UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Diseño de un plan de recuperación ante desastres (DRP), del centro de datos para continuidad de servicios de la empresa NetPay.

AUTOR:
Ing. Vásquez Díaz, Ronald Richard

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:
Ing. Bohórquez Escobar, Celso Bayardo, PhD

Guayaquil, Ecuador
13 de marzo de 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el presente trabajo de titulación fue realizado en su totalidad por **Vásquez Díaz, Ronald Richard**, como requerimiento para la obtención del Título de Magister en Telecomunicaciones.

TUTOR

f. _____

Ing. Bohórquez Escobar, Celso Bayardo, Ph.D

DIRECTOR DEL PROGRAMA

f. _____

Ing. Bohórquez Escobar, Celso Bayardo, Ph.D

Guayaquil, a los 13 días del mes de marzo del año 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Ing. Vásquez Díaz, Ronald Richard**

DECLARO QUE:

El Trabajo de Titulación **Diseño de un plan de recuperación ante desastres (DRP), del centro de datos para continuidad de servicios de la empresa NetPay.**, previo a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 13 días del mes de marzo del año 2025

EL AUTOR

f. _____
Ing. Vásquez Díaz, Ronald Richard

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Ing. Vásquez Díaz, Ronald Richard**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación **Diseño de un plan de recuperación ante desastres (DRP), del centro de datos para continuidad de servicios de la empresa NetPay.**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 13 días del mes de marzo del año 2025

EL AUTOR

f. _____

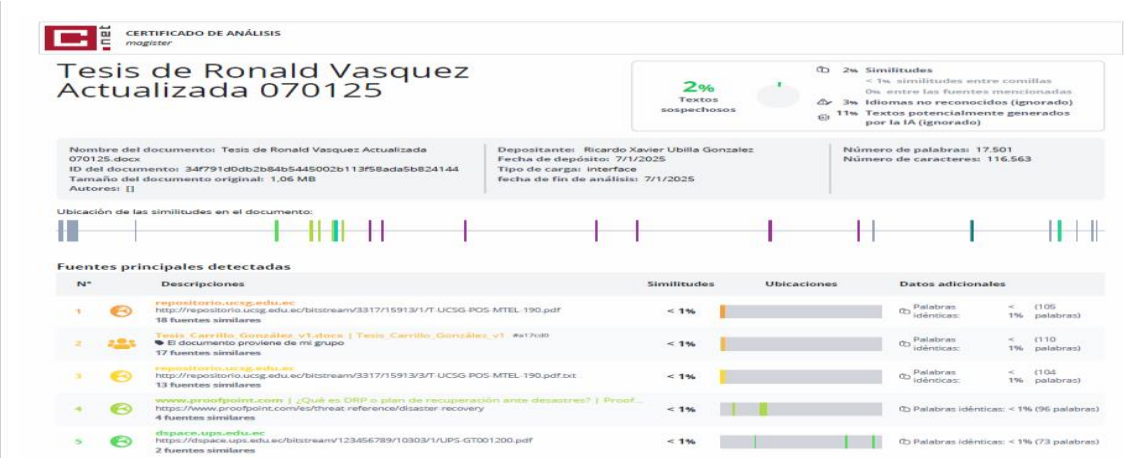
Ing. Vásquez Díaz, Ronald Richard

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

REPORTE COMPILATIO


CERTIFICADO DE ANÁLISIS
magister

Tesis de Ronald Vasquez Actualizada 070125

2% Textos sospechosos

2% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas
3% Idiomas no reconocidos (ignorado)
11% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: Tesis de Ronald Vasquez Actualizada 070125.docx
ID del documento: 34f791d0db2b84b5445002b113f58ada5b824144
Tamaño del documento original: 1,06 MB
Autores: []

Depositante: Ricardo Xavier Ubilla Gonzalez
Fecha de depósito: 7/1/2025
Tipo de carga: interface
fecha de fin de análisis: 7/1/2025

Número de palabras: 17.501
Número de caracteres: 116.563

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.ucsg.edu.ec http://repositorio.ucsg.edu.ec/bitstream/3317/15913/1/T-UCSG-POS-MTEL-190.pdf 18 fuentes similares	< 1%		Palabras idénticas: < 1% (105 palabras)
2	Tesis_Carrillo_González_v1.docx | Tesis_Carrillo_González_v1 #a17cd0 El documento proviene de mi grupo 17 fuentes similares	< 1%		Palabras idénticas: < 1% (110 palabras)
3	repositorio.ucsg.edu.ec http://repositorio.ucsg.edu.ec/bitstream/3317/15913/3/T-UCSG-POS-MTEL-190.pdf.txt 13 fuentes similares	< 1%		Palabras idénticas: < 1% (104 palabras)
4	www.proofpoint.com | ¿Qué es DRP o plan de recuperación ante desastres? | Proof... https://www.proofpoint.com/es/threat-reference/disaster-recovery 4 fuentes similares	< 1%		Palabras idénticas: < 1% (96 palabras)
5	dspace.ups.edu.ec https://dspace.ups.edu.ec/bitstream/123456789/10303/1/UPS-GT001200.pdf 2 fuentes similares	< 1%		Palabras idénticas: < 1% (73 palabras)

Certifico que después de revisar el documento final del trabajo de titulación **Diseño de un plan de recuperación ante desastres (DRP), del centro de datos para continuidad de servicios de la empresa NetPay,** presentado por el estudiante **Ronald Richard Vásquez Díaz**, fue enviado al Sistema Anti plagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 2%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

f._____

Ing. Bohórquez Escobar, Celso Bayardo, PhD

AGRADECIMIENTO

A Dios por la bendición dada, y por la fuerza para poder continuar, a pesar de los obstáculos presentados.

Y a todos los que hicieron posible, que de una u otra forma colaboraron y estuvieron pendientes para que esto sea posible.

Ing. Ronald Richard Vásquez Díaz

DEDICATORIA

Este trabajo se encuentra dedicado en primer lugar a Dios, por haberme dado la fuerza, sabiduría y la salud para poder llegar hasta este momento tan importante de mi vida profesional. A mi esposa, padres y hermanos, que estuvieron junto a mí en cada momento, apoyándome y no dejando que desmaye en ningún instante, a pesar de todos los momentos difíciles que pasamos. A todos los docentes que aportaron con su granito de arena para poder cumplir con la meta trazada.

lng. Ronald Richard Vásquez Díaz

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f._____

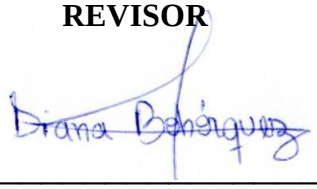
Ing. Bohórquez Escobar, Celso Bayardo, PhD

TUTOR

f._____

Ing. Zamora Cedeño, Néstor Armando, MSc.

REVISOR



f._____

Ing. Bohórquez Heras, Diana Carolina, MSc.

REVISOR

f._____

Ing. Bohórquez Escobar, Celso Bayardo, PhD

DIRECTOR DEL PROGRAMA

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

Resumen

El presente proyecto consiste en el diseño de un plan de recuperación de servicios ante algún desastre para el Centro de Datos del Sitio Principal de la empresa y brindar una solución de darle continuidad de servicios indispensables para que la organización siga operativa antes alguna incidencia que provoque una interrupción de servicios.

Los Centros de Datos en la nube que hoy en día ofrecen múltiples funcionalidades siendo estas consideradas como una estrategia de respaldo y restauración de servicios manteniendo al mismo tiempo almacenado copias de los últimos registros o modificaciones efectuadas en los servicios del cliente, esto proporciona contingencia de manera que la restauración de servicios se realice mediante la conmutación de todo el tráfico inmediatamente a la nube en el caso de alguna incidencia en el centro de datos de la empresa.

En este caso en la empresa NetPay S.A. cuenta con servicios críticos que deben estar siempre habilitados para permitir la continuidad del negocio, para llevar a cabo este plan de recuperación de desastres como complementario a la nube, también existen servicios que todavía no son totalmente factibles en la nube por ende se contempla un tipo de hospedaje y administración de infraestructura con tecnología de punta con un proveedor de servicios para restaurar estos servicios como por ejemplo el core transaccionalidad y ciertos servicios de telefonía, para llevar a cabo se debe analizar a granularidad la situación actual y todos los requerimientos mínimos para que la restauración de servicios en la nube y los hosteados se lleva a cabo de manera efectiva y en el menor tiempo posible la restauración de los servicios.

Para ello se requiere levantar un diseño lógico para que todos los servicios críticos sean considerados en el plan de recuperación de desastres cuando ocurra algún incidente que impida que el centro de datos levante dichos servicios críticos de la empresa y luego del análisis proponer una mejora con el plan de recuperación de desastres que tenga el menor impacto posible en el centro de datos actual.

Palabras Claves: Centro de Datos, plan de recuperación, conmutación, nube, respaldos, continuidad, hospedaje y administración, restauración, core transaccional.

Abstract

This project consists of designing a service recovery plan in the event of a disaster for the Data Center of the company's Main Site and providing a solution to provide continuity of essential services for the organization to remain operational before an incident that causes an interruption of services.

Cloud Data Centers today offer multiple functionalities, which are considered as a backup and service restoration strategy, while keeping stored copies of the latest records or modifications made to the client's services. This provides contingency so that the restoration of services is carried out by switching all traffic immediately to the cloud in the event of an incident in the company's data center.

In this case, NetPay S.A., has critical services that must always be enabled to allow business continuity. To carry out this disaster recovery plan as a complement to the cloud, there are also services that are not yet fully feasible in the cloud, therefore a type of hosting and infrastructure management with cutting-edge technology is contemplated with a service provider to restore these services, such as the core transactionality and certain telephone services. To carry this out, the current situation and all the minimum requirements must be analyzed in granularity so that the restoration of services in the cloud and the hosts is carried out effectively and in the shortest possible time.

To do this, it is necessary to raise a logical design so that all critical services are considered in the disaster recovery plan when an incident occurs that prevents the data center from raising said critical services of the company and after the analysis, propose an improvement with the disaster recovery plan that has the least possible impact on the current data center.

Keywords: Data Center, recovery plan, switching, cloud, backups, continuity, hosting and management, restoration, transactional core.

CAPÍTULO 1: PLANTEAMIENTO DEL PROBLEMA

En este capítulo consiste en dar a conocer la metodología de la investigación, detallando los objetivos, el problema y su respectiva justificación del proyecto.

1.1 Introducción

Las transacciones económicas entre los bancos y compañías de pago ofrecen a las empresas y a sus clientes una variedad de opciones que se adaptan a su modelo y mercado. En este contexto se detalla a NetPay S.A. que realiza el ciclo de transacciones en el medio de un sistema de pago. Se sostiene que son un pilar para el sistema financiero, entre ellas se encuentra NetPay S.A. Estas empresas tienen un número importante de años en el mercado ecuatoriano y han ido construyendo y creciendo a partir de la constante innovación. En este caso, la empresa ofrece una variada gama de productos y servicios que cuenta con una cobertura a nivel nacional.

Por un lado, las instituciones bancarias están interconectadas, mientras que, por el otro lado, los vendedores que utilizan los servicios de transferencia de fondos están interconectados. Estos servicios se clasifican dependiendo de los diferentes productos ofrecidos, como es el caso de los terminales de caja registradora. Cada servicio tiene sus diferentes tipos de terminales que inician el flujo de transacciones y están respaldados por los sistemas de telecomunicaciones que están diseñados para ajustarse a los requisitos.

Se conectan por un lado las entidades bancarias y por el otro se conectan los comercios que prestan el servicio para realizar las transacciones financieras. Estos servicios se intercambian de acuerdo con la categoría del producto, como, por ejemplo, los servicios de punto de venta. Existen también diferentes tipos de terminales para cada servicio, cuyo a comienzos se inicia la corriente transaccional, la telefonía que cumple con las necesidades y la facilidad de uso de cada comercio.

En un diseño de un plan de recuperación ante desastres, es una estrategia que está siendo tomada mucho en cuenta por las empresas considerando la situación actual del Ecuador que ha sufrido de sismos de magnitudes considerables o ya sea un error humano que provoque que los centros de datos se vean afectados y las empresas se vean

perjudicadas al no contar con algún plan de recuperación de desastres que les permita levantar sus servicios y por ende darle continuidad a su giro de negocio.

Las diferentes soluciones en recuperación ante desastres está siendo tendencia en el Ecuador para el respaldo y restauración de servicios teniendo en cuenta que ofrece adicional almacenar y mantener actualizado hasta el último registro o modificación efectuada por el sistema que es manipulado por los operarios de la empresa, existe múltiples beneficios que hacen que estas soluciones se hayan convertido en tendencia para pequeñas, medianas y grandes empresas como variedad de métodos de implementación siendo estas parciales o totales refiriéndose a los servicios críticos, ya sea uno en específico o de todo el centro de datos de la empresa (Aguaded & Tirado, 2018).

Los proveedores de estos servicios que ofrecen la solución de plan de recuperación de desastre ganan por recursos ofrecidos y consumidos; es decir por el uso ya sea de almacenamiento, capacidad, ancho de banda y otros consumo de recursos que son alquilados comúnmente mensualizados, estos proveedores proporcionan toda una infraestructura, ahorrándole al cliente la adquisición de hardware adicional para la recuperación y restauración de servicios y lo más importante el mantenimiento, viéndolo como un servicio.

1.2. Antecedentes

Las soluciones de plan de recuperación de desastres en la nube, han ido tomando importancia al transcurrir el tiempo por los mismos motivos que promovieron su existencia, la caída de servicios, un estudio en el 2012 de muy conocida firma de inteligencia de mercado, presento una estimación con respecto al mundo empresarial y su aumento considerable de interrupción de servicios provocando un tiempo de inactividad muy significativo en la continuidad de servicios que brinda la empresa, estas interrupciones pueden ser provocadas por distintos factores como simple error humano, desastres naturales, o fallas técnicas en el hardware (Arango, 2016).

La recuperación de desastres como servicio, se está volviendo tendencia por convertirse en una atractiva opción para darle continuidad a los servicios y obviar las

interrupciones y/o inactividad de la empresa. Según Garner (2017), en el avance del tiempo las medianas empresas ya habrán adoptado la recuperación de desastres en la nube para darle continuidad de servicios a sus empresas, mucho más las empresas que se les complica construir un nuevo centro de datos para recuperación y restauración de servicios, estas soluciones son muy modelables ya que puede crecer y decrecer bajo de manda de consumo.

1.3. Justificación del Problema

Este proyecto se llevará a cabo ya que permitirá proporcionar continuidad de servicios, adicional este diseño de un plan de recuperación ante desastres en la nube permite almacenar y mantener actualizado todos los últimos registros realizados por los operadores que manipulan los servicios en un entorno computacional como medida de seguridad, evitando la construcción de un centro de recuperación y todo lo que influye su puesta en marcha y mantenimiento.

1.4. Definición del Problema

Se determina los problemas externos e internos que son relevantes para su propósito y que afecta a su capacidad para lograr el resultado deseado, se conoce las funciones, servicios y actividades de la empresa, vincular los objetivos, las políticas, las estrategias para definir el propósito y el alcance de la gestión de continuidad de negocios.

La interrupción de los servicios y la inactividad empresarial, afectan en consideración a la empresa al momento de no permitir flujo transaccional con sus comercios y emisores, siendo este su principal servicio en el Centro de Datos tradicional que, por factores como simple error humano, desastres naturales, o fallas técnicas en el hardware, ya sea provocado por falta de mantenimiento o adquisición de una marca no tan confiable, se interrumpan los servicios (Arango, 2016)

1.5. Objetivos del Problema de Investigación

1.5.1. Objetivo General

Presentar un diseño de un plan de recuperación de servicios del centro de datos ante desastres de la empresa NetPay S.A.

1.5.2. Objetivos Específicos

- Diagnosticar la situación actual mediante la definición y justificación del problema.
- Analizar el marco teórico de Centro de Datos actuales.
- Proponer un diseño integral que proporcione restauración de servicios ante una interrupción de servicios.
- Detallar el plan estratégico para aplicación del plan de recuperación de servicio ante desastre y restauración de servicios.

1.6. Hipótesis

El diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de recuperación ante desastres para ayudar a una organización a ejecutar procesos de restablecimiento en respuesta a un fallo para proteger la infraestructura de tecnología de la información empresarial.

1.7. Metodología

Según el objetivo planteado la investigación es descriptiva, es decir, por cuestión que se sistematiza toda la información concerniente a los planes de recuperación de desastre en la nube, y es explicativa porque realiza una caracterización toda la solución planteada.

Este proyecto se realiza con el fin de proporcionar información relevante para las empresas que ya tienen como proyección a corto plazo adoptar un plan de recuperación de desastre en la nube promoviendo en primera instancia a las empresas a nivel nacional.

CAPÍTULO 2: MARCO TEÓRICO

En este capítulo tendrá como enfoque recopilar y detallar toda la información disponible para estudiar y analizar de los planes de recuperación en nube.

2.1. Planificación de la continuidad del negocio.

La planificación de la continuidad del negocio se refiere al conjunto de estrategias de respuesta ante contingencias para los sistemas de información, que representan elementos críticos de un sistema de control interno. Este plan se ejecuta con el objetivo de asegurar la continuidad de los procesos fundamentales ante la ocurrencia de una falla. El elemento más crítico de este sistema es garantizar el soporte financiero del sistema de información. La disponibilidad de la información comercial es fundamental para la existencia y el desarrollo de cualquier empresa en la mayoría de los casos. (BSCCONSULTORES, 2010).

Ilustración 1. Plan de Continuidad del Negocio.

Nota. Diferentes planes de continuidad del Negocio que se utilizan en la actualidad.

Elaborado por: (DeltaProtect)

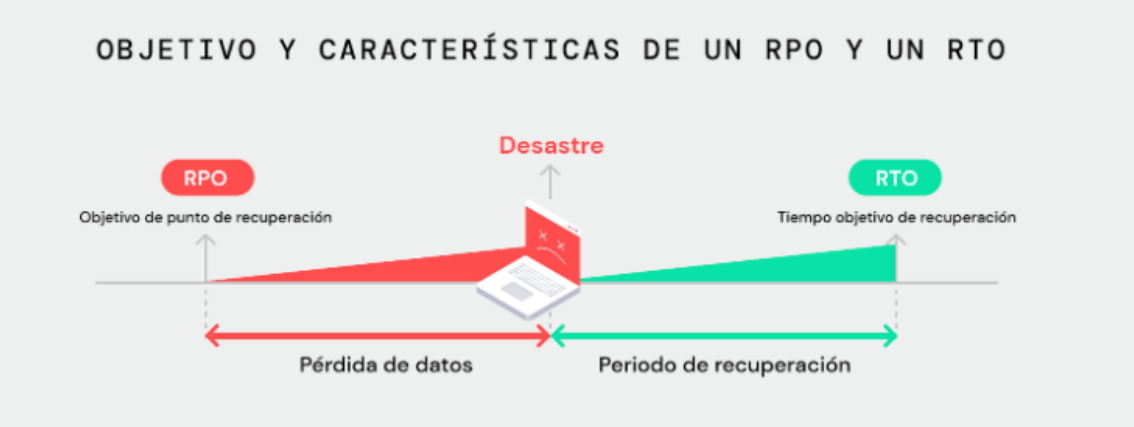
2.2. Diferencias entre Plan de Continuidad del Negocio y Plan de Recuperación ante Desastres.

La principal diferencia se encuentra en las diferencias de alcance. Los planes de continuidad del negocio se implementan para garantizar que los servicios empresariales esenciales no sufran interrupciones y puedan restaurar todas las capacidades lo antes posible.

El Plan de Recuperación de Desastres es un componente de un Plan de Continuidad del Negocio, sin embargo, este último es más comprensivo en su alcance ya que incluye todas las actividades de la organización. Por otro lado, el Plan de Recuperación de Desastres se centra en la infraestructura de TI que sirve para restablecer el acceso de los usuarios a los sistemas de la organización después de un desastre. Es el plan de recuperación de servicios ante desastres especifica qué pasos deben seguirse para restaurar la información necesaria para que el personal obtenga acceso suficiente al sistema. El Plan de Continuidad del Negocio, por otro lado, presenta una estrategia global que debe implementarse independientemente del escenario y no solo de los inesperados. (DeltaProtect).

2.3. Objetivo y Características de un RPO y RTO

Ilustración 2. Objetivo y Características de RPO y un RTO



Nota. Gráfica de recuperación basado en Objetivo y Características de RPO y un RTO. Elaborado por: (DeltaProtect)

Para asegurar que tu Plan de Continuidad de Negocio sea efectivo es crucial considerar tres métricas importantes en la estrategia de recuperación ante desastres empresariales; el RPO, RTO y MTD.

El Objetivo del Punto de Recuperación (RPO), se define como el intervalo de tiempo máximo que puede pasar desde la última copia de seguridad de los datos hasta que ocurra el incidente.

El Objetivo de Tiempo de Recuperación (RTO), es el lapso de tiempo en el que una empresa debe restablecer sus sistemas después de un incidente.

El Período Máximo de Inactividad Tolerable (MTD) es el tiempo máximo que puede transcurrir antes de que las aplicaciones más esenciales y los datos críticos ya no estén accesibles sin provocar consecuencias perjudiciales irreparables.

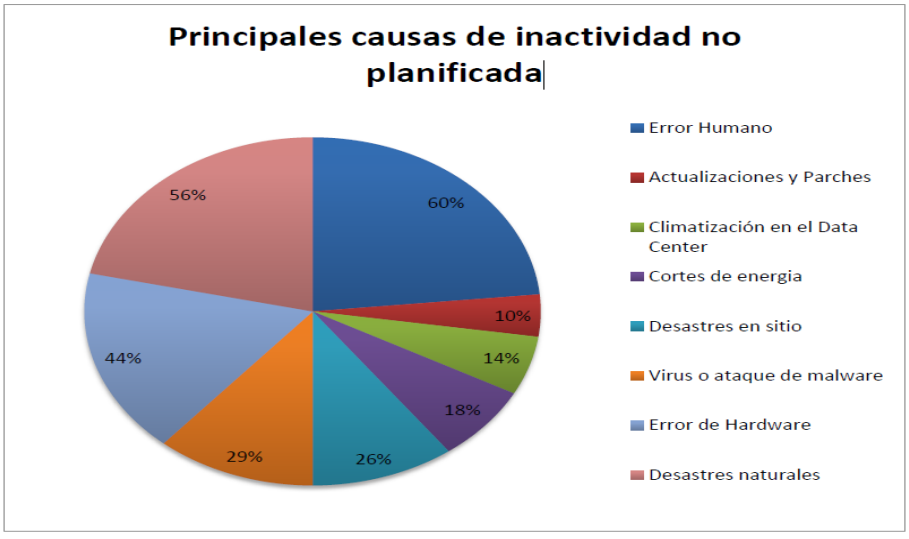
2.4. La recuperación ante desastres

La capacidad de una organización para hacer frente a situaciones de emergencia se refiere a su habilidad para reaccionar y restablecer sus actividades y estructuras luego de eventos devastadores que impactan negativamente en su funcionamiento normalizado.

Tras un ataque cibernético es crucial que los equipos cuenten con un plan de recuperación en caso de desastres para solucionar los problemas de forma rápida y eficiente. Sin una planificación adecuada cada minuto perdido puede aumentar los costos de los daños y retrasar la recuperación. La ciberseguridad es un campo en constante crecimiento y la recuperación ante desastres juega un papel crucial en la gestión de las amenazas. Este glosario aborda los aspectos esenciales de la recuperación ante desastres y todo lo necesario para desarrollar un plan efectivo. (Proofpoint, 2024)

2.5. Principales causas de inactividad no planificada.

Ilustración 3. Principales causas de inactividad no planificada



Nota. Gráfico de Principales causas de inactividad no planificada. Elaborado por: Autor

Las principales causas de interrupciones de servicios no planificada pueden variar según el tipo de arquitectura tecnológica implementada, pero en general, las siguientes son las causas más comunes:

Error humano:

- **Configuración mal aplicada o incorrecta**: Los errores al configurar dispositivos, redes o bases de datos pueden interrumpir los servicios.
- **Fallo en la gestión de cambios**: No tener un proceso óptimo para gestionar controles de cambios en la infraestructura que puede resultar en errores no planificados.
- **Eliminación accidental de archivos críticos**: Los administradores pueden eliminar, sin intención, archivos o configuraciones necesarias para el funcionamiento de los servicios internos o externos.

Actualizaciones y Parches de software:

- **Actualizaciones o parches fallidas:** las actualizaciones de software y los parches de seguridad que no se instalan correctamente pueden causar problemas en el sistema.
- **Bugs o errores en el sistema operativo**: Los errores en los sistemas pueden causar problemas de funcionalidad que interrumpen el servicio.

Climatización en el Centro de Datos:

- **Alta temperatura**: Los Servidores y otros dispositivos deben tener una temperatura adecuada para su correcto funcionamiento por tal motivo se requiere que los sistemas de climatización este en óptimas condiciones.
- **Falta de Mantenimiento preventivo**: Al no realizar el mantenimiento preventivo de los sistemas de climatización provocan su mala funcionalidad.

Cortes de Energía:

- **Cortes de energía**: Las cortes en el abastecimiento eléctrico pueden causar apagones abruptos de servidores y todo el Centro de Datos.

- **Fallas en sistemas de respaldo**: Los sistemas de alimentación ininterrumpida pueden fallar o tener energía con insuficiente capacidad para mantener encendido todo el Centro de Datos.

Desastres en sitio o eventos externos:

- **Accidentes físicos**: Daños físicos en los Centros de Datos debido a accidentes (por ejemplo, caídas, accidentes de tráfico cercanos, etc.) pueden afectar los servicios.

Virus o Ataques cibernéticos:

- **Ataques DDoS (Denegación de Servicio Distribuida)**: estos ataques consisten en una sobrecarga de solicitudes a un servicio que termina provocando afectación de servicios.
- **Malware o ransomware**: El malware o ransomware puede afectan directamente los archivos del sistema y hacer que los servicios sean inaccesibles.
- **Vulnerabilidades de seguridad**: los cibercriminales pueden explotar fugas de seguridad para interrumpir sistemas o tomar el control sobre ellos.

Error de hardware:

- **Desgaste de componentes**: Discos duros, memorias, fuentes de alimentación y otros componentes pueden fallar debido al desgaste.
- **Fallas en servidores o dispositivos de red**: Los servidores pueden colapsar debido a fallos de hardware como placas madre, CPU o tarjetas de interfaz de red.

Desastres naturales:

- **Desastres naturales**: como inundaciones, incendios, terremotos y tormentas pueden dañar la infraestructura tecnológica, lo que lleva a la interrupción de servicios.

Para resumir, el tiempo de inactividad no planificado en los servicios puede deberse a una variedad de razones, incluidos defectos del sistema, errores de empleados o ataques

maliciosos. No hacerlo expondría a la organización a riesgos sustanciales. Por lo tanto, es imperativo que los riesgos de seguridad se gestionen a través de una cultura de mantenimiento, monitoreo continuo y gestión de seguridad.

2.6. Tipos de recuperación de servicios informáticos.

Los desastres tienen varias formas y pueden amenazar la integridad y estabilidad de una gran cantidad de sistemas y activos. Algunos de los tipos más generales de recuperación ante desastres y algunas de los planes que los respaldan son:

2.6.1. Recuperación ante desastres para centros de datos

En este tipo de recuperación ante desastres se protege la infraestructura física y los datos en respaldo o copias de seguridad. Los planes se centran en que para no interrumpir las operaciones durante un desastre, se activa una página de conmutación por error en un sitio que no es el principal.

2.6.2. Recuperación ante desastres en la nube

Una estrategia en la que no puede faltar un componente, en cualquiera de los planes de recuperación ante desastres que sean elaborados, son las estrategias aquí indicadas ya que permiten replicar y alojar en la nube servidores físicos y virtuales de manera más eficiente. Este tipo de estrategia de recuperación sería capaz de otorgar un failover automático a la nube pública en caso de ocurrir un desastre, eliminando completamente la necesidad de tener un segundo sitio.

2.6.3. Recuperación ante desastres en redes

La operabilidad de la red es imperativa para el intercambio de datos, el acceso a aplicaciones y la comunicación en caso de amenazas. El enfoque de este componente se centra en tener datos y ubicaciones de respaldo, y en planificar la recuperación del control sobre los servicios de red en el caso de que se vean afectados, donde se requiere acceso alternativo como la conectividad remota fuera de banda para asegurar la recuperación del acceso a los administradores de las diferentes plataformas y soporte.

2.6.4. Recuperación ante desastres virtualizada

La recuperación ante desastres virtualizada abarca múltiples estrategias que permiten copiar las cargas de trabajo a la nube o a otro emplazamiento. Este proceso ofrece al personal de ciberseguridad más opciones, y es más efectivo y fácil de aplicar.

2.6.5. La recuperación ante desastres como servicio

Es un servicio comercial proporcionado por empresas subcontratadas y que realiza tareas de duplicado y alojamiento de servidores físicos y virtuales de las organizaciones. La parte proveedor subcontratado toma la iniciativa en la ejecución y administración del marco y la planificación de la recuperación en caso de desastres de la entidad.

2.7. Recuperación ante desastres vs. continuidad de negocio

Sin embargo, en primer lugar, cabe mencionar que la recuperación ante desastres, así como la continuidad de negocio, están asociadas entre sí y se entrelazan con las actividades de ciberseguridad de la entidad, al igual son dos cosas diferentes. La recuperación ante desastres consiste en un conjunto de actividades que contienen procedimientos que están orientados en la restauración del acceso a los datos y a la infraestructura de TI de la organización después de la ocurrencia de un desastre. La continuidad del negocio se ocupa en mantener en funcionamiento las actividades de la organización, cuando se produce un desastre.

Los planes de recuperación ante desastres describen cómo un equipo debe restaurar sistemas y bases de datos después de un ataque o desastre. Por otro lado, los planes de continuidad del negocio tienen como objetivo asegurar que las actividades sigan funcionando durante el incidente. El objetivo principal de la recuperación ante desastres es reducir los impactos negativos de un desastre y ayudar a que la organización vuelva a su estado operativo en el menor tiempo posible. El objetivo de la continuidad del negocio es hacer que la organización pueda seguir trabajando para sus clientes internos y externos, proveedores y socios incluso en caso de un desastre. (Proofpoint, 2024)

2.8. Gestión de incidencias vs. recuperación ante desastres

La recuperación ante desastres y la gestión de incidencias son conceptos que tienen algo en común pero que también presentan ciertas diferencias conceptuales. Desde el punto de vista de un incidente que debe gestionarse y solucionarse, se concibe la recuperación de un desastre como un enfoque para que la organización administre planes orientados a restablecer toda la operación.

La gestión de los incidentes es una característica micro de la recuperación ante desastres que trata de mitigar la situación de una incidencia específica a la que se le tenga que actuar con mayor celeridad con el único fin de que las operaciones vuelvan a la normalidad. (Proofpoint, 2024).

2.9. Centro de Datos

Un Centro de Datos es un edificio o un espacio dentro de una edificación o un conjunto de edificaciones que se destinan a resguardar equipos, sistemas informáticos, sistemas de almacenamiento y telecomunicaciones. (Díaz O. &., 2017).

Cabe resaltar que existen otros componentes e infraestructura, generalmente de redundancia o respaldo, tales como suministro de energía, conexiones de comunicación de datos, controles ambientales (aire acondicionado, dispositivos de extinción de incendios, varios dispositivos de seguridad). Cuando se trata de un lugar donde hay que interrumpir las vías inexistentes, es una operación a escala industrial que entra en la definición de un gran centro de datos. (Arango, 2016).

Ilustración 4. Principales Centro de Datos Actuales

Nota. Principales Centro de Datos Actuales y sus diferentes soluciones para cada necesidad. Elaborado por: (Velatia)

Tabla 1. Principales Tipos de Centros de Datos

Centro de Datos Empresarial	El Centro de Datos está ubicado en un espacio dedicado dentro de la misma corporación y está diseñado para cumplir con los requisitos de seguridad y almacenamiento de un negocio. Está atendido, mantenido y asegurado por especialistas de la corporación.
Centro de Datos de Colocación	Para el centro de datos de colocación, muchas organizaciones alquilan espacio a un proveedor externo que proporciona servicios de datos. Los servidores y la infraestructura de red utilizados por la empresa son de propiedad privada y son administrados por la empresa, pero requieren las instalaciones de un Centro de Datos profesional
Centro de Datos de Proveedores de Servicio	Un Centro de Datos de Proveedor de Servicios (Centro de Datos de Proveedor de Nube o Centro de Datos de Colocación) es una instalación que está equipada con infraestructura de TI construida para este propósito que permite a emprendedores o empresas alquilar espacio que les permita almacenar y procesar sus grandes volúmenes de datos.
Centro de Datos en la nube	Este tipo de centro de datos es proporcionado por proveedores de servicios en la nube. Los recursos se alquilan bajo demanda en múltiples sitios a través de diferentes regiones geográficas.

Nota. Principales Tipos de Centros de Datos. Elaborado por: Autor

2.10. Requisitos para centros de datos modernos

La actualización y modernización del centro de datos mejora el rendimiento y la eficiencia energética.

La seguridad de la información también es una preocupación y por esta razón, un Centro de Datos debe proporcionar un entorno seguro que reduzca las posibilidades de una violación de seguridad. Así, un centro de datos debe cumplir con las más altas medidas para asegurar que la integridad y la funcionalidad del entorno informático alojado se mantengan.

La International, empresa de investigación, señala que la antigüedad promedio de un centro de datos es de nueve años. Además, Gartner, otra empresa de investigación, también está de acuerdo y asegura que los centros que superan los siete años se consideran que están obsoletos. El aumento del crecimiento de los datos es un factor que exige la modernización de los Centros de Datos. (Arias & Portela, 2018)

La orientación hacia la modernización no es reciente; las instalaciones inadecuadas fueron criticadas en el año 2007 y en el 2011 también el instituto Uptime mostraba preocupación por lo arcaico que se volvían los equipos que contenía. Hacia el 2018 la preocupación ya había cambiado una vez más, pero esta vez hacia la edad del personal: “el personal del Centro de Datos envejece más rápidamente que el equipo". (Patiño, Evaluación de seguridad informática basada en ICREA e ISO27001. , 2018).

2.11. Cumplimiento de estándares para centros de datos

El estándar de infraestructura de telecomunicaciones para Centros de Datos de la Asociación de la industria de telecomunicaciones es un requisito mínimo para la infraestructura de telecomunicaciones de la sala de datos, incluyendo el centro de datos corporativo de un solo inquilino y el centro de datos de alojamiento en internet multi inquilino. La topología presentada en este documento tiene como objetivo ser aplicable a salas de datos de cualquier tamaño.

Ilustración 5. Cumplimiento de estándares de Centro de Datos

Nota. Detalle de cumplimiento de estándares de Centro de Datos para su funcionalidad. Elaborado por: (Velatia)

Requisitos para equipos y espacios de Centros de Datos de telecomunicaciones, establece parámetros para los espacios de Centros de Datos dentro de las redes de telecomunicaciones y ambientales de los equipos que estén destinados a ser instalaciones en dichos espacios. (Costas, 2017).

Estos criterios fueron desarrollados y representantes de la industria. Dos criterios posibles fueron formulados para los espacios de los Centros de Datos que contienen equipos de procesamiento de datos o de tecnología de la información. El equipo se puede utilizar para:

- Gestionar y administrar toda la red de telecomunicaciones de un operador.
- Ofrecer aplicaciones basadas en centros de datos de una manera que los clientes del operador se dirijan directamente.
- Disponer de aplicaciones que están alojadas para que un determinado tercero brinde servicios a sus clientes.
- Ofrecer una aplicación de este tipo en combinación con otras del tipo de simultáneos a Centros de Datos.

2.12. Transformación del Centro de Datos

La actualización de los Centros de Datos se realiza por fases por medio de diferentes proyectos, esto se da con el tiempo. Este mecanismo se distingue del procedimiento estandarizado de completar todas las etapas o componentes de un ciclo de actualización de un centro de datos. Por lo general, los esfuerzos realizados en el contexto de un proyecto transformador del centro de datos incluyen: estandarización / consolidación, virtualización, automatización, seguridad. (Terán, 2017)

- Estandarización / consolidación: Eliminación de la expansión de los servidores que son tanto físicos como virtuales, lo que implica incluir la renovación de antiguos equipos del centro de datos.
- Virtualización: disminuye el gasto operativo y de capital, aumenta la eficiencia energética. Los escritorios virtualizados pueden ser almacenados y alquilados desde centros de datos a través de suscripción.
- Automatización: procesos como la configuración de aprovisionamiento, parches, gestión de versiones y cumplimiento también deberán ser automatizados, no solo al tener personal de TI menos calificado.
- Protección: la protección de los sistemas virtualizados se basa en la seguridad existente de las infraestructuras físicas.

2.13. Diseño de Centro de Datos

Por ejemplo, el diseño del centro de datos o la arquitectura del Centro de Datos es un campo que ha estado expandiéndose durante varias décadas desde la construcción de grandes nuevas instalaciones e incluso pequeñas, hasta la ingeniosa reutilización de las existentes, como tiendas abandonadas, minas de sal y búnkeres de guerra. (Téllez Valdés, 2017).

Los códigos locales de construcción pueden regular las alturas mínimas de los techos y otros parámetros. Algunas de las consideraciones en el diseño de centros de datos son:

- Un rack de servidores generalmente empleado en colocación.

- Tamaño: una habitación de un edificio, uno o varios pisos o un edificio completo y puede acomodar 1000 servidores o más.
- Espacio, energía, refrigeración y costos del centro de datos.
- Manejador de aire.
- Infraestructura de ingeniería mecánica: calefacción, ventilación y aire acondicionado; equipos de humidificación y deshumidificación; presurización.
- Diseño de desarrollo de infraestructura de ingeniería - planificación de servicios eléctricos; distribución de fuentes de energía, conmutación y multiplicación; sistemas de alimentación ininterrumpida; etc.
- Criterios de diseño y compensaciones.
- Expectativas de disponibilidad: el costo de prevenir el tiempo de inactividad no debe ser mayor que el costo del tiempo de inactividad.
- Selección del sitio: Los factores de ubicación incluyen la distancia a las redes eléctricas, infraestructura de telecomunicaciones, servicios de red, enlaces de transporte y servicios de emergencia. Otros son rutas de vuelo, usos del suelo vecinos, peligros geológicos y clima (relacionado con los costos de refrigeración). (Piattini, 2016).
- En muchas ocasiones, la potencia disponible es más difícil de cambiar.

2.14. Análisis de dinámica de fluidos computacional

Este tipo de análisis lógicamente debe predecir el comportamiento del aire y de la temperatura de un centro de datos, además de la presión, para así poder evaluar su rendimiento y modelo energético, y esto se hace con modelos numéricos numerados. Y para entender el centro que se tiene como objeto se utilizan herramientas y técnicas.

En este caso, dentro del Centro de Datos, se introducen factores relacionados con el mantenimiento programado de la infraestructura o si el aire acondicionado falla o se

apaga, lo que lleva a medio o incluso a alta temperatura. Se va a suponer que el aire acondicionado se apagó. (Costas, 2017).

2.15. Servicios para el centro de datos empresarial

En cuanto al Centro de Datos de Internet, se consideran los servidores y otros dispositivos específicos para las aplicaciones de comercio electrónico dentro de la red del centro de datos de la corporación. En ciertas circunstancias, los servidores de Internet están físicamente separados del resto de la red. Esto implica que esos servidores están físicamente conectados a un centro de datos de intranet a través de un conjunto de enlaces que no se pueden enrutar y que no tienen acceso físico a ninguna otra parte de la red. (Costas, 2017)

El centro de datos de la extranet ayuda a realizar transacciones b2b dentro de la red de la corporación del Centro de Datos. Por lo general, se ingresa a estos servicios mediante conexiones remotas seguras o enlaces dedicados. (Costas, 2017).

La red del Centro de Datos de Intranet tiene aplicaciones y servicios de una red de centro de datos de la Empresa que usualmente tienen funciones de soporte a la manufactura, marketing, recursos humanos, investigación y desarrollo, nómina y otros negocios.

El centro de datos proporciona ofertas integrales que incluyen servicios y todos los componentes necesarios enfocados en la infraestructura que facilita la configuración, mantenimiento, desarrollo y mejora de un centro de datos, que es una instalación que proporciona recursos informáticos como procesamiento de datos, almacenamiento, redes, gestión y distribución de datos para empresas.

2.16. Servicios de apoyo

Los servicios de apoyo para Centros de Datos pueden definirse en términos generales como una especie de soporte técnico, que se ocupa de proporcionar ayuda en la resolución de problemas relacionados con dispositivos tecnológicos. Los servicios de soporte técnico para centros de datos sirven para abordar los problemas con servidores, almacenamiento,

software y equipos de red que constituyen un centro de datos, o con los procesos relacionados con la gestión de esos activos del Centro de Datos. (Arias & Portela, 2018)

El conjunto de servicios de los centros de datos incluye la asistencia a la instalación y/o entrenamiento en el uso de los dispositivos técnicos. Dentro de la industria se encuentran:

- Analista Técnico.
- Ingeniero de Coordinación - Mesa de ayuda
- Especialistas en Soporte.

2.17. Servicios de formación técnica

La naturaleza de la capacitación técnica se entiende de forma distinta dependiendo de la industria y la labor. Ofrezco que la palabra técnico implica mucho, en este caso puede referirse a una actividad (una tarea, deber o habilidad laboral) que es particular a un arte, ciencia, profesión, oficio o algo así. Así, los servicios de capacitación técnica forman conocimientos, habilidades y competencias para el desempeño de trabajos, oficios o profesiones específicos. (Echenique, 2016)

En el contexto de los servicios del centro de datos, la formación técnica podría ofrecer conocimiento aplicable al manejo de cualquier herramienta o equipamiento o a procesos referidos a la administración de un centro de datos o bien a la mantención, actualización, integración o administración de alguno de los equipamientos de un Centro de Datos.

2.18. El papel del Centro de Datos

Los centros de datos son un elemento vital de la empresa, cuyo propósito es apoyar aplicaciones empresariales y proporcionar servicios como:

- Almacenamiento, gestión, respaldo y recuperación de datos
- Aplicaciones de productividad, como correos electrónicos
- Transacciones de comercio electrónico de alto volumen
- Servicio a comunidades de juegos en línea
- Datos, aprendizaje automático e inteligencia artificial

En la actualidad se informa que hay más de 7 millones de Centros de Datos en todo el mundo. Casi cada empresa y agencia gubernamental construye y opera su propio centro de datos o tiene la capacidad de acceder a los modelos de otros, si no ambos.

Adicional, hay muchas opciones disponibles, como alquilar servidores en una instalación de colocación, usar servicios de centro de datos administrados por un tercero o usar servicios públicos basados en la nube como Amazon, Microsoft, Sony y Google (Terán, 2017).

2.19. Clasificación TIER de Centros de Datos

La certificación TIER es una categorización a nivel de los Centros de Datos desarrollado por el Uptime Institute. Este estándar define ciertos niveles de certificación, cada uno con requisitos específicos de redundancia de componentes y disponibilidad de equipamiento.

Tabla 2. Clasificación de TIER para Centros de Datos

Tipo de Centro de Datos	**Características**	**Capacidad**
Tier I	Centro de datos básico sin capacidad redundante, los componentes tienen un UPS o razón de proveedores de datos. Básico.	Básica. El fallo puede ser de distribución o de capacidad que afectará a la sede, dentro de las condiciones hay requerimientos de que se deben de tener todas las funciones de la sede, esto es para permitir ejecutar actividades de mantenimiento o reparación.
Tier II	Centro de Datos Redundante. Nivel 1 + Dispositivos con Componentes Redundantes.	Cuando se deben realizar tareas de mantenimiento rutinario regulares, aún son necesarias las interrupciones completas del sitio por ahora. Las interrupciones de capacidad del sitio pueden ser un problema. Las interrupciones de distribución del sitio plantearán una preocupación para el sitio.

Tier III	Centro de Datos Mantenible Concurrentemente. Nivel 1 + Nivel 2 + Equipos de Alimentación Doble y Vínculos de Salida Múltiples	Mantenimiento Simultáneo. Todos y cada uno de los componentes de capacidad del sitio y las rutas de distribución se pueden retirar de un sitio para mantenimiento o reemplazo de tal manera que no interfiera con sus actividades comerciales. Un sitio sigue siendo vulnerable incluso a que falle un único equipo o ocurra un error del operador.
Tier IV	Centro de datos tolerante a fallos.	La falla de un equipo individual o la falla de un camino de distribución no tendrá impacto en las operaciones comerciales. Una instalación tolerante a fallos también se puede mantener de manera concurrente.

Nota. Clasificación de TIER para Centros de Datos según sus características y capacidades. Elaborado por: Autor

2.20. Los componentes principales de un Centro de Datos

Los planos y las especificaciones para el Centro de Datos pueden ser relativamente diferentes en naturaleza. Para ilustrar el caso, un centro de datos construido para un proveedor de servicios en la nube como Amazon difiere enormemente en términos de necesidades de instalaciones, infraestructura y seguridad de un centro de datos completamente privado, como uno construido para una instalación gubernamental con un mandato de protección de datos clasificados.

Cualquiera que sea la clasificación, una operación eficiente del centro de datos es posible a través de inversiones que están distribuidas de manera uniforme en la instalación y el equipo que alberga. Además, dado que los centros de datos suelen ser el hogar de aplicaciones críticas para el negocio y datos de una organización, es de suma importancia que tanto la instalación como el equipo interno estén protegidos de accesos físicos y ciberataques. (Costas, 2017)

Los componentes principales de un centro de datos se clasifican en las siguientes categorías:

- Instalación: el área utilizable disponible para el equipo de TI. Proporcionar acceso a la información 24 horas al día convierte a los centros de datos en una de las instalaciones que más energía consumen en el mundo. Se presta atención a la distribución para aprovechar al máximo el área y al control de temperatura para garantizar que el equipo no supere rangos específicos de temperatura/humedad.
- Componentes principales: hardware y software que se utilizan para realizar TI y almacenar datos y aplicaciones. Algunos de estos pueden ser sistemas de almacenamiento, servidores, equipo de red como conmutadores y enrutadores, y otros elementos de seguridad de la información, como cortafuegos. (Calo & Ortiz, 2018)
- Infraestructura de soporte: el equipo que ayuda a garantizar que la máxima disponibilidad se mantenga en todo momento de manera segura. Correlacionando con los requisitos, se han definido cuatro niveles de centros de datos, con un nivel de tiempo de actividad que varía entre el 99.671% por ciento y el 99.995% por ciento. Algunos componentes para la infraestructura del equipo de soporte son:
    - Fuentes de energía ininterrumpida: bancos de baterías, generadores y fuentes de energía redundantes.
    - Control ambiental: aire acondicionado para salas de computadoras, sistemas de calefacción, ventilación y aire acondicionado con sistemas de escape.
    - Sistemas de seguridad física: sistemas de biometría y videovigilancia.
    - Personal de operaciones: personal que puede supervisar las operaciones y mantener la infraestructura y el equipo informático en todo momento.

Los centros de datos han madurado en los últimos años y, dado que la demanda de TI de la empresa sigue transitando hacia servicios bajo demanda, la arquitectura del centro de datos ha cambiado de servidores locales a infraestructura virtualizada que puede soportar cargas de trabajo en un conjunto de infraestructura física y múltiples entornos en

la nube. Hay un dicho en la actualidad: el centro de datos moderno es donde están tus cargas de trabajo. (Echenique, 2016).

2.21. Importancia de los centros de datos

Casi todas las empresas contemporáneas y oficinas gubernamentales requieren la propiedad de un centro de datos o tienen la opción de arrendar uno. Las grandes empresas y las instituciones gubernamentales pueden construir y utilizar estos centros, pero solo si la economía lo permite. Mientras que otras personas prefieren alquilar servidores en centros de colocación. Algunos propietarios de negocios también tienen la posibilidad de utilizar servicios basados en la nube.

Las empresas que operan en el sector de telecomunicaciones, educación, redes sociales, finanzas y comercio pueden agrupar la enorme cantidad de información que procesan a diario. Estas corporaciones que producen y utilizan datos necesitan centros de datos para llevar a cabo sus actividades. De no tener estos centros, estas empresas padecerán de una falta de rápido y seguro acceso a información que se vuelve vital para el funcionamiento del negocio. La ausencia de este tipo de servicios afectará de manera definitiva la aserción de clientes y las ganancias de la compañía. (Arias & Portela, 2018).

Es por eso por lo que los centros de datos se convierten en un recurso vital para cualquier empresa que desee realizar de forma efectiva sus deportes. Los centros de datos en el mundo moderno han aumentado su importancia en un diez por ciento por las necesidades de comercio de información que están en aumento. (Arias & Portela, 2018)

Procediendo de la misma manera, cuando dos computadoras están conectadas a una zona, los servidores de computadora utilizan la tecnología de la información para relajar datos a navegadores de internet. La información guardada en un servidor de centro de datos se digitaliza en paquetes antes de ser enviada a enrutadores que determinan el camino óptimo para que tal información pase.

Luego, esto pasa a través de varias redes cableadas e inalámbricas que están conectadas a la computadora del usuario final a través de la red de los proveedores de servicios. Cada vez que un usuario escribe una dirección web en un navegador, eso lo lleva al sitio del

servidor relevante y el servidor solicita inmediatamente información. Además, si el usuario final desea descargar archivos, la secuencia es simplemente la opuesta.

2.22. Alquiler Compartido de Centro de Datos: Hospedaje y Administración

Los alquileres de compartido se han convertido en una opción viable para las empresas. Proporciona la flexibilidad muy necesaria de tener las instalaciones sin la necesidad de plazos específicos y compromisos financieros ni para extender ni para construir las instalaciones necesarias por cuenta propia. El compartido de Centros de Datos es un arreglo por el cual un cliente alquila espacio físico dentro del centro de datos de una tercera parte para albergar las computadoras, dispositivos de almacenamiento y otro equipo de red del cliente. Este sistema permite a las empresas utilizar la última tecnología de infraestructura de vanguardia sin tener que hacer gastos en el establecimiento y cada aspecto de su propio centro de datos. Permite a las empresas concentrarse en su negocio principal al externalizar la gestión del centro de datos a los profesionales. En este entorno, se proporcionan tecnologías avanzadas e incluso recursos de propiedad intelectual que serían costosos y difíciles de implementar de otra manera.

El alquiler compartido ahora es una estrategia que la mayoría de las organizaciones utilizan considerando su agilidad, seguridad y eficiencia. Se describen los siguientes beneficios:

Fiabilidad de una infraestructura infalible: Sistemas de refrigeración ininterrumpidos, suministro de energía ininterrumpido, medidas de respaldo de datos, planes de recuperación ante desastres y monitoreo continuo son todo lo que se necesita para asegurar que los servicios funcionen sin problemas a un alto nivel, que es el principal punto de énfasis en términos de promoción y adquisición de negocios en el mercado. Sin embargo, una falla del servidor y un corte a menudo implican un alto costo para la organización, como la pérdida de ingresos y una reputación dañada. En lo que respecta a la venta de Centros de Datos, se destaca por su fiabilidad, que es bastante excepcional.

Rendimiento y un entorno optimizado para la excelencia: En un Centro de Datos enfocado en el alquiler de instalaciones compartidas, los sistemas de refrigeración disponibles son de última generación, lo que permite que la temperatura dentro de la instalación se mantenga como se desea, de modo que los aparatos estén en un rango ideal.

Gestionar la electrónica junto con el uso es una excelente manera de mantener el control de temperatura. Pero el rendimiento no es solo alta potencia de computación, aunque ese es un aspecto importante. La latencia y la velocidad de datos son igualmente importantes. Las instalaciones utilizadas para el alquiler y el uso compartido de equipos proporcionan todo esto, resultando en baja velocidad.

Seguridad física que reduce los riesgos: La custodia de un centro de datos puede resultar costosa. De ahí que la seguridad física de dicho centro sea considerada como uno de los elementos que se incluye en el coste de la colocación. Sistemas de protección complejos, la presencia de guardias profesionales a tiempo completo y sistemas de vigilancia tecnológicamente avanzados son buenos factores que explican el nivel de protección que el proveedor de alquiler compartido está en la posición de ofrecer. Además del control de acceso, se requiere la implementación de los adecuados métodos de protección para toda persona que se presente a su jaula o sala.

Posibilidades de escalabilidad: La habilidad para escalar es un aspecto crucial a la hora de seleccionar una solución de alquiler compartido. Las demandas de las compañías cambian rápidamente, y los proveedores de alquiler compartido poseen una variedad de alternativas en torno a espacio. Ya sea que necesite una sola jaula o varias salas en privado, los centros de renta compartida cumplen con sus requerimientos de manera flexible. La expansión no se restringe al crecimiento dentro de una sola ubicación. Los arrendadores compartidos de espacios, por lo regular, ofrecen capacidad de crecimiento a otras locaciones y hasta otras regiones. Esta flexibilidad geográfica ayuda a los departamentos de informática en los países a redefinir su implementación sin grandes dificultades. Aquellos detalles que aún tienen reserva de suelo tienen un excelente espacio para ofrecer esa flexibilidad, en especial en mercados en crecimiento.

Compromiso sostenible: En la actualidad, donde el alquiler de espacios compartidos está en auge, ese proveedor puede ser un aliado que gane respeto en su lucha por la sostenibilidad. Esto repercute en el propio mantenimiento de las instalaciones (eficiencia del uso de energía eléctrica, control de la temperatura, etc.). Para poder considerarse con un nivel de prestigio a nivel técnico, un Centro de Datos, ha de acreditar respaldos medioambientales. Por ejemplo, todas las instalaciones deben ser operadas bajo regulaciones que son estándares en la administración de medioambientes y uso de

recursos energéticos. También, lo que respecta a la supervisión del PUE de los edificios ha de estar reglamentado. Por último, las prácticas de desarrollo sostenible deben mejorarse estratégicamente conforme a otras regulaciones que se esperan instaurar, impulsando buenas prácticas a seguir. Esto implica hacer, además de realizar buenas estimaciones, una gestión constante del impacto que se genera y crear buenos informes que permitan establecer análisis evaluativos del avance.

Mejor gestión del riesgo: La defensa número uno consiste en tratar las instalaciones físicas de la forma más segura posible. Las instalaciones de alquiler de espacios compartidos generalmente tienen dispositivos de seguridad tales como cámaras de vigilancia y cerraduras de control de acceso biométrico. Estas son una gran adición a un sistema de control de seguridad de vanguardia que incluye firewalls avanzados y sistemas de detección de intrusiones. El nicho de gestión también se dedica a cumplir con la legislación del país. Se realizan auditorías a los centros de alquiler compartido periódicamente para garantizar el cumplimiento con las normas del sector en lo que respecta a la protección de datos o seguridad física. La gestión del riesgo clave en el alquiler compartido es un tema clave que abarca una serie de aspectos para garantizar la seguridad.

Alquilar espacio en un centro de datos ha ido más allá de ser una mera opción para la gestión de la infraestructura de TI y ahora es esencial para las empresas que buscan ser más competitivas en un mundo que avanza rápidamente hacia la globalización. Ni siquiera estoy considerando los beneficios directos en costos, rendimiento y seguridad, junto con la reducción de costos de ventas; alquilar ofrece perspectivas increíbles para la innovación y un alcance para la transformación de una entidad empresarial en este mundo global. Teniendo en cuenta las bases de la Internet de las Cosas, 5G y la era de la Inteligencia Artificial, la demanda de procesamiento y almacenamiento de datos va a crecer enormemente. Mantener sus aplicaciones y datos en un espacio compartido de alquiler facilita pensar en el futuro.

2.23. Computación en la nube

La computación en la nube es la provisión de recursos computacionales a través de Internet en base a un modelo de pago por uso y según las necesidades. Ya no es necesario

comprar, poseer y mantener servidores físicos y centros de datos porque puede obtener servicios de TI como potencia informática, almacenamiento de datos y bases de datos de un servicio en la nube en lugar de comprarlos directamente. (Amazon Web Services).

2.24. Modelos de Implementación de Centros de Datos en la nube

Tabla 3. Modelos de Implementación de Centros de Datos en la nube

Tipos	**Ventajas**	**Desventajas**
Nube Pública	Menores inversiones iniciales. Escalabilidad ilimitada. Acceso desde cualquier lugar con falta de control sobre la infraestructura.	Puede no funcionar para organizaciones con legislación que requiera estricta privacidad o seguridad de datos. Control limitado sobre la infraestructura.
Nube Privada	Más control de recursos y seguridad. Mejor cumplimiento regulatorio.	Más costo con mayor complejidad de gestión y administrativa. La escalabilidad se reduce a diferencia de la evacuación pública.
Nube Híbrida	Flexibilidad para el rango de tamaño y escalabilidad. Mejor preparado para responder a los requisitos de seguridad y cumplimiento.	La integración de ambos entornos requiere una gestión más compleja.

Nota. Descripción como ventajas y desventajas de cada Modelo de Implementación en Centros de Datos en la nube. Elaborado por: Autor

2.25. Beneficios de la informática en la nube

2.25.1. Agilidad

La nube ofrece un fácil acceso a una multitud de tecnologías que pueden ayudarte a innovar más rápidamente y a construir prácticamente cualquier cosa que puedas imaginar. Puede activar recursos rápidamente a medida que los necesite, desde servicios de infraestructura, como cómputo, almacenamiento y bases de datos, a Internet de las cosas, aprendizaje automático, lagos de datos y análisis, entre otros.

Es posible implementar tecnológicamente cualquier tipo de servicios en cuestión de varios minutos, lo que representa un aumento drástico con respecto al enfoque tradicional de abogar por ideas antes de la implementación. Así, obtienes la independencia que necesitas para experimentar con nuevas ideas que pueden cambiar la experiencia del cliente y ayudar a redefinir las operaciones de la organización.

2.25.2. Elasticidad

Con la computación en la nube, ya no es necesario provisionar recursos en exceso en anticipación a niveles máximos de negocio que puedan surgir en el futuro. En su lugar, solo se provisionan los recursos que se necesitan. Estos recursos pueden aumentarse o disminuirse rápidamente según los requisitos de tu organización.

2.25.3. Ahorro de costos

La nube le permite convertir sus costos fijos, como el alquiler de centros de datos y servidores físicos, en costos variables, en donde solo se le cobrará por los recursos de TI que haya requerido. También es más costoso hacerse cargo por su cuenta de esos recursos que pagar por ellos, por lo que, gracias a las economías de escala, se tiene que pagar mucho menos.

2.25.4. Seguridad Avanzada

El acceso a la infraestructura de muchos proveedores de nube radica en centros de datos ubicados en diferentes partes del mundo, de esta forma los usuarios pueden tener acceso a esos servicios desde el punto más cercano lo que reduce la latencia y mejora la experiencia.

2.25.5. Mejor Rendimiento y Baja Latencia

Los proveedores de nube han instalado en sus sistemas el uso de cifrado de datos, autenticación avanzada y control de accesos, lo que impide el acceso no autorizado a la infraestructura y datos de la nube.

2.25.6. Recuperación ante Desastres y Respaldo

Las instalaciones de nube se basan en centros de datos creando mecanismos de respaldo y recuperación de datos, garantizando que haya protección de la información aun con eventos como fallos en el hardware o en caso de ciberataques.

2.25.7. Implementación de aplicaciones a nivel mundial

Con la nube, geografías anteriormente inaccesibles pueden ser alcanzadas y soluciones proporcionadas a una audiencia global en cuestión de minutos. Por ejemplo, Amazon opera desde la nube y tiene una red global de infraestructura, por lo tanto, puede desplegar su aplicación en varias geografías en un par de pasos. La disminución de la distancia entre aplicaciones y los usuarios finales elimina latencias y enriquece la experiencia.

2.26. Almacenamiento en la nube

El almacenamiento de datos en la nube es un modelo de servicio mediante el cual los datos se envían y almacenan en sistemas de almacenamiento remotos donde se mantienen, gestionan, respaldan y ponen a disposición de los usuarios a través de una red (generalmente Internet). Típicamente, los usuarios de datos en la nube pagan por su almacenamiento mensualmente en función del uso. Aunque este costo ha sido reducido en gran medida, los proveedores de almacenamiento en la nube han trasladado algunos gastos operativos a los usuarios, lo que puede hacer que el uso de la tecnología sea bastante costoso. (Aguaded & Tirado, 2018).

Las preocupaciones sobre la seguridad relacionadas con los servicios de almacenamiento en la nube aún persisten entre muchos usuarios.

Los proveedores de servicios han intentado aliviar esos temores mejorando sus capacidades de seguridad al incorporar cifrado de datos, autenticación multifactor y seguridad física mejorada a sus servicios.

2.26.1. Consideraciones de almacenamiento en la nube

Para entender si la transferencia a la nube generará eficiencias en costos, una empresa debe tomar los siguientes pasos:

- Determinar los costos iniciales y continuos asociados con la propiedad y gestión de la capacidad de almacenamiento en sitio en comparación con los costos continuos de gestión y recuperación de los datos en la nube.
- Evaluar la posible necesidad de un gasto adicional en telecomunicaciones para asegurar un acceso suficiente al proveedor del servicio.
- Evaluar la adecuación de la seguridad y el control de datos proporcionados por el proveedor del servicio en la nube.
- Crear políticas y procedimientos organizacionales sobre el uso del almacenamiento en la nube para hacer cumplir una gestión efectiva de datos y control de gastos.

2.27. Contratos en la nube como servicio

El tipo de servicio que se haya contratado ya sea IaaS, PaaS o SaaS, influye en qué gran medida el contrato de servicio en la nube esté estipulado. Existen diferentes tipos de contrato que abarcan múltiples elementos y condiciones los cuales determinan el alcance de control, personalización y la cantidad de riesgos que el cliente está dispuesto a tener ante el proveedor del servicio en la nube. Por lo tanto, el cumplimiento de regulaciones en privacidad y seguridad de datos se ve influenciado, por el hecho de que las instituciones hayan tenido el entendimiento adecuado de los tipos de contratos que existen para satisfacer sus necesidades tecnológicas.

2.27.1. Contrato de Infraestructura como Servicio (IaaS)

Según este contrato, al cliente se le ofrece computación en nube que abarca los servidores, almacenamiento, redes entre otros. A diferencia de otros contratos donde el

cliente es responsable de gestionar el hardware, en este el consumidor ejerce control únicamente sobre el sistema operativo y recursos disponibles. (Thomas Erl)

Recursos de Infraestructura: La computación en la nube habilita a que el proveedor ofrezca recursos básicos como el almacenamiento y red.

Escalabilidad: Se incluye cómputo para demanda plus y en relación con el uso que haga el cliente también se ajustan los recursos.

Facturación: En la mayoría de los casos, para los contratos del tipo IaaS, se aplica el modelo de cobro por uso donde se paga de acuerdo con el consumo de recursos que se utilicen (p. e. horas de CPU, almacenamiento de datos, etc.).

Soporte y Mantenimiento: Los términos relativos al soporte, mantenimiento técnico, la disponibilidad y la garantía de un cierto nivel de servicio (SLA).

2.27.2. Contrato de Plataforma como Servicio (PaaS)

Proporciona una plataforma completa para el desarrollo, implementación y gestión de aplicaciones sin tener que preocuparse por la infraestructura subyacente. Este tipo de contrato es común para empresas cuyo negocio principal es el desarrollo de aplicaciones y necesitan plataformas de desarrollo, pero no quieren gestionar la infraestructura. (McGrath)

Desarrollo y Ejecución de Aplicaciones: Los servicios que implican el desarrollo de aplicaciones, bases de datos, entornos de ejecución y las API disponibles para el cliente están dentro de los parámetros del contrato.

Automatización de Procesos: A diferencia de otros modelos, los proveedores de PaaS suelen proveer herramientas que permiten llevar a cabo la automatización del despliegue, escalado y mantenimiento de aplicaciones.

Escalabilidad: En IaaS los contratos PaaS también poseen condiciones con respecto a recursos que se puedan ampliar en cantidad que cumplan con la necesidad.

Modelo de Pago: Típicamente el modelo de pago lleva como inclusión tarifas que dependen del uso de ciertos recursos y servicios específicos como bases de datos, almacenamiento y servicios de monitoreo.

2.27.3. Contrato de Software como Servicio (SaaS)

Ofrece a los usuarios un acceso a un conjunto de programas completos mediante una nube. Los clientes no tienen la gestión o control de la infraestructura o plataforma, sino que lo que hacen es usar el software a través del navegador web o una interfaz. Los contratos SaaS son los más utilizados en negocios con aplicaciones como CRM, ERP y otras aplicaciones de productividad. (Nick Antonopoulos)

Acceso al Software: En el contrato se definen las condiciones para el tema del acceso a la aplicación y uso con respectiva y posible modificación del software.

Licencia de Uso: A diferencia de la licencia de uso que se permite irrenunciablemente a un software tradicional por tiempo indefinido, en los contratos de servicio SaaS, el cliente durante la validez del contrato, solamente adquiere una licencia que le permite acceder al servicio.

Facturación: Los contratos de servicios SaaS son generalmente por una tasa de suscripción, que puede ser mensual o anual, o simplemente por pago por uso. Esto puede incluir tarifas por usuarios, tarifas por volumen de datos y consumo de funcionalidades.

Nivel de Servicio (SLA): Rigurosamente se establecen acuerdos o contratos de nivel de servicio por la disponibilidad o uptime, el tiempo de respuesta, el soporte técnico al software y las garantías sobre disponibilidad.

Actualizaciones y Mantenimiento: El proveedor se encarga de estas tareas sobre el software, dejando al cliente libre de realizar cualquier actividad.

2.28. Desafíos en los Centros de Datos en la nube

Tabla 4. Desafíos en los Centros de Datos en la nube

Dependencia de Acceso a Internet para acceder	Para poder acceder a los servicios contratados, se requiere una conectividad a internet que sea eficiente en calidad, sin retrasos ni demoras.
Cumplimiento Regulatorio	Hay organizaciones que están obligadas a cumplir con ciertas regulaciones de privacidad de datos y protección de datos. Esto significa que los datos en tales casos solo pueden ser almacenados en relación con la región comprada.
Control Limitado sobre la infraestructura	Si bien los proveedores de servicios en la nube ofrecen una serie de controles, el cliente, sin embargo, tiene un control limitado de la infraestructura subyacente, lo que puede resultar un problema para las empresas con requisitos muy precisos.

Nota. Detalle de los principales desafíos de implementar Centros de Datos en la nube. Elaborado por: Autor

CAPITULO 3: DISEÑO DEL PLAN DE RECUPERACION DE SERVICIO.

En este capítulo se muestra el diseño de un plan de recuperación de servicio ante desastres para el Centro de Datos en caso de que se llegue a presentar una interrupción de servicios, sea este de manera natural como un terremoto, algún error cometido por el hombre o falla del sistema. Toda la propuesta del diseño del plan de recuperación de servicio para el Centro de Datos será aplicada para la empresa NetPay S.A.

El diseño de un protocolo de recuperación ante desastres permite que una organización sea capaz de afrontar y resurgir de cualquier evento que ponga en peligro su normal funcionamiento y continuidad del negocio.

El objetivo de este plan será asegurar la recuperación de las copias de seguridad de los datos, de acuerdo con las políticas y procedimientos establecidos por la compañía.

3.1. Identificación y Valoración de riesgos

Todo el personal que trabaja dentro de la empresa, así como sus equipos e instalaciones se encuentran en constante exposición a diferentes riesgos, sean estos naturales o provocados por el hombre, teniendo la posibilidad de que se puedan materializar y provocar daños en cualquier momento. Es por eso por lo que se debe empezar definiendo los posibles riesgos y amenazas que puedan afectar a la empresa.

Riesgos y Amenazas naturales

Se define como riesgo natural a los diferentes fenómenos físicos (geológicos, geofísicos, sismológicos, meteorológicos entre otros) de carácter impredecibles que pueden generar un impacto negativo al ser humano y al ambiente en general (Reyes, Montilla, Castillo, & Zambrano, 2017).

Entre las amenazas naturales a considerar están:

Meteorológicas

- Tormentas locales severas (granizo, eléctricas, tornados).
- Tormentas de polvo.

- Sequía.
- Inundaciones, marejadas.
- Incendios.
- Temperaturas extremas (frío y calor).
- Ciclones y huracanes tropicales.

Geológicos-Geofísicos

- Terremotos y tsunamis.
- Erupciones volcánicas.
- Deslizamientos, derrumbe.
- Desbordamiento de ríos.
- Hundimientos.
- Avalanchas de nieves.

Medio Ambiente

- Lluvias ácidas.
- Contaminación del aire, agua, suelo y atmósfera.
- Plagas.
- Problemas con las cosechas.
- Apertura de la capa de ozono.
- Deshielo de los glaciares.
- Aumento del nivel del mar.

Riesgos y Amenazas Antrópicas

Los riesgos y amenazas antrópicas se definen como situaciones de peligro causadas directamente por acciones humanas. Este tipo de accidentes pueden ser desde problemas tecnológicos hasta conflictos internacionales como las guerras (Lacambra, Lozano, Alonso, & Fontalvo, 2003).

Entre los riegos antrópicos están:

- Incendios.
- Transporte y logística.

- Industriales.
- Actividades deportivas.
- Atentados.
- Epidemias y plagas.
- Conflictos internacionales.
- Tecnológicos.

Con respecto a los riesgos tecnológicos que no estén relacionados con amenazas naturales o antrópicas, entre los principales tenemos:

- Falla del proveedor de internet.
- Falta de mantenimiento de los equipos.
- Caída de un servidor específico.
- Espionaje corporativo.
- Falla en la renovación de licencias.
- Falta en la capacidad de almacenamiento.
- Error en la copa de respaldo de un servidor.
- Falla en intermitencias o latencias de redes.

Una vez que se han identificado los riesgos y amenazas que se pueden producir de manera natural o antropológica, se procederá a analizar y clasificar cada una de las amenazas en una Matriz de Riesgos de acuerdo con los criterios de probabilidad e impacto.

Luego de clasificar los riegos y amenazas a suscitar dentro de la empresa, se procederá a priorizar los datos a recuperar.

3.2. Prioridades de Recuperación

El primer paso será la clasificación los datos de acuerdo con su nivel de prioridad de recuperación durante el plan de contingencia. Se determina como **“Nivel de Riesgo Operativo”**, considerando la afectación a los servicios críticos empresariales y los siguientes factores de evaluación:

Tabla 5. Nivel de Riesgo Operativo

Nivel de Riesgo Operativo				
Servicios	**Subproceso**	**IMPACTO REPUTACIONAL**	**IMPACTO FINANCIERO**	**IMPACTO REGULATORIO**
Transaccional	Gestión del Flujo Transaccionalidad	MAYOR= INTERRUPCIÓN 1,01 - 4 Horas La exposición (quejas), por no entregar el servicio se presenta mediante redes sociales, medios de comunicación, correos electrónicos y/o directo a entidades Emisoras y/o clientes	MENOR= INTERRUPCIÓN 1,01 - 4 Horas SLA acordado con entidades emisores 99,80%, indisponibilidad permitida mensual: 1hora y 26 minutos = 86 minutos. No hay multas o sanciones porque la recuperación (78min), se realizó dentro del SLA acordado.	MAYOR= INTERRUPCIÓN 1,01 - 4 Horas SLA dispuesto por la SIB 99,99%, indisponibilidad permitida anual: 52 min 34 seg.
Standin	Gestión del Servicio Standin para Entidades Emisoras			

Nota. Nivel de Riesgo Operativo empresarial. Elaborado por: Autor

Prioridad Alta

- Flujo Transaccionalidad
- Canal de comunicación
- Infraestructura de red local
- Canal de internet local
- Infraestructura de apoyo
- Herramientas de gestión de servicios y su infraestructura de apoyo

Prioridad Media

- Página web principal
- Correo electrónico
- Servicios internos

3.3. Procedimientos de Notificación para la activación de los servicios

Una vez que se hayan clasificado los niveles de prioridad para el plan de recuperación, se deberán asignar un código de notificación que nos permita definir la magnitud del problema, de esta saber cuál será el procedimiento para aplicar para la recuperabilidad de los datos.

Para asignar los criterios de activación de datos se tomarán en cuenta los siguientes parámetros:

- Magnitud de los daños en la infraestructura.
- Tiempo estimado de interrupción.
- Magnitud de los daños de las instalaciones.

3.4. La Magnitud de los Riesgos

Tenga en cuenta que solo puedo proporcionar una visión general de los riesgos relacionados con la adopción de tecnología en la nube. Visión general Debido a los factores ambientales variables, algunos riesgos en la nube pueden ser mayores que en otros servicios, por ejemplo: dependencia de la infraestructura, seguridad, regulación, controles para costos y datos. Sin embargo, es importante mencionar que todas las áreas asociadas con la nube también tienen algunos riesgos comunes, tales como: seguridad, violación de la privacidad, incumplimiento de acuerdos y bloqueo de proveedores. Descripción de los riesgos comunes asociados con esta tecnología, los riesgos se dividen en los siguientes grupos: riesgos de seguridad, tecnológicos, organizacionales y legales.

3.4.1. Riesgos de Seguridad

La seguridad se encuentra entre los riesgos más importantes, ya que determina la credibilidad en el mercado. La magnitud del riesgo está asociada con el tipo de datos proporcionados y los tipos de características de seguridad ofrecidas por el proveedor. Por ejemplo, para evitar violaciones de datos, se aconseja a los proveedores de servicios que utilicen cifrado fuerte, autenticación, controles de integridad y capacitación de empleados no confiables para que la información de las organizaciones evite el acceso no deseado a su información confidencial. Si los datos a los que se accede son extremadamente sensibles, los problemas derivados de ello podrían arruinar a la organización. (Tim Mather)

Riesgos asociados:

- **Filtraciones de datos**: Acceso no autorizado o robo de información sensible.
- **Ataques cibernéticos**: Malware, ransomware, o DDoS dirigidos a los servicios en la nube.
- **Falta de visibilidad**: Las organizaciones pueden perder visibilidad de sus propios datos cuando se alojan en infraestructuras de terceros.

3.4.2. Riesgos de Privacidad

La preocupación por la privacidad es otro riesgo importante, especialmente cuando se almacenan datos sensibles en los servidores de proveedores externos. Los riesgos también aumentan en caso de que el proveedor de servicios en la nube no opere dentro de las regulaciones de privacidad o si los datos se exportan a países con una regulación de privacidad más débil. (Hoofnagle)

Riesgos asociados:

- **Incumplimiento de normativas**: Como el Reglamento General de Protección de Datos en Europa, Ley de Portabilidad y Responsabilidad de Seguro Médico en EE. UU., etc.

- **Transferencia transfronteriza de datos**: Los datos se almacenan en ubicaciones que no tienen medidas de protección de privacidad suficientes.
- **Acceso no autorizado**: Existe la posibilidad de que empleados del proveedor tengan acceso a alguna información sensible sin autorización.

3.4.3. Riesgos de Dependencia del Proveedor

La dependencia del proveedor puede ser muy peligrosa. Imagínese una situación donde el servicio del proveedor ya no está disponible o sus condiciones de servicio han cambiado. Por ejemplo, si las empresas desean cambiar de proveedor, pueden quedar atrapadas en un mal trato o incurrir en altos costos de cambio. (Thomas Erl)

Riesgos asociados:

- **Bloqueo del proveedor:** Una dependencia excesiva de la tecnología de un proveedor en particular hace que cambiar de proveedores sea caro y difícil.
- **Interrupciones de servicio**: Si los proveedores de servicios en la nube tienen dificultades técnicas o cierran su negocio, el servicio en la nube puede verse afectado.
- **Modificación de términos**: Tendrían la capacidad de alterar los términos de prestación del servicio, lo que a su vez influiría en cuán accesible y asequible sería para el cliente final.

3.4.4. Riesgos de Cumplimiento Normativo

Es fundamental cumplir con las leyes y regulaciones locales e internacionales en industrias como la salud, la educación y las finanzas. Las organizaciones corren el riesgo de enfrentar consecuencias legales y daños a su reputación si no siguen las regulaciones de privacidad y seguridad.

Riesgos asociados:

- **Multas y sanciones**: No cumplir puede someter a la organización a multas financieras sustanciales. (Vasilenko)
- **Auditoría y trazabilidad**: Cuando los datos no tienen la supervisión adecuada, se vuelve difícil autenticar el cumplimiento de regulaciones

específicas, ya que las personas no pueden presentar la evidencia requerida.

3.4.5. Riesgos Financieros

Los servicios en la nube pueden volverse costosos si hay un exceso en lo que se requiere, lo que resulta en costos inesperados. El nivel del riesgo en cuestión depende en gran medida de la previsión financiera de la organización. (Stroud)

Riesgos asociados:

- **Modelos de pago impredecibles**: La facturación basada en el uso tiene un alto precio si se es descuidado con la supervisión de los recursos.
- **Costos de migración y capacitación**: Migrar de una solución local a una basada en la nube puede resultar tanto costoso como que consuma tiempo.

3.4.6. Riesgos de Pérdida de Control sobre los Datos

Una vez que una organización decide que va a mover el centro de datos a la nube, puede perder los poderes de administración para supervisar directamente cómo se almacenan los datos, cómo se accede a ellos y cómo se aseguran; esto puede convertirse fácilmente en un problema si las expectativas establecidas para el proveedor no se cumplen. (Implementation)

Riesgos asociados:

- **Desaparición o daño de datos**: El riesgo de eliminación o corrupción de datos debido a fallas del proveedor de servicios o brechas de seguridad.
- **Acceso no autorizado**: Existe el riesgo de que los datos sean vistos por personal no autorizado debido a ciberseguridad inadecuada.

Los riesgos asociados con los servicios en la nube en términos de magnitud son diferentes según la ubicación y la preparación de la respectiva organización. De estos riesgos clave, están la seguridad, la privacidad, el cumplimiento regulatorio, el costo y el bloqueo del proveedor. Las fuentes bibliográficas proporcionadas presentan un análisis

detallado de cada uno de estos riesgos y ayudan a las empresas a comprender cómo minimizar y gestionar los riesgos asociados con la computación en la nube.

3.5. Diseño de comunicación de Alto Nivel para su aplicación

Para implementar esta propuesta, es importante entender la situación actual y los requisitos mínimos para la implementación. Se explicará cómo se llevará a cabo la comunicación en caso de que ocurra un incidente en el sitio principal con un sitio secundario como sitio de respaldo para apoyar el protocolo de comunicaciones con una arquitectura de alto nivel para el diseño de la comunicación.

Requisitos clave para desplegar un sitio de contingencia efectivo en el contexto de un Protocolo de Recuperación ante Desastres:

Ubicación

- Geográficamente Distante: Debe estar ubicada lejos del sitio principal para no verse afectada por desastres específicos de la región, como inundaciones locales, incendios o terremotos.
- Accesibilidad: La profundidad es fácilmente accesible siempre que se requiera la reflexión del personal clave en un evento de activación.

Infraestructura

- Espacio Adecuado: Debe haber suficiente capacidad no solo para acomodar el único sistema crítico de la estructura, sino también a todo el personal adicional requerido.
- Conectividad de Red: Debe haber acceso a internet y redes privadas seguras, con planes de respaldo para garantizar la comunicación efectiva cuando se trata de diversos proveedores de servicios externos.

Equipamiento Técnico

- Servidores y Hardware: Una variedad de dispositivos que ayudarán a restaurar los sitios interrumpidos, incluido un rango de servidores y dispositivos de red que facilitan un almacenamiento de datos sin interrupciones.

- Software Necesario: Licencias y subcomponentes que estén actualizados para el sitio de contingencia requerido antes del evento.

Sistemas de Energía

- Alimentación Ininterrumpida: Suministrando energía de respaldo y generadores para garantizar que el sitio tenga un suministro continuo de trabajo.
- Redundancia Energética: Tener acceso a diversas fuentes de energía para prevenir interrupciones de energía.

Seguridad Física

- Controles de Acceso: Implementando sistemas de seguridad física que incluyan cerraduras, tarjetas de acceso y cámaras de vigilancia.
- Protección contra Desastres: Estructuras que siguen códigos de seguridad prescritos para aquellas estructuras que están practicadas en regiones propensas a terremotos e inundaciones.

Sistemas de Monitoreo

- Monitoreo Remoto: Herramientas que se utilizan para monitorear el estado de los sistemas de energía y la infraestructura de manera remota.
- Alertas y Notificaciones: Una forma de mantener al personal al tanto de los problemas que pueden surgir con un sistema de alertas.

Plan de Comunicaciones

- Sistema de Telefonía: Considerar como la capacidad de comunicarse mediante llamadas con el personal y partes interesadas.
- Red de Comunicación Alternativa: Medios de comunicación alternativos (como mensajería instantánea) en caso de que exista un fallo en la red principal.

Documentación y Procedimientos

- Manual de Operaciones: Documentación detallada sobre cómo trabajar desde el sitio de contingencia.

- Procedimientos de Activación: Activar en un determinado ciclo, en determinadas circunstancias o en un momento específico en el tiempo el sitio de contingencia.

Capacitación del Personal

- Entrenamiento Regular: a capacitación se hace obligatoria para todos los profesores sobre cómo se debe actuar en el sitio de contingencia.
- Simulacros de Emergencia: Llevar a cabo ejercicios regulares para que el personal se familiarice con los procedimientos.

Plan de Recuperación y Mantenimiento

- Revisión y Pruebas: Revisiones del sitio a tiempo cuando se considera conveniente para garantizar un adecuado nivel de preparación y estado general.
- Mantenimiento de Equipos: Mantenimiento para garantizar que el hardware y software estén al día.

Estos requisitos aseguran que un Sitio de Contingencia esté bien preparado para operar eficazmente en caso de un desastre. El análisis e implementación de un plan detallado son primordiales para el funcionamiento ininterrumpido de un negocio.

¿Cuáles son los requisitos para el diseño del plan de recuperación de servicios?

El modelo tradicional de recuperación ante desastres incluye la configuración de un sitio de recuperación, que necesita mantenimiento constante y asistencia por parte del cliente. En este caso, la protección de datos y los servicios de recuperación ante desastres se realizan en modo manual, lo que es potencialmente una actividad que consume tiempo y recursos.

La recuperación ante desastres en la computación en la nube significa que todos los datos y aplicaciones cruciales se almacenan en la nube y, en caso de desastre, el proceso de recuperación se cambia a un sitio secundario. Este tipo de servicio asegura que se cobrará por uso y estará disponible desde cualquier lugar en cualquier momento. La copia de seguridad y recuperación ante desastres en la computación en la nube pueden ser automatizadas. (Costas, 2017)

Tener un plan de recuperación ante desastres en su lugar, ponerlo en acción y mantenerlo actualizado permite a la organización recuperarse de cualquier evento imprevisto y proteger y sostener el negocio.

La planificación de emergencias para la recuperación implica consultar a un especialista considerando la infraestructura de la organización, las amenazas y debilidades, los activos más críticos y su priorización en el proceso de recuperación, y los servicios apropiados para la reconstrucción tras un desastre.

La integración de la computación en la nube evita que los planes de recuperación formulados se pierdan en los recovecos de la mente al permitir que cada paso del proceso sea mecánico.

¿Cuál es el plan de recuperación cuyo diseño se presentará?

Copia de seguridad y recuperación ante desastres en la nube. La computación en la nube se puede definir como un sistema económico de provisión de servicios informáticos que se utilizan por demanda y son accesibles por medio de la red de internet. Los proveedores de computación en la nube generalmente brindan acceso a los servicios.

3.6. Metodología del plan de recuperación ante desastres

Si bien cada empresa es única, esta lista de verificación del plan de recuperación ante desastres describe algunas de las mejores prácticas fundamentales que se pueden aplicar a casi cualquier organización. la integración de la lista de verificación en este documento es invaluable para la construcción de tales equipos en cualquier compañía, cualquiera que compre copias de sus documentos y perpetuo mantenimiento de esta. Aun así, la metodología de desarrollo del sistema de gestión de la organización resultará más efectiva.

Determinar el personal clave

Si se está creando un plan de continuidad comercial formal, uno de los primeros pasos más importantes es definir el "quién" en situaciones de desastre:

¿Quién está a cargo? ¿Quién tiene el poder de tomar decisiones para implementar sus procedimientos de recuperación ante desastres? ¿Quién tiene acceso a datos y sistemas

clave? ¿Quién necesita ser contactado durante un evento crítico (y por qué métodos de comunicación)?

Evaluar riesgos

Cada plantilla de plan de recuperación ante desastres de TI debe incluir un lugar para la evaluación de riesgos. Aquí es donde identifica los puntos de vulnerabilidad específicos de la organización en varios tipos de desastres.

3.6.1. Análisis del Diseño del plan de recuperación

En este punto se analizará las alternativas de diseño de plan de recuperación tomando en cuenta la situación actual del centro de datos del Sitio Principal, Además, se formularán estrategias de comunicación y respaldo, así como medios de comunicación para respaldar en el Sitio de Contingencia, teniendo en cuenta el Servicio de Recuperación de Desastres del Centro de Datos Híbrido.

En esta fase si identificará y verificará el inventario de dispositivos que se cuentan actualmente en el Sitio Principal frente a los que se vayan a contemplar para Sitio de Contingencia, con los objetivos de tener replicado a nivel de comunicaciones y datos.

Además, establecer los procedimientos de recuperación considerando la calidad de servicio, la tolerancia a fallos y alta disponibilidad.

3.6.2. Sitios para recuperación de servicios.

Para esta propuesta es implementar un diseño para el Sitio de Contingencia y Sitio en la Nube, se pretende detallar los dos métodos sus ventajas de cada uno de ellos.

Plan de recuperación mediante Centro de Datos de Proveedores de Servicios (Sitio de Contingencia).

- Bajo costo con referencia a servicios en la nube.
- Inversión inicial elevada (Equipamiento, cableado de red, suministro eléctrico, implementación de proveedores de servicios de comunicación, etc.

- Tiempo de reanudación de las operaciones se requiere una gestión manual, dicho proceso debe ser probado anualmente para cumplimiento de normas.
- Costos de mantenimiento del Sitio de Contingencia con el Proveedor de Servicios contratado.

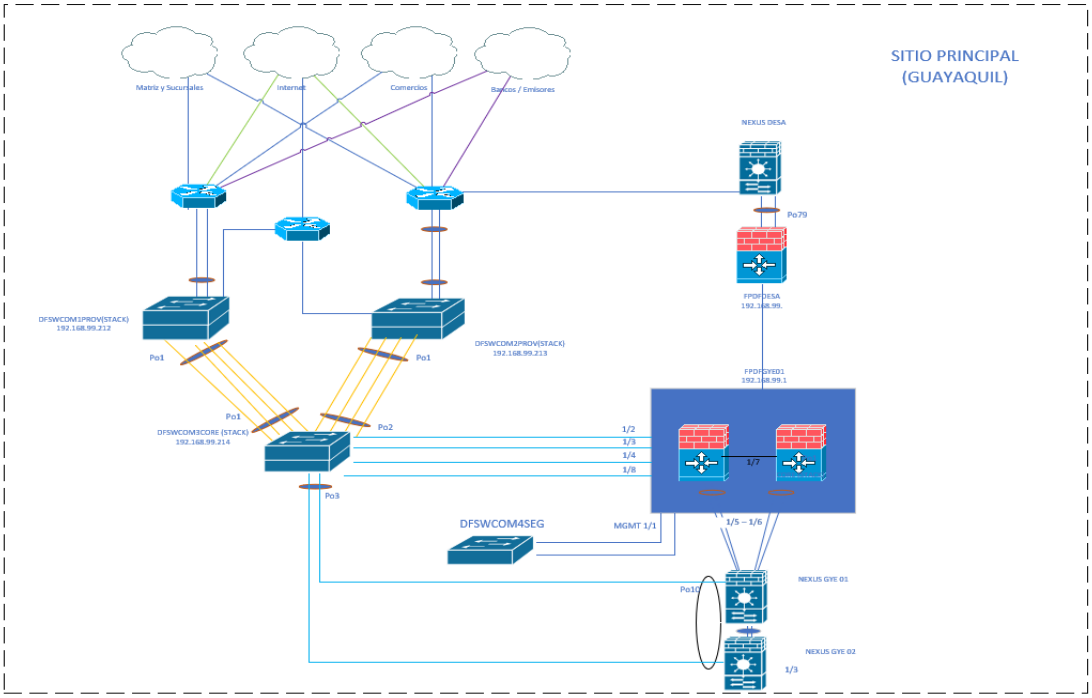
Plan de recuperación mediante Centro de Datos en la nube (Nube Privada).

- Costo dependiente a la capacidad de uso y método de pago por uso.
- Costos muy altos con respecto al plan de recuperación tradicional.
- Seguridad Gestionada.
- Mantenimiento de especialidades en distintos ambientes, servicio disponibilidad 24x7.
- Centro de Datos con infraestructuras redundantes para brindar funcionalidad como alta disponibilidad.
- Fiabilidad y agilidad en el método de recuperación de servicios.

3.7. Propuesta de Diseño para plan de recuperación de servicios

3.7.1. Diseño Actual de Alto Nivel del Sitio Principal

Ilustración 6. Diseño Actual de Alto Nivel de comunicaciones del Sitio Principal.



Nota. Diseño de infraestructura de Red Actual de Alto Nivel en el Sitio Principal.
Elaborado por: Autor

En la actualidad el Sitio de Principal como se puede observar cuenta con muchos componentes que se describen a continuación:

Conmutadores de comunicación para proveedores de servicios y con su respectiva contingencia a nivel de enlaces, así como equipamiento de conmutadores, aplicando el protocolo de redundancia a nivel de equipamiento para contingencia y protocolos de enlaces redundantes.

Configuración de Enlaces Redundantes para conexión entre dispositivos tiene configurado enlaces redundantes.

Enrutadores o Encaminadores de proveedores de servicios, estos dispositivos son propiedad de los proveedores y su administración, los mismos proporcionan los servicios de enlaces como acceso a internet, emisores, comercios y oficinas a nivel nacional, adicionales enlaces redundantes para que se puede proporcionar comunicación al conmutador de proveedores de contingencia ubicado en otro armario.

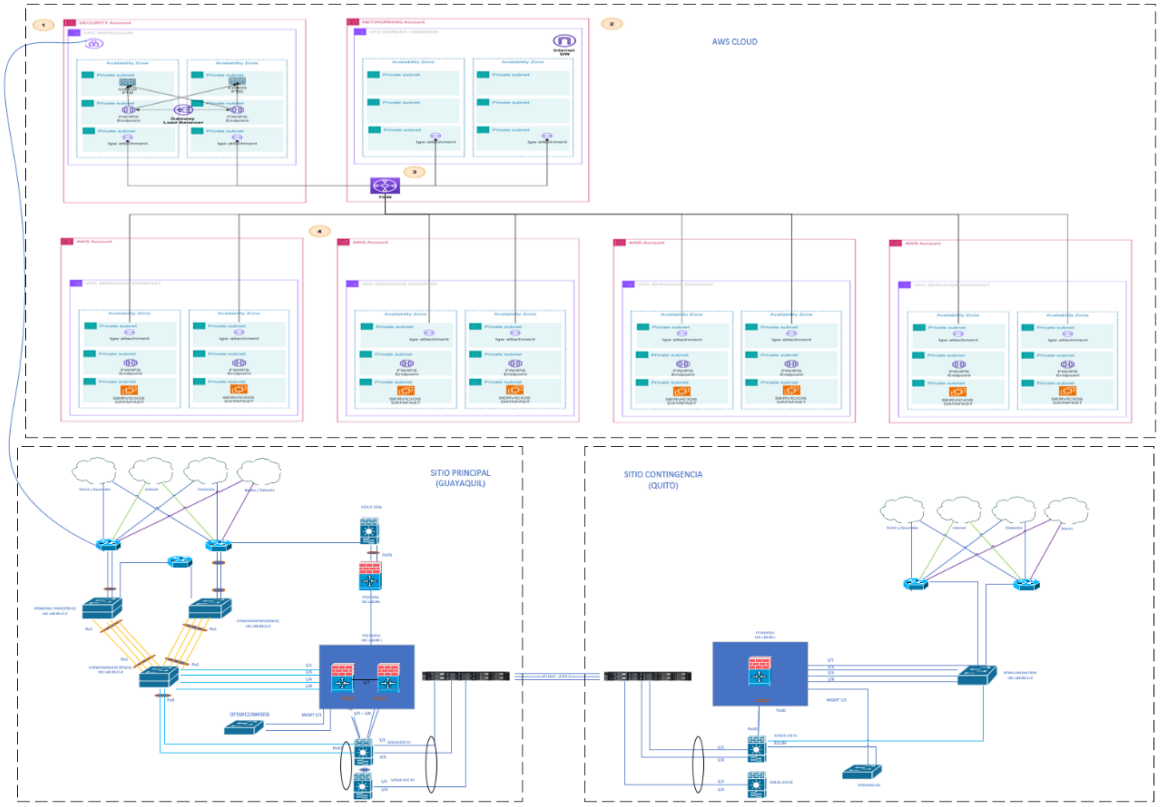
Cortafuegos perimetral que cuenta con una construcción de alta disponibilidad de dos dispositivos modo espejo para que en caso que falle existe un equipo de contingencia en el mismo Sitio de Principal, este es la puerta enlace principal para todas las redes locales de la empresa y proporciona todas las funcionalidades como controles de acceso, filtro de navegación, control de aplicaciones, servicio de prevención de intrusos, control de amenazas externas, de esta manera proporcionar seguridad perimetral para los servicios internos, así como servicios publicados.

Conmutadores Núcleo para conectividad de redes locales, debido a sus características como densidad de puertos y alto consumo de tráfico que soporta para la conectividad a los chasis de servidores para infraestructura virtual.

Configuración de Canal de Puerto Canal permite que los enlaces que están conectados físicamente a dos conmutadores de núcleo y se establezca altas velocidades de transmisión y pueda fluir grandes volúmenes de tráfico.

3.7.2. Propuesta de Diseño Propuesto con Sitio de Contingencia y nube.

Ilustración 7. Propuesta de Diseño de Alto Nivel con Sitio de Contingencia y en la Nube

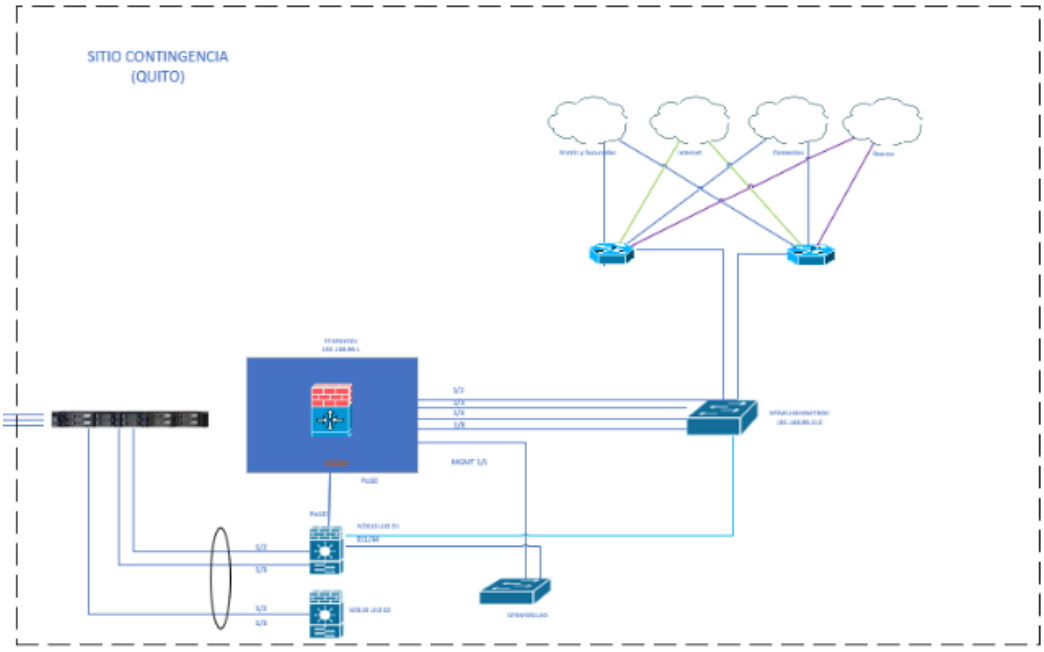


Nota. Propuesta de Diseño de Alto Nivel con Sitio Principal, Sitio de Contingencia y Nube. Elaborado por: Autor

3.7.3. Centro de Datos para Sitio de Contingencia

Para el Centro de Datos de proveedores de servicio llamado Sitio de Contingencia en la ciudad de Quito se considera un esquema con componentes similares a los servicios que brinda el Sitio Principal debido que en caso de requerirse todos los componentes del Sitio de Contingencia deben cumplir con un rol de activo y ponerse en producción.

Ilustración 8. Centro de Datos para Sitio de Contingencia

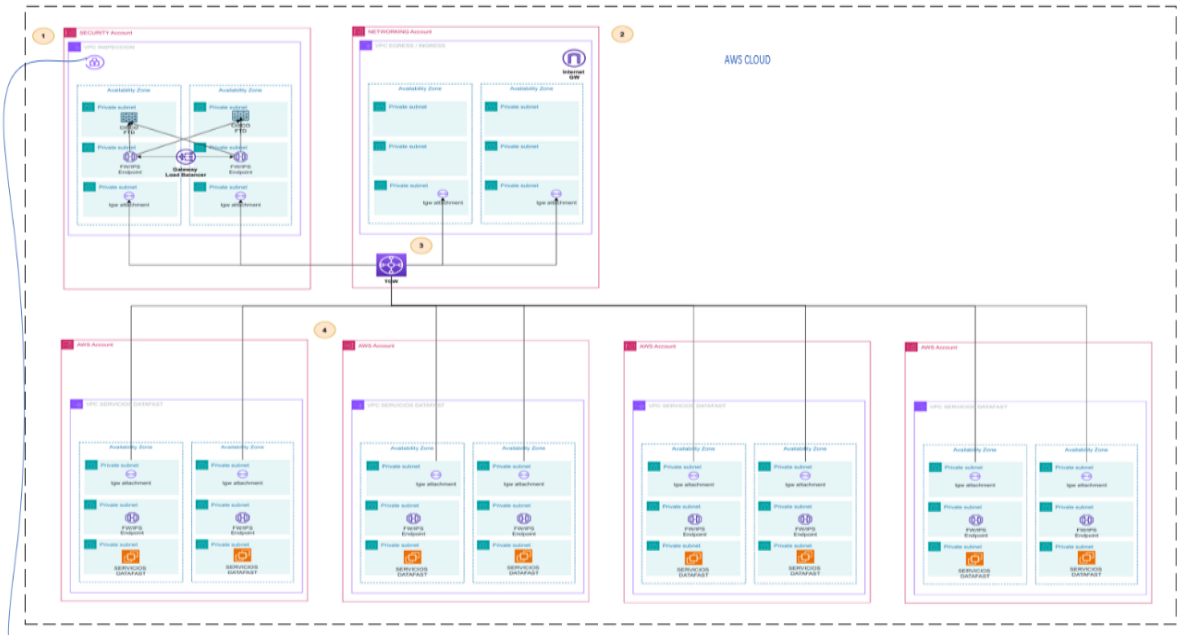


Nota. Ilustración de componentes similar al Sitio Principal. Elaborado por: Autor

3.7.4. Centro de Datos en la nube

Para mejor comprensión del diseño propuesto para el Centro de Datos en la nube se detalla en la siguiente tabla los componentes:

Ilustración 9. Centro de Datos para la nube



Elaborado por: Autor

Tabla 6. Detalle de componente de AWS del Centro de Datos en la nube

Componentes de AWS	**Detalle del componente**
VPC (Virtual Private Cloud)	Es el componente fundamental para crear redes aisladas dentro de la nube de AWS. Crea un ambiente de subred privado con direcciones IP y rutas.
Private Subnet	Permite dividir en subredes la VPC en segmentos más reducidos para organizar cada instancia y otros recursos de manera óptima.
Gateway de Internet (Internet Gateway)	Puerta de Enlace de Internet es indispensable para que los recursos dentro de una VPC, como las instancias, puedan acceder a Internet.
Gateway NAT (Network Address Translation)	Permite que las subredes privadas se comuniquen con Internet para realizar actualizaciones, parches o acceder a servicios externos, para tráfico hacia internet desde las subredes.
VPN (Virtual Private Network)	AWS permite conectar tu red local en premisa a través de una red virtual privada VPN a la nube.
Conexión Directa (AWS Direct Connect)	Proporciona un enlace dedicado entre tu infraestructura local y AWS, de esta manera no depender de Internet. Es útil para aplicaciones que requieren baja latencia o requieran alta disponibilidad.
Elastic Load Balancer (ELB)	Distribuye automáticamente el tráfico de red entrante entre las instancias en una VPC. Hay varios tipos de ELB según el tipo de tráfico.
AWS Transit Gateway	Un servicio que permite interconectar múltiples VPCs y redes en premisa, facilitando la gestión de rutas entre ellas. Es útil para entornos más complejos donde se manejan varias VPCs.

Elaborado por: Autor

Para el Centro de Datos en la nube tiene como objetivo que se migren los servicios críticos, así como también implementar las nuevas tendencias para desarrollo empresarial soportados en la nube como los siguientes ejemplos:

Hospedaje de Aplicaciones Empresariales

Aplicaciones empresariales tradicionales, como ERP, CRM, y otras aplicaciones comerciales tradicionales, puede ser alojado en la nube, lo que elimina la necesidad de mantener infraestructura local.

Escalabilidad en la Nube para Aplicaciones Web

Las aplicaciones de auto escalables son uno de los casos de uso más comunes en la nube, especialmente con aplicaciones web que experimentan un tráfico intenso durante ocasiones o cargas inesperadas. Los servicios en la nube proporcionan la flexibilidad de pagar solo por los recursos que necesite.

Desarrollo y Pruebas de Aplicaciones

Los centros de datos en la nube permiten a los desarrolladores establecer entornos de prueba y desarrollo rápidamente sin tener que instalar una infraestructura física compleja. Los recursos se pueden provisionar bajo demanda y desmantelar cuando ya no sean necesarios, lo que reduce costos.

Big Data y Análisis de Datos

Las empresas requieren un número masivo de procesamiento de datos a gran escala almacenados y en la nube para almacenar todo el volumen de información que poseen, y la combinación entre ambas facilita su manejo de forma sorpresiva. Esto, a su vez, permite el uso de amplias plataformas.

Internet de las Cosas (IoT)

Las infraestructuras en la nube tienen un impacto positivo en el mercado de los dispositivos conectados gracias a su capacidad de manejar y guardar importantes cantidades de datos.

Aplicaciones de Realidad Virtual

Las experiencias inmersivas requieren ser sometidas a un gran esfuerzo de procesamiento mediante el uso de las aplicaciones de la arquitectura existente, y para recibirlas se pueden usar Centros de Datos en la nube.

3.7.5. Interconexión entre Centro de Datos

Interconexión entre Centro de Datos del Sitio Principal y Sitio de Contingencia

Se contempla un enlace de red extendida en capa dos con la intención que la misma red del Sitio Principal se propaguen al Sitio de Contingencia de esta forma cuando los componentes del Sitio de Contingencia tomen rol de activo se transparente su puesta en marcha, como por ejemplo en caso de las pruebas generales de continuidad controlada.

Interconexión entre Centro de Datos del Sitio Principal y Centro de Datos en la nube

Para la interconexión con el Centro de Datos en la nube se realizará por etapas inicialmente mediante una red virtual privada y luego mediante un enlace dedicado mediante el componente “Conexión Directa”.

CAPITULO 4: PLANIFICACIÓN DE DRP

En este capítulo tiene como detallar la planificación para llevar a cabo las pruebas de continuidad del negocia alineándose a las normas corporativas y las que exigen las entidades bancarias.

4.1. Antecedentes

Con la finalidad de cumplir lo establecido por la Superintendencia de Bancos del Ecuador mediante resolución No. SB-2021-2126, NetPay S.A., planifica la prueba anual de continuidad de negocio.

Mediante el "Comité de Continuidad del Negocio y Gestión de Crisis" se presenta la información de planificación de la "Prueba General Anual" de continuidad de negocio y de la documentación relacionada para su ejecución.

4.2. Objetivo de la planificación

Ejecutar una prueba de continuidad servicios y comprobar la efectividad de los planes, mediante procedimientos de "Chequeo de Lista" y comunicados establecidos ante situaciones que demanden la activación de contingencias para mantener la continuidad del negocio y reestablecer oportunamente la disponibilidad de los servicios críticos para las partes interesadas (Entidades Emisoras, Establecimientos Afiliados, Proveedores, etc).

4.3. Alcance de la planificación

Activar el Centro de Datos del Sitio de Contingencia situado en la ciudad de Quito NetPay S.A., para recuperar la operación de los servicios críticos ante una falla general del Centro de Datos del Sitio Principal situado en la ciudad de Guayaquil.

Los servicios empresariales de NetPay S.A., que formarán parte de la prueba y se verán afectados temporalmente son:

- Transaccionalidad
- Standin para Entidades Emisoras

4.4. Base Normativa

Las Normas y buenas prácticas relacionadas a la ejecución de las pruebas son:

4.4.1. Norma ISO 22301:2019, punto 8.5

"La organización deberá implementar y mantener un programa de ejercicios y pruebas para validar en el tiempo la efectividad de sus estrategias y soluciones de continuidad del negocio […].".

4.4.2. Superintendencia de Bancos, Libro I 'Normas de Control para las Entidades de los Sectores Financieros Público y Privado', Título IX 'De la Gestión y Administración de Riesgos', Capítulo V 'Norma de Control para la Gestión del Riesgo Operativo', Sección V 'Gestión de la Continuidad del Negocio', Artículo 19, numeral 8.

"Procedimientos de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o, al menos, una vez al año […].".

4.5. Planificación de la Prueba DRP

Para llevar a cabo una prueba de continuidad controlada "Prueba General Anual", se definieron y cumplieron las siguientes actividades:

4.5.1. Escenario de la Prueba

"Falla General del Centro de Datos Principal y Activación del Centro de Datos de Continencia", por afectación al servicio crítico "Transaccional" (recepción de transacciones, revisión, ruteo a Emisor, recepción y reenvío de respuesta).

4.5.2. Criterios de Éxito de la Prueba

- Probar la contingencia de todos los componentes tecnológicos planificados para la prueba.

- Cumplir las actividades y los tiempos referenciales establecidos en los "Chequeo de Lista" de los componentes tecnológicos.
- Gestión de los servicios críticos "Transaccional" y "Standin" (disponibles y con desempeño correcto) mediante la infraestructura del Centro de Datos de Contingencia
- Cumplimiento de Pruebas sin novedades internas que impidan su ejecución

4.5.3. Participantes de la Prueba

- Comité de Continuidad del Negocio y Gestión de Crisis
- Departamento de tecnología de la información y seguridad de la información
- Riesgos Integrales y Cumplimiento – Continuidad del Negocio
- Auditoría Interna
- Entidades Emisoras
- Proveedores de Servicios Críticos

4.5.4. Componentes tecnológicos incluidos en la prueba

- Cortafuegos
- Enlaces con las Entidades Emisoras
- Balanceador de servicios
- Distribuidor Intellinac
- Switch Transaccional Smart Vista (Servicio "Transaccional" y Servicio "Standin" para las Entidades Emisoras)

4.5.5. Pre – Requisitos de la Prueba

- Incrementar el ancho de banda en los canales de lan extendida capa dos, con los proveedores que la brindan.
- Validar la salud y operación de los componentes tecnológicos incluidos en la "Prueba General Anual" (1 hora antes).

4.5.6. Preparación y formalización de la Prueba

- Realizar pruebas aisladas de los componentes tecnológicos incluidos en la "Prueba General Anual", para prevenir, identificar y solventar posibles novedades.

- Establecer y preparar los requisitos para ejecutar la "Prueba General Anual":
  - ✓ Personal técnico interno (Producción - Infraestructura).
  - ✓ Proveedores encargados de la Administración y Soporte de la infraestructura y servicios.
  - ✓ Chequeo de lista para Pruebas actualizado para cada componente tecnológico incluido.
  - ✓ Capacitación para el personal que participará en la "Prueba General Anual"
  - ✓ Fecha propuesta para ejecutar la "Prueba General Anual".

- Notificar al responsable de la Continuidad del Negocio – Jefe de Riesgos Integrales y Cumplimiento, la documentación de la "Prueba General Anual", para la aprobación en el Comité de Continuidad del Negocio:

  - ✓ Fecha propuesta para la ejecución
  - ✓ Planificación de la "Prueba General del Anual"
  - ✓ "Chequeo de Lista" de Prueba para cada componente tecnológico incluido
  - ✓ Capacitación del personal

- Recibir del responsable de la Continuidad del Negocio – Jefe de Riesgos Integrales y Cumplimiento la notificación de aprobación de la fecha propuesta y la documentación soporte para la ejecución de la "Prueba General Anual".

- Remitir comunicados a Entidades de Control, Entidades Emisoras y Clientes mediante los canales de comunicación autorizados notificando la ejecución de la “Prueba General Anual”.

- Mantener sesiones de trabajo y coordinación con las Entidades Emisoras y Proveedores, su participación y disponibilidad durante toda la ejecución de la “Prueba General Anual”, para asegurar:
  - ✓ Ejecución oportuna de las actividades contingentes y verificación de recuperación de servicios.
  - ✓ Atención inmediata en el caso de presentarse novedades.

- Verificar la asistencia del personal técnico interno y proveedores, y el cumplimiento de pre – requisitos establecidos para el desarrollo de la “Prueba General Anual” en la fecha y hora aprobada.

4.6. Alcance de la planificación

El alcance de la planificación de la “Prueba General Anual”, abarca el valioso detalle que protege la continuidad del negocio al considerar la recuperación de sistemas críticos. Cuáles son los principales componentes que engloban esta planificación expuesta a continuación:

- Identificación de Activos Críticos: Identificar qué partes de los sistemas, aplicaciones y datos son parte sustancial del negocio.
- Análisis de Riesgos: Examinar las amenazas que a la infraestructura pueden ser un riesgo, ya sean naturales, tecnológicas o humanas.
- Estrategias de Recuperación: Idear formas de recuperación de sistemas y datos que utilizan copias de seguridad, redundancia, soluciones en la nube, entre otras.
- Definición de Tiempos de Recuperación: Determinación del RTO y el RPO que establecen el límite de tiempo máximo permitido de inactividad y el mínimo de datos que se acepta perder.

- Procedimientos de Comunicación: Estratégicamente prepararse sobre cómo se comunicarán las actualizaciones a los empleados, clientes y otras partes interesadas cuando ocurra un evento y cuando ya haya pasado.
- Roles y Responsabilidades: Designar tareas específicas a todos los miembros del equipo para asegurar una respuesta efectiva y organizada ante un desastre.
- Pruebas y Simulaciones: Sometiendo el plan a ejercicios repetidos para comprobar su funcionamiento y haciendo modificaciones a los procedimientos cuando sea necesario.
- Documentación: Mantener registros de cada control de cambios y actualizados del plan, que integren todos los procedimientos, contactos y recursos necesarios.
- Capacitación: Proveer capacitación continua a los empleados que intervengan en la planificación y su papel en la recuperación.
- Revisión y Mejora Continua: Establecer un proceso para revisar y actualizar el DRP regularmente, asegurando que se mantenga alineado con las necesidades del negocio y las amenazas emergentes.

La planificación es crucial para minimizar el tiempo de inactividad y las pérdidas financieras, asegurando que la organización pueda recuperarse de manera eficiente tras un desastre.

Conclusiones

Dentro del desarrollo del proyecto presentado, se detallan las siguientes conclusiones:

- Se explico detalladamente el planteamiento del problema, objetivo general específico, justificación del problema y su respectiva hipótesis.

- Se realizo el estudio de forma exhaustiva de los diferentes Centro de Datos Actuales para su respectiva aplicación en la empresa NetPay S.A., comprendiendo de manera integral todo lo referente al diseño de plan de recuperación de servicios ante desastres.

- Se propuso un diseño de alto nivel enfocado en los componentes actuales de toda la infraestructura IT contemplando un Centro de Datos de Servicios de Proveedores para el Sitio de Contingencia con un proveedor de servicios para los servicios de transaccionalidad y Centro de Datos en la nube para servicios importantes.

- Se detalla toda la planificación para la aplicación de "Prueba General Anual", sus criterios de cumplimiento con las entidades correspondientes, plan de acción ante la prueba y el alcance de la planificación de las pruebas.

Por lo antes expuesto, se concluye que se cumple con el objetivo general del proyecto, puesto que se presentó el diseño para restauración de servicios ante alguna interrupción de servicios contemplando un Centro de Datos para Sitio de Contingencia y Centro de Datos en la nube.

Recomendaciones

Conforme al desarrollo del presente trabajo se detallas las siguientes recomendaciones:

- Realizar las pruebas generales de continuidad de negocio anualmente para el cumplimiento de normas y validación de servicio óptimo en el Centro de Datos del Sitio de Contingencia.

- Migrar todos los servicios que sean factibles al Centro de Datos en la nube dado que es tendencia tecnológica y por todos los beneficios que brinda los servicios en la nube.

- Monitorear constantemente los Centros de Datos de Sitio Principal y de Contingencia a nivel de software y hardware para evitar cualquier situación de inactividad no programada.

- Renovar tecnológicamente el equipamiento de todos los componentes de Sitio de Principal y Sitio de Contingencia para alineamiento de cumplimiento de seguridad y funcionalidad.

- Auditar frecuentemente la arquitectura implementada para mantener una mejora continua en los Centros de Datos.

Glosario de Términos

Centro de Datos: Es un lugar donde se aloja toda la infraestructura de una organización como, por ejemplo: equipamiento red, comunicación externa, almacenamiento servidores necesaria para procesar, organizar, asegurar y conservar la información.

Uptime Institute: es una institución que regulariza estándares y certificaciones para el diseño, construcción, y operación de Centros de Datos.

TI: es término para hacer referencia a Tecnología de la Información.

BCP (siglas del inglés *business continuity plan*), es la planificación de la contingencia para los sistemas de información que son elementos de un sistema de control interno, que se establece para gestionar la disponibilidad de los procesos críticos en el caso de una interrupción.

RPO: El objetivo de punto de recuperación.

RTO: El tiempo objetivo de recuperación

MTD: El tiempo de inactividad máximo tolerable

Bugs: hace referencia a errores de software de sistema operativo.

Ataques DDoS: Ataque de Denegación de Servicio Distribuida

Malware o ransomware: El malware o ransomware puede comprometer los archivos del sistema esto provoca sean inaccesibles.

TIER: La certificación para clasificar a los Centros de Datos según el cumplimiento de estándares de redundancia y disponibilidad de los componentes.

IaaS: El contrato de Infraestructura como Servicio.

PaaS: En un contrato de Plataforma como Servicio.

SaaS: El contrato de Software como Servicio.

DRaaS: El contrato de Recuperación ante Desastres como Servicio.

Virtualización: Emulación de recursos tecnológicos en un sistema informático.

Virtualización de servidores: Tecnología basada en un software que posibilita la ejecución de varios sistemas operativos diferentes entre sí, como invitados dentro de un único host del servidor físico.

AWS: Amazon Web Services

VPC: (Virtual Private Cloud)

Private Subnet es componente de AWS que permiten dividir la VPC en subredes más pequeños para organizar las instancias y otros recursos de manera eficiente.

Gateway de Internet (Puerta de Enlace de Internet), es un componente de AWS.

Gateway NAT (Network Address Translation) componente de AWS que permite que las instancias en subredes privadas se comuniquen hacia con Internet.

VPN (Virtual Private Network) componente de AWS que permite conectar tu red local a la nube a través de una VPN.

Conexión Directa (AWS Direct Connect) componente de AWS que proporciona un enlace dedicado a tu Centro de Datos en premisa.

Elastic Load Balancer (ELB) componente de AWS que distribuye automáticamente el tráfico de red entrante.

AWS Transit Gateway componente de AWS que permite interconectar múltiples VPCs y redes en premisa.

Big Data y Análisis de Datos: proporcionan plataformas potentes para el procesamiento de grandes volúmenes de datos generados por empresas.

Internet de las Cosas (IoT): se beneficia enormemente de los centros de datos en la nube debido a la capacidad de gestionar y almacenar grandes volúmenes de datos provenientes de dispositivos conectados.

BIBLIOGRAFÍA

Aguaded, J., & Tirado, M. (2018). Ordenadores en los pupitres: informática y telemática en el proceso de enseñanza-aprendizaje en los centros TIC de Andalucía. Pixel-Bit. *Revista de Medios y Educación*.

Amazon Web Services. (s.f.). *Computación en la nube.*

Arango, L. (2016). Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa cibersecurity de Colombia Ltda.

Arias, C., & Portela, J. (2018). Centro de soluciones para el futuro informático en el municipio de Flandes Tolima "CESOFI" (Doctoral dissertation, Corporación Universitaria Minuto de Dios). *Dialnet*, 12.

Bobadilla, G. (2016). Propuesta para la implementación de una red de datos con cableado estructurado y del centro de datos de la empresa MKG informática EIRL–Lima; 2018.

BSCCONSULTORES. (2010).

Calo, P., & Ortiz, O. (2018). Sistema de gestión de ventas para el centro de servicios informáticos la biblioteca. *Dialnet*.

Costas, J. (2017). Seguridad informática. . *Madrid: RA-MA, SA.*

DeltaProtect. (s.f.).

Díaz, O. &. (2017). Implementación de un enfoque DevSecOps+ Risk Management en un Centro de Datos de una organización Mexicana. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (26), 43-53.*

Díaz, O., & Muñoz, M. (2017). Implementación de un enfoque DevSecOps+ Risk Management en un Centro de Datos de una organización Mexicana. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (26), 43-53.*

Echenique, M. (2016). Auditoría en informática. *Compañía Editorial Continental.*

Gartner. (2017). Software-Defined Data Center. *Rackspace*.

Hoofnagle, C. J. (s.f.). *Privacy and Cloud Computing.*

Implementation, C. C. (s.f.). *Srinivasan S.*

Lacambra, C., Lozano, C., Alonso, D., & Fontalvo, M. (2003). *Amenanazas Naturales y Antrópicas en las zonas costeras colombianas.* . Medellin : INVEMAR .

Mayo, E. M. (2020). Diseño del plan de recuperación de desastres informáticos para el centro de datos de la gobernación del departamento del chocó (Master's thesis, Escuela de Ingenierías).

McGrath, M. K. (s.f.). *Cloud Computing: Business and Technology.*

Nick Antonopoulos, L. G. (s.f.). *Cloud Computing: Principles, Systems and Applications.*

Patiño, S. M. (2016). Evaluación de seguridad informática basada en ICREA e ISO27001. Universidad Ciencia y Tecnología, 21(85).

Patiño, S. M. (2018). Evaluación de seguridad informática basada en ICREA e ISO27001. . *Universidad Ciencia y Tecnología, 21(85).*

Piattini, M. &. (2016). Auditoria informática. . *Un enfoque práctico, 6, 1-2.*

Proofpoint. (2024). *DRP o plan de recuperación ante desastres.*

Ramos, M., & Hurtado, A. (2017). Seguridad informática. *Editorial Paraninfo.*

Reyes, A., Montilla, A., Castillo, P., & Zambrano, M. (2017). *Amenaza, vulnerabilidad y riesgo ante eventos naturales. Factores socialmente construidos.* (No. 6 ed., Vol. 2). Journal of Science and Research.

Rivas, G. A. (2018). Auditoría informática. *Ediciones Díaz de Santos.*

Rodríguez, F. (2018). Las actitudes del profesorado hacia la informática. Pixel-Bit. . *Revista de Medios y Educación, 15, 91-103.*

Santana Espinosa, M. C. (2018). Sistema informático para la gestión de datos del docente. . *Educación Médica Superior, 31(1), 89-98.*

Stroud, J. H. (s.f.). *Cloud Economics: The Science of Cloud Business.*

Téllez Valdés, J. (2017). Derecho informático. McGraw Hill Educación.

Terán, D. (2017). Administración Estratégica de la función informática. . *Alfaomega Grupo Editor.*

Thomas Erl, Z. M. (s.f.). *Cloud Computing: Tecnology & Architecture.*

Tim Mather, S. K. (s.f.). *Cloud Security and Privacy.*

Vasilenko. (s.f.). *Regulating the Cloud: Policy for Computing Infrastructure.*

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Vásquez Díaz, Ronald Richard**, con C.C: # **0920835667** autor del trabajo de titulación: **Diseño de un plan de recuperación ante desastres (DRP), del centro de datos para continuidad de servicios de la empresa NetPay,** previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 13 de marzo de 2025

f. _____

Nombre: **Vásquez Díaz, Ronald Richard**

C.C: **0920835667**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	Diseño de un plan de recuperación ante desastres (DRP), del centro de datos para continuidad de servicios de la empresa NetPay.		
AUTOR(ES)	Vásquez Díaz, Ronald Richard		
REVISOR(ES)/TUTOR(ES)	Zamora Cedeño, Néstor Armando Zamora Cedeño, Néstor Armando Bohórquez Escobar, Celso Bayardo		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	13 de marzo de 2025	**No. DE PÁGINAS:**	**65 p.**
ÁREAS TEMÁTICAS:	Sistemas Telecomunicaciones, Redes De Comunicaciones, Tecnología E Infraestructura.		
PALABRAS CLAVES/ KEYWORDS:	Centro De Datos, Plan De Recuperación, Conmutación, Nube, Respaldos, Continuidad, Hospedaje Y Administración, Restauración, Core Transaccional.		

RESUMEN/ABSTRACT: El presente proyecto consiste en el diseño de un plan de recuperación de servicios ante algún desastre para el Centro de Datos del Sitio Principal de la empresa y brindar una solución de darle continuidad de servicios indispensables para que la organización siga operativa antes alguna incidencia que provoque una interrupción de servicios.

Los Centros de Datos en la nube que hoy en día ofrecen múltiples funcionalidades siendo estas consideradas como una estrategia de respaldo y restauración de servicios manteniendo al mismo tiempo almacenado copias de los últimos registros o modificaciones efectuadas en los servicios del cliente, esto proporciona contingencia de manera que la restauración de servicios se realice mediante la conmutación de todo el tráfico inmediatamente a la nube en el caso de alguna incidencia en el centro de datos de la empresa.

En este caso en la empresa NetPay S.A. cuenta con servicios críticos que deben estar siempre habilitados para permitir la continuidad del negocio, para llevar a cabo este plan de recuperación de desastres como complementario a la nube, también existen servicios que todavía no son totalmente factibles en la nube por ende se contempla un tipo de hospedaje y administración de infraestructura con tecnología de punta con un proveedor de servicios para restaurar estos servicios como por ejemplo el core transaccionalidad y ciertos servicios de telefonía, para llevar a cabo se debe analizar a granularidad la situación actual y todos los requerimientos mínimos para que la restauración de servicios en la nube y los hosteados se lleva a cabo de manera efectiva y en el menor tiempo posible la restauración de los servicios.

Para ello se requiere levantar un diseño lógico para que todos los servicios críticos sean considerados en el plan de recuperación de desastres cuando ocurra algún incidente que impida que el centro de datos levante dichos servicios críticos de la empresa y luego del análisis proponer una mejora con el plan de recuperación de desastres que tenga el menor impacto posible en el centro de datos actual.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-993555418	E-mail: **ronald.vasquez@cu.ucsg.edu.ec**
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: MSc. Celso Bayardo Bohórquez Escobar**	
	Teléfono: +593-995147293	
	E-mail: celso.bohorquez@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	