UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingeniera de Sistemas

TEMA:

DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO BASADO EN COBIT, ITIL Y DE ACUERDO A LA NORMA ISO 22301, PARA EL CENTRO DE PROCESAMIENTO DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO, CAMPUS SUR

AUTORA:

THALIA MICHELLE ATI GUILLEN

TUTOR:

JORGE ENRIQUE LÓPEZ LOGACHO

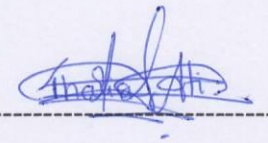
Quito, agosto del 2018

CESIÓN DE DERECHOS DE AUTOR

Yo, Thalia Michelle Ati Guillen, con documento de identificación N° 1725103285, manifestó mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del trabajo de titulación con el tema "DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO BASADO EN COBIT, ITIL Y DE ACUERDO A LA NORMA ISO 22301, PARA EL CENTRO DE PROCESAMIENTO DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO, CAMPUS SUR", mismo que ha sido desarrollado para optar por el título de INGENIERA DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autora me reservo los derechos morales de la obra antes citada.

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



THALIA MICHELLE

ATI GUILLEN

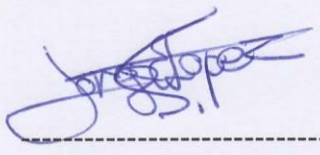
C.I.: 1725103285

Quito, agosto del 2018

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema: "DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO BASADO EN COBIT, ITIL Y DE ACUERDO A LA NORMA ISO 22301, PARA EL CENTRO DE PROCESAMIENTO DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO, CAMPUS SUR", realizado por Thalia Michelle Ati Guillen, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, agosto del 2018



JORGE ENRIQUE LÓPEZ LOGACHO

CI: 1712082484

DEDICATORIA

Dedico el trabajo a mis padres a Edison y Marcia quienes que con su amor y dedicación implantaron en mí, los valores que hoy me hacen ser quien soy, a mis abuelos quienes siempre me han brindado apoyo incondicional, y a mis hermanos que me han visto, acompañado en todas las etapas de mi vida.

Thalia Michelle Ati Guillen

AGRADECIMIENTO

Agradezco a la Universidad Politécnica Salesiana que contribuyo en mi formación profesional y a mi tutor el Ingeniero Jorge López que bajo su tutela se culminó con éxito el desarrollo de este proyecto

Thalia Michelle Ati Guillen

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

En el presente documento, se encuentra detallado el proceso de desarrollo del plan de recuperación de desastres y continuidad de negocio, siendo estos de vital importancia para el centro de procesamiento de datos, debido que mediante el despliegue del mismo de modo que se minimiza los efectos de eventos que atenten a las operaciones, por este motivo, se ha desarrollado los planes de acuerdo con los marcos de referencia COBIT e ITIL, en conjunto con las norma ISO-22301; para ello, se han identificado los riegos, vulnerabilidades y amenazas a los que se encuentra sujeto un centro de procesamiento de datos, con el fin de realizar la evaluación de los riegos, siendo así que se determine las acciones a ser realizadas para contrarrestar los efectos adversos dando como resultado un procedimiento claro en el cuál se identifique el orden de los procesos a ser ejecutados y las acciones que cada miembro del escenario cumpla para el correcto despliegue de los planes antes mencionados.

Abstract

In this document, the development process of the disaster recovery and business continuity plan is detailed, being these vitally important for the data processing center, due to the fact that it is deployed in a way that minimizes the effects of events that threaten operations, for this reason, plans have been developed in accordance with the COBIT and ITIL reference frameworks, in conjunction with ISO-22301; for this, the risks, vulnerabilities and threats to which a data processing center is subject have been identified, in order to carry out the evaluation of the risks, so that the actions to be taken to counteract the effects are determined adverse events resulting in a clear procedure in which the order of the processes to be executed and the actions that each member of the scenario meets for the correct deployment of the aforementioned plans are identified.

INTRODUCCIÓN

En la actualidad las tecnologías que son implementadas dentro de un CPD se ajustan al modelo de negocio de las organizaciones, de esta manera se gestiona información y recursos orientados al servicio del usuario, asegurando la disponibilidad del recurso. Al momento de ofertar los servicios que se prestan se debe considerar que están sujetos a riesgos, vulnerabilidades y amenazas mismas que pueden ser conocidas como desconocidas, las cuales atentan con el desarrollo normal del centro de procesamiento de datos.

Las tecnologías de información usadas están diseñadas con sistemas tolerantes a fallos, puesto que los equipos de hardware y software tienen funcionalidades de auto gestión, siendo así que ante la presencia de una incidencia se pueda mantener las operaciones, no sin antes enviar el respectivo trap por medio de SNMP, sin embargo existen riesgos y amenazas que tienden a convertirse en desastres, causados por errores humanos, informáticos o de carácter natural, razón por la cual se hace necesario contar con planes de continuidad de negocio y recuperación de desastres.

Dichos planes permiten la identificación, mitigación, reducción del tiempo de interrupción que puede causar algún desastre, estos contienen la información necesaria de los procesos y procedimientos a seguir para reestablecer las operaciones críticas dentro del CPD. En este caso de estudio, este escenario se encuentra operando desde hace muy poco tiempo por lo tanto se evidencia que la gestión de procesos y procedimientos aún no ha sido desarrollada y menos aún implementada en el escenario real, adicionalmente que aún no se encuentran definidos en su totalidad, por dichos motivos se evidencia que no se cuenta con planes de continuidad de negocio y recuperación de desastres.

Siendo así que en el primer capítulo se encuentra la descripción del estado actual en el que se encuentra el Centro de Procesamiento de datos, además de las bases teóricas y legales para el desarrollo del plan de recuperación de desastres y continuidad del negocio. En el capítulo 2 se encuentra detallado el plan de continuidad de negocio y los elementos que lo conforman. Por otra parte, en el capítulo 3 se encuentra detallado el desarrollo del plan de recuperación de desastres, en el cual se incluye el análisis de riesgos, impacto definición de roles y responsabilidades de los miembros del entorno analizado.

Planteamiento del problema

La carrera de Ingeniería en Ciencias de la Computación, de la Universidad Politécnica Salesiana, sede Quito, Campus Sur, actualmente cuenta con un Centro de Procesamiento de Datos (CPD) recién implementado, el cual cuenta con una infraestructura compuesta de: servidores de alto rendimiento, almacén de datos, dispositivos de comunicación de datos, equipos de control ambiental y energización; razón por la cual el Centro de Datos requiere del desarrollo de un plan de continuidad de negocio y de recuperación de desastres, puesto que en éste se alberga información y adicionalmente se oferta servicios para tres grandes campos académicos e investigativos tales como: material académico de las cátedras dictadas, tesis de grado y post-grado, investigaciones de proyectos doctorales e investigaciones de proyectos interdisciplinarios.

Por las razones antes mencionadas, el Centro de Procesamiento de Datos aún no cuenta con procesos y procedimientos claramente definidos, no existe los siguientes planes de seguridad, contingencia, recuperación de desastres y continuidad de negocio, esto pone en evidencia que este escenario se encuentra expuesto ante una diversidad de amenazas y vulnerabilidades, mismas que pueden ser tanto conocidas como

desconocidas, siendo así que es un escenario susceptible a la interrupción de servicios o perdida de información, es por eso que se requiere diseñar un plan para la recuperación de desastres y la continuidad del negocio, los cuales se diseñan desde cero en base a políticas y buenas prácticas, para que de esta manera mitigar el impacto recibido frente a una incidencia afecte a las operaciones.

Justificación

Con el desarrollo de este proyecto se identifican los activos críticos, además se presenta los procesos y procedimientos a realizarse ante cualquier eventualidad anormal o sorpresiva que atente a la ininterrupción de los servicios prestados o perdida de información almacenada dentro del CPD, además que así se asegura que el impacto a los usuarios de aquellos servicios e información albergados en este escenario sea mínimo, de tal modo que estos no se van mayormente afectados bajo circunstancias de emergencia.

Con el fin de minimizar las interrupciones y pérdidas tanto de servicios como información, se diseña el plan de recuperación ante desastres y la continuidad del negocio, mediante el cual permite la detección de los activos físicos y lógicos que son críticos, para de esta manera enfrentar posibles desastres que imposibilitan, afectan o atentan a la integridad de las funciones normales del Centro de Procesamiento de Datos, para que este sea capaz de mantener o reanudar rápidamente sus funciones, además de incluir la prevención ante ciertos eventos que afecten al servicio normal prestado.

Mismo que se base en los marcos de referencia COBIT, ITIL y la norma ISO 22301, los mismos que permiten medir el desempeño de las Tecnologías de Información dentro del escenario presentado, permitiendo así la integración de buenas prácticas de

gestión, procesos y procedimientos relacionados con las actividades que se encuentran desarrollándose dentro del CPD.

Objetivos

Objetivo general

Diseñar un plan de recuperación de desastres y continuidad del negocio basado en COBIT, ITIL y de acuerdo a la norma ISO 22301, para el Centro de Procesamiento de Datos de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Salesiana, Sede Quito, Campus Sur.

Objetivo específicos

Identificar los riesgos y vulnerabilidades del Centro de Procesamiento de Datos para la aplicación de acciones para la mitigación de los mismos.

Desarrollar el plan de continuidad de negocio y de recuperación de desastres para mitigar el impacto recibido sobre el Centro de Procesamiento de Datos ante la posibilidad un evento de desastre de modo que las actividades no se vean mayormente afectadas.

Generar la documentación de los procesos y procedimientos a realizarse durante y después de un evento de desastre.

Marco metodológico

Para el desarrollo del plan de continuidad y recuperación de desastres se lo realiza en base a los marcos de referencia COBIT, ITIL y la norma ISO 22301, los cuales disponen de sus propias metodologías, procesos, procedimientos y mejores prácticas a ser implementadas.

El proyecto se inicia con una reunión con el administrador del Centro de Procesamiento de Datos, el cual proveerá la información necesaria para realizar el

análisis estado inicial, donde se contempla la infraestructura de TI a nivel físico y lógico, para de esta manera establecer el objetivo de continuidad del proyecto.

Una vez que se ha realizado el análisis del CPD con la identificación de los activos críticos para la detección de los potenciales riesgos y vulnerabilidades que existan, se procede con la realización de la clasificación, para que de esta manera se viabilice la definición de las estrategias de mitigación,

Para el desarrollo de este proyecto se genera se analizan escenarios en los cuales se vea comprometida la infraestructura, servicios y operaciones del CPD, las cuales se toman en base a la detección de las amenazas que se encuentra sujeto el escenario.

Posteriormente a partir de los resultados obtenidos se procede al desarrollo del plan de continuidad de negocio y recuperación de desastres, en el cual se encuentra de manera detallada las acciones a tomar para la prevención y mitigación, además de los procesos y procedimientos a ser cumplidos en un evento de desastre.

CAPÍTULO 1

1 Fundamentos

1.1. Fundamento teórico

1.1.1 Plan de continuidad de negocio (BCP)

Es una colección de procedimientos alternativos a lo normalmente realizado en un centro de datos, dentro de este se encuentra contemplado las estrategias y tácticas a ser realizas ante eventos que atenten con las operaciones que normales del mismo, teniendo como objetivo mitigar el impacto y la interrupción generada de manera improvista.(«4 pasos para armar un Plan de Continuidad del Negocio», 2014)

Dicho de otra manera, el BCP es un plan donde se contemplan los procedimientos a seguir, además que se encuentra identificadas las medidas técnicas, logísticas y organizativas para ser realizadas antes, durante y después de un evento de desastre, para que de esta manera los servicios críticos identificados de antemano sean reestablecidos, con el fin de continuar brindando servicios a sus usuarios.(Ibarra, s. f.)

1.1.2 Plan de contingencia

Es un caso particular del plan de continuidad del negocio. En este se dispone las actividades a seguir para prevenir una eventualidad puede presentarse en cualquier momento atentando con la continuidad de las operaciones de la entidad.(«Plan de contingencia en seguridad Informática - EcuRed», s. f.)

Este plan muchas veces se suele confundir con el plan de recuperación de desastres o con el de continuidad del negocio, pero se perecen solo en que estos tres tienen como objetivo el mantener las operaciones del centro de datos ante la presencia de un evento que atente con a los servicios normales, la diferencia entre estos es que el plan de continuidad de negocios es lo que se puede hacer para mantener o reestablecer el

estado normal de las actividades, aquí se encuentra contemplado el plan de contingencia y el de recuperación de desastres.

Este a diferencia del plan de recuperación de desastres, contiene los procesos y actividades de prevención para que el centro de datos no se vea afectado ante la presencia de un desastre, mientras que el plan de recuperación de desastres se contempla los procesos y actividades a ser realizadas después de un evento que interrumpió las operaciones, para regresarlo al estado antes de verse afectado.

1.1.3 Plan de recuperación de desastres (DRP)

Es el que contiene los procedimientos a ser desplegados por una institución después de un evento de desastre que imposibilite las funciones normales, con el objetivo de recuperar las actividades críticas del centro de datos de esta manera se minimice al máximo el tiempo que se presente la interrupción de las operaciones.(«¿Qué es ¿Qué es Plan de Recuperación de Desastres (DRP)?», s. f.)

En este se contemplan las precauciones y acciones que se deben tomar para mantener o reanudar las operaciones del centro de datos, durante una eventualidad que atente con la continuidad del negocio, además que dentro de este se contempla el análisis de los riesgos y amenazas tanto a nivel de hardware, como software al que se encuentra expuesto el centro de datos.(«¿En qué consiste un Plan de Recuperación ante Desastres (DRP)?», 2014a)

Es así que consta de los manuales de reconfiguraciones, reinicios y recuperación de todos los elementos que se encuentran dentro de la infraestructura definidos como críticos, tanto de equipos de comunicación y sistemas de servicios.

1.1.4 Desastre

Es un hecho que se lo denomina catastrófico el cual no es predecible, es decir que no se tiene el completo conocimiento de cuál será la magnitud y área en la que se presenten daños que afecten de manera grave a la sociedad, tampoco se tiene conocimiento en qué momento determinado se presentará un evento que trastorne agresivamente la continuidad de las actividades productivas.(«Concepto de desastre - Definición en DeConceptos.com», s. f.)

Al hablar de desastre se contemplan dos áreas que afectan directamente a un centro de datos, una de ellas son los desastres informáticos los cuales se pueden presentar a partir de ataques de niveles físicos y lógicos, es decir ataques al hardware y software, errores humanos, etc. Otra área abarca los desastres naturales, los mismos que no se puede predecir cuándo, cómo o cuál es su nivel de impacto en la sociedad.

1.1.5 Análisis de impacto en el Negocio (BIA)

Se encuentra directamente contemplado dentro del plan de recuperación de desastre y continuidad del negocio, ya que es una fase primordial en la cual se cuantifica el impacto generado por la pérdida o interrupción de las operaciones criticas del CPD. Es decir que el objetivo es conocer cuál es la afección a presentarse en el tiempo en que las actividades se encuentren paralizadas, además se toma en cuenta el tiempo que tarda el restablecimiento de los servicios que se vieron afectados, para que de este modo se tenga de forma clara el nivel de impacto provocado a la entidad. («Business Impact Analysis (BIA) y la importancia de priorizar procesos», 2014)

1.1.6 Activo

Es un componente definido como critico dentro de la infraestructura de un CPD, este puede ser a nivel de hardware o software. Se dice activo aquel que es indispensable

para el desarrollo de las actividades del negocio, cumpliendo un papel importante para la organización, además se ve en la necesidad de protegerlo ante la presencia de diversas situaciones que pongan en riesgo las actividades normales que se encuentre cumpliendo. («Activo (seguridad informática) - Copro, la enciclopedia libre», s. f.)

1.1.7 Vulnerabilidad

Una vulnerabilidad es una brecha de seguridad que se puede presentar por un fallo o generado a partir de una debilidad que pudiese existir dentro del CPD, estos atentan a la continuidad del negocio de modo que se pone en riesgo la integridad, seguridad y disponibilidad de la información albergada, de tal forma que se vean interrumpidas las operaciones y servicios normales.(«Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? - Aprende a Programar - Codejobs», s. f.)

1.1.8 Amenaza

Al definir que es una amenaza se encuentra con que aquel factor o evento que sea capaz de atentar contra las operaciones del CPD, mismas que pueden presentarse a nivel de software y hardware, además de que estas se encuentran vinculadas directamente con las vulnerabilidades *"*una amenaza sólo existe si existe una vulnerabilidad*"*(«Amenazas a la Seguridad de la Información | Departamento de Seguridad Informática», s. f.).

1.1.9 Riesgo

Es la probabilidad de que un evento afecte a las operaciones normales de la infraestructura de un CPD, causando la pérdida o interrupción de los servicios que se encuentran prestando; es posible tener el conocimiento del motivo que puede causar una discontinuidad de las operaciones, pero se desconoce cuándo esté se

presente.(«Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? - Aprende a Programar - Codejobs», s. f.)

1.2. Fundamento legal

1.2.1. Norma ISO 22301

Esta norma contiene las especificaciones de los lineamientos orientados al desarrollo de un plan de continuidad del negocio, esta se encuentra basada en la norma británica BS25999, teniendo como objetivo dar las referencias para la gestión del negocio ante la posibilidad de la presencia de un desastre informático o natural. Además, esta facilita la identificación de las amenazas y las funciones críticas de la organización, para que en caso de la acción de una amenaza la entidad tenga la capacidad de mantener o minimizar el tiempo que las funciones se vean afectadas.

Se toma en cuenta el modelo PDCA(Planificación-Implementación-Verificación-Mantenimiento), que incluye el alcance, las referencias, definiciones, el escenario, la gobernanza, el alcance y el sistema de gestión de la continuidad; descritos a lo largo del documento. («¿Qué es norma ISO 22301?», s. f.)

1.2.2. COBIT

Ofrece un marco de referencia el cual asegura una adecuada administración de la continuidad del negocio, en este se establecen las acciones a seguir, así como los roles y responsabilidades de los miembros que se encuentran encargados del CPD.

A esto también se añade las políticas y lineamientos a ser realizadas como parte de la prevención de desastres quedando de manera que se asegura, que la organización cuenta con los planes y el entrenamiento necesario para enfrentar y recuperarse ante acción de una eventualidad de desastre.

Otro de los puntos que se dimensiona dentro de COBIT que se encuentran orientados al plan de continuidad del negocio, es el análisis de riesgos y del enfoque metodológico a ser usado para cumplir con el objetivo de continuidad, para ello se usaran 4 de los 34 dominios que maneja, de modo que se usaran los siguientes: planear y organizar, adquirir e implementar; entregar y dar soporte; monitorear y evaluar.(ORTEGÓN & SÁNCHEZ, 2015)

Finalmente, mediante el uso de este marco se logra que el CPD que el plan de continuidad de negocio y recuperación de desastre se encuentren en un lenguaje que sea entendido por todos actores que se encuentran involucrados, definiendo las acciones y responsabilidades que se deben llevar acabo ante un evento que atente a las operaciones normales.

1.2.3. ITIL

Es marco de referencia en el cual se encuentran detalladas las maneras de controlar los riesgos que atenten con la continuidad, además da los lineamientos para la planificación de la recuperación de los servicios, de tal manera que se mitigue o reduzca al mínimo el tiempo que un servicio se ve interrumpido, para que de esta manera el impacto de la interrupción del servicio sea aceptable.

Dentro de la gestión de la Continuidad de los Servicios se debe llevar acabo las siguientes actividades:

- Establecer las políticas y alcance de la continuidad de los servicios
- Evaluar el impacto, es ente caso las consecuencias que traigan consigo la interrupción del servicio.
- Analizar y prever los riesgos, realizar un estudio de los posibles riesgos a los que se encuentran expuestos los servicios.

- Establecer las estrategias de continuidad.
- Adoptar medidas de modo preventivo ante riesgos, como el desarrollo de planes de contingencia.
- Poner a prueba los planes.
- Capacitar personal para el despliegue de los planes cuando sea necesario.
- Revisar periódicamente los planes, esto permite la adaptación y mejoras continuas de las estrategias para contrarrestar una interrupción de los servicios.(«Gestión de la Continuidad de servicios TI > Proceso [Curso ITIL® Foundation > Diseño de los Servicios TI]», s. f.)

Mediante el uso de ITIL el CPD mejora la implementación de todos aquellos procesos inherentes al desarrollo del ciclo del proyecto, al establecer procesos orientados a las mejores prácticas. Adicionalmente facilita los procesos de gestión de riegos, mediante la identificación puntual de las vulnerabilidades y amenazas a los que está sujeto el escenario analizado.

1.2.4. NTE INEN-ISO/IEC 27031

El Instituto Ecuatoriano de Normalización establece la normativa dentro del territorio nacional, mismo que es un conjunto de criterios orientados a la administración de un desastre y manejo de la continuidad del negocio para las entidades gubernamentales, organizaciones sin fines de lucro y entes privados, brindando una base de información con las referencias de los campos y documentos que se debe tomar en cuenta durante el desarrollo de los planes de continuidad y recuperación de desastres que se debe implementar de manera normada dentro de la organización.

Dentro de esta se establece de forma necesaria los siguientes apartados para el desarrollo y recolección de la información orientados hacia los planes de continuidad de negocio y recuperación de desastres:

- Alcance del programa, metas, objetivos y método de evaluación del mismo.
- Administración y finanzas, de modo que la entidad pueda sostener las actividades durante una eventualidad de desastre.
- Se debe desarrollar las políticas para manejo de los log, de manera que se mantengan clasificados, confidenciales, manteniendo la integridad de esa información junto con una adecuada gestión del almacenamiento de los datos obtenidos.
- Se debe manejar el proceso de planeación, evaluación de riesgo, los peligros a ser evaluados (desastres naturales, antropogénicos y desastres informáticos), realizar un análisis de impacto (continuidad de las operaciones, infraestructura crítica, condición económica y financiera) de acuerdo a los procesos y aplicaciones identificadas como críticas.
- Prevención, con los riesgos definidos se debe incluir las estrategias de prevención, las que deben ser actualizadas constantemente.
- Estrategia de mitigación, debe estar basada en los resultados de la identificación de riesgos a corto y largo plazo.
- Realizar pruebas, las mismas que deben tener una metodología estandarizada que facilite la evaluación del diseño de los planes.
- Mejora continua de los planes, para ello se realiza revisiones programadas periódicamente, facilitando la re-evaluación cuando sea necesario.
- Realizar acciones correctivas a través de procesos definidos sobre las deficiencias identificadas.(«nte_iso_iec_27031.pdf», s. f.)

CAPÍTULO 2

2. PLAN DE CONTINUIDAD DE NEGOCIO

2.1. Plan de continuidad de negocio

El plan de continuidad de negocios se encuentra enfocado en mantener o reanudar las operaciones frente a la presencia de eventualidades que atenten a los servicios prestados por el CPD, mitigando el impacto en desarrollo de las actividades y minimizando los tiempos de respuesta ante el evento, siendo así que se tenga la capacidad de una puesta en marcha de las actividades vitales, de modo que se encuentre de la mano con los objetivos de la Carrera, es así que se dimensiona tres parámetros fundamentales que son: los datos que se almacena y se manejan, la nueva infraestructura tecnológica que ahí se encuentra implementada, y el recurso humano responsable de la gestión.

El plan de continuidad de negocio se lo realiza a partir de 5 etapas identificadas mismas que facilitan su definición:

- Definición de los elementos, se realiza el inventario de los elementos que forman parte de la infraestructura del CPD, mismos que requieren ser protegidos ante cualquier evento que genere afectación a su estado normal.
- Establecer los niveles de protección, en este punto se realiza un análisis que permita la identificación de cuáles son los requisitos y elementos mínimos para mantener las operaciones, es decir que se determina los activos críticos que deben tomarse en cuenta ante la presencia de una eventualidad que atente a la continuidad del negocio, mismos que deben ser protegidos permitiendo mantener las actividades desarrolladas dentro del CPD.

- Definición de requisitos de protección, en este punto se realiza un análisis de que estrategias y los roles de todos los miembros parte del CPD, para definir los procesos, procedimientos y actividades que se llevaran a cabo ante la presencia de un evento que atente a las operaciones normales que se realizan dentro de este escenario.
- Identificación de eventos de desastre, una vez que se han identificado los activos críticos y definido las estrategias a ser realizadas, el siguiente paso es proceder con el análisis de los posibles escenarios donde se vean comprometidas las actividades del CPD, permitiendo la identificación los procesos y procedimientos a ser ejecutados cuando sea necesario de modo que evento pueda ser mitigado.
- Comprobación de la funcionalidad de los procesos y procedimientos, una vez que se ha definido los escenarios, estrategias, procesos y procedimientos a ser realizados, el siguiente paso es someter a pruebas que validen la eficacia, eficiencia y seguridad de lo anteriormente mencionado. Una vez realizadas las pruebas de funcionalidad del plan se recomienda programar un mantenimiento periódico que permita la adaptación de las necesidades que se vayan presentando dentro del CPD, de modo que el plan se mantenga actualizado y funcional. («Los 7 mandamientos de un buen Plan de Continuidad de negocio», 2016)

Al hablar de un plan de continuidad de negocio se define como la unión de éste con los planes de contingencia y recuperación de desastres, de modo que el primero a ser desarrollado es el plan de continuidad junto con el plan de recuperación de desastres, a partir de los planes anteriormente mencionados a estos se agrega el plan de contingencia el cual se adapte y permita realizar los cambios requeridos para cubrir las áreas requeridas del CPD, además se incluye el análisis de impacto como parte del

desarrollo de los planes, puesto que identifica los tiempos que se tardan en retomar las actividades o tolerar frente a un evento no previsto.

2.2. Plan de contingencia

El plan de contingencia abarca las acciones y procedimientos preventivos que se pueden tomar dentro de un CPD, como medida preventiva ante la posibilidad de la presencia de eventos que atenten con las operaciones normales que se llevan a cabo dentro del entorno, es decir este es un plan que se desarrolla como medida cautelar para salvaguardar los componentes tanto de hardware como software que forman parte de los activos del CPD. («Seguridad Informatica / Plan de Contingencia», s. f.)

El desarrollo de este plan es identificar y describir todas las acciones necesarias para prever y dar una respuesta rápida, eficaz y confiable ante la posibilidad que un evento atente con las actividades y servicios que se encuentra prestando el CPD. («Que es un plan de contingencia», s. f.)

Para elaborar este plan se identifican 3 fases generales que se describen a continuación:

- Planificación, en este punto se realiza el análisis de las actividades a tomar en cuenta, para de este modo poder seguir con la identificación de todos los activos y servicios que forman parte del CPD, además se definen todos los puntos que abarcará el desarrollo de este plan como; definición del enfoque, comunicación de las metas y objetivos, identificación del entorno, todo esto en concatenación con el plan de recuperación de desastres que se ha diseñado con anterioridad.
- Identificación de riegos, en este punto se busca las fallas, riegos, amenazas y se busca vulnerabilidades que pueden estar dentro del área, también se identifica los activos críticos mediante el uso de técnicas o marcos de referencia que faciliten el

reconocimiento de los procesos, procedimientos y servicios que se encuentran sujetos a posibles escenarios donde se vean atentadas las operaciones normales.

- Identificación de soluciones, se definen los procesos y procedimientos con ayuda de marcos de referencia, normas y buenas practicas mismas que serán tomadas como medida de mitigación de los riegos que ya han sido identificados, además de constar con la reducción de aquellos posibles eventos que pueden generar interrupciones de las operaciones del CPD, finalmente se debe añadir un sistema de alerta contra fallas que permita una acción rápida y eficiente de todos aquellos objetos y personal involucrado dentro del área analizada. («GUIA PARA ELABORAR UN PLAN DE CONTINGENCIA INFORMATICO | IT VDELGADO», s. f.)

2.3. Plan de recuperación de desastres

El plan de recuperación de desastres o DRP forma parte del plan de continuidad del negocio, este plan contempla los procesos, procedimientos y actividades que se realizarán para la reanudación de las operaciones después que haya ocurrido un evento de desastre, siendo este un incidente que nulifica la continuidad de las actividades que se encuentran siendo procesadas y almacenadas dentro de la infraestructura del CPD.

Para el desarrollo del plan de recuperación de desastres se consideran 6 fases generales, las que describen a continuación:

- Determinación de objetivos del plan recuperación de desastres, aquí se describe el cuales son las razones por que es necesario el desarrollo del plan con enfoque a la continuidad del negocio, además se hace necesaria la gobernanza de la institución, con el fin de identificar los elementos críticos y los servicios más utilizados.

- Identificación de riesgos, en esta fase se especifica, clasifica y analiza los riegos a los que se encuentra sujeto la infraestructura, mismos que causen una interrupción en las operaciones, además se determina los activos que se definen como críticos, siendo éstos los elementos a ser protegidos.
- Análisis de impacto, dentro de esta se cuantificará los tiempos máximos que el CPD puede seguir con sus operaciones, de modo que junto con los ya identificados activos críticos permitan la recuperación de las funciones a un punto anterior que se encuentre normal, para lograr la mitigación o minimización de las secuelas dejadas por un evento de desastre.
- Planeación de estrategias, en base al análisis previo de los riesgos, activos críticos, y el impacto, se procederá al desarrollo de los procesos y procedimiento que serán realizados después de un evento que interrumpa las operaciones del CPD, particularizando de acuerdo al tipo de desastre presentado.
- Asignación de roles y responsabilidades, se designará de acuerdo al diagrama organizacional las responsabilidades de cada participante miembro del CPD, junto con la concientización, capacitación de los procesos y procedimientos a ser realizados después de la eventualidad de desastre.
- Adaptaciones del plan, en este se realizar un mantenimiento periódico para la identificación de los cambios necesarios con el fin de mejorar el plan, las que se modelarán de acuerdo a los cambios que se vayan realizando dentro del CPD y de la agregación de nuevos planes para la continuidad del negocio.(«¿En qué consiste un Plan de Recuperación ante Desastres (DRP)?», 2014b)

2.4. Tipos de desastres

Los desastres son eventos que se presentan de forma inesperada causando daños tanto a recursos como a organizaciones, además que genera interrupciones en las actividades

que se encuentran siendo desarrolladas en la zona de impacto. Ante la presencia de los desastres es posible contar con actividades que contrarresten los efectos de los mismos, pero teniendo en cuenta que es de forma inesperada no se puede cuantificar los daños que pudiesen causar, el tiempo de inactividad, el tiempo de restauración; es decir que al referirse a desastre se maneja la incertidumbre debido a que se puede conocer qué y cómo lo causa, pero no se puede valorar los daños obtenidos ante el paso de un evento de desastre.(«1.- Tipos y Fases de Desastres.pdf», s. f., pp. 4-5)

Al hablar de desastres se identifican tres grandes tipos:

- Desastres naturales, se definen como aquellos eventos causados por cambios repentinos en la naturaleza, de modo que deja daños significativos a la infraestructura por lo tanto se desconoce con exactitud la magnitud de las afecciones. Algunos de los desastres naturales que pueden afectar al CPD son: terremotos, inundaciones, incendios, erupciones volcánicas («Tipos de desastres naturales», 2017)
- Desastres provocados por el hombre, se conocen así a aquellos eventos catastróficos causados por el hombre, por acción u omisión deliberada, algunos de ellos son: conmoción social, negligencia en la operación del sistema, atentados terroristas, suspensión mal intencionada de servicios.(«1.- Tipos y Fases de Desastres.pdf», s. f., p. 8)
- Desastres informáticos, se conoce como a aquellos eventos donde los datos se ven afectados en su integridad, confidencialidad, disponibilidad y autentificación, dentro de estos se tomará en cuenta los siguientes tipos: interrupción, intercepción, modificación y fabricación. («¿Qué es la seguridad informática y cómo puede ayudarme? | VIU», s. f.)

CAPÍTULO 3

3. DESARROLLO DE PLAN DE RECUPERACIÓN DE DESASTRES

3.1. Descripción del escenario

La descripción de los parámetros en los cuales se encuentra ubicado el CPD es de vital importancia, debido a que a este escenario se encuentra sujeto a diversos factores que frente a la presencia de un riego puede causar daños en distintos niveles de su conformación de modo que hace necesaria la identificación de parámetros físicos y lógicos.

3.1.1. Ubicación geográfica

El CPD se encuentra ubicado en la Universidad Politécnica Salesiana, sede Quito, Campus Sur, entre la Av. Rumichaca y Moran Valverde. Ésta ubicada en el edifico denominado como bloque D, primer piso, la ubicación está especificada en las siguientes coordenadas; latitud: 0°16'57.66"S y longitud: 78°33'2.61"O.

Ubicación Geográfica del CPD

Figura 1. Visualización de la ubicación geográfica del CPD
Fuente: Tomado desde google earth

3.1.2. Descripción de la infraestructura

El CPD se cuenta con un área aproximada de 21.14 m^2 en la que se encuentra dispuesto el piso y techo falso, los cuales se encuentran a 30cm de altura sobre el piso y techo de la obra física.

En esta área se distribuyen 3 rack los cuales se encuentran distribuidos de la siguiente manera; el rack 1 esta implementado servidor HP Proliant DL38067, el segundo rack es exclusivo de HPE en él se albergan 4 servidores HPE APOLLO, en este mismo sitio se encuentra el storage 3PAR de HPE junto con los switch SAN, el tercer rack está destinado para comunicaciones, es decir contiene 2 ODF, 1 switch de core Cisco 9300, 1 switch de administración Cisco 500 y 2 switch de acceso Cisco 550 y un Watchdog para monitoreo de variables ambientales, dentro de la misma área se halla un acondicionador de aire, el cual se encuentra dispuesto de manera que se encuentre enfriando mediante la técnica de pasillo frío y pasillo caliente, además que se cuenta con un tablero de distribución eléctrica, sistema de provisión de energía ininterrumpida UPS, sistema de protección contra incendios, cuenta con un ventanal ubicado de manera didáctica para los estudiantes.

Todo esto se encuentra dispuesto de manera que exista redundancia en comunicación y energización, de acuerdo con los estándares de normas TIER, este caso el sistema de climatización no se encuentra dispuesto de la forma N+1, lo que significa que este no es redundante, de modo que es el único componente que no se encuentra de esta forma. Como se muestra en la Figura 2.

Ubicación física de los equipos del CPD

Figura 2. Plano de la distribución de los componentes físicos del CPD.
Fuente: Tomado de la memoria técnica de los proveedores(PLAGECONS, 2017)

3.1.3. Topología física

El CPD tiene 4 servidores HPE de los cuales 3 son APOLLO 6000 XL230A gen 9, estos se encuentran con un sistema ESXI 6.5 de VMware de modo que forman un clúster, con una capacidad total 96 núcleos, 0.7 TB en memoria RAM, además cuenta con un servidor HPC del modelo XL250A, este cuenta con una tarjeta gráfica NVidia Tesla K80, la cual cuenta con aproximadamente 5000 GPU, para el almacenamiento se ha dispuesto un storage HPE 3PAR 8200, con una capacidad total de 20TB y para la comunicación entre los servidores y el storage se la realiza mediante el uso de dos switch SAN SN3000B, siendo así que la comunicación se la realiza mediante fibra canal (FC),como se muestra en la Figura 3.

Diagrama de la topología física del CPD.

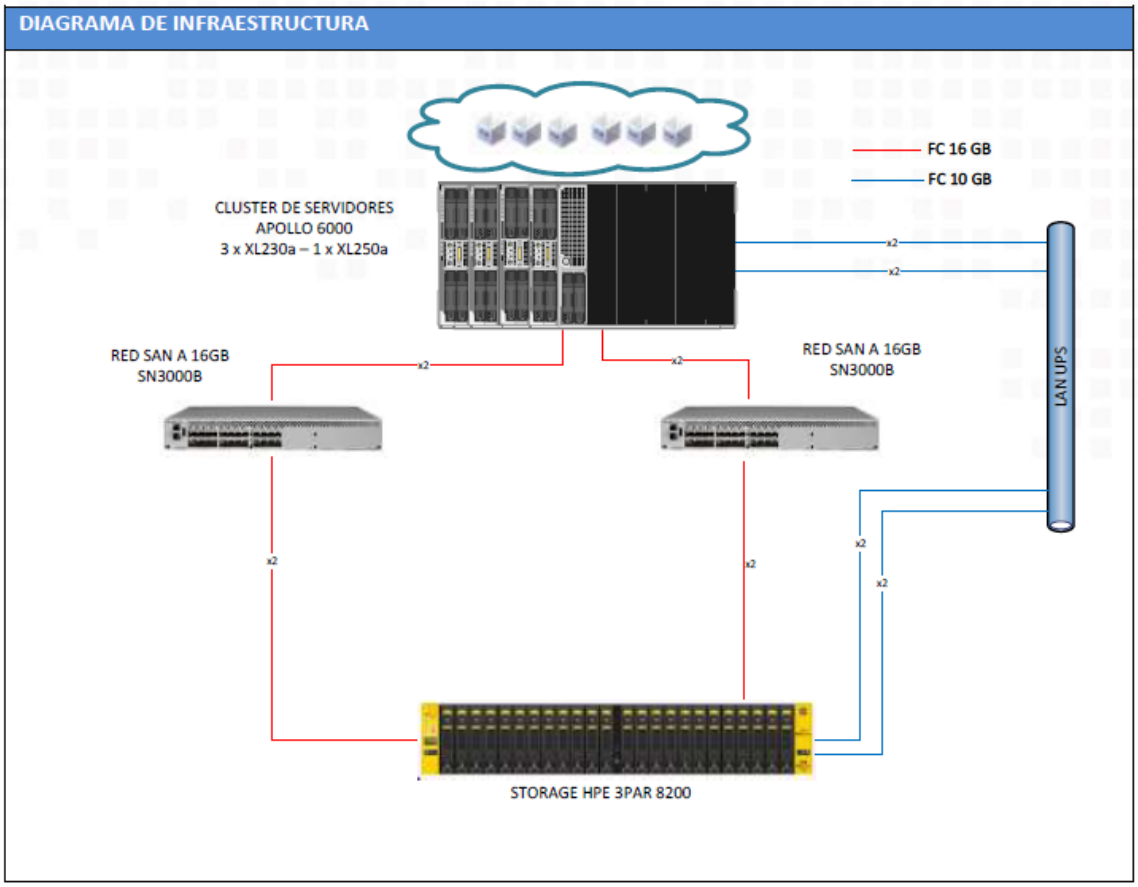


Figura 3. Topología Física
Fuente: Tomado de la memoria técnica del CPD realizado por Akros

3.1.4. Topología lógica

Dentro de la topología lógica se ha implementado un modelo colapsado, donde se tiene un switch Cisco 9300 de core para salida a Internet, a este se encuentran conectados 3 switch con una capacidad de transmisión a 10GBps de los cuales, dos de ellos son switch dedicados a acceso y uno para administración en este se encuentra conectado los servidores y storage los cuales se interconectan a 10 GBps a través de cableado de cobre UTP CAT 7. Entre los servidores y el storage se encuentra conectados mediante fibra óptica con tecnología fibra canal a 16GBps. Como se muestra en la Figura 4

Topología lógica del CPD

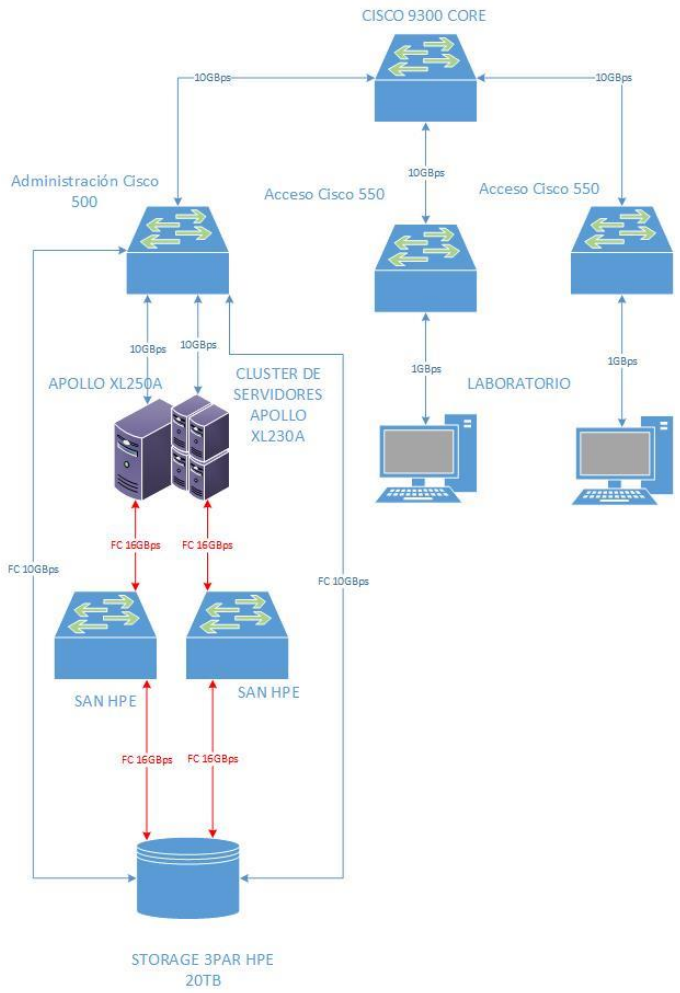


Figura 4. Topología Lógica
Elaborado por: Thalia Ati

3.2. Elaboración del plan de recuperación de desastres

Este plan tiene como objetivo definir los procesos, procedimientos, roles y buenas prácticas a ser realizadas después de una eventualidad de desastre para que de este modo se minimice al máximo el tiempo que el CPD se encuentre con sus actividades suspendidas a causa del paso de un desastre ya sea causado por la naturaleza, por errores humanos o por fallos de índole informático, además éste se desarrolla junto con el plan de continuidad de negocio, el mismo que permite la identificación y valoración de las afecciones obtenidas por la interrupción generada.

Gracias a los marcos de referencia dados por COBIT y ITIL se determina cuáles son los activos y servicios críticos, así también como la determinación de los roles y responsabilidades de los miembros que forman parte mismo que se encuentra a cargo de la administración y gestión de los recursos del CPD, incluyendo los procesos y procedimientos que se llevan a cabo para restablecer las actividades a un punto anterior donde todo se encuentre correctamente.

Por otra parte, en base a la norma ISO 22301 misma que da la metodología PDCA (Planificación-Implementación-Verificación-Mantenimiento) para el desarrollo de este plan y junto con la norma NTE INEN-ISO/IEC 27031, que es el ente regulador dentro del territorio ecuatoriano, define los puntos como el alcance, administración, políticas de manejo de logs, prevención, mitigación y mantenimiento, mismos que se deben incluir dentro de la documentación a ser posteriormente entregada.

3.3. Evaluación de riesgos

De acuerdo con ITIL y la gestión de riesgos se tiene que este inicia con la definición de los activos a ser protegidos, para ello se identifican escenarios donde las amenazas,

riegos, vulnerabilidades generan una interrupción en las operaciones que lleva a cabo el CPD.

3.3.1. Activo

El centro de procesamiento de datos cuenta con una infraestructura nueva, misma que contiene componentes de hardware y software que en conjunto brindan servicios de virtualización de equipos los cuales están dispuestos para el desarrollo de investigación y academia.

Los activos de hardware con los que cuenta el CPD son los activos que se detallan en la Tabla1.

Tabla 1. Activos de Hardware del CPD.

Fabricante	Descripción	Modelo	Número de serie	Propio/ Alquiler
HPE	Chassis	APOLLO 6000	2M274600VL	Propio
HPE	Servidor	XL230A	2M274600VG	Propio
HPE	Servidor	XL230A	2M274600VH	Propio
HPE	Servidor	XL230A	2M274600VJ	Propio
HPE	Servidor	XL250A	2M274600VK	Propio
HP	Servidor	Proliant DL38067	2M204500J2	Propio
HPE	Storage	3PAR 8200	2M27320157	Propio
HPE	Switch	HPE SN3000B	USB7282019	Propio
HPE	Switch	HPE SN3000B	USB728202E	Propio
Cisco	Switch	SG5550XG	DNI211113VD	Propio
Cisco	Switch	SG5550XG	DNI211113UP	Propio
Cisco	Switch	SG500	DNI2119064R	Propio

Cisco	Switch	Catalyst 9300	FOC2145Z0EZ	Propio
APC	UPS	Symmetra LX	SYA8K16P	Propio
APC	UPS	Symmetra LX	SYA8K16P	Propio
Samsung	Monitor 49inch	LH49PMHP	06S2HCSJB01918A	Propio
Samsung	Monitor 49inch	LH49PMHP	0652HCJB019199K	Propio
Epson	Impresora	L575 MULTIFUNCION	W98Y190439	Propio
DELL	Desktop	OptiPlex 7040	8MFDHD2	Propio
DELL	Desktop	OptiPlex 7040	8MLBHB2	Propio
DELL	Desktop	OptiPlex 7050	3KM0JK2	Propio
GEIST	Watchdog	G1600P		Propio
APC	ATS	AP77504	5A1735T59095	Propio
Cisco	SFP	ENTERPRISE - CLASS	FNS214901EW	Propio
Cisco	SFP	ENTERPRISE - CLASS	AVD2144D2RX	Propio
Cisco	SFP	ENTERPRISE - CLASS	AVD2145D8N1	Propio
Cisco	SFP	ENTERPRISE - CLASS	FNS214901GZ	Propio
Cisco	SFP	ENTERPRISE - CLASS	AVD2144D07A	Propio
Cisco	SFP	ENTERPRISE - CLASS	AVD2145DF6Z	Propio

STULZ	Acondicionamiento de Aire	CompTrol 7000	10061749	Propio

Nota: la tabla contiene todos los componentes de hardware del CPD

En la Tabla 2, se detallan los activos de software.

Tabla 2. Activos de Software del CPD.

Nombre de la aplicación	Crucial Sí / No	Activos fijos Sí / No	Fabricante	Comentarios
Vmware vSphere 6.5.0	si	si	Vmware	Ejecución Continua
Vmware vRealize 6.5.0	si	si	Vmware	Ejecución Continua
Vmware vRealize Log Insigth 4.3.0	si	si	Vmware	Ejecución Continua
Vmware ESXi 6.5.0	si	si	Vmware	Ejecución Continua
DHCP	si	si	Microsoft	Ejecución Continua
DNS	si	si	Microsoft	Ejecución Continua
Active Directory	si	si	Microsoft	Ejecución Continua
Windows 10	no	si	Microsoft	Ejecución bajo demanda
pfSense-CE-2.4.3-AMD64	si	si	GNU Linux	Ejecución Continua
CACTIOS	no	si	GNU Linux	Ejecución Continua
ZKTeco 3.5.3	no	si	PuisSDK	Ejecución Continua
Milestone Xprotect 2018 2.1a	si	si	Milestone Systems	Ejecución Continua

GEIST Watchdog 3.16.3	si	si	GEIST	Ejecución Continua
HPE 3PAR SSMC	si	si	HPE	Ejecución Continua

Nota: la tabla contiene todos los componentes de Software del CPD

3.3.2. Vulnerabilidad

El CPD cuenta con una infraestructura donde alberga información de ámbito investigativo, educativo, desarrollo científico y tecnológico, por todo esto lo hace susceptible a interrupciones mismos que atentan con la integridad, seguridad, fiabilidad y autenticación de los datos, por dicho motivo es importante la identificación de las vulnerabilidades sabiendo que son vías potenciales por las cuales se vea comprometido los servicios prestados.

Tabla 3. Vulnerabilidades en el CPD.

VULNERABILIDAD
• **Bugs** • **Fallos de Hardware** • **Suplantación de identidad** • **Configuración de puertos** • **Metadatos** • **Configuraciones del sistema ineficientes** • **Comunicaciones inseguras** • **Software desactualizado** • **Contraseñas inseguras**

Nota: la tabla contiene la lista de vulnerabilidades detectadas dentro del CPD

3.3.3. Amenazas

Son posibles peligros que se encuentran latentes dentro de un entorno, haciéndose necesaria la identificación de las amenazas que se encuentran dentro del CPD, para de esto modo se viabilice el realizar actividades tanto de protección y mitigación de las mismas como medida de protección ante la acción de eventos que pongan en riesgo las actividades normalmente realizadas.

Tabla 4. Amenazas del CPD

Amenazas
• **Sobrecalentamiento** • **Phishing** • **Robo de información** • **Gusanos** • **Colapso de estructura** • **Hurto** • **Backdoor** • **Virus** • **Malware** • **DDOS** • **Perdida de conectividad** • **Spyware** • **Usuarios mal intencionados** • **Troyanos** • **Ransomware**

Nota: la tabla contiene la lista de amenazas detectadas dentro del CPD

3.3.4. Riesgo

Se identifica como aquello que tiene la posibilidad de causar un daño o perdida con la particularidad que se conoce la causa, pero no se puede identificar con claridad cuándo se presentará, por esta razón al momento de desarrollar el plan de recuperación de desastres es vital importancia conocer cuáles son los riesgos a los que la infraestructura del CPD se encuentra sujeto, dentro de estos se presentan una diversidad de acciones que puedes afectar al escenario como: la ubicación geográfica, elementos de comunicación, procesamiento de datos, se han determinado los que se detallan en la tabla 5.

Tabla 5. Riesgos del CPD.

Riesgos
• **Suministro eléctrico** • **Inundación** • **Sismo** • **Vientos fuertes** • **Incendios** • **Tormenta Eléctrica** • **Erupciones volcánicas** • **Manifestaciones civiles violentas** • **Atentados terroristas** • **Ataques informáticos** • **Negligencia** • **Climatización**

Nota: la tabla contiene la lista de riegos detectadas dentro del CPD

3.3.5. Identificación de los activos a proteger

En este caso para realizar la identificación de activos a ser protegidos se realiza una categorización de los activos como se muestra en la Tabla6, en base a dicha categorización se realiza una cuantificación de las cualidades, de modo que permita la definición de cuales son aquellos componentes primordiales que deben ser restablecidos en la primera instancia después de una eventualidad de desastre de modo que se minimice el tiempo de una interrupción.

Tabla 6. Categorización de Activos

Categorización de activos	
Servidores	APOLLO 6000 CHASIS
	Servidor XL230A
	Servidor XL230A
	Servidor XL230A
	Servidor XL250A
	Servidor Proliant DL38067
Almacenamiento	Storage 3PAR 8200
Switch SAN	Switch HPE SN3000B
	Switch HPE SN3000B
Core	Switch Catalyst 9300
Administración	Switch SG500
Acceso	Switch SG550XG
	Switch SG550XG
	6 SFP
Monitoreo y gestión	Monitor LH49PMHP
	Monitor LH49PMHP
	Desktop OptiPlex 7040
	Desktop OptiPlex 7040
	Desktop OptiPlex 7050
	Watchdog G1600P
Energización	UPS Symmetra LX
	UPS Symmetra LX
	ATS AP77504
Climatización	Acondicionamiento de Aire CompTrol 7000
Software de administración y gestión	Vmware vSphere 6.5.0
	DHCP
	DNS

	Active Directory
	pfSense-CE-2.4.3-AMD64
	ZKTeco 3.5.3
	HPE 3PAR SSMC
Software de monitoreo	Vmware vRealize 6.5.0
	Vmware vRealize Log Insigth 4.3.0
	CACTIOS
	Milestone Xprotect 2018 2.1a
	GEIST Watchdog 3.16.3
Hipervisor	Vmware ESXi 6.5.0
Varios	Impresora L575 MULTIFUNCION

Nota: la tabla contiene la agrupación de por categoría de los activos del CPD

Es así que para el CPD se ha tomado como cualidades a ser valoradas los siguientes puntos, interrupción del servicio (IS), interrupción del monitoreo y gestión (Adm), seguridad de la información (SI), alteración de la información (AI), fuga de información (FI), mismos que tomaran un valor entre 1 y 5 siendo uno el valor más bajo y 5 el valor más alto como se muestra en la Tabla7.

Tabla 7. Valores de priorización para la evaluación de los activos.

Valores de priorización	
1	Muy baja
2	Baja
3	Medio
4	Alto
5	Muy alto

Nota: la tabla contiene los valores a ser designados a los activos

En base a la valoración de los aspectos mencionados para determinar la criticidad de los activos, se identifican tres características que son: integridad, confidencialidad y disponibilidad, mediante estos se determina los activos críticos mismos que van a ser protegidos, para esto se realiza la sumatoria de tres de las cualidades antes descritas asignado a cada uno de los parámetros principales, lo cual se lo realiza de la siguiente manera:

$$Confindencialidad = SI + AI + FI$$

$$Integridad = IS + Adm + AI$$

$$Disponibilidad = IS + Adm + SI$$

De modo que para la valoración de los servidores se tiene que

$$Confindencialidad = 5 + 5 + 5$$

$$Confindencialidad = 15$$

$$Integridad = 5 + 5 + 5$$

$$Integridad = 15$$

$$Disponibilidad = 5 + 5 + 5$$

$$Disponibilidad = 15$$

De tal manera que:

$$Total = \ Confindencialidad + Integridad + Disponibilidad$$

$$Total = 15 + 15 + 15$$

$$Total = 45$$

Siendo que para la ponderación en un rango de 1 a 5 es:

$$Ponderado = \frac{Total * 5}{45}$$

$$Ponderado = \frac{45 * 5}{45}$$

$$Ponderado = 5$$

De modo que el ponderado es el nivel de criticidad que tiene cada uno de los activos que se encuentran siendo valorados, como se encuentra especificado en la tabla 8.

Tabla 8. Matriz de activos críticos a ser protegidos

Activo	IS	Adm	SI	AI	FI	Confidencialidad	Integridad	Disponibilidad	Total	Ponderación
Servidores	5	5	5	5	5	15	15	15	45	5
Almacenamiento	5	5	5	5	5	15	15	15	45	5
Switch SAN	5	5	5	5	5	15	15	15	45	5
Core	5	3	3	1	1	5	9	11	25	3
Administración y gestión	5	5	1	1	1	3	11	11	25	3
Acceso	5	3	1	1	1	3	9	9	21	2
Equipo de Monitoreo	2	4	1	1	1	3	7	7	17	2
Energización	5	4	1	1	1	3	10	10	23	3
Climatización	5	1	1	1	1	3	7	7	17	2
Software de administración y gestión	5	5	5	5	4	14	15	15	44	5
Software de Monitoreo	4	4	2	1	3	6	9	10	25	3
Hipervisor	5	5	5	5	4	14	15	15	44	5
Varios	1	1	1	1	1	3	3	3	9	1

1		No crítico
2		Bajamente crítico
3		Medianamente crítico
4		Crítico
5		Muy crítico

Nota: La tabla contiene la cuantificación para determinar el la criticidad de los activos

De éste modo se obtiene el resultado mismo que toma un valor máximo de 15 el cual será sometido a una ponderación donde se evaluará en un rango de 1 a 5 donde el valor más alto a tener es 5 lo que significa que el activo es muy crítico y 1 como el mínimo determinando que el activo es el no reviste criticidad.

Una vez que se han identificado los activos a ser protegidos en base a una valoración de los activos que se muestra en el apartado 3.3.5 en el cual se refleja los componentes que se catalogan como críticos, es decir los primeros en ser restablecidos después de una eventualidad de desastre, el siguiente paso es la evaluación de riegos a los que se encuentra sujeto el CPD, los que fueron considerados en base a parámetros como: la geografía de la ubicación, la estructura de la edificación, vulnerabilidades, amenazas, componentes de infraestructura, lo cual ha dado como resultado un total de 12 riesgos, han sido cada uno de ellos valorados en función de 7 características que se encuentran de definidas por la norma ISO 27005, misma que habla sobre la gestión de riesgos en tecnologías de información en la cual detalla los factores que facilitan la evaluación de un evento de desastre.

Para la valoración de los riegos-factor se la realizó mediante una entrevista con el administrador del CPD de modo que se los cuantificó en base a un rango entre 1 y 5 donde 1 es el valor menor que se define como una bajo y 5 el máximo identificado como alto, como se muestra en la tabla 9.

Con los valores de los riegos registrados se realiza una sumatoria de los puntos obtenidos por cada uno de los escenarios, mismo que como máximo tendrán un valor de 35 y como mínimo 7 en base a esto se realiza una proporción en donde 35 es 100% de modo que se determinó que el riesgo más crítico son los ataques informáticos el cual tiene un porcentaje de afectación estimado del 83%, seguido por sismos con un

77%, suministro eléctrico y tormentas eléctricas por un 71%, incendios y erupciones volcánicas 69%, negligencia 66%, climatización 60%, atentados terroristas 54%, vientos fuertes y manifestaciones civiles violentas 37% e inundaciones con 29%, como se muestra en la Tabla9.

Tabla 9. Evaluación de riesgos

Riesgo / Parámetro	Suministro eléctrico	Inundación	Sismo	Viento fuerte	Incendio	Tormenta Eléctrica	Erupción volcánica	Manifestaciones civiles violentas	Atentado terrorista	Ataques informáticos	Negligencia	Climatización
Probabilidad	2	1	4	1	3	5	3	1	1	5	1	2
Consecuencias	5	1	4	2	5	3	5	2	5	5	5	5
Ocurrencia	2	1	3	1	1	5	2	1	1	3	1	1
Urgencia	5	2	4	2	5	2	5	1	5	5	5	5
Maleabilidad	4	3	4	3	4	3	2	4	1	1	5	2
Dependencia	5	1	5	3	5	4	5	3	5	5	5	5
Proximidad	2	1	3	1	1	3	2	1	1	5	1	1
Total	25	10	27	13	24	25	24	13	19	29	23	21
Porcentaje de afecciones por cada riesgo	71	29	77	37	69	71	69	37	54	83	66	60
Criticidad	4	2	4	2	4	4	4	2	3	5	4	3

Impacto		
1	Baja	
2	Media-baja	
3	Media	
4	Media-alta	
5	Alta	

Criticidad			
1	Baja	1% -20%	
2	Media-baja	21% - 40%	
3	Media	41% -60%	
4	Media-alta	61% - 80%	
5	Alta	81% -100%	

Nota: La tabla contiene la evaluación de los riegos que pueden afectar a las operaciones normales del CPD

3.4. Análisis de impacto

Es vista como la necesidad de la identificación de los activos críticos que existen dentro del CPD, de modo que la valoración de activos y la evaluación de los riesgos latentes de cada uno delos componentes a los que se encuentra sujeto, permite la priorización de los elementos que son vitales para mantener o restaurar las actividades que normalmente se encuentra desarrollando.

3.4.1. Desarrollo del BIA

Para el desarrollo es importante realizar entrevistas y reuniones con los miembros responsables del CPD, mismos que faciliten la identificación de los procesos y procedimientos de todos los servicios principales de modo que se realicen se identifiquen todas las actividades críticas además de los servicios mínimos para que se el tiempo que dure la interrupción se lo mas corto, así también establecer el tiempo estimado de recuperación (RTO) y el punto de recuperación objetivo (RPO). Según el manual de administración del plan de continuidad de negocio de ICETEX dice que:

> Todos los procedimientos de la Entidad, así como los recursos tecnológicos en los que se soportan tales actividades son clasificados de acuerdo con su prioridad de recuperación. Para ello se mide el tiempo que puede dejar de realizar tal actividad sin que ello cause pérdidas financieras, quejas de los clientes, y/o penalizaciones legales o contractuales. En caso de continuidad todo gira alrededor del impacto, buscando sostener la operación crítica de la Entidad. («Manual_continuidad_negocio.pdf», s. f., p. 19)

En base a lo mencionado anteriormente, se ha realizado la evaluación de criticidad donde se encuentra valorado de manera que se colocan los activos ordenadamente de mayor a menor en orden de criticidad del riesgo.

Tabla 10. Valoración de activos frente a riegos.

Riesgo / Activo	Ataque informático	Sismos	Suministro eléctrico	Tormenta eléctrica	Incendios	Erupciones volcánicas	Negligencia	Climatización	Atentados terroristas	Vientos fuertes	Manifestaciones civiles violentas	Inundaciones
Servidores	5	3	5	2	5	3	3	5	1	1	1	1
Almacenamiento	5	3	5	2	5	3	3	5	1	1	1	1
Switch SAN	5	3	5	2	5	3	3	5	1	1	1	1
Software de administración y gestión	5	2	2	2	2	2	5	1	2	2	2	2
Hipervisor	5	2	5	2	2	2	5	2	2	2	2	2
Core	5	3	5	2	5	3	3	5	1	1	1	1
Sistema de energía continua	1	3	5	5	5	1	5	2	1	1	1	2
Software de Monitoreo	5	2	2	2	2	2	5	1	2	2	2	2
Sw administración	5	3	5	2	5	3	3	5	1	1	1	1
Climatización	1	3	5	3	5	5	5	5	2	3	2	5
Equipo de monitoreo	2	1	4	2	2	1	3	1	1	1	1	2
Sw acceso	2	3	5	4	5	2	5	3	1	1	1	1
Varios	1	1	1	1	1	1	1	1	1	1	1	1

Impacto	
1	Insignificante
2	Menor
3	Moderado
4	Alto
5	Catastrófico

Nota: La tabla contiene la cuantificación de los activos frente a la presencia de una eventualidad que atente con la continuidad de las operaciones

En la Tabla 10, se encuentran colocados de manera ordenada en forma descendente del más crítico al menos crítico, de modo que en el eje vertical se ubican los activos y en el eje horizontal se encuentran los riegos que han sido identificados, los mismos que se da un valor entre 1 y 5 donde 1 es insignificante lo cual muestra que los daños son bajos o nulos, mientras que 5 se identifica como catastrófico, es decir, que los daños y afecciones son altos.

Con base en lo anterior se tiene que frente a un ataque informático los servidores, el almacenamiento, los switch SAN, el software de administración y gestión, el hipervisor, el switch core, software de monitoreo, los switch de administración, son los activos que permiten mantener o dar servicios a los usuarios, por dicho motivo estos son los primeros en ser recuperados en orden de criticidad dado que la pérdida o fuera de servicio de alguno de estos componentes se le valoro con 5, mientras que los equipos de monitoreo y los switch de acceso son los siguientes en ser restaurados debido a que se los estimo con 2, por otro lado siendo los componentes de suministro de energía continua, junto con climatización y varios se les asignó en peso de 1 por lo cual son los que se quedan en la etapa final del proceso de recuperación, mismo que dará como resultado la restauración del servicio en su estado normal.

Es así que se determina que los activos que cuentan con más riegos latentes son: servidores, almacenamiento, switch SAN, switch de core, el software de administración y gestión, estos se identifican 4 riegos cada uno con una valoración de 5, además se detectó que el activo con más riegos es el de climatización el cual se muestra con un total de 6 escenarios donde se encuentra altamente vulnerable, además del impacto que afecta cada riego a cada activo también se puede hablar del impacto que sufría todo el CPD ante cualquier de los mencionados casos de desastre.

En el desarrollo del análisis de impacto la identificación del tiempo de recuperación objetivo RTO es una etapa fundamental ya que esta forma parte de la continuidad del negocio debido a que éste es el tiempo tolerable que se puede presentar una interrupción antes que las pérdidas de información sean altas.

El CPD al ser un ambiente orientado al desarrollo investigativo, tecnológico y académico, tiene una demanda con mayor carga de trabajo que se localiza en un rango que inicia a las 7:00 y termina a las 20:00,a partir de esta hora la infraestructura presenta un uso bajo debido a que en la Institución cesan las actividades académicas, dando como resultado una ventana que empieza 20:00 y finaliza a las 6:00, esto se lo pudo observar durante un periodo de 15 días, en el cual se evidencia la demanda de utilización de los recursos como el uso de CPU y memoria, de esta manera se puede evidenciar las tendencias que se ha tenido durante el tiempo de evaluación antes mencionadas.

Graficas de la tendencia de uso de CPU que tiene el cluster de servidores

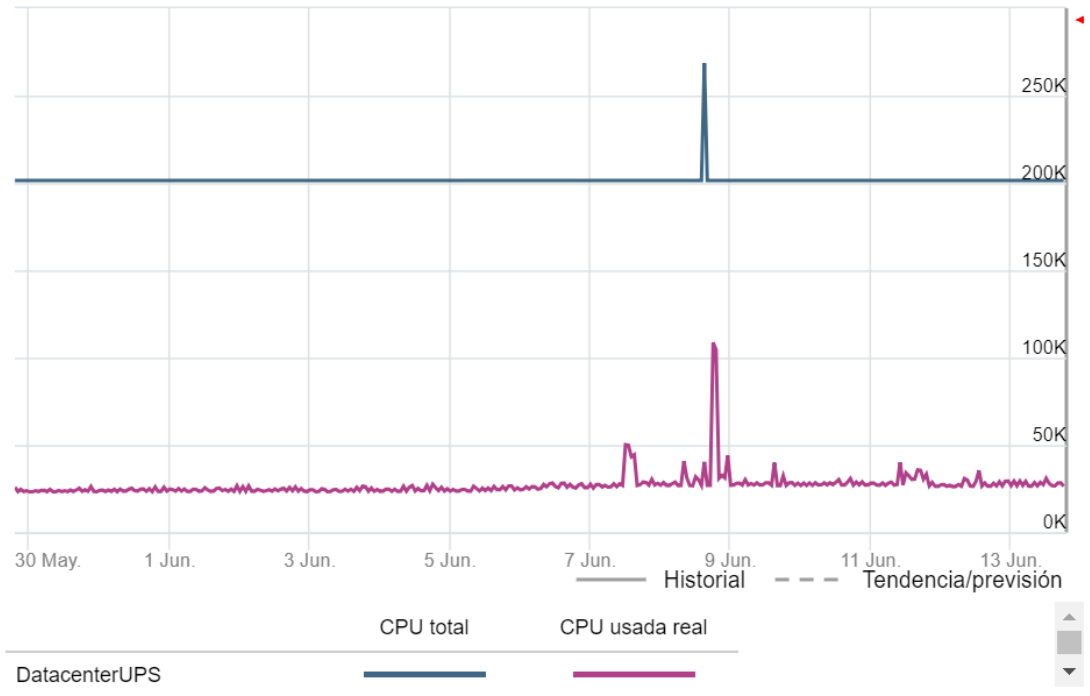


Figura 5. Tendencia de uso de CPU.
Realizado por: Thalia Ati

Graficas de la tendencia de uso de memoria que tiene el clúster de servidores

Figura 6. Tendencia de uso de capacidad de memoria.
Realizado por: Thalia Ati

En base a las Figuras 5 y 6, se evidencian las tendencias de utilización de los recursos provistos por el CPD en las cuales se muestra que la demanda de recursos es baja, además que los picos de se presentan en rangos están dentro de un rango de tiempo más corto.

Graficas de la tendencia de uso de CPD en 24 horas

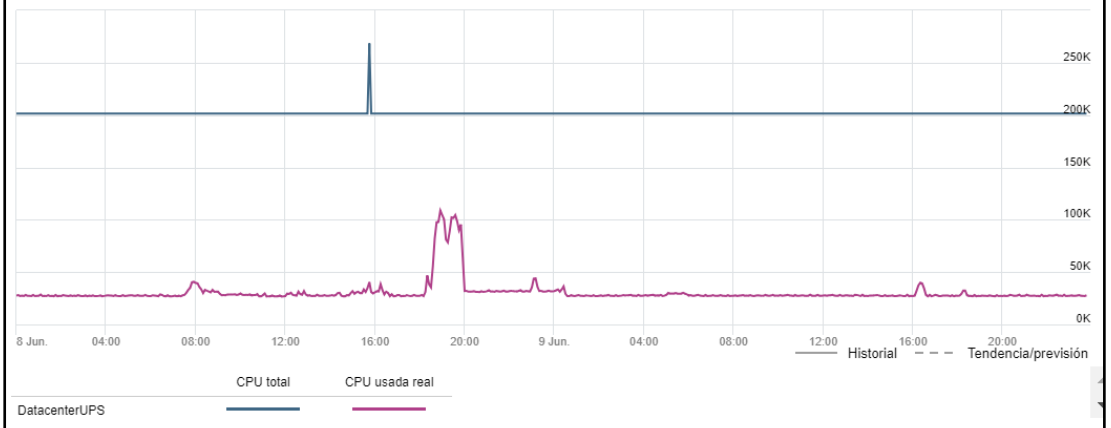


Figura 7. Tendencia de utilización de CPU.
Realizado por: Thalia Ati

Una vez que se ha visualizado el comportamiento en un lapso de tiempo de 15 días, se procede a la muestra de los datos de uso de CPU en el pico de utilización más grande,

que se evidencia que es de un día, por lo tanto, en la Figura7 se observa que inicia con una linealidad bastante marcada a partir de las 00:00 del día 8 de junio y que va hasta las 8:00 del mismo día, además muestra que el uso de este recurso inicia desde aproximadamente las 8:00 del día 8 de junio y que va hasta las 20:00 del mismo día, a partir de esta hora regresa a estar en un estado lineal para el siguiente día.

Graficas de la tendencia de uso de CPD en 24 horas

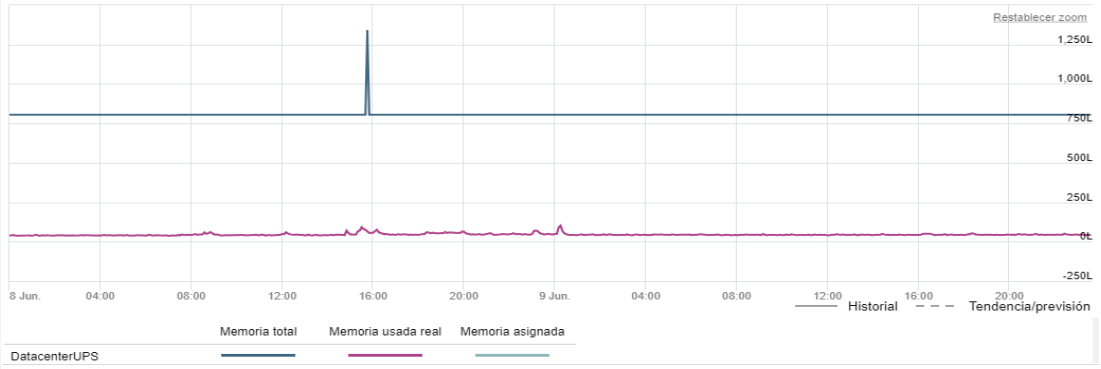


Figura 8. Tendencia de utilización de capacidad de memoria.
Realizado por: Thalia Ati

Para detectar el lapso temporal donde hay más carga de trabajo se procede a tomar una muestra más pequeña que se encuentre en el rango dentro de los 15 días anteriormente mostrados, de modo que el rango de análisis es minimizado a 24 horas, el cual inicia a partir de las 00:00 del día 8 de junio hasta el día 9 de junio del 2018, siendo así que dentro de éste rango se evidencia que de 00:00 hasta las 8:00 aproximadamente la tendencia de uso no presenta una variación maraca, mientras que a partir de esta hora se observa que inicia a presentar picos los cuales demuestra que se está usando la memoria, de modo que alrededor de las 20:00 hasta las 00:00 del siguiente día regresa a su estado inicial, lo cual se evidencia en la Figura 8, además este comportamiento recurrente durante 5 días (Lunes a Viernes), mientas que los dos siguientes días el proceder de es similar al que se presenta en las horas nocturnas, por dicho motivo el CPD cuenta con un total de 103 horas semanales en las cuales no presenta una demanda de recursos alta.

Tabla 11. Tiempos máximos antes que se reporten perdidas.

Riesgo / Activo	Ataque informático	Sismo	Suministro eléctrico	Tormenta eléctrica	Incendio	Erupción volcánica	Negligencia	Climatización	Atentado terrorista	Viento fuerte	Manifestación civil violenta	Inundación
Servidores	2	24	2	0,3	Ind	24	1	0,5	ind	2	2	1
Almacenamiento	2	24	2	0,3	Ind	24	1	0,5	ind	2	2	1
Switch SAN	2	24	2	0,3	Ind	24	1	0,5	ind	2	2	1
Software de administración y gestión	2	24	2	0,3	Ind	24	1	N/A	ind	N/A	N/A	N/A
Hipervisor	2	24	2	0,3	Ind	24	1	N/A	ind	N/A	N/A	N/A
Core	2	24	2	1	Ind	N/A	2	5	ind	N/A	N/A	2
Sistema de energía continua	N/A	24	2	0,3	Ind	0,5	1	N/A	ind	2	2	0,5
Software de Monitoreo	8	N/A	4	N/A	Ind	N/A	5	N/A	ind	N/A	N/A	N/A
Sw administración	2	24	2	0,3	Ind	N/A	1	5	ind	N/A	N/A	2
Climatización	N/A	24	1	0,3	Ind	1	1	1	ind	1	1	1
Equipo de monitoreo	N/A	24	2	1	Ind	3	2	3	ind	N/A	N/A	1
Sw acceso	4	24	2	1	Ind	N/A	2	5	ind	N/A	N/A	2
Varios	N/A	24	4	4	Ind	N/A	5	N/A	ind	N/A	N/A	N/A

Terminología	
ind	indeterminado
N/A	No aplica

Nota: En la tabla se muestra los tiempos que se tardaría en recuperar los activos de pendiendo del evento de desastre presentado

De acuerdo con el tiempo y uso de los servicios del CPD, se tiene un total de 13 horas diarias en las cuales la tendencia de utilización de los recursos es evidente lo cual deja una ventana para diversos trabajos de mantención, recuperación o corrección de 11 horas por día de trabajo, además que se evidenció que durante los fines de semana los recursos se mantienen de manera constante, prácticamente sin cambios o variaciones, a diferencia de los días laborables que son de lunes a viernes en los cuales se observó que hay un ligero cambio en el uso durante los periodos de tiempo antes descritos.

En base a lo expuesto se tiene que ante la presencia de una vulnerabilidad o amenaza es necesario el despliegue de acciones de corrección, mismas que se recomienda ser realizadas dentro del rango de tiempo con menos carga de trabajo, ya que estas proveen del espacio necesario para la realizar las actividades de rectificación requeridas, además que estas deben estar planificadas con anterioridad, de modo que si se llegaran a presentar un evento de desastre, se cuenta con tiempos disponibles para la recuperación con periodos de tiempo necesarios para el despliegue de las actividades de recuperación.

De esta manera dentro de la infraestructura del CPD la cuantificación temporal que tomaría en restaurar cada activo que forme parte del entorno tiene un tiempo estimado de recuperación frente a uno de riegos de los que fueron identificados anteriormente, como se muestra en la Tabla 11, donde se especifican los tiempos máximos que la infraestructura no experimentas pérdidas significativas, mismos que se midieron en horas, además que se encuentra distribuida de modo que los activos se encuentren en fila ordenada de manera descendente del mas al menos crítico, mientras que las columnas se localizan los riegos ordenados los cuales se ubican de modo que el primero es el que tiene mayor valor de riesgo y el ultimo es el que menos impacto puede causar, cabe recalcar que los tiempos son los estimados.

Al momento de hablar de RTO es importante destacar que, por ser una infraestructura nueva, ésta se encuentra dentro de un periodo de garantía, de modo que tiene una dependencia de terceros, por dicho motivo el tiempo que tomaría la restauración se acogen a los niveles de soporte dados por el proveedor dentro de los cuales se contemplan 3 niveles de soporte mismos que dependiendo del SLA se acogen a los distintos niveles, además que los tiempos se acogen a los niveles de servicio, siendo así que el tiempo de respuesta es de 1 hora la cual se encuentra comprendida desde que el usuario abre el ticket hasta la asignación de un especialista, el tiempo de solución es aquel que toma solucionar el problema o incidente presentado, y el tiempo de soporte comprende entre el tiempo que está disponible el servicio de soporte.(AKROS, 2016)

Por otro lado, el RPO el punto objetivo de restauración en base al diseño de la infraestructura y a la entrevista realizada los operadores del CPD se determinó que no cuenta con un proceso de backup, por lo cual en caso de desastre la recuperación de la información sería un proceso con alto grado de dificultad.

3.5. Estrategias de recuperación

Ante la presencia de un evento de desastre, mismas que inhabiliten las operaciones normales del CPD, es de vital importancia la definición de las estrategias para restablecer el estado normal, en un período de tiempo corto, de modo que las perdidas e interrupción sean minimizadas al máximo.

3.5.1. Tipos de estrategias de recuperación

Al hablar de estrategias de recuperación hace referencias a las operaciones a ser hechas como medidas de prevención y de restauración de las actividades en un tiempo corto, de modo que se minimice el impacto de un evento de desastre, es así que se tienen las siguientes estrategias:

Backups

Son copias de la información que realizan para respaldar los equipos que forman parte de CPD , de modo que si ocurriese un evento de desastre el cual modifique, altere o elimine, poder regresar al punto anterior donde se encontraba con las operaciones normales de modo que las pérdidas son mínimas, además que los servicios afectados tengan un tiempo de interrupción mínimo; por otro lado en caso de algún desastre las copias facilitan el proceso de recuperación después de un evento de desastre.(«¿Qué es Backup?», s. f.)

Siendo beneficioso como restablecer el servicio en un corto periodo de tiempo y regresando a un punto anterior donde se encontraba con las operaciones normales, además que se obtiene seguridad adicional. .(Selva, 2018)

Energías alternativas

En éste caso son una fuente de energía que no se encuentra contemplada dentro del sistema de energización del CPD, por tanto es una fuente extra la cual provee de la energía eléctrica necesaria para mantener las operaciones normales, además que protege de posibles interrupciones del servicio minimizando o mitigando el tiempo de suspensión de las operaciones, debido a que es una fuente exclusiva que tiene el fin de alimentar únicamente al CPD.(«¿Qué son las energías alternativas? - ¿Sabías que? - Compromiso RSE», s. f.)

Climatización

Al ser el CPD un lugar donde se albergan equipos de comunicación, almacenamiento, procesamiento, monitoreo y energización es así que según el portal MUNDOHVAC&R *"90% de la energía generada por los equipos que operan en estos lugares se transforma en calor"*, de este modo es de vital importancia que el sitio

donde se encuentran operando cuente con el equipo necesario para que de este modo los componentes cumplan con sus actividades.(«Acondicionamiento en Data Center», s. f.)

Además de las estrategias de recuperación, también se incluye tácticas de mitigación, para mantener las operaciones ante la presencia de un evento de desastre, siendo así que se recomienda un monitoreo en tiempo real y manejo de un control de acceso tanto al área del CPD como a la institución.

Monitoreo en tiempo real

El monitoreo consiste en mantener un registro de todas las variables tanto físicas como lógicas mismas que forman parte del CPD, además que se acceda a dicha información desde cualquier lugar y en cualquier momento, de modo que permita la acción rápida y eficaz ante la variación de uno de los parámetros que se encuentre siendo vigilados, de modo que se realicen acciones correctivas y preventivas ante la presencia de un evento que atente a la continuidad del negocio o que altere las operaciones, para que de esta manera se minimice o se mitigue el tiempo de reacción ante estos acontecimientos.(«Monitoreo DataCenter», s. f.)

Control de acceso físico

En el control de acceso se tiene dos enfoques que son: una es a nivel físico y otra a nivel lógico, de modo que en los dos tipos se mantiene un registro de los individuos que acceden a este escenario, siendo en el momento determinado en el cual se presente una violación de acceso se pueda identificar quien está implicado en dicho evento, siendo así que se genere una política de acceso que garantice la seguridad de la información, además que permita una acción a tiempo frente a un evento que atente a la continuidad del negocio.

3.5.2. Desarrollo de estrategias de recuperación

Backup

En base al servicio crítico, el tiempo de operación, horas de mayor demanda se tiene las siguientes políticas para la realización de backups.

- Se deben realizar backup de tipo snapshot de cada una de las máquinas virtuales de modo que la captura se la realice con los últimos cambios generados.
- Los respaldos se deberán almacenar en una cloud perteneciente a una cuenta propia del CPD.
- Se debe realizar los snapshot una vez por semana, los días viernes a partir de las 20:00.
- Los backup deberán mantenerse de manera que se tenga una versión anterior al último snapshot realizado.

Energías alternas

Para el sistema energético del CPD se cuenta con un sistema redundante de modo que los servidores no se vean afectados ante una pérdida de energía eléctrica para ello se alimenta de dos líneas de tensión distintas, es así que al formar parte de la institución lo cual lo hace susceptible a una perdida completa de las continuidad energética, por dicho motivo para sustentar el riesgo de una perdida de suministro energético se recomienda el uso de un sistema híbrido de energización, en el cual se use una fuente alterna fuera de la convencional, una de estas alternativas es un sistema de fotovoltaico con la ventaja radica en que con un correcto dimensionamiento tiene la capacidad de proveer de la energía necesaria, además que por provenir del aprovechamiento de la energía solar la hace una fuente no contaminante y con una vida útil de

aproximadamente 30 años, lo cual junto con el sistema existente la posibilidad que el CPD se encuentre sin energía es mínima.

Climatización

Siendo el CPD un lugar en el que se encuentra equipos de alta densidad los cuales por el trabajo que desempañan generan un porcentaje de calor considerable, de modo que es de vital importancia mantener y cuidar el estado de los componentes, siendo así que actualmente el entorno a nivel de climatización cuenta con un aire acondicionado de precisión, evidenciando que si éste llagase a fallar no hay nada que lo pueda suplir, para ello como medida preventiva se propone el agregado de un sistema de acondicionamiento ambiental extra, para que de este modo se tenga un arreglo de N+1.

Monitoreo en tiempo real

Dentro de un ambiente donde se hospedan una variedad de equipos mismos que en conjunto brindan un servicio para distintas disciplinas como académico, investigativo, de modo que el manejo y mantenimiento de los servicios de todos sus componentes que se encuentren involucrados es de vital importancia para el desarrollo de las actividades que se encuentren desempeñando, siendo así que actualmente el CPD cuenta con plataformas de monitoreo de variables ambientales, componentes físicos y el aprovisionamiento de los servicios los cuales se encuentran en funcionamiento durante 24 horas los 7 días de los cuales el monitoreo completo se lo tiene desde el Lunes hasta Sábado en un horario de 7:00 a 20:00, además se añade que estos sistemas de monitoreo envía un reporte del estado actual a los correos institucionales de los miembros encargados del manejo del entorno, de modo que el tiempo de reacción ente una variación desfavorable sea minimizado mientras que se previene y mitigar una potencial causa de interrupción de los servicios.

Se propone un agregado dentro del sistema de monitoreo para mantener la continuidad, es así que para ello se recomienda el uso de herramientas de acceso que permita una administración remota la misma la cual viabilice el acceso remoto desde cualquier lugar y en todo momento durante 24 horas y los 7 días de la semana, de modo que el personal de monitoreo del CPD en pueda acceder en todo momento, para una respuesta oportuna ante una eventualidad adversa. Otra opción para el monitoreo continuo es el agregado de accesos VPN mismos que se deberán generar en base a perfiles de usuarios pertenecientes al área de monitoreo.

Control de acceso físico

Siendo el CPD un lugar que cuenta con una infraestructura e información de alto valor es necesario el control del área física, de modo que actualmente para el cumplimiento de ésta tarea, cuenta con un sistema de acceso biométrico ZKTeco en el cual se encuentra registrado todo el personal autorizado de los cuales se encuentra almacenado registrando el nombre, rol, horario de acceso, nivel de acceso (lugares a donde se puede acceder), con lo cual se mantiene un control el cual muestra la siguiente información: fecha, hora, lugar, medio de acceso (huella o tarjeta), por otro lado para la parte de invitados el acceso se lo realiza mediante el uso único de tarjetas magnéticas las cuales se encuentra asignado a un usuario invitado mismo que es de uso general en el cual solo se modifican los nivel de acceso y los horarios, evidenciando una falla en control de acceso de usuarios invitados, para ello se propone el uso de un registro de invitados más estricto en el cual se coloque nombre, apellido, entidad a la que pertenece, la fecha que se entregó la tarjeta, los niveles de acceso, los días y las horas en las que se podrá acceder con dicho medio por parte del CPD, como se muestra en los anexos.

Al ser el CPD parte de una institución educativa se encuentra sujeta a las políticas de acceso de la misma, de modo que se recomienda convenir entre ambas partes para la mejora de acceso a estos sitios de alto nivel crítico, con la finalidad de mantener un mejor de ingreso de los usuarios a estas instancias.

3.6. Asignación de roles y responsabilidades

La identificación de los roles y responsabilidades de cada uno de los actores junto con una correcta asignación de las actividades, representa una parte fundamental dentro del manejo de las labores llevadas a cabo en el CPD, debido que una designación adecuada da forma a un equipo de trabajo eficiente y ágil, con una capacidad de respuesta rápida.

3.6.1. Gobernanza y gestión

De acuerdo a COBIT y su 5to principio el cual es “Separar el gobierno de la administración”, de modo que la gobernanza se encuentra orientada al cumplimiento de los objetivos, mientras que la gestión se enfoca en la administración, siendo así que para el CPD.

El proceso de evaluación se lo realiza de forma vertical en un sentido bidireccional el mismo que inicia en consejo de carrera, pasando a la siguiente instancia que es dirección de carrera siendo esta la encargada de la dirección de las actividades, el siguiente ente es el administrador el cual cumple las funciones de monitoreo y la verificación de las acciones que se llevan a cabo dando cumplimiento a los objetivos de la carrera. Por otro lado, se encuentra la parte administradora en la cual se tiene dos entidades, se maneja de manera horizontal, dado que se cumple con la planificación, construcción, operación y monitoreo de los servicios dados por parte del CPD, además

que la administración se comunica directamente con la parte administradora, para el cumplimiento de metas y objetivos. Como se muestra en la Figura9

Organización del CPD

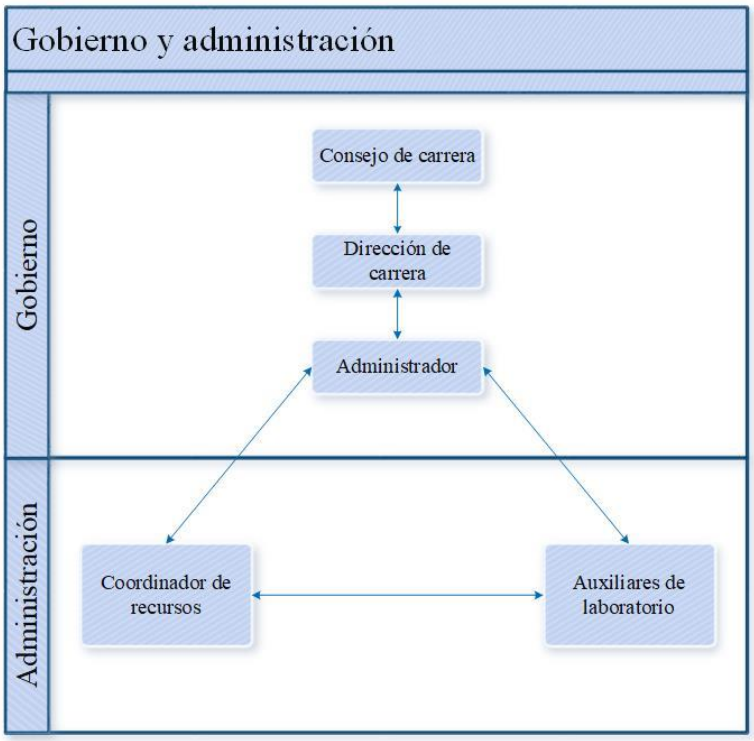


Figura 9. Gobierno y administración del CPD
Realizado por: Thalia Ati

3.6.2. Roles y responsabilidades

Dentro del CPD se cuenta con una organización donde cada uno de los actores cumple una función pre establecida, mismas que son designadas con la visión de cumplir los objetivos de la carrera, para ello una correcta la asignación de los roles y las responsabilidades que cada uno debe cumplir, forma parte de un momento vital.

Siendo así que a partir de esta instancia se determinará el grupo de trabajo de acuerdo a las habilidades que cada uno de los miembros tenga, de modo que se obtenga el mejor resultado, además que así se viabiliza la delimitación de las actividades que cada miembro debe cumplir, promoviendo la seguridad debido a que en caso de algún fallo u atentado a las operaciones normales ya se tendrá las acciones a ser realizadas, junto con el miembro que las llevara a cabo, de modo que cada trabajo se realice de la mejor

manera mediante acciones de detección, corrección, mitigación del objeto o evento que se encuentre generando problemas.

Es así que para la designación de las actividades y los roles que cada actor cumple dentro del CPD, se lo realiza mediante el uso de una matriz RACI la cual se encuentra definido dentro de los marcos de referencia COBIT y ITIL para la determinación de los roles y responsabilidades.

Tabla 12. Matriz RACI

ROL / Actividad	Consejo de carrera	Dirección de carrera	Administrador	Coordinador de recursos	Auxiliar 1	Auxiliar 2
Evaluación de daños	I	I	R	R	R	R
Comunicación de crisis	I	I	R	I	R	R
Restauración de servicios		I	I	C	R	R
Restauración de conectividad		I	I	C	R	R
Reporte de evento		R	R	R	R	R
Reporte de incidencia		I	I	I	R	R
Recuperación de capacidad de gestión			R	I	R	R
Mantenimiento del plan			A	I	R	R
Reanudación de operaciones	I	I	A	C	R	R
Acciones correctivas		I	A	C	R	R

Nota: La tabla corresponde a la asignación de roles y responsabilidades

Las actividades que cada miembro del CPD debe llevar a cabo esta descrita mediante RACI donde R es hacer, es decir el responsable de la tarea; A es aprobación, es decir que es la verificación de que las acciones realizadas están correctas; C es consultar, de modo que habla de la consulta de acciones a ser tomadas antes de ser realizadas; I representa informado de modo que es a quien se le informa de las acciones o resultados obtenidos.(«Qué es una matriz RACI», 2015)

De acuerdo con la Tabla 12, se encuentran descritas las actividades y los roles de acuerdo a la gobernanza mostrada en la Figura9. Las actividades descritas son una serie de acciones a ser realizadas ante un evento que atente con la continuidad de las operaciones, de modo que se minimice le tiempo de respuesta y recuperación del CPD.

3.6.3. Flujo de comunicación

La comunicación interna durante, antes y después de un evento de desastre es vital debido a que con este se puede informar de manera eficiente y rápida a todos los miembros necesarios del escenario o en caso de emergencia a las organizaciones de defensa correspondientes.

Forma de comunicación dentro del CPD ante un evento de desastre

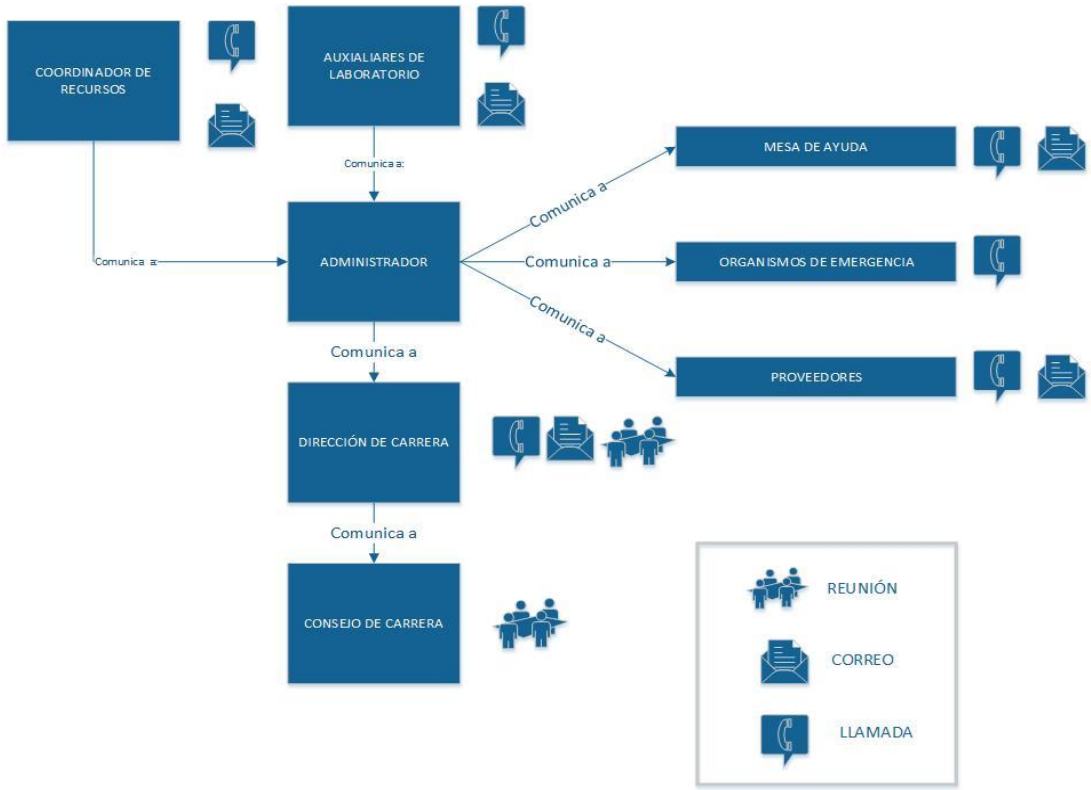


Figura 10. Flujo de comunicación.
Realizado por: Thalia Ati

Siendo así que ante un evento que atente a las operaciones normales del CPD es necesario la comunicación ya sea para realizar acciones de mitigación, corrección o prevención es necesario que se las comunique y sean aprobadas, para ello dentro de

este entorno la comunicación es bidireccional con los miembros de la gobernanza mostrada en la Figura 9, mientras que hacia medios externos o servicios fuera de la organización se la realiza a través de otra instancia.

Por ello en la Figura 10 se muestra la comunicación y lo medios que se usan como: correo electrónico, llamadas o reuniones de pendiendo del caso, además los entes que se comunican, siendo así que tanto auxiliares como coordinador se comunican con el administrador, el cual está encargado de comunicarse con la mesa de ayuda, organismos de emergencia y proveedores, además también se comunica con dirección de carrera, siendo así que desde este punto se comunique a través de reuniones con consejo de carrera. Cabe mencionar que al ser una institución la comunicación con los organismos de defensa dependiendo del caso emergente se la puede realizar desde cualquiera de las instancias antes expuestas.

3.7. Mantenimiento del plan

El CPD es un ambiente el cual está sujeto a cambios, modificaciones o actualizaciones mismas ya se las realiza para la mejora para resguardar la información que se encuentra dentro de este escenario, por este motivo el plan de recuperación de desastres debe ir de la mano con los cambios que se vayan presentando en el desarrollo de las operaciones, de modo que éste se encuentre actualizado y de acuerdo al escenario más actual en el cual se pueda encontrar, para que así de un evento de desastre este sea efectivo sabiendo que éste contiene la información necesaria para la minimización del impacto y tiempos que afecten a los servicios brindados.

3.7.1. Tipos de cambios que afectan al plan

Como es un lugar sujeto a cambios de distintas índoles, se debe tomar en cuenta que existen variaciones mismas que no afectan directamente sobre el plan ya que estas

pueden estar contenidas dentro de lo desarrollado, pues bien, si por el contrario los cambios son evidenciables estos afectan directamente al plan siendo que es necesario una actualización o mejora del plan, de modo que los casos en que es necesario realizar estas acciones se describen a continuación

Hardware siendo que se puede añadir, mover o actualizar algún componente físico del CPD, lo cual causa una variación del ambiente evidenciando la necesidad de realizar una actualización al plan que se encuentre manejando, de modo que siga acorde al entorno en el cual se desplegaría.

Software, al ser el CPD un lugar donde el principal servicio es de virtualización es importante contemplar que el software debe mantenerse actualizado, ya que debido al avance tecnológico debe contemplar ciertos cambios mismos que como en el caso anterior hace evidente una actualización del plan.

Personal del CPD, cada miembro que forma parte del entorno juega un papel importante ya que sobre ellos se encuentra designadas un rol y responsabilidades que están cumpliendo, si llegase a faltar o que aumentase uno se debería nuevamente redistribuir las actividades que se desarrollan.

Ahora bien, una vez que se han contemplado los factores internos que hacen evidente el mater un plan actualizado y acorde con el escenario, hay que hablar de los factores externos que podrían realizar cambios sobre las actividades, procesos y procedimientos que se lleven a cabo.

Uno de los factores externos que puede causar un cambio en el CPD es el cambio de las leyes a las cuales se encuentra sujeto, otro factor son los cambios en el modelo de negocio, además por otra parte independientemente que ser realice o no un cambio el plan debe ser sometido a un mantenimiento periódico mismo que para este caso se lo

recomienda que sea realizado al menos una vez por año, de modo que siempre se encuentre adaptado al medio donde se lo desplegará.

3.8. Manejo del plan

El plan de recuperación de desastre contiene los parametrtos necesarios para el despliege del mismo cuando sea necesario, pero si bien encuentra esta información no significa que se conozca el forma de manejar dicho plan.

Dentro del plan se encuentra contempladas los riesgos, vulnerabilidades y amenazas que el escenario presenta de modo que mediante la identificación de los riesgos se generó las medidas que permitan contrarrestar el impacto que estas puedan tener, asi tambien de determino los tiempos o el punto objetivo al cual se desea regresar donde dicho estado es considerodo el momento donde se encontraba con las operaciones normales, es decir, para así reaudar las actividades que se encontraba desarrollando sobre el entorno, pero esto no es suficiente para el despliege del plan para ello se debe contar con un equipo el cual tenga identificados con claridad las acciones que se deben realizar ante la presencia de un evento de desastre o que atente a la continuidad del negocio, esté grupo debe tener el conocimiento de las acciones y el orden en el cual se debe realizar dichos procesos.

Es asi que el despligue de éste plan inicia a partir del evento de desastre continuando por una serie de acciones que deben ser realizadas hasta llegar el cierre mismo que finaliza con el infarmar que no es mas que un registro del evento ocurrido.

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

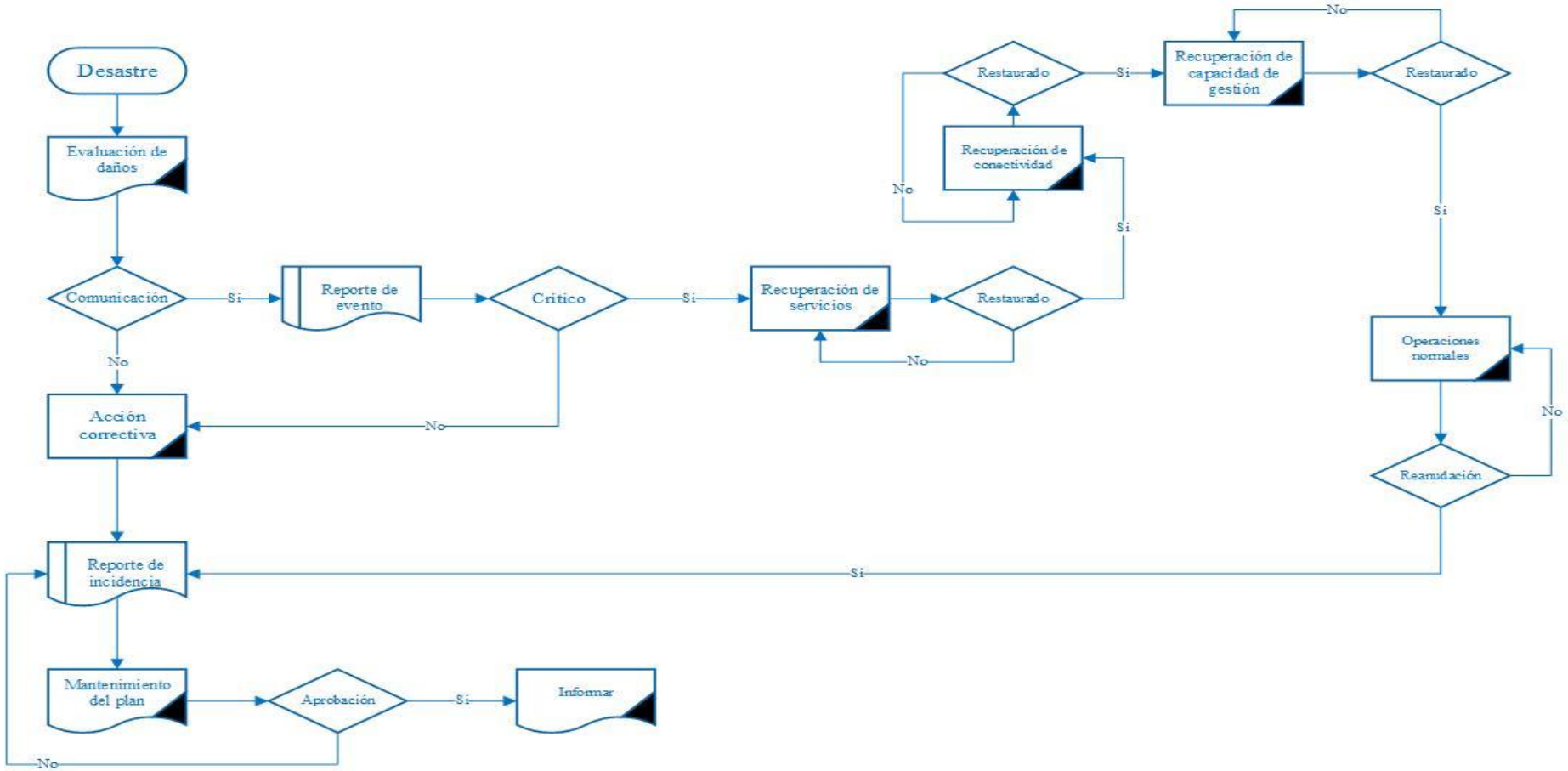


Figura 11. Flujograma del manejo del plan.
Realizado por: Thalia Ati

En la figura 11, se encuentra la forma de uso del plan, el cual inicia desde la presencia del evento de desastre, una vez que ha terminado el siguiente paso es la evaluación de los daños, en base a este decide si se lo comunica o no, ya que dependiendo del daño este necesitaría otro tipo de tratamiento, de modo que si no se comunica se procede a la realización de las actividades de corrección, a continuación se reporta el incidente, además que se realizan los cambio necesarios sobre el plan, si se lo aprueba este es informado a los miembros pertinente necesarios; en caso de que se decidió el comunicar se determina si los daños son críticos o no en caso de no serlo, se procede a la corrección y se continua con el proceso, si es crítico la siguiente instancia es la recuperación de los servicios, dentro de este se realizan las actividades de restauración de datos, reemplazo de equipos, corrección de errores del sistema, una vez que se ha restaurado se procede a la recuperación de la conectividad de modo que los usuarios puedan acceder remotamente a los servicios provistos, una vez que se establezcan de manera adecuada se procede al momento de recuperar la capacidad de gestión misma que permite la administración, monitoreo de los servicios y todos los componentes del CPD, a continuación se comprueba que se encuentren las operaciones normales ya con esta etapa finalizada se procede con el reporte de incidencia en el cual se encuentra detalladas todas las acciones antes mencionadas, desde este punto continua con el proceso que se describió anteriormente.

CONCLUSIONES

- Mediante la elaboración del plan se logró la identificación de riegos y vulnerabilidades que se encuentran latentes dentro del CPD, siendo así que se evidencia la necesidad de una intervención urgente en la cual se desarrolle medidas de mitigación, corrección y prevención, ya que dentro de este entorno se almacena y procesa datos de distintas índoles académicas como: desarrollo investigativo y tecnológico.
- Adicionalmente se logró la identificación de los factores que tienen una probabilidad de generar interrupciones en la continuidad de los servicios, de modo que se ha reconocido cuáles son los componentes físicos y lógicos que se encuentran formando parte del CPD, de esta manera se determinó la criticidad que cada uno de ellos tiene, para tener la capacidad de definir la secuencia en la cual se deberán realizar las de acciones para recuperar las operaciones normales.
- Mediante el análisis de impacto realizado se evidenció que el CPD no cuenta con un punto de restauración debido a que no tiene ningún tipo de políticas de respaldo, además que el tiempo de respuesta junto con el tiempo de recuperación mínimos para la realización de las actividades de restauración fueron determinados en base a los riesgos identificados, como resultado de esto el plan de recuperación de desastres y continuidad de negocios contiene una serie de acciones ordenadas a ser realizadas con el fin de responder ante una eventualidad de desastre, además está conformado por dos enfoques uno preventivo y otro correctivo, orientadas a la restauración de las operaciones normales después de la acción de un evento que ponga en riesgo la continuidad

de los servicios prestados por el CPD, de modo que el tiempo que dure la interrupción sea mínimo y que la afectación generada sea de bajo impacto.

- El plan de recuperación de desastres y continuidad de negocio está compuesto por el inventario de los equipos y el software con el que cuenta el CPD, además de las especiaciones de los tiempos que se tiene para la realización de las actividades, en este también se incorpora los roles y responsabilidades de cada actor deberá cumplir en caso de un desastre, adicionalmente se ha definido el proceso mediante el cual debe ser desplegado el plan.
- Gracias al desarrollo del presente proyecto de titulación se ha obtenido una documentación adecuada que se ajusta al estado actual del CPD, la cuela está compuesta por información necesaria para contrarrestar acciones que atenten a las operaciones normales, de modo que tenga una capacidad de respuesta eficiente y eficaz.

RECOMENDACIONES

- Desarrollar los planes de emergencias y de contingencias mismos que se encuentran contemplados dentro del plan de continuidad del negocio, adicionalmente a estos planes se le debe ir realizando los cambios pertinentes al plan de recuperación, de modo que todo en conjunto mitiguen los riesgos, vulnerabilidades y amenazas detectados.
- Realizar la automatización de todos los procesos y procedimientos necesarios para la generación de respaldos remotos, de modo que en caso de la presencia de un evento de desastre el CPD tenga la capacidad de regresar a un estado anterior donde las operaciones son llevadas a cabo de forma normal.
- Someter al CPD sea a un proceso de auditoria mismo que permita determinar el nivel de madurez, definir los procesos y procedimientos que se encuentran llevando a cabo, permitiendo así que se lleve de mejor manera la gestión de los recursos a más de brindar los puntos clave para mejorar la seguridad con la que cuenta.
- En base al desarrollo del plan de recuperación de desastres y continuidad del negocio, se detectó que tanto el sistema de climatización y energización no cuentan con un sistema de respaldo, por dicho es importante que a la climatización se le añada un elemento de redundancia, mientras que para el sistema de energización se le añada un sistema de energía alterna propio del CPD.

LISTA DE REFERENCIAS

1.- Tipos y Fases de Desastres.pdf. (s. f.). Recuperado a partir de http://www.ispch.cl/sites/default/files/1.-%20Tipos%20y%20Fases%20de%20Desastres.pdf

4 pasos para armar un Plan de Continuidad del Negocio. (2014, mayo 14). Recuperado 28 de junio de 2018, a partir de https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/

Acondicionamiento en Data Center. (s. f.). Recuperado 19 de junio de 2018, a partir de https://www.mundohvacr.com.mx/2009/04/acondicionamiento-en-data-center/

Activo (seguridad informática) - Copro, la enciclopedia libre. (s. f.). Recuperado 28 de junio de 2018, a partir de https://copro.com.ar/Activo_(seguridad_informatica).html

AKROS. (2016, enero). Proceso de mesa de ayuda AKROS. Recuperado a partir de C:\Users\Administrador.DESKTOP-3Q9TG3I\Documents\Plagecons\Proceso de Mesa de Ayuda V.2

Amenazas a la Seguridad de la Información | Departamento de Seguridad Informática. (s. f.). Recuperado 14 de mayo de 2018, a partir de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Business Impact Analysis (BIA) y la importancia de priorizar procesos. (2014, noviembre 6). Recuperado 28 de junio de 2018, a partir de https://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

Concepto de desastre - Definición en DeConceptos.com. (s. f.). Recuperado 12 de mayo de 2018, a partir de https://deconceptos.com/ciencias-naturales/desastre

¿En qué consiste un Plan de Recuperación ante Desastres (DRP)? (2014a, octubre 14). Recuperado 28 de junio de 2018, a partir de https://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/

¿En qué consiste un Plan de Recuperación ante Desastres (DRP)? (2014b, octubre 14). Recuperado 29 de mayo de 2018, a partir de https://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/

Gestión de la Continuidad de servicios TI > Proceso [Curso ITIL® Foundation > Diseño de los Servicios TI]. (s. f.). Recuperado 23 de mayo de 2018, a partir de http://faquinones.com/gestiondeserviciosit/itilv3/diseno_servicios_TI/gestion_continuidad_servicios_ti/proceso.php

GUIA PARA ELABORAR UN PLAN DE CONTINGENCIA INFORMATICO | IT VDELGADO. (s. f.). Recuperado 26 de mayo de 2018, a partir de https://victdelr.wordpress.com/category/guia-para-elaborar-un-plan-de-contingencia-informatico/

Ibarra, J. Á. P. (s. f.). CobiT aplicado para asegurar la continuidad de las operaciones. *IT GOVERNANCE*, 26.

Los 7 mandamientos de un buen Plan de Continuidad de negocio. (2016, julio 25). Recuperado 28 de mayo de 2018, a partir de https://www.claranet.es/blog/los-7-mandamientos-de-un-buen-plan-de-continuidad-de-negocio

Manual_continuidad_negocio.pdf. (s. f.). Recuperado a partir de https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf

Monitoreo DataCenter. (s. f.). Recuperado 18 de junio de 2018, a partir de http://www.etherpower.net/cms/index.php/monitoreo-datacenter/#.Wyg_uaczbIU

nte_iso_iec_27031.pdf. (s. f.). Recuperado a partir de http://181.112.149.204/buzon/normas/nte_iso_iec_27031.pdf

ORTEGÓN, M. A. C., & SÁNCHEZ, C. C. G. (2015). DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES EN EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA FUNDACIÓN NEUMOLÓGICA COLOMBIANA, 62.

Plan de contingencia en seguridad Informática - EcuRed. (s. f.). Recuperado 12 de mayo de 2018, a partir de https://www.ecured.cu/Plan_de_contingencia_en_seguridad_Inform%C3%A1tica

¿Qué es Backup? - Su Definición, Concepto y Significado. (s. f.). Recuperado 18 de junio de 2018, a partir de http://conceptodefinicion.de/backup/

¿Qué es la seguridad informática y cómo puede ayudarme? | VIU. (s. f.). Recuperado 29 de mayo de 2018, a partir de https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/

¿Qué es norma ISO 22301? (s. f.). Recuperado 29 de mayo de 2018, a partir de https://advisera.com/27001academy/es/que-es-iso-22301/

¿Qué es ¿Qué es Plan de Recuperación de Desastres (DRP)?? - Definición en WhatIs.com. (s. f.). Recuperado 28 de junio de 2018, a partir de https://searchdatacenter.techtarget.com/es/definicion/Que-es-Plan-de-Recuperacion-de-Desastres-DRP

Que es un plan de contingencia. (s. f.). Recuperado 26 de mayo de 2018, a partir de http://www.forodeseguridad.com/artic/discipl/4132.htm

Qué es una matriz RACI. (2015, febrero 27). Recuperado 23 de junio de 2018, a partir de http://www.cantabriatic.com/que-es-una-matriz-raci/

¿Qué son las energías alternativas? - ¿Sabías que? - Compromiso RSE. (s. f.). Recuperado 18 de junio de 2018, a partir de http://www.compromisorse.com/sabias-que/2010/03/30/que-son-las-energias-alternativas/

Seguridad Informatica / Plan de Contingencia. (s. f.). Recuperado 26 de mayo de 2018, a partir de https://www.segu-info.com.ar/politicas/contingencia.htm

Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? - Aprende a Programar - Codejobs. (s. f.). Recuperado 28 de junio de 2018, a partir de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Selva, G. (2018, febrero 20). ¿Qué es un backup? Y, ¿Cuáles son los beneficios de realizarlo? | Clavei. Recuperado 18 de junio de 2018, a partir de https://www.clavei.es/blog/backup-que-es/

Tipos de desastres naturales. (2017, diciembre 2). Recuperado 29 de mayo de 2018, a partir de https://tiposde.eu/tipos-de-desastres-naturales/

ANEXOS

Registro de acceso a usuarios invitados o temporales

Modelo de formato de registro de acceso a usuarios invitados, mismo que se encuentra en formato Excel por lo cual se adjunta en un documento grabado en el CD.

Formato de registro de usuarios invitados.

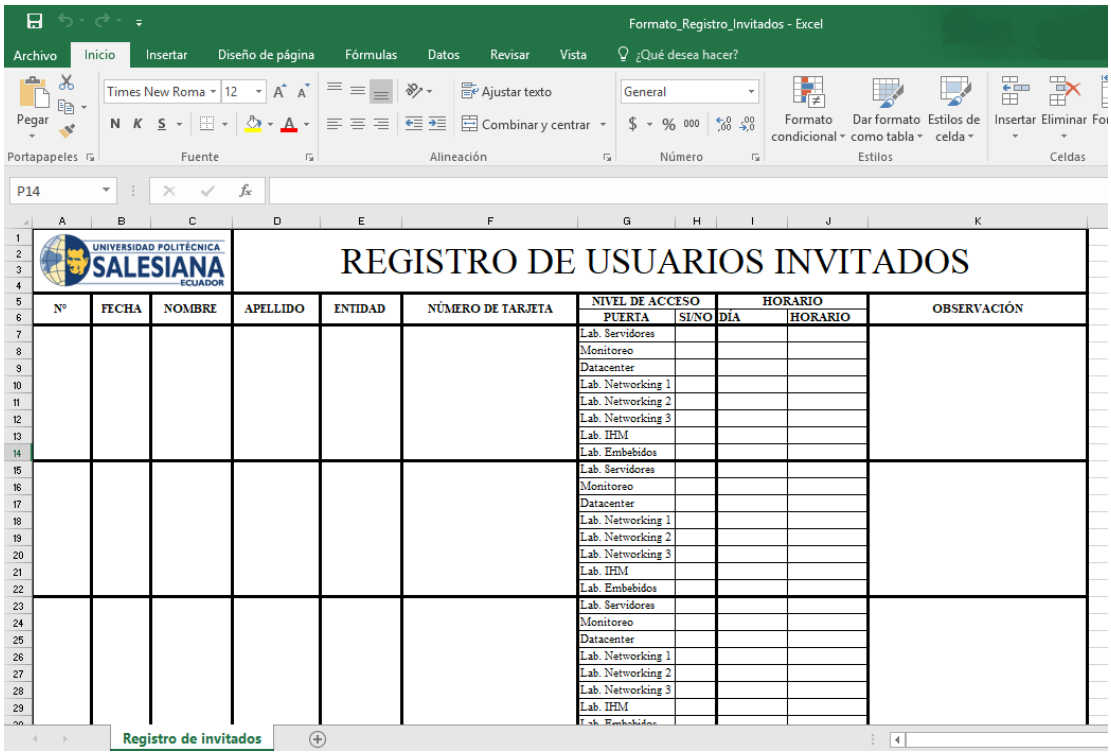


Figura 12. Registro de usuarios invitados
Elaborado por: Thalia Ati

Plan de recuperación de desastres y continuidad del negocio

A continuación, se presenta el plan de recuperación de desastres, el cual será desplegado cuando se necesario, además que las tablas de revisión de inventario, reporte de evento para evaluación de los daños y reporte de las incidencias

CENTRO DE PROCESAMIENTO DE DATOS(CPD)

PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DE NEGOCIO

UNVERSIDAD POLITÉCNICA SALESIANA

Versión 1.0

1. Introducción

Este plan es desarrollado con el fin de brindar el procedimiento con las medidas a ser desplegadas frente a una eventualidad que atente con las operaciones normales es así que la carrera de Ingeniería en Ciencias de la Computación, de la Universidad Politécnica Salesiana, sede Quito, Campus Sur, actualmente cuenta con un recién implementado Centro de Procesamiento de Datos (CPD), el cual consta de: servidores, almacén de datos, dispositivos de comunicación de datos, equipos de control ambiental y energización, en este medio se encuentra albergada información y servicios para tres grandes campos académicos e investigativos tales como; material académico de las cátedras dictadas, tesis de grado y post-grado, investigaciones de proyectos doctorales e investigaciones de proyectos interdisciplinarios.

2. Objetivos y alcance

2.1. Objetivos

Diseñar un plan de recuperación de desastres y continuidad del negocio basado en COBIT, ITIL y de acuerdo a la norma ISO 22301, para el Centro de Procesamiento de Datos de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Salesiana, Sede Quito, Campus Sur.

2.2. Objetivos específicos

- Identificar los riesgos y vulnerabilidades del Centro de Procesamiento de Datos para la aplicación de acciones para la mitigación de los mismos.
- Desarrollar el plan de continuidad de negocio y de recuperación de desastres para mitigar el impacto recibido sobre el Centro de Procesamiento de Datos ante la posibilidad un evento de desastre de modo que las actividades no se vean mayormente afectadas.

2.3. Alcance

Ser identificaran los activos críticos, además se presentará los procesos y procedimientos a realizarse ante cualquier eventualidad anormal o sorpresiva que atente a la ininterrupción de los servicios prestados o perdida de información almacenada dentro del Centro de Procesamiento de Datos, además que así se asegura que el impacto a los usuarios de aquellos servicios e información albergados en este escenario sea mínimo, de tal modo que estos no se van mayormente afectados bajo ninguna circunstancia.

Con el fin de minimizar las interrupciones y pérdidas tanto de servicios como información, se detectará los activos físicos y lógicos que son críticos, para de esta manera enfrentar posibles desastres que imposibilitan, afectan o atentan a la integridad de las funciones normales del Centro de Procesamiento de Datos, para que este sea capaz de mantener o reanudar rápidamente sus funciones.

3. Desastres

Es un hecho que se lo denomina catastrófico el cual no es predecible, es decir que no se tiene el completo conocimiento de cuál será la magnitud y área en la que se presenten daños que afecten de manera grave a la sociedad, tampoco se tiene conocimiento en qué momento determinado se presentará un evento que trastorne agresivamente la continuidad de las actividades productivas.

Al hablar de desastre se contemplan dos áreas que afectan directamente a un centro de datos, una de ellas son los desastres informáticos los cuales se pueden presentar a partir de ataques de niveles físicos y lógicos, es decir ataques al hardware y software, errores humanos, etc. Otra área abarca los desastres naturales, los mismos que no se puede predecir cuándo, cómo o cuál es su nivel de impacto en la sociedad.

4. Evaluación de riegos

L a evaluación de riesgos se la realizo mediante la identificación de los mismos junto con los activos que forman parte del CPD, de modo que se valora de la siguiente manera

Impacto		
1	Baja	
2	Media-baja	
3	Media	
4	Media-alta	
5	Alta	

Criticidad			
1	Baja	1% -20%	
2	Media-baja	21% - 40%	
3	Media	41% -60%	
4	Media-alta	61% - 80%	
5	Alta	81% -100%	

De tal manera que la valoración queda de la siguiente manera

Riesgo / Parámetro	Suministro eléctrico	Inundación	Sismo	Viento fuerte	Incendio	Tormenta Eléctrica	Erupción volcánica	Manifestaciones civiles violentas	Atentado terrorista	Ataques informáticos	Negligencia	Climatización
Probabilidad	2	1	4	1	3	5	3	1	1	5	1	2
Consecuencias	5	1	4	2	5	3	5	2	5	5	5	5
Ocurrencia	2	1	3	1	1	5	2	1	1	3	1	1
Urgencia	5	2	4	2	5	2	5	1	5	5	5	5
Maleabilidad	4	3	4	3	4	3	2	4	1	1	5	2
Dependencia	5	1	5	3	5	4	5	3	5	5	5	5
Proximidad	2	1	3	1	1	3	2	1	1	5	1	1
Total	25	10	27	13	24	25	24	13	19	29	23	21
Porcentaje de afecciones por cada riesgo	71	29	77	37	69	71	69	37	54	83	66	60
Criticidad	4	2	4	3	4	4	4	2	3	5	4	3

5. Análisis de impacto

La identificación de los procesos y procedimientos de todos los servicios principales de modo que se realicen se identifiquen todas las actividades críticas además de los servicios mínimos para que se el tiempo que dure la interrupción se lo mas corto, así también establecer el tiempo estimado de recuperación (RTO) y el punto de recuperación objetivo (RPO).

En base a la información obtenida se tiene que el punto objetivo de restauración en base al diseño de la infraestructura y a la entrevista realizada los operadores del CPD se tiene que no cuenta con un proceso de backup, por lo cual en caso de desastre la recuperación de la información sería un proceso con alto grado de dificultad.

Por otro lado la infraestructura del CPD el tiempo que tomaría en restaurar cada activo que forme parte del entorno tiene un tiempo estimado de recuperación frente a uno de riegos de los que fueron identificados anteriormente, como se muestra en la tabla1, donde se especifican los tiempos máximos que la infraestructura no experimentas pérdidas significativas, mismos que se midieron en horas, además que se encuentra distribuida de modo que los activos se encuentren en fila ordenada de manera descendente del mas al menos crítico, mientras que las columnas se localizan los riegos ordenados los cuales se ubican de modo que el primero es el que tiene mayor valor de riesgo y el ultimo es el que menos impacto puede causar, cabe recalcar que los tiempos son los estimados.

Al momento de hablar de RTO es importante destacar que, por ser una infraestructura nueva, ésta se encuentra dentro de un periodo de garantía, de modo que tiene una dependencia de terceros, por dicho motivo el tiempo que tomaría la restauración se acogen a los niveles de soporte dados por el proveedor dentro de los cuales se contemplan 3 niveles de soporte mismos que dependiendo del SLA se acogen a los distintos niveles, además que los tiempos se acogen a los niveles de servicio, siendo así que el tiempo de respuesta es de 1 hora la cual se encuentra comprendida desde que el usuario abre el ticket hasta la asignación de un especialista, el tiempo de solución es aquel que toma solucionar el problema o incidente presentado, y el tiempo de soporte comprende entre el tiempo que está disponible el servicio de soporte

Riesgo / Activo	Ataque informático	Sismo	Suministro eléctrico	Tormenta eléctrica	Incendio	Erupción volcánica	Negligencia	Climatización	Atentado terrorista	Viento fuerte	Manifestación civil violenta	Inundación
Servidores	2	24	2	0,3	Ind	24	1	0,5	ind	2	2	1
Almacenamiento	2	24	2	0,3	Ind	24	1	0,5	ind	2	2	1
Switch SAN	2	24	2	0,3	Ind	24	1	0,5	ind	2	2	1
Software de administración y gestión	2	24	2	0,3	Ind	24	1	N/A	ind	N/A	N/A	N/A
Hipervisor	2	24	2	0,3	Ind	24	1	N/A	ind	N/A	N/A	N/A
Core	2	24	2	1	Ind	N/A	2	5	ind	N/A	N/A	2
Sistema de energía continua	N/A	24	2	0,3	Ind	0,5	1	N/A	ind	2	2	0,5
Software de Monitoreo	8	N/A	4	N/A	Ind	N/A	5	N/A	ind	N/A	N/A	N/A
Sw administración	2	24	2	0,3	Ind	N/A	1	5	ind	N/A	N/A	2
Climatización	N/A	24	1	0,3	Ind	1	1	1	ind	1	1	1
Equipo de monitoreo	N/A	24	2	1	Ind	3	2	3	ind	N/A	N/A	1
Sw acceso	4	24	2	1	Ind	N/A	2	5	ind	N/A	N/A	2
Varios	N/A	24	4	4	Ind	N/A	5	N/A	ind	N/A	N/A	N/A

Terminología	
ind	indeterminado
N/A	No aplica

6. Estrategias de recuperación

4. Backup

- Se deben realizar backup de tipo snapshot de cada una de las máquinas virtuales de modo que la captura se la realice con los últimos cambios generados.
- Los respaldos se deberán almacenar en una cloud perteneciente a una cuenta propia del CPD.
- Se debe realizar los snapshot una vez por semana, los días viernes a partir de las 20:00.
- Los backup deberán mantenerse de manera que se tenga una versión anterior al último snapshot realizado.

5. Energías alternas

Un sistema híbrido de energización, en el cual se use una fuente alterna fuera de la convencional, una de estas alternativas es un sistema de fotovoltaico con la ventaja radica en que con un correcto dimensionamiento tiene la capacidad de proveer de la energía necesaria.

6. Climatización

Agregado de un sistema de acondicionamiento ambiental extra, para que de este modo se tenga un arreglo de N+1.

7. Monitoreo en tiempo real

Uso de herramientas de acceso que permita una administración remota la misma la cual viabilice el acceso desde cualquier lugar y en todo momento, de modo que el personal de monitoreo del CPD en pueda acceder en todo momento, para una respuesta oportuna ante una eventualidad adversa. Otra opción para el monitoreo continuo es el agregado de accesos VPN mismos que se deberán generar en base a perfiles de usuarios pertenecientes al área de monitoreo.

8. Control de acceso físico

Un registro de invitados más estricto en el cual se coloque nombre, apellido, entidad a la que pertenece, la fecha que se entregó la tarjeta, los niveles de acceso, los días y las horas en las que se podrá acceder con dicho medio por parte del CPD, como se muestra a continuación

7. Roles y responsabilidades

Las actividades que cada miembro del CPD debe llevar a cabo esta descrita mediante RACI donde R es hacer, es decir el responsable de la tarea; A es aprobación, es decir que es la verificación de que las acciones realizadas están correctas; C es consultar, de modo que habla de la consulta de acciones a ser tomadas antes de ser realizadas; I representa informado de modo que es a quien se le informa de las acciones o resultados obtenidos. («Qué es una matriz RACI», 2015)

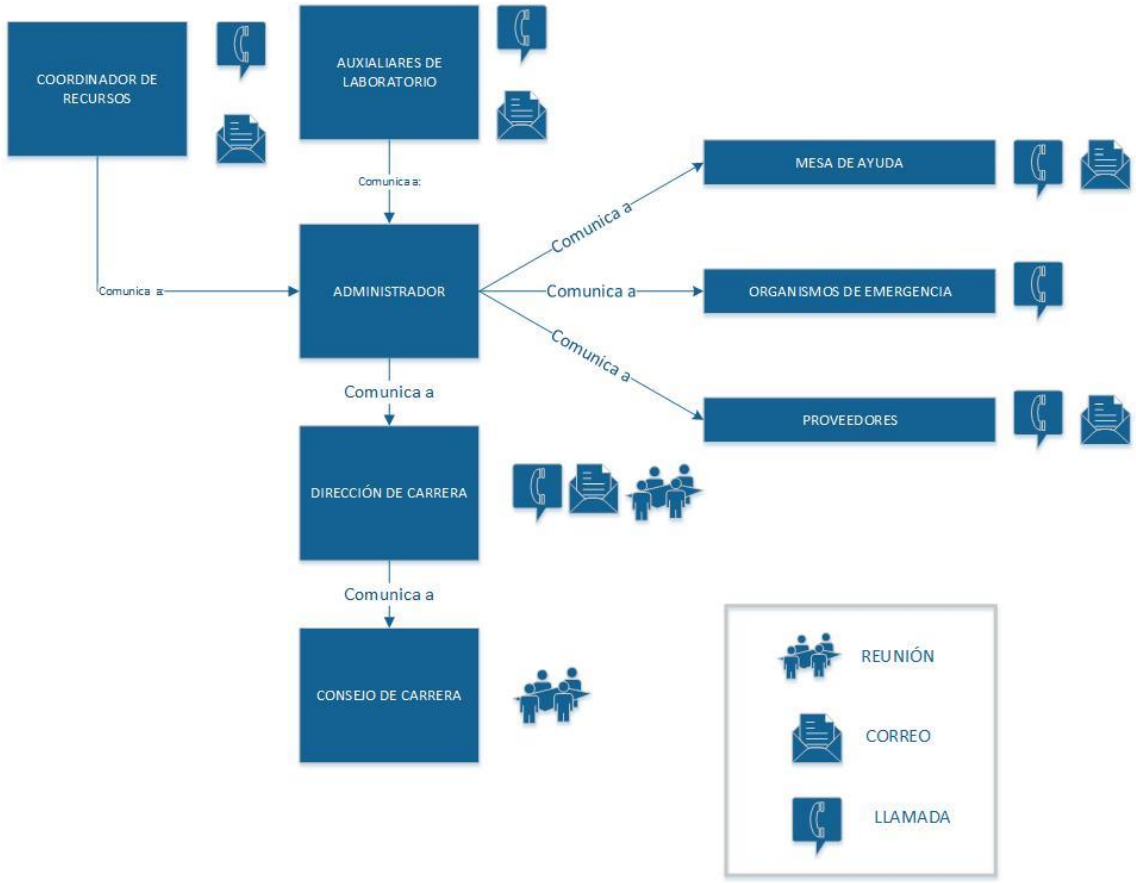
ROL / Actividad	Consejo de carrera	Dirección de carrera	Administrador	Coordinador de recursos	Auxiliar 1	Auxiliar 2
Evaluación de daños	I	I	R	R	R	R
Comunicación de crisis	I	I	R	I	R	R
Restauración de servicios		I	I	C	R	R
Restauración de conectividad		I	I	C	R	R
Reporte de evento		R	R	R	R	R
Reporte de incidencia		I	I	I	R	R
Recuperación de capacidad de gestión			R	I	R	R
Mantenimiento del plan			A	I	R	R
Reanudación de operaciones	I	I	A	C	R	R
Acciones correctivas		I	A	C	R	R

Las actividades mostradas son una serie de acciones a ser realizadas ante un evento que atente con la continuidad de las operaciones, de modo que se minimice le tiempo de respuesta y recuperación del CPD.

7.1. Flujo de comunicación

La comunicación y los medios que se usan como: correo electrónico, llamadas o reuniones de pendiendo del caso, además los entes que se comunican, siendo así que tanto auxiliares como coordinador se comunican con el administrador, el cual está encargado de comunicarse con la mesa de ayuda, organismos de emergencia y proveedores, además también se comunica con dirección de carrera, siendo así que desde este punto se comunique a través de reuniones con consejo de carrera. Cabe mencionar que al ser una institución la comunicación con los

organismos de defensa dependiendo del caso emergente se la puede realizar desde cualquiera de las instancias antes expuestas. Como se muestra a continuación:



8. Despliegue del plan

8.1. Evaluación de daños

Para ello mediante el uso del inventario mostrado a continuación se realiza la evaluación de los daños causados en el cual se registra el activo, si esta correcto o no y las observaciones. Esto será registrado a continuación:

Activos de Hardware

Fabricante	**Descripción**	**Modelo**	**Número de serie**	**Correcto**	**Observaciones**
HPE	Chassis	APOLLO 6000	2M274600VL		
HPE	Servidor	XL230A	2M274600VG		
HPE	Servidor	XL230A	2M274600VH		
HPE	Servidor	XL230A	2M274600VJ		
HPE	Servidor	XL250A	2M274600VK		
HP	Servidor	Proliant DL38067	2M204500J2		

HPE	Storage	3PAR 8200	2M27320157		
HPE	Switch	HPE SN3000B	USB7282019		
HPE	Switch	HPE SN3000B	USB728202E		
Cisco	Switch	SG5550XG	DNI211113VD		
Cisco	Switch	SG5550XG	DNI211113UP		
Cisco	Switch	SG500	DNI2119064R		
Cisco	Switch	Catalyst 9300	FOC2145Z0EZ		
APC	UPS	Symmetra LX	SYA8K16P		
APC	UPS	Symmetra LX	SYA8K16P		
Samsung	Monitor 49inch	LH49PMHP	06S2HCSJB01918A		
Samsung	Monitor 49inch	LH49PMHP	0652HCJB019199K		
Epson	Impresora	L575 MULTIFUNCION	W98Y190439		
DELL	Desktop	OptiPlex 7040	8MFDHD2		
DELL	Desktop	OptiPlex 7040	8MLBHB2		
DELL	Desktop	OptiPlex 7050	3KM0JK2		
GEIST	Watchdog	G1600P			
APC	ATS	AP77504	5A1735T59095		
Cisco	SFP	ENTERPRISE - CLASS	FNS214901EW		
Cisco	SFP	ENTERPRISE - CLASS	AVD2144D2RX		
Cisco	SFP	ENTERPRISE - CLASS	AVD2145D8N1		
Cisco	SFP	ENTERPRISE - CLASS	FNS214901GZ		
Cisco	SFP	ENTERPRISE - CLASS	AVD2144D07A		
Cisco	SFP	ENTERPRISE - CLASS	AVD2145DF6Z		
STULZ	Acondicionamiento de Aire	CompTrol 7000	10061749		

Activos de Software

Nombre de la aplicación	Crucial Sí / No	Activos fijos Sí / No	Fabricante	Correcto	Observaciones
Vmware vSphere 6.5.0	si	si	Vmware		
Vmware vRealize 6.5.0	si	si	Vmware		
Vmware vRealize	si	si	Vmware		

Log Insigth 4.3.0					
Vmware ESXi 6.5.0	si	si	Vmware		
DHCP	si	si	Microsoft		
DNS	si	si	Microsoft		
Active Directory	si	si	Microsoft		
Windows 10	no	si	Microsoft		
pfSense-CE-2.4.3-AMD64	si	si	GNU Linux		
CACTIOS	no	si	GNU Linux		
ZKTeco 3.5.3	no	si	PuisSDK		
Milestone Xprotect 2018 2.1a	si	si	Milestone Systems		
GEIST Watchdog 3.16.3	si	si	GEIST		
HPE 3PAR SSMC	si	si	HPE		

8.2. Reporte de evento

Para el reporte de eventos se la realiza de la siguiente manera:

Evento			
Tiempo de duración del evento:			
Fecha:			
Dispositivo	**Daño**	**Recuperable Si/No**	**Observaciