DE INCIDENTE	LUGAR DEL INCIDENTE	DESCRIPCIÓN	DURACION DEL INCIDENTE
lunes, 30 de octubre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Sincronización en el Service Proccesor del 3PARMASTER	2 horas
lunes, 27 de noviembre de 2023	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el disco #17 del MSA	24 horas
martes, 23 de enero de 2024	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo del UPS 1	25 de marzo
miércoles, 14 de febrero de 2024	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Falla en el disco #5 del MSA	25 de Marzo
viernes, 23 de febrero de 2024	Universidad Politécnica Salesiana Campus Sur Bloque D - Data Center ICC	Fallo del UPS 1	25 de Marzo
miércoles, 28 de febrero de 2024	Universidad Politécnica Salesiana Campus Sur	Fallo de baterias del sistema contraincendios	5 horas

FECHA DEL REPORTE DE INCIDENTE	LUGAR DEL INCIDENTE	DESCRIPCIÓN	DURACION DEL INCIDENTE
	Bloque D - Data Center ICC		

Nota. La siguiente tabla detalla la fecha de los incidentes junto con el motivo y duración del Data Center desde el periodo 59 hasta el 64. Elaborado por: El Autor.

Se han presentado varios incidentes relacionados con los sistemas de almacenamiento 3PAR y MSA. En el caso del 3PAR, se produjo un fallo en el sistema de discos el 12 de marzo, lo que afectó el rendimiento hasta que se sustituyó el disco afectado. Además, el 27 de abril, una actualización de firmware causó errores que interrumpieron el acceso a datos.

Con respecto al MSA, el 5 de mayo se experimentó una interrupción en la conexión SAN, la causa fue un problema en los cables de conexión. A principios de junio, se reportó latencia alta y errores de entrada/salida debido a una configuración incorrecta en la gestión de la caché del sistema.

Unidades de Suministro Ininterrumpido (UPS). El 15 de marzo, la batería de la UPS principal falló durante una prueba de rutina, El 22 de abril, una sobrecarga en la UPS secundaria llevó a un apagado de emergencia, lo que provocó un corte de energía en parte del centro de datos durante aproximadamente 30 minutos. La sobrecarga fue causada por una configuración incorrecta de la distribución de carga

Las consecuencias de estos incidentes para los servicios de almacenamiento y virtualización se presentan en los fallos repetidos en los discos de almacenamiento que pueden llevar a la pérdida de datos y afectar la disponibilidad de la información necesaria para las operaciones diarias. Los problemas con los UPS pueden provocar cortes de energía que impacten la integridad de los sistemas y la continuidad del servicio, afectando la estabilidad de

las plataformas de virtualización. La pérdida de conectividad de los servidores puede interrumpir el acceso a las máquinas virtuales y los recursos compartidos, impactando negativamente la productividad del área de investigación y de los estudiantes que requieren recursos de virtualización para sus clases o prácticas.

Las funciones críticas identificadas en el análisis de incidentes**.** se ven presentes en el almacenamiento, afectado por fallos en discos específicos como el 3PAR-MASTER y el MSA, que comprometen la integridad de los datos y la disponibilidad del servicio de almacenamiento. Los servidores están comprometidos por interrupciones en la conectividad de servidores Apollo y problemas en el funcionamiento del servidor Apollo 3, son importantes para la operación y el procesamiento de datos. La climatización y la energización, evidenciadas por sobrecargas de voltaje y fallos en UPS críticos como el UPS A, son cruciales para mantener condiciones ambientales adecuadas y asegurar la continuidad energética, los problemas con el sistema contraincendios, como fallos en las baterías, resaltan la importancia de la seguridad física del entorno.

4.1.3.1.1 ***Activos de almacenamiento.*** La identificación de activos que se encuentra en el Data Center se puede apreciar en las siguientes tablas, los componentes que conforman los dispositivos de almacenamiento se ven listados en la siguiente tabla.

Tabla 6
Activos de almacenamiento del Data Center

Storage 3PAR HPE			
Modelo	3PAR 8200	**Modelo**	3PAR 8200
Name	3PAR - UPS	**Name**	3PAR - MASTER
Storage MSA 2050			

Modelo	MSA 2050
Capacidad	50 GB
Name	MSA2050-UPS

Nota. Presentación de componentes de almacenamiento del Data durante el periodo 64 Center. Elaborado por: El Autor.

4.1.3.1.2 ***Los activos de procesamiento del Data Center.*** Se componen principalmente de servidores, entre los cuales destacan seis unidades. De estos, dos están equipados con GPU para manejar cargas de trabajo exigentes. En la Tabla No.4 se detalla específicamente cada producto, incluyendo su nombre y la presencia de GPU correspondiente.

Tabla 7
Servidores del Data Center

HPE Apollo 1		HPE **Apollo** 2		**HPE Apollo 3**	
Product Name	ProLiant XL230a Gen9	**Product Name**	ProLiant XL230a Gen9	**Product Name**	ProLiant XL230a Gen9
HPE Apollo 4+GPU		**HPE Apollo 5**		**HPE Apollo 6**	
Product Name	ProLiant XL250a Gen9	**Product Name**	ProLiant XL190r Gen10	**Product Name**	ProLiant XL190r Gen10
GPU	NVidia Tesla K80	**GPU**	NVidia Tesla V100		

Nota. Tabla de representación de servidores del Data Center durante el periodo 64. Elaborado por: El Autor.

4.1.3.1.3 ***El sistema de Aire Acondicionado.*** Es de suma importancia ya

que según (Criterios de diseño del entorno, 2021) una temperatura adecuada es 18° – 27°C, en base a este criterio, se detalla en la siguiente tabla los componentes del aire acondicionado.

Tabla 8
Sistema de aire acondicionado

INVENTARIO DE SISTEMA AIRE ACONDICIONADO AIRE 1	
Marca	STULZ
Modelo	Mini Space CCD 151 A
Procedencia	Alemana
Tipo	Aire acondicionado de precisión
Ubicación Condensadora	Parte externa superior del edificio
Control	C 7000

Nota. Descripción de componente aire acondicionado que usa el Data Center. Elaborado por: El Autor.

4.1.3.1.4 ***Los sistemas de alimentación ininterrumpida.*** Que posee el Data Center, se ven detalladas en la siguiente tabla

Tabla 9
Sistema de alimentación Ininterrumpida

Inventario de UPS			
UPS 1-A		**UPS 2-B**	
Marca	APC	**Marca**	APC
Modelo	Symmetra LX	**Modelo**	Symmetra LX

Nota. La tabla indica el modelo y marca de los UPS que usa el Data Center. Elaborado por: El Autor.

4.1.3.1.5 ***Los activos de red.*** Compone al Data Center contienen más dispositivos, que comunican diferentes áreas para brindar servicios, debido a esto se desarrolla la Tabla No.7 en la cual se detalla cada uno de los dispositivos que forman dicha red.

Tabla 10
Dispositivos de red del Data Center

RACK COMUNICACIÓN - DC ICC					
SWITCH CORE					
Marca:	Cisco				
Modelo:	Catalyst 9300 - 48P - POE+ NETWORK ADVANTAGE				
IOS Version:	12.2(85) SE5				
SWITCH ADM DC ICC 1					
Marca:	Cisco				
Modelo:	Swicth Catalyst 3650				
SWITCH DATOS 1 - IHM					
Marca:	Cisco				
Modelo:	Swicth Catalyst 2960				
SWITCH ADM SERVIDORES					
Marca:	Cisco				
Modelo:	SG5550XG-24T				
SWITCH ADM CD ICC 2		**SWITCH DATOS 2 - IHM**		**SWITCH ADM SERVIDORES**	
Marca:	Cisco	**Marca:**	Cisco	**Marca:**	Cisco
Modelo:	Swicth Catalyst 3650	**Modelo:**	SG500-28	**Modelo:**	SG5550XG-24T

Nota. La siguiente tabla detalla los dispositivos que conforman la red del Data Center durante el periodo 64. Elaborado por: El Autor.

4.1.3.1.6 ***El inventario de switch SAN.*** se encuentran detallados en la siguiente tabla, este dispositivo logra conectar los servidores junto con las unidades de almacenamiento se hace uso de los siguientes componentes.

Tabla 11
Descripción switch san

SWITCH SAN 1 - ESPACIO 38	
Modelo:	HPE SN3000B 24/12 FC Switch
SWITCH SAN 2 - ESPACIO 36	
Modelo:	HPE SN3000B 24/12 FC Switch

Nota. La siguiente tabla indica el modelo de switch SAN que usa el Data Center. Elaborado por: El Autor.

4.1.3.1.7 ***El switch de Comunicación.*** Los componentes de comunicación que implementa y usa el Data Center se detallan en la Tabla No.12

Tabla 12
Switch de comunicación

SWITCH COMUNICACION - NETWORKING 1	
SWITCH Datos 1 - Laboratorio Networking 1	
Marca:	Cisco
Modelo:	Catalyst WS-C2960+48TC-L
N° Puertos	48
SWITCH Datos 2 - Laboratorio Networking 1	
Marca:	Cisco
Modelo:	Catalyst WS-C2960+48TC-L
N° Puertos	48
SWITCH Datos 3 - Laboratorio Networking 1	

Marca:	Cisco
Modelo:	Swicth Catalyst 2960
N° Puertos	24

Nota. La siguiente tabla muestra el modelo, marca y numero de puertos de los diferentes switches que usa el Data Center para comunicarse con otras áreas. Elaborado por: El Autor

4.1.3.1.8 ***Los componentes del área de NOC.*** Son igual de importantes que cualquier otra sección analizada, puesto que esta nos permite tener un monitoreo en tiempo real de un Data Center y en base a dicha supervisión constante tener la capacidad de notificar problemas en los dispositivos del Data Center, los componentes del área de NOC se detallan en la tabla No.13

Tabla 13
Dispositivos de hardware del área de NOC

Inventario de Área de NOC	
MONITOR 1	
Ubicación	NOC
Descripción	MONITOR 49INC LH49PMHP SERIES EDGE-LIT LED
Marca	Samsung
MONITOR 2	
Ubicación	NOC
Descripción	MONITOR 49INC LH49PMHP SERIES EDGE-LIT LED
Marca	Samsung
TELEVISOR 1	
Ubicación	NOC
Descripción	TELEVISOR LED 4K UN-40MU6103G
Marca	Samsung
CPU	
Modelo	Optiplex 7050 - Core i5-7500 - 8GB RAM - 1TB HDD
Modelo	Optiplex 7040 - Core i7-6700 - 8GB RAM - 1TB HDD
Modelo	Optiplex 7040 - Core i7-6700 - 8GB RAM - 1TB HDD

Inventario de Área de NOC	
MONITORES COMPUTADORAS	
Modelo	Dell E2020H
Modelo	Dell E2020H
Modelo	Dell E2020H
TECLADO	
Modelo	KB216P
Modelo	KB216T1
Modelo	KB216P
MOUSE	
Modelo	MS116T
Modelo	MS111L
Modelo	BRISANE

Nota. Esta tabla muestra todos los dispositivos de monitoreo con los que cuenta el área de NOC del Data Center en el periodo 64. Elaborado por: El Autor.

4.1.3.1.9 ***Los activos de software.*** son componentes sumamente importantes para el funcionamiento del Data Center. Estos incluyen aplicaciones de gestión, herramientas de seguridad y software de virtualización, se detallará de mejor manera en la Tabla No.14

Tabla 14
Activos de software

Activos de software en Data Center	
Hipervisor:	ESXI 7
Gestor y controlador de hosts ESXi	VCenter Server 7
Software de administración de almacenamiento	Storage Management Utility (MSA), plataformas propias de HPE
Software de administración de arreglos de almacenamiento	SSMC Appliance 3.8.0.0.330

Software de control de acceso	ZKAccess 3.5
Software de videovigilancia	Milestone Xprotect - Management 2018

Nota. En la siguiente tabla se muestran los activos que el Data Center usa hasta el periodo 64.

Elaborado por: El Autor.

4.1.3.1.10 ***Los activos de Seguridad del Data Center.*** Permite el mantener cada activo seguro se detallan a continuación.

El activo de sistema contra incendios que implementa el Data Center es el siguiente.

Tabla 15
Tabla de sistema de incendios del Data Center

Sistema de Incendios (Bombona de Ecaro)	
Modelo	Ecaro 25

Nota. La siguiente tabla detalla el modelo del sistema contra incendios del Data Center.

Elaborado por: El Autor.

4.1.3.1.11 ***El tablero de control*** que se usa actual mente es el siguiente.

Tabla 16
Tabla de sistema de control

Tablero de Control	
Modelo	**Marca**
10-063 Series	Single Hazard Panel SHP Pro

Nota. La siguiente tabla detalla el modelo y marca del tablero de control del Data Center.

Elaborado por: El Autor.

4.1.3.1.12 ***Biométricos.*** Se usan para salvaguardar los componentes físicos del Data Center, se detallan a continuación.

Tabla 17
Tabla de biométricos del Data Center

Inventario de Biométricos	
BIOMETRICO 1	
Ubicación	Data Center
Descripción	Biometrico para acceso de puerta
Marca	ZKTECO
BIOMETRICO 2	
Ubicación	NOC
Descripción	Biometrico para acceso de puerta
Marca	ZKTECO
BIOMETRICO 3	
Ubicación	Laboratorio IHM
Descripción	Biometrico para acceso de puerta
Marca	ZKTECO

Nota. La siguiente tabla muestra los biométricos que implementa el Data Center para mantener un estricto acceso. Elaborado por: El Autor.

Las cámaras de vigilancia desempeñan un papel sumamente importante ya que proporciona una visión integral de las instalaciones y disuadiendo actividades no autorizadas.

Tabla 18
Tabla de Inventario de cámaras

Inventario de Cámaras	
CÁMARA 1	
Ubicación	Armario IHM

Inventario de Cámaras	
Modelo	Cámara - DS-2CD2121G0-I
Marca	Hikvision
Inventario de Cámaras (Data Center)	
CÁMARA 1	
Ubicación	DC ICC - Pasillo Caliente
Modelo	AXIS M3004 Network Camera
Marca	Hikvision
CÁMARA 2	
Ubicación	DC ICC - Pasillo Frio
Modelo	AXIS M3004 Network Camera
Marca	AXIS

Nota. La siguiente tabla detalla la ubicación, descripción y marca de las cámaras que usa el Data Center en el periodo 64. Elaborado por: El Autor.

4.1.3.2 ***Evaluación de Impacto y Dependencias.*** Para evaluar el impacto que este Data Center presentara es necesario identificar los activos cruciales para la operatividad de este, A continuación, se presenta un listado de los activos cruciales de la infraestructura tecnológica, categorizados por su función principal. En la Tabla No.19 incluyen sistemas de almacenamiento, servidores, equipos de climatización, dispositivos de red, soluciones de comunicación, sistemas de energización, herramientas de monitoreo y gestión, hipervisores y software especializado. Cada categoría detalla los componentes específicos y sus modelos, proporcionando una visión general de los recursos.

Tabla 19
Listado de Activos Cruciales del Data Center

Activos Cruciales	
Almacenamiento	3PAR 8200 (UPS) 3PAR 8200 (MASTER) MSA 2050 MSA2050 (UPS)
	ProLiant XL230a Gen9

Activos Cruciales	
Servidores	ProLiant XL230a Gen9
	ProLiant XL230a Gen9
	ProLiant XL250a Gen9
	ProLiant XL190r Gen10
	ProLiant XL190r Gen10
Climatización	CCD 151A STULZ
Switch Core	Catalyst 9300 - 48P - POE+ NETWORK ADVANTAGE
Switch SAN	HPE SN3000B 24/12 FC Switch (ESPACIO 38)
	HPE SN3000B 24/12 FC Switch (ESPACIO 36)
Comunicación	Swicth Catalyst 3650
	Swicth Catalyst 3650
	Swicth Catalyst 2960
	SG500-28
	SG5550XG-24T
Energización	APC Symmetra LX (UPS)
	APC Symmetra LX (UPS)
Monitoreo y Gestión	MONITOR 49INC LH49PMHP SERIES EDGE-LIT LED
	MONITOR 49INC LH49PMHP SERIES EDGE-LIT LED
	TELEVISOR LED 4K UN-40MU6103G
	Optiplex 7050 - Core i5-7500 - 8GB RAM - 1TB HDD
	Optiplex 7040 - Core i7-6700 - 8GB RAM - 1TB HDD
	Optiplex 7040 - Core i7-6700 - 8GB RAM - 1TB HDD
	Dell E2020H
	Dell E2020H
	Dell E2020H
	KB216P
	KB216T1
	KB216P
	MS116T
	MS111L
	BRISANE
Hipervisor	ESXI 7
Software	VCenter Server 7
	Storage Management Utility (MSA), plataformas propias de HPE
	SSMC Appliance 3.8.0.0.330
	ZKAccess 3.5
	Milestone Xprotect - Management 2018
	Ecaro 25
	10-063 Series Single Hazard Panel SHP Pro
	ZKTECO (Biométrico)

Activos Cruciales	
Varios	ZKTECO (Biométrico)
	ZKTECO (Biométrico)
	Cámara - DS-2CD2121G0-I
	AXIS M3004 Network Camera
	AXIS M3004 Network Camera

Nota. Tabla de activos cruciales del Data Center. Elaborado por: El Autor.

Se presentan las siguientes vulnerabilidades que se presentan en el Data Center en el 2024. Estas vulnerabilidades se han planteado en base a la ubicación geográfica y diferentes tipos de amenazas que este presenta, se dividirán en lógicas, físicas.

Tabla 20
Vulnerabilidades Lógicas del Data Center

Vulnerabilidades Lógicas
Vulnerabilidades
Bugs en software
Configuraciones del sistema ineficientes
Comunicaciones inseguras
Software desactualizado
Contraseñas inseguras
Configuración incorrecta de puertos
Metadatos incorrectos
Incompatibilidades de software y hardware obsoletos

Nota. En esta tabla se plantean las vulnerabilidades que presenta el Data Center. Elaborado por: El Autor.

Tabla 21
Vulnerabilidades Físicas del Data Center

Vulnerabilidades Físicas
Fallos de hardware
Intermitencia de luz
Desgaste de la infraestructura del edificio
Inconvenientes con proveedor de suministro
No contar con redundancia en aire acondicionado

Nota. En esta tabla se plantean las vulnerabilidades físicas que presenta el Data Center.

Elaborado por: El Autor.

Tabla 22
Vulnerabilidades debido a factor humano del Data Center

Vulnerabilidades debido a factor humano
Fugas de información debido a errores humanos
Falta de capacitación del personal en ciberseguridad
Dependencia de proveedores externos

Nota. En esta tabla se plantean las vulnerabilidades debido a factor humano que presenta el Data Center. Elaborado por: El Autor.

Las amenazas actuales que enfrenta el Data Center, dichas amenazas son consideradas en base a riesgos tecnológicos, físicos y sociales que presenta Ecuador en la actualidad, se dividirán de la misma forma en lógicas, físicas y debido a factor humano.

Tabla 23
Amenazas Lógicas del Data Center

Amenazas Lógicas
Phishing
Gusanos
Backdoor
Virus
Malware
DDoS
Spyware
Troyanos
Ransomware
Pérdida de conectividad

Nota. Tabla de Amenazas lógicas que presenta el Data Center. Elaborado por: El Autor.

Tabla 24

Amenazas Físicas del Data Center

Amenazas Físicas
Sobrecalentamiento de equipos
Colapso de estructura
Falla en el suministro eléctrico
Interrupciones de servicio por manifestaciones sociales
Conmoción social

Nota. Tabla de Amenazas físicas que presenta el Data Center. Elaborado por: El Autor.

Tabla 25

Amenazas debido a factor humano del Data Center

Amenazas debido a factor humano
Robo de información
Hurto de activos
Usuarios malintencionados

Nota. Tabla de Amenazas debido a factor humano que presenta el Data Center. Elaborado por: El Autor.

Los riesgos actuales del Data Center se basan en las amenazas identificadas tomando en cuenta las condiciones lógicas, físicas y debido a factor humano.

Tabla 26

Riesgos Lógicos del Data Center

Riesgos Lógicos
Ataques informáticos
Pérdida de datos

Nota. Tabla de riesgos lógicos que presenta el Data Center. Elaborado por: El Autor.

Tabla 27

Riesgos Físicos del Data Center

Riesgos Físicos
Interrupción del suministro eléctrico
Inundación
Sismo
Vientos fuertes
Incendios
Tormenta eléctrica
Erupciones volcánicas
Ceniza de volcanes
Daños por manifestaciones civiles violentas
Fallos en el sistema por climatización
Virus biológicos
Fallos en equipos por sobrecalentamiento
Infraestructura deficiente del edificio del Data Center

Nota. Tabla de riesgos físico que presenta el Data Center. Elaborado por: El Autor.

Tabla 28
Riesgos debido a factor humano del Data Center

Riesgos debido a factor humano
Pérdida de equipos por hurto

Nota. Tabla de riesgos debido a factor humano del Data Center. Elaborado por: El Autor.

Para el Data Center para valorar todos los activos previamente analizados se implementará las siguientes medidas, Para valorar los activos en base a los criterios de confidencialidad (C)

Tabla 29
Valoración de confidencialidad del Data Center

CONFIDENCIALIDAD	CRITERIO
Alto (3)	La exposición no controlada de datos o información sensibles genera un impacto incontrolable para el Data Center
Medio (2)	El manejo inadecuado de la información sensible genera un perjuicio controlado para el Data Center
Bajo (1)	La exposición de datos no genera ningún impacto para el Data Center

Nota. Tabla de criterios de confidencialidad del Data Center. Elaborado por: El Autor.

Para valorar la integridad (I) de los activos, identificando su importancia para el Data Center.

Tabla 30
Valoración de integridad del Data Center

INTEGRIDAD	CRITERIO
Alto (3)	La manipulación indebida de la información sensibles genera un impacto incontrolable para el Data Center
Medio (2)	La modificación no autorizada de información sensible genera un perjuicio considerable para el Data Center.
Bajo (1)	La exposición de información no genera ningún impacto para el Data Center

Nota. Tabla de criterios de integridad del Data Center. Elaborado por: El Autor.

La disponibilidad (D), evaluando la razón por la cual es importante la constante disponibilidad de servicio o información crucial, detallado en la Tabla No.31

Tabla 31
Valoración de disponibilidad del Data Center

DISPONIBILIDAD	CRITERIO
Alto (3)	La interrupción de servicios o a la información sensibles genera un impacto incontrolable para el Data Center
Medio (2)	La interrupción de servicios o a la información sensibles genera un efecto considerable para la institución
Bajo (1)	La interrupción de servicios o a la información sensibles genera un efecto mínimo para la institución

Nota. Tabla de criterios de disponibilidad del Data Center. Elaborado por: El Autor.

Junto con estas valoraciones, se ponderará en una escala del uno al tres, siendo el uno la escala más baja y tres la más critica a proteger, dicha ponderación se basa en el cálculo de (VA) que se interpreta como valoración de activos, seguido de la sumatoria de Confidencialidad, Integridad, Disponibilidad, para después este resultado dividirlo para tres y obtener un valor estimado al nivel de importancia.

Ecuación 1:Ecuación de valoración de activos

$$VA = \frac{C + I + D}{3}$$

Nota. Valoración del impacto de un activo. Elaborado por: Ministerio de telecomunicaciones y de la sociedad de la información (2020).

Definiremos los rangos de interpretación de riesgos, en base a colores y cantidades a las que se pueden aproximar, se detallara más a profundo en la siguiente tabla.

Tabla 32
Tabla de interpretación de ponderación de activos del Data Center

INTERPRETACIÓN DE PONDERACIÓN DE ACTIVOS		
2.66 < VA ≤ 3	ACTIVO CRITICO	
2 < VA < 2.66	ACTIVO IMPORTANTE	
1 ≤ VA < 2	ACTIVO LEVE	

Nota. Interpretación de activos según su criticidad. Elaborado por: El Autor.

En la siguiente tabla en base a las valoraciones de Confiabilidad, Integridad, Disponibilidad, se evaluarán los activos planteados, implementando la Formula No.1 Previamente analizada, el valor del activo que resulte de dicha operación se clasificara con la ayuda de la Tabla No.23, Dicha Ponderación se realiza en la Tabla No.33

Tabla 33
Ponderación de activos a ser protegidos

ACTIVOS PARA PROTEGER EN EL DATA CENTER				
Categoría	**(C)**	**(I)**	**(D)**	**Valor Activo (VA)**
Almacenamiento	3	3	3	3
Servidores	3	3	3	3
Climatización	1	3	3	2
Core	2	2	3	2.33
Switch SAN	2	2	3	2.33
Comunicación	2	2	2	2
Energización	1	2	3	2
Monitoreo y Gestión	2	2	2	2
Hipervisor	3	3	3	3
Software	3	3	3	3
Varios	1	2	1	1.33

Nota. En esta tabla se pondera los activos del Data Center. Elaborado por: El Autor.

Los activos críticos, con un VA de entre 2.66 y 3 son almacenamiento, servidores, hipervisor y software, cuya falla puede causar pérdida de datos, interrupciones en las operaciones y comprometer la estabilidad del Data Center.

Los activos importantes, con un VA entre 2 y 2.66, como climatización, Core, comunicación, energización y monitoreo, son esenciales para la operatividad y gestión de los servicios.

Los activos leves, con un VA entre 1 y 2, comprenden equipos y accesorios no críticos, cuyo impacto en caso de falla es menor.

El siguiente paso por valorar es los riesgos que se mantienen en el Data Center en base a los parámetros que adapta el Data Center, para esto se identificó 13 riesgos potenciales, valorados en función de 4 características: Probabilidad (P), Consecuencias (CS), Ocurrencia (O) y Urgencia (U), la formula la cual se implementará para hallar el valor critico será la

siguiente:

Ecuación 2:Ecuacion para obtener valor critico

$$VC = \frac{P + CS + O + U}{4}$$

Nota. Fórmula para hallar el valor critico en base a parámetros. Elaborado por: El Autor.

Con base en las especificaciones establecidas, cada parámetro será calificado en una escala del 1 al 3. La suma de estos valores individuales se considerará como el TOTAL. Este valor total, en conjunto con la suma de todos los parámetros, permitirá aplicar la Ecuación No. 2. El resultado obtenido de dicha ecuación, en relación con la Tabla No. 32, permitirá clasificar el riesgo como crítico, importante o leve.

Tabla 34
Evaluación de Riesgos en base a Parámetros

	PARAMETROS					
RIESGOS	**PROBABILIDAD (P)**	**CONSECUENCIAS (CS)**	**OCURRENCIA (O)**	**URGENCIA (U)**	**TOTAL**	**VALOR CRITICO (VC)**
Suministro eléctrico	2	3	3	3	11	2.75
Inundación	1	1	1	1	4	1
Terremoto	2	3	2	2	10	2.5
Viento fuerte	1	1	1	1	4	1
Incendio	2	3	1	3	7	2.25
Tormenta Eléctrica	3	2	2	2	9	2.25

RIESGOS	PROBABILIDAD (P)	CONSECUENCIAS (CS)	OCURRENCIA (O)	URGENCIA (U)	TOTAL	VALOR CRITICO (VC)
Erupción volcánica	2	3	2	3	10	2.5
Manifestaciones civiles violentas	2	2	2	1	7	1.75
Ataques informáticos	3	3	3	3	12	3
Negligencia	1	2	1	3	7	1.75
Climatización	2	3	1	3	9	2.25
Hurto	2	3	1	3	9	2.25
Virus biológicos	1	1	1	1	4	1

Nota. En esta tabla se evalúan los riesgos en base a los parámetros del Data Center. Elaborado por: El Autor.

De acuerdo con la Tabla No. 34, representa la evaluación de los riesgos que pueden afectar a los activos del centro de datos, considerando principalmente los daños potenciales al hardware. La valoración de activos (VA) se basa en estos riesgos y sus posibles consecuencias. Se determinó que los activos con mayor cantidad de riesgos críticos incluyen almacenamiento, servidores, climatización, switch CORE, switch SAN y comunicación. Estos riesgos son principalmente relacionados con el suministro eléctrico, incendios, terremotos y ataques informáticos. La razón de esta clasificación es que cualquier daño al hardware provocaría un impacto significativo debido al tiempo de respuesta necesario por parte del proveedor o de la organización, afectando así la capacidad de continuar brindando servicio. Los riesgos importantes fueron más prevalentes en los activos de energía, monitoreo y gestión, hipervisor y software, especialmente en relación con sismos, tormentas eléctricas y manifestaciones civiles violentas. Los riesgos leves se identificaron predominantemente en activos varios, con impactos menores asociados a inundaciones, viento fuerte y virus biológicos.

De acuerdo con esta información, compararemos nuestros activos pertinentes en función de los riesgos, tal como se detalló en la tabla No. 19. Estos activos se ponderarán en una escala del 1 al 3, donde el nivel 1 es el más leve, el nivel 2 es importante (amarillo) y el nivel 3 es crítico (rojo). estos activos se evaluarán en la tabla No.35.

Para simplificar la carga de información los riesgos se identifican con siglas. El suministro eléctrico es (SE), la inundación (I), el terremoto (T), el viento fuerte (VF) y el incendio (INC), tormenta eléctrica (TE), erupción volcánica (EV), manifestaciones civiles violentas (MCV), ataques informáticos (AI), la negligencia (N), la climatización (C), el hurto (H), virus biológicos (VB).

Tabla 35

Tabla de análisis de riesgos en base a los activos

EVALUACION DE ACTIVOS EN BASE A RIESGOS													
	RIESGOS												
ACTIVOS	**SE**	**I**	**T**	**VF**	**INC**	**TE**	**EV**	**MCV**	**AI**	**N**	**C**	**H**	**VB**
Almacenamiento	3	3	3	1	3	2	2	2	3	1	3	1	1
Servidores	3	3	3	1	3	2	2	2	3	1	3	1	1
Climatización	3	3	3	1	3	2	2	2	3	1	3	1	1
Switch Core	3	3	3	1	3	2	2	2	3	2	3	2	1
Switch SAN	3	3	3	1	3	2	2	2	3	2	3	2	1
Comunicación	3	3	3	1	3	2	2	2	3	2	3	2	1
Energización	3	3	3	1	2	2	1	1	1	2	3	1	1
Monitoreo y Gestión	2	3	3	1	3	2	2	2	3	2	1	1	1
Hipervisor	3	1	2	1	2	2	2	2	3	1	1	1	1
Software	2	1	1	1	1	1	1	1	3	3	1	1	1

Varios	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Nota. En esta tabla se evalúan los riesgos en base a los activos del Data Center. Elaborado por: El Autor

En la evaluación de activos basada en riesgos, que se centra en los daños al hardware de los activos, se determinó que la mayor cantidad de riesgos críticos (nivel 3) incluyen almacenamiento, servidores, climatización, switch CORE, switch SAN y comunicación. Estos riesgos están principalmente asociados con el suministro eléctrico, incendios, terremotos y ataques informáticos. La razón de esta clasificación radica en que cualquier daño al hardware provocaría un impacto significativo debido al tiempo de respuesta necesario por parte del proveedor o de la organización, afectando así la capacidad de continuar brindando servicio.

Los riesgos importantes (nivel 2) fueron más prevalentes en los activos de energía, monitoreo y gestión, hipervisor y software, especialmente en relación con sismos, tormentas eléctricas y manifestaciones civiles violentas. Por último, los riesgos leves (nivel 1) se identificaron predominantemente en activos varios, con impactos menores asociados a inundaciones, viento fuerte y virus biológicos.

4.1.3.3 ***Definición de Parámetros Temporales.*** Para definir nuestros parámetros temporales, es fundamental considerar los elementos que se analizarán: el RTO y el RPO. Estos parámetros nos proporcionarán una perspectiva clara de la cantidad de información y del tiempo de servicio que se pueden perder. Para una mejor comprensión de estas terminologías, se procederá a definirlas a continuación.

Según (Trejo, 2014), “El tiempo de tolerancia (RPO) es el que determina la cantidad de datos que estamos dispuestos a perder” (Párrafo tres)

El RPO representa la cantidad máxima de datos que el centro de datos puede permitirse perder entre la última copia de seguridad y el momento de una interrupción. Este parámetro es

fundamental para establecer las estrategias adecuadas de respaldo y recuperación de datos en el centro de datos.

Mientras que el RTO se interpreta como.

> El tiempo de recuperación (RTO) es el que determina la cantidad de tiempo de no disponibilidad que estamos dispuestos a asumir ante un problema, es decir, durante cuánto tiempo la organización puede permitirse tener los sistemas apagados sin afectar considerablemente a la continuidad del negocio. (Trejo, 2014, Parrafo cuatro)

Tomando en cuenta esta información, se comenzará por el RTO y en base a las tablas de los riesgos que presentan los activos del Data Center, procederemos a valorar los tiempos estimados de recuperación del Data Center en base a los riesgos latentes que este presenta, en la Tabla No.36 la cual implementara las mismas siglas, con el fin de no sobrecargar la tabla de información. El suministro eléctrico se representa como (SE), la inundación como (I), el terremoto como (T), el viento fuerte como (VF) y el incendio como (INC). Otros riesgos incluyen la tormenta eléctrica (TE), la erupción volcánica (EV), las manifestaciones civiles violentas (MCV), los ataques informáticos (AI), la negligencia (N), la climatización (C), el hurto (H) y los virus biológicos (VB).

Tabla 36

Tabla de tiempo de inactividad de activos en base a riesgos

	TIEMPO OBJETIVO DE RECUPERACION												
	RIESGOS												
ACTIVOS	**SE**	**I**	**T**	**VF**	**INC**	**TE**	**EV**	**MCV**	**AI**	**N**	**C**	**H**	**VB**
Almacenamiento	0,5	1	INDF	1	INDF	1	24	2	2	2	INDF	INDF	INDF
Servidores	0,5	1	INDF	2	INDF	0,3	24	2	2	2	INDF	INDF	INDF
Climatización	IND	2	INDF	1	INDF	2	24	1	NA	1	INDF	INDF	INDF
Switch Core	0,5	2	INDF	NA	INDF	2	24	2	2	2	INDF	INDF	INDF
Switch SAN	0,5	1	INDF	2	INDF	0,3	24	2	2	2	INDF	INDF	INDF
Comunicación	0,5	2	INDF	NA	INDF	0,3	24	2	2	2	INDF	INDF	INDF
Energización	NA	0,5	INDF	NA	INDF	0,3	0,5	2	NA	2	INDF	INDF	INDF
Monitoreo y Gestión	4	4	INDF	NA	INDF	4	4	4	4	4	INDF	INDF	INDF
Hipervisor	1	NA	NA	NA	NA	0,3	24	NA	2	2	NA	NA	NA
Software	1	NA	NA	NA	NA	0,3	24	NA	2	2	NA	NA	NA

TIEMPO OBJETIVO DE RECUPERACION													
	RIESGOS												
ACTIVOS	**SE**	**I**	**T**	**VF**	**INC**	**TE**	**EV**	**MCV**	**AI**	**N**	**C**	**H**	**VB**
Varios	4	NA	24	NA	INDF	NA	NA	NA	NA	5	NA	INDF	INDF

INDF	Indefinido
NA	No Aplica

Nota. En esta tabla se evalúan los tiempos en base a los riesgos del Data Center. Elaborado por: El Autor

La siguiente tabla ilustra el Tiempo Objetivo de Recuperación (RTO) para diversos activos del centro de datos, considerando distintos riesgos. Los activos y riesgos han sido evaluados para determinar el período máximo de inactividad permitido antes de afectar significativamente las operaciones del centro de datos. Este análisis se realiza en horas para proporcionar una perspectiva del tiempo necesario para restaurar cada activo en caso de interrupción.

El almacenamiento es el servicio primordial para las operaciones del centro de datos. El tiempo de recuperación objetivo para el almacenamiento varía según el tipo de riesgo. En caso de un fallo en el suministro eléctrico, el tiempo de recuperación es de 0.5 horas. Para una inundación, el tiempo de recuperación es de 1 hora. Los riesgos de terremoto, incendio y daños por climatización se consideran indefinidos, ya que el tiempo de recuperación puede depender de factores externos significativos. Otros riesgos incluyen viento fuerte, con un tiempo de recuperación de 1 hora, tormenta eléctrica con 1 hora, erupción volcánica con 24 horas, manifestaciones civiles violentas con 2 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

Los servidores también tienen tiempos de recuperación variados. Para un fallo en el suministro eléctrico, el tiempo de recuperación es de 0.5 horas, mientras que para una inundación es de 1 hora. Los riesgos asociados con terremotos, incendios y climatización tienen tiempos de recuperación indefinidos. En el caso de viento fuerte, el tiempo de recuperación es de 2 horas. Otros riesgos incluyen tormenta eléctrica con 0.3 horas, erupción volcánica con 24 horas, manifestaciones civiles violentas con 2 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

La climatización es crucial para mantener el ambiente del centro de datos. Los tiempos de recuperación para el suministro eléctrico son indefinidos, ya que dependen del proveedor y

no se puede determinar con exactitud cuándo se restablecerá la energía. Además, la climatización no está conectada a los sistemas de energía ininterrumpida. Para las inundaciones, el tiempo de recuperación es de 2 horas. Los riesgos de terremoto, incendio y daño por climatización tienen tiempos de recuperación indefinidos. En caso de viento fuerte, el tiempo de recuperación es de 1 hora. Otros riesgos incluyen tormentas eléctricas con un tiempo de recuperación de 2 horas, erupciones volcánicas con 24 horas, y manifestaciones civiles violentas con 1 hora. Los daños por ataques informáticos y virus biológicos no son aplicables.

El switch CORE, Presenta tiempos de recuperación de 0.5 horas para fallos en el suministro eléctrico e inundaciones. Los riesgos asociados con terremotos, incendios y climatización tienen tiempos de recuperación indefinidos. En el caso de viento fuerte, no aplica. Otros riesgos incluyen tormenta eléctrica con 2 horas, erupción volcánica con 24 horas, manifestaciones civiles violentas con 2 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

El switch SAN, es un dispositivo importante para la gestión del almacenamiento, tiene tiempos de recuperación de 0.5 horas para fallos en el suministro eléctrico y 1 hora para inundaciones. Los riesgos de terremoto, incendio y climatización tienen tiempos de recuperación indefinidos. En el caso de viento fuerte, el tiempo de recuperación es de 2 horas. Otros riesgos incluyen tormenta eléctrica con 0.3 horas, erupción volcánica con 24 horas, manifestaciones civiles violentas con 2 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

La comunicación presenta los tiempos de recuperación son de 0.5 horas para fallos en el suministro eléctrico y 2 horas para inundaciones. Los riesgos de terremoto, incendio y climatización tienen tiempos de recuperación indefinidos. En el caso de viento fuerte, no aplica.

Otros riesgos incluyen tormenta eléctrica con 0.3 horas, erupción volcánica con 24 horas, manifestaciones civiles violentas con 2 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

La energización tiene tiempos de recuperación indefinido para fallos en el suministro eléctrico ay que depende del proveedor, 0.5 horas para inundaciones. Los riesgos de terremoto, incendio y climatización tienen tiempos de recuperación indefinidos. En el caso de viento fuerte, no aplica. Otros riesgos incluyen tormenta eléctrica con 0.3 horas, erupción volcánica con 0.5 horas, y manifestaciones civiles violentas con 2 horas. Los daños por ataques informáticos y virus biológicos no aplican.

El monitoreo y gestión, crucial para la supervisión del centro de datos, tiene tiempos de recuperación de 4 horas para fallos en el suministro eléctrico y 4 horas para inundaciones. Los riesgos asociados con terremotos, incendios y climatización tienen tiempos de recuperación indefinidos. En el caso de viento fuerte, no aplica. Otros riesgos incluyen tormenta eléctrica con 4 horas, erupción volcánica con 4 horas, manifestaciones civiles violentas con 4 horas, ataques informáticos con 4 horas, y negligencia con 4 horas.

El hipervisor, importante para la virtualización, tiene tiempos de recuperación de 1 hora para fallos en el suministro eléctrico. Los riesgos de inundación, terremoto, viento fuerte, incendio y climatización no aplican. Otros riesgos incluyen tormenta eléctrica con 0.3 horas, erupción volcánica con 24 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

El software tiene tiempos de recuperación de 1 hora para fallos en el suministro eléctrico. Los riesgos de inundación, terremoto, viento fuerte, incendio y climatización no aplican. Otros riesgos incluyen tormenta eléctrica con 0.3 horas, erupción volcánica con 24 horas, ataques informáticos con 2 horas, y negligencia con 2 horas.

El activo "Varios" tiene un tiempo de recuperación de 4 horas para fallos en el suministro eléctrico y 24 horas para inundaciones. Los riesgos de terremoto y hurto tienen tiempos de recuperación indefinidos. Otros riesgos incluyen viento fuerte con 24 horas, manifestaciones civiles violentas no aplica, y negligencia con 5 horas.

Además, respecto al RPO, La probabilidad de pérdida de información se ha evaluado como improbable. Esto se debe a que el sistema de almacenamiento principal está configurado específicamente, el sistema de almacenamiento puede soportar la falla simultánea de hasta dos discos dentro del mismo arreglo.

4.1.3.4 ***Establecimiento de Recursos Necesarios.*** Para asegurar la continuidad operativa del Data Center de la Universidad Politécnica Salesiana, se requiere una planificación detallada de los recursos necesarios para restaurar las operaciones a un nivel aceptable en caso de interrupciones. Esto implica la identificación clara de personal capacitado, tecnología adecuada, instalaciones preparadas y cualquier otro recurso esencial para mitigar los impactos derivados de posibles incidentes. A continuación, se detalla la estructura necesaria:

Tabla 37
Personal Capacitado del Data Center

PERSONAL CAPACITADO	
Puesto de trabajo	**Descripción**
Ingenieros de sistemas	Con experiencia en gestión de data centers.
Técnicos especializados	En mantenimiento de hardware y software.
Personal de seguridad y vigilancia	Encargado del control de accesos y monitoreo continuo.

Nota. En esta tabla se detalla el personal capacitado con el que center el Data Center en el periodo 64. Elaborado por: El Autor.

Tabla 38
Tecnologías y Equipamiento del Data Center

TECNOLOGÍA Y EQUIPAMIENTO	
Recurso	**Descripción**
Servidores redundantes	Garantizan la continuidad operativa
Sistemas de almacenamiento con replicación	Disponibilidad de datos
UPS (Sistemas de Alimentación Ininterrumpida)	Protegen equipos electrónicos de interrupciones y sobretensiones
Equipos de climatización y refrigeración	Mantienen condiciones ambientales óptimas

Nota. En esta tabla se detalla las tecnologías y equipamiento que center del Data Center.

Elaborado por: El Autor

Tabla 39
Instalaciones Físicas

Instalaciones Físicas	
Recurso	**Descripción**
Infraestructura de red	Dispositivos de red configurados para generar disponibilidad de servicio.
Centros de monitoreo	Equipados con pantallas y sistemas de gestión de red.

Nota. En esta tabla se detalla las instalaciones físicas del Data Center. Elaborado por: El Autor

4.1.4 Estrategias y soluciones de continuidad de negocio

La estrategias y soluciones se detallan a continuación.

4.1.4.1 ***Climatización.*** Se plantea la instalación de un sistema adicional de climatización (N+1) para garantizar la redundancia. Este sistema no solo ayudará a mantener temperaturas óptimas para los equipos, sino que también reducirá el

riesgo de fallos por sobrecalentamiento.

4.1.4.2 ***Mejora de Infraestructura del Edificio del Data Center.*** Un aspecto crucial para abordar es la condición estructural del edificio. Actualmente, el edificio presenta fisuras en las paredes y techos, lo cual es alarmante para la integridad y seguridad del Data Center. Se debe realizar una evaluación estructural detallada y proceder con las reparaciones necesarias. Las fisuras deben ser reparadas adecuadamente para evitar problemas de humedad y posibles filtraciones de agua. Adicionalmente, la ubicación del edificio plantea un riesgo significativo debido a su proximidad a una quebrada, ubicada a solo 82,29 metros. Esta cercanía aumenta la vulnerabilidad del Data Center a inundaciones y otros desastres naturales. Se deben implementar medidas de mitigación, como la construcción de barreras de contención y sistemas de drenaje mejorados, para reducir el riesgo de inundación y proteger la infraestructura del Data Center.

4.1.4.3 ***Contratación de Personal Adiciona.*** Actualmente, el Data Center cuenta únicamente con dos roles: un administrador y un auxiliar. Esta estructura puede presentar inconvenientes significativos si ninguno de los dos responsables está presente, especialmente durante los fines de semana. En base a una entrevista con el auxiliar del Data Center, se verifica que durante los fines de semana solo se realiza una revisión el sábado y otra el domingo, lo que resulta en un análisis y monitoreo inadecuado, para mejorar esta situación, se propone la contratación de personal adicional para cubrir los turnos de fin de semana, asegurando una

supervisión continua del Data Center.

4.1.5 Planes de continuidad de negocio.

Como se explicó en el apartado 3.6, los planes de continuidad de negocio se centrarán en la distribución de roles y responsabilidades del Data Center, siguiendo la normativa COBIT. Esta normativa facilita la comprensión de la gobernanza y administración del Data Center, los planes de recuperación ante desastres se elaborarán estratégicamente en su apartado correspondiente, En la siguiente tabla se detalla la composición de la administración y gobernanza del Data Center.

Tabla 40
Gobernanza y Administración del Data Center

Gobernanza y Administración del Data Center	
Administración	**Gobernanza**
Administrador del Data Center	Vicerrectorado Consejo de carrera

Nota. En esta tabla se detalla la estructura de gobernanza y administración de Data Center durante el periodo 64. Elaborado por: El Autor.

Una vez establecida la administración y gobernanza del Data Center, es oportuno detallar las actividades que comprenden los roles específicos. En la siguiente tabla se especifican.

Tabla 41
Actividades que desempeñan los Roles del Data Center

	ROLES			
	Consejo de carrera	**Vicerrectorado**	**Administrador del Data Center**	**Auxiliar**
ACTIVIDADES	Aprobación	Aprobación	Aprobación	Desarrolla las actividades

Nota. En esta tabla se detalla las actividades que desempeñan los diferentes roles en el Data Center durante el periodo 64. Elaborado por: El Autor.

4.2 DESARROLLO DE DRP

4.2.1 Descripción del escenario

La descripción integral del Data Center se encuentra detallada en el apartado 4.1.1, donde se describe el escenario, comenzando desde su ubicación geográfica con coordenadas precisas. Además, se aborda un análisis basado en la topología en el apartado 4.1.1.2. Asimismo, se presenta una visión topológica de la red física en el apartado 4.1.1.3. La fuente de energía eléctrica que suministra a los dispositivos del Data Center está detallada en el apartado 4.1.1.5.

4.2.2 Analizar los riesgos

Para abordar el análisis de riesgos, primero se plantea conocer los antecedentes de incidentes del Data Center, detallados en la Tabla No. 5. Esto permite determinar los componentes más frecuentes en presentar fallas.

Los activos con mayor incidencia de fallos se detallan en el apartado 4.1.3.1. Las vulnerabilidades se encuentran descritas en las Tablas 20, 21 y 22, mientras que las amenazas están detalladas en las Tablas 23, 24 y 25. Finalmente, los riesgos detectados en el Data Center se encuentran en las Tablas 26, 27 y 28.

4.2.3 Análisis de impacto al negocio (BIA)

El análisis de impacto al negocio se encuentra desarrollado en el apartado 4.1.3, donde se valoran los antecedentes de incidentes del Data Center. Este apartado profundiza en las amenazas, vulnerabilidades y riesgos, además de detallar los activos de software, hardware y de seguridad del Data Center. Asimismo, se especifican los tiempos objetivos de recuperación (RTO) y el punto objetivo de recuperación (RPO), evaluando de manera integral los activos del Data Center.

4.2.4 Estrategias de recuperación

Las estrategias de recuperación adaptadas a la problemática del Data Center se abordan en el apartado 4.1.4. Estas fueron evaluadas basándose en un análisis topológico del Data Center, resultando en la identificación de la falta de redundancia en un componente específico, detallado en el apartado 4.1.4.1. Además, se señala la insuficiencia de personal en el apartado 4.1.4.3, identificada a partir de una entrevista con el personal del Data Center. Por último, se abordan los problemas de infraestructura en el apartado 4.1.4.2, donde se detalla que el edificio presenta numerosas fisuras, lo cual podría desencadenar problemas en el futuro.

4.2.5 Establecer roles y responsabilidades

Como se especificó previamente en el apartado 4.1.5, se determinó, en base a la normativa COBIT, la gobernanza y administración detallada en la Tabla No. 40. Además, se describen las actividades desempeñadas por los roles que constituyen el Data Center en La Tabla No.41.

Una vez reconocidos los roles que comprenden el funcionamiento del Data Center, es crucial determinar las responsabilidades asociadas a cada uno.

La matriz RACI es una herramienta que define roles y responsabilidades dentro de un proyecto o proceso organizacional. En esta estructura, "R" representa a los responsables, quienes son responsables de ejecutar las tareas asignadas. "A" corresponde a los que tienen Autoridad, quienes revisan y aprueban el trabajo completado. "C" se refiere a los Consultores, a quienes se consulta antes de tomar decisiones. Y finalmente, "I" son los Informadores. (Santos, 2024)

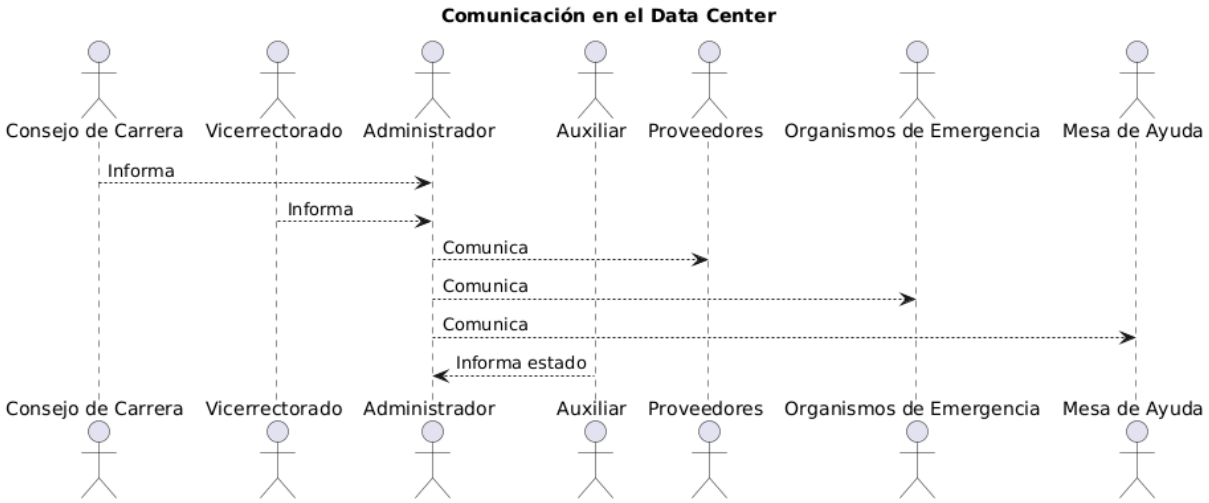
Tabla 42
Matriz de RACI enfocada al Data Center

	ROL			
Actividad	**Consejo de carrera**	**Vicerrectorado**	**Administrador**	**Auxiliar**
Evaluación de daños	I	I	R	R
Comunicación de crisis	I	I	R	R
Restauración de servicios		I	I	R
Restauración de conectividad		I	I	R
Reporte de evento		R	R	R
Reporte de incidencia		I	I	R
Recuperación de capacidad de gestión			R	R
Mantenimiento del plan			A	R
Reanudación de operaciones	I	I	A	R
Acciones correctivas		I	A	R

Nota. En esta tabla se establecen las responsabilidades de cada rol que conforma el Data Center. Elaborado por: El Autor.

Una vez establecidas dichas responsabilidades, se representan en la Figura No. 6, donde se detallan las interacciones en el Data Center. El Consejo de Carrera y el Vicerrectorado proporcionan directrices y decisiones estratégicas al Administrador, quien, junto con su Auxiliar, se encarga de implementar estas políticas. Además, el Administrador desempeña un papel crucial al comunicarse con proveedores para asegurar suministros, licencias o acuerdos de garantías, además de comunicarse con las mesas de ayuda, En situaciones de emergencia, tanto el Administrador como el Auxiliar son responsables de contactar y coordinar con los organismos de emergencia para manejar y resolver crisis de manera eficiente.

Figura 6
Comunicación del Data Center



Nota. Representación de comunicación entre roles ante incidentes o nuevas políticas. Elaborado por: El Autor.

4.2.6 Mantenimiento del plan

El Data Center de la Universidad Politécnica Salesiana, conforme a todo el contenido analizado, se encuentra en constante actualización. Es fundamental mantener una adaptabilidad continua en tecnologías, infraestructura, personal y planes, como el Plan de Continuidad del Negocio (BCP), el Plan de Recuperación ante Desastres (DRP), el Análisis de Impacto en el Negocio (BIA) y el Plan de Contingencia (CP). Por este motivo, los planes actualmente

implementados están actualizados conforme a las nuevas políticas y tecnologías disponibles en el Data Center.

4.2.6.1 ***Cambios que afectan al plan.*** Dichos cambios son los siguientes.

4.2.6.1.1 ***Hardware.*** La introducción, reubicación o actualización de componentes físicos del Data Center, como servidores o sistemas de almacenamiento, es esencial. Sin embargo, se debe considerar que muchos de estos dispositivos están quedando obsoletos.

4.2.6.1.2 ***Software.*** Dado que la virtualización es un servicio clave del Data Center, es crucial mantener el software actualizado. Los avances tecnológicos y las actualizaciones de software deben estar reflejados en los componentes que este posee. Es importante que el Data Center cuente con software compatible con su hardware y evite el uso de software desactualizado.

4.2.6.1.3 ***Personal del CPD.*** Los roles y responsabilidades asignados al personal del Data Center son fundamentales. Cualquier cambio en el equipo, ya sea por la incorporación o salida de miembros, requiere una redistribución de actividades y una actualización del plan para reflejar estos cambios.

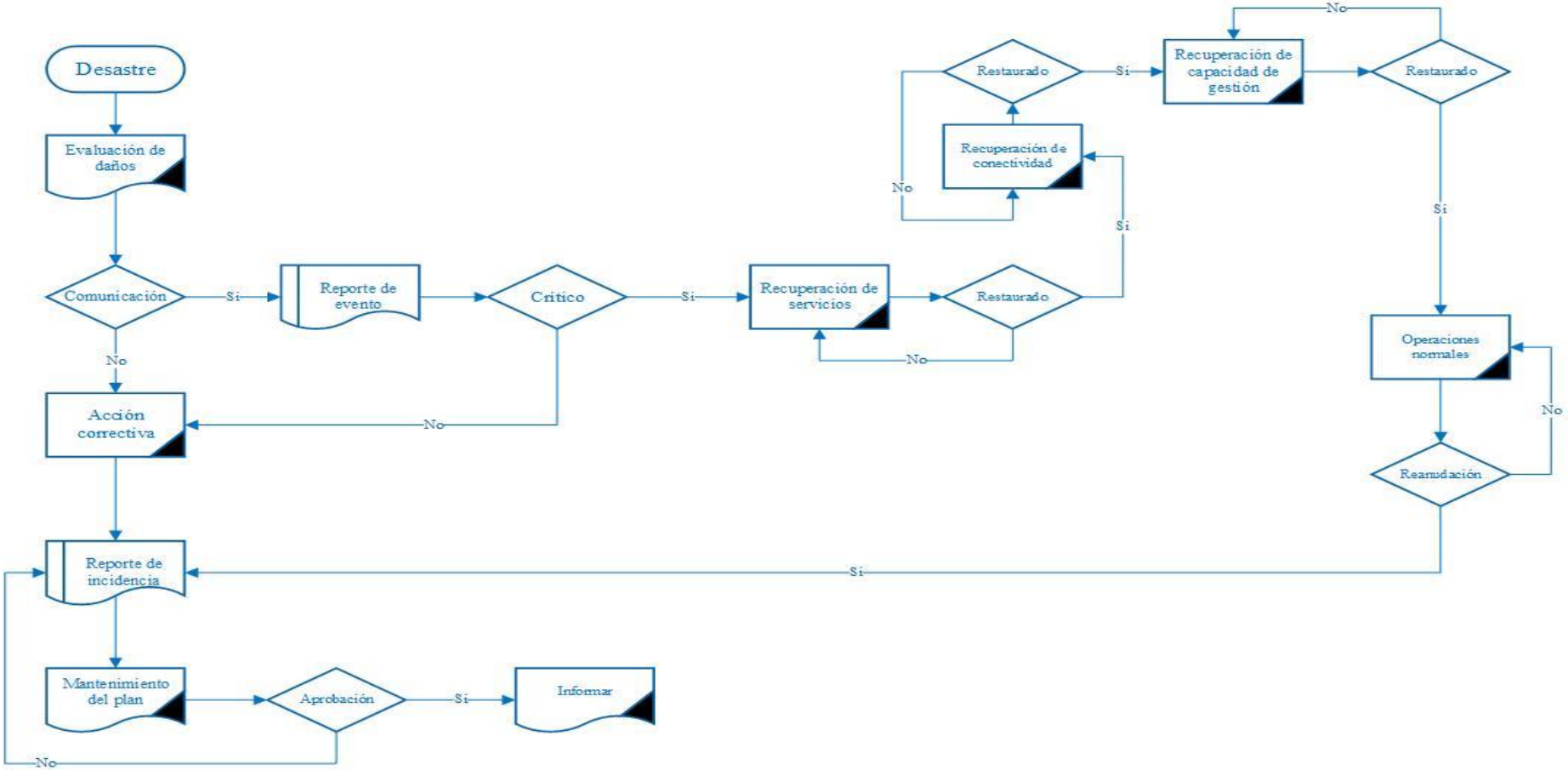
4.2.6.1.4 ***Mantenimiento Periódico.*** Es recomendable realizar una revisión y mantenimiento del plan al menos una vez al año, independientemente de los cambios específicos. Esto asegura que el plan esté siempre adaptado a las necesidades y circunstancias actuales del Data Center.

4.2.7 Manejo del plan

El plan desarrollado abarca diversos tipos de riesgos, incluyendo amenazas y vulnerabilidades de tipo lógico, físico y humano. Se establecen el tiempo objetivo de recuperación y el punto objetivo de recuperación para determinar la tolerancia a la pérdida de información. Sin embargo, reconocer que esta información y análisis no son suficientes para abordar problemas específicos es crucial. Se requiere la experiencia del personal del Data Center para identificar y diferenciar los tipos de incidentes o desastres que puedan surgir. Basándose en su conocimiento individual y colectivo, deben asegurar la continuidad de los servicios de virtualización y almacenamiento. Además, es esencial considerar los roles, acciones, responsabilidades y compromisos del personal con la institución. A continuación, se describe el proceso de despliegue del plan de recuperación de desastres previamente establecido para el Data Center de la Universidad Politécnica Salesiana.

Figura 7

Diagrama del proceso de despliegue del plan de recuperación de desastre y continuidad del negocio



Nota. Flujograma del manejo del plan. Elaborado por: Guillen (2018).

4.3 DESARROLLO DE CP

4.3.1 Evaluación de riesgo

Las evaluaciones de riesgos, amenazas y vulnerabilidades se encuentran detalladas en las tablas 20, 21, 22, 23, 24, 25, 26, 27 y 28. Estas tablas abordan aspectos físicos, lógicos y del factor humano. Los activos se valoran según su criticidad para el Data Center en la Tabla No.33, y los riesgos se evalúan basándose en parámetros específicos detallados en la Tabla No.34. Asimismo, se realiza una evaluación de los activos en función del riesgo, la cual está detallada en la Tabla No.35.

4.3.2 Definición de objetivos.

Los objetivos se establecieron considerando las necesidades actuales del Data Center y las políticas vigentes, en conformidad con las normativas COBIT e ITIL. Los objetivos generales se detallan en el apartado 1.4, mientras que los objetivos específicos se encuentran en el apartado 1.4.1.

4.3.3 Formación de un equipo

Los equipos previamente mencionados se encuentran detallados en el área de administración y gobernanza, tal como se refleja en la Tabla No.40. Además, se especificó sus responsabilidades dentro del Data Center, información que se detalla en la Tabla No.42.

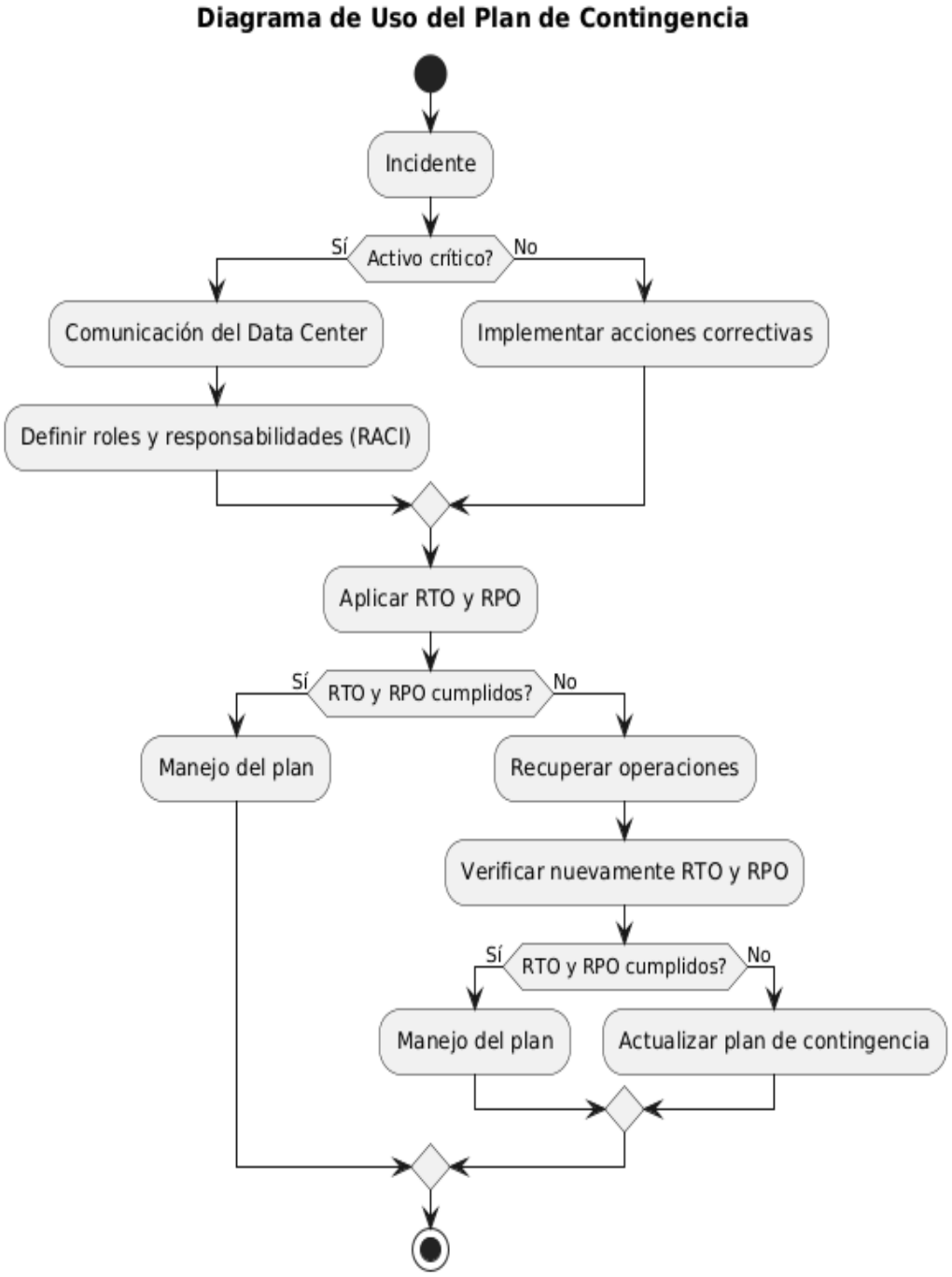
4.3.4 Plan de comunicación

El plan de comunicación se ha detallado en la Figura No.6, donde se representan todos los roles del Data Center y sus interacciones para la implementación de nuevas políticas. Se describe cómo se aplican estas políticas y las funciones realizadas por el administrador en este contexto.

4.3.5 Manejo del Plan

El diagrama de uso del plan de contingencia representa un enfoque estructurado para la gestión de incidentes. Comienza con la identificación de un incidente; si se determina que afecta a un activo crítico, se procede según lo establecido en la Figura No. 6 del plan de comunicación del Data Center y se aplica la matriz RACI definida en la Tabla No. 42. En caso contrario, se implementan acciones correctivas. Posteriormente, se evalúa el cumplimiento de los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) para estimar el tiempo y los datos potencialmente perdidos. En caso de incumplimiento inicial, se ejecutan operaciones de recuperación. En todas las situaciones, se enfatiza la importancia de visualizar el manejo del plan, ya que permite una representación cronológica de cómo abordar un incidente. El diagrama correspondiente se detalla en la Figura No. 8.

Figura 8
Diagrama de uso de plan de contingencia



Nota. Se especifica como se despliega el plan de contingencia para el Data Center. Elaborado por: El Autor

4.3.6 Pruebas de planes

Durante el análisis, se utilizó un diagrama de procedimientos que comenzó con el análisis del activo y su criticidad. Luego, se implementó la comunicación planteada en la Figura 6 y se realizó un análisis basado en los tiempos objetivos de recuperación (RTO) y los puntos objetivos de recuperación (RPO), conforme a la normativa ISO 22301, COBIT e ITIL. Esta información fue proporcionada por el auxiliar del Data Center con quien se realizaron las pruebas. Se ha procedido con las pruebas de este, teniendo como resultado que el despliegue del plan se ajusta al escenario actual del Data Center.

4.3.7 Mantenimiento

En el apartado 4.2.6 se detallan el mantenimiento del plan y los requisitos planteados para mejorar dicho enfoque de mantenimiento. Es importante recordar que estos planes están estrechamente relacionados y comparten el mismo enfoque de mantenimiento, ya que se valoran los mismos activos y se cuenta con el mismo personal, infraestructura y componentes en base a la propuesta actual. Si existen modificaciones o se contrata personal nuevo, estos cambios afectan el plan. Por lo tanto, es fundamental considerar la información de este apartado para asegurar la actualización y efectividad continua del plan.

CONCLUSIONES

El Plan de Continuidad del Negocio del Data Center de la Universidad Politécnica Salesiana se enfoca en proteger sus activos mediante un análisis de vulnerabilidades, amenazas y riesgos tanto físicos como lógicos. Su implementación fortalece la resiliencia ante sucesos desafortunados, estableciendo estrategias para minimizar el impacto y asegurar la continuidad de los servicios de almacenamiento y virtualización. La actualización periódica del BCP para adaptarse a los avances tecnológicos del Data Center es esencial para mantener su efectividad. La comunicación efectiva y la experiencia de los miembros del Data Center, junto con la capacitación ante nuevas amenazas y las pruebas continuas del BCP, son clave para una preparación adecuada y una respuesta efectiva frente a las adversidades.

El Análisis de Impacto al Negocio ha identificado los activos críticos y los servicios clave para los estudiantes y el área investigativa. Se evaluaron diversos tipos de riesgos, tanto físicos como lógicos, para determinar su impacto en la disponibilidad, integridad y confidencialidad de datos y servicios. Se utilizaron ponderaciones matemáticas basadas en niveles de criticidad, fundamentadas en un historial de incidentes, para establecer tiempos objetivos de recuperación y considerar la cantidad y capacidad de datos aceptables para perder. Esto asegura una visión de escenarios hipotéticos de desastres y cómo estos pueden afectar la funcionalidad del Data Center.

RECOMENDACIONES

Se recomienda priorizar la protección de activos críticos contra riesgos físicos y lógicos mediante la actualización constante de los planes realizados, la implementación de medidas de comunicación efectivas, y la definición clara de roles y responsabilidades. Esto establecerá un entorno proactivo y funcional para la aplicación de los planes de recuperación de desastres como el BCP, DRP, BIA y CP. Es importante el mantener una revisión constante del manejo y mantenimiento de estos planes para garantizar que el Data Center esté preparado no solo para las necesidades actuales, sino también para enfrentar cualquier incidente futuro.

Para fortalecer las actividades del Data Center, se recomienda considerar la contratación de personal adicional especializado. Además, es crucial actualizar el software y hardware que próximamente pueden ser obsoletos para mejorar el desempeño operativo, la seguridad y facilitar la adaptación a nuevas tecnologías. Además, se sugiere mejorar la infraestructura del edificio del Data Center para garantizar condiciones óptimas.

REFERENCIAS BIBLIOGRÁFICAS

axessnet. (2 de Julio de 2023). *Plan de contingencia para tecnologías de la información*. Obtenido de axessnet: https://axessnet.com/plan-de-contingencia-para-tecnologias-de-la-informacion/

Bevan, T. (Octubre de 2019). *ISO 22301:2019 GUÍA DE IMPLANTACIÓN DE LA CONTINUIDAD DE NEGOCIO.* Obtenido de nqa: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

G, S. (8 de Abril de 2024). *Business Impact Analysis (BIA): Protecting Your Business Continuity*. [Publicación]. linkedin. https://www.linkedin.com/pulse/business-impact-analysis-bia-protecting-your-continuity-santosh-g-cxahc/

Gonzales, D. (1 de Diciembre de 2023). *Business Impact Analysis (BIA): Resiliencia Empresarial*. https://ubtcompliance.com/blog/business-impact-analysis-bia-resiliencia-empresarial/

Gonzales, H. (31 de Mayo de 2021). *ISO 22301 – CUÁNDO IMPLEMENTAR UN PLAN DE CONTINUIDAD DE NEGOCIO*. https://calidadgestion.wordpress.com/2021/05/31/iso-22301-cuando-implementar-un-plan-de-continuidad-de-negocio/

Guillen, T. M. (Agosto de 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) de la carrera de ingeniería en ciencias de la computación de la Universidad Politecnica Salesiana.* [Tesis de Pregrado,

Universidad Politécnica Salesiana del Ecuador]. https://dspace.ups.edu.ec/bitstream/123456789/15904/1/UPS-ST003686.pdf

Guillen, T. M. (Agosto de 2023). Info DC. *Info DC*. Quito, Pichincha, Ecuador.

HAZOP. (s.f.). *HAZOP (Hazard and Operability Study)*. https://www.tema.es/seguridad/analisis-riesgo-de-proceso-hazop

IBM. (8 de Marzo de 2021). *Criterios de diseño del entorno*. https://www.ibm.com/docs/es/power7?topic=planning-environmental-design-criteria

IBM. (2023). *¿Qué es un plan de contingencia?*. https://www.ibm.com/es-es/topics/contingency-plan

IBM. (2023). *What is a disaster recovery plan (DRP)?*. https://www.ibm.com/topics/disaster-recovery-plan#:~:text=Data%20center%20DRPs%20create%20operational,broader%20in%20scope%20than%20others.

informacion, M. d. (2020). GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. 31.

Mauricio Olivari Tavera, C. E., & Ramírez Coll, C. E. (2013). *PLAN DE CONTINUIDAD DEL NEGOCIO*. [Tesis de Pregrado, Universidad Piloto de Colombia]. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2612/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Moreno, L. M., & Galeano Sánchez, R. R. (2013). *Análisis de Impacto al Negocio*. [Tesis de Pregrado, Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00000815.pdf

PÚBLICA, E. S. (2022). PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS 2021- 2022. *Escuela Superior de Administracion Publica*, 41.

RCR, A. I. (15 de Octubre de 2021). *¿Cómo hacer un plan de continuidad de negocio o BCP?*. [Publicación]. linkedin. https://www.linkedin.com/pulse/c%C3%B3mo-hacer-un-plan-de-continuidad-negocio-o-bcp-asesorias-iso/

Santos, D. (25 de Enero de 2024). *Matriz RACI: qué es y cómo crearla en Excel (con ejemplos)*. https://blog.hubspot.es/marketing/matriz-raci#que-es

Solutions, G. C. (18 de Junio de 2024). *Plan de continuidad del negocio (BCP): corazón de ISO 22301:2019*. [Publicación]. linkedin. https://www.linkedin.com/pulse/plan-de-continuidad-del-negocio-bcp-coraz%C3%B3n-iso-avfxe/

Tech-Blog. (09 de Marzo de 2023). *ISO, COBIT e ITIL: Conoce estas normas y estándares internacionales.* https://www.gb-advisors.com/es/normas-y-estandares-internaciones/

Terreros, D. (13 de Marzo de 2023). *Qué es el método FMEA, cómo se aplica y ejemplo*. https://blog.hubspot.es/marketing/metodo-fmea

Trejo, D. R. (24 de Febrero de 2014). *RPO Y RTO*. https://www.davidromerotrejo.com/2014/02/rpo-y-rto.html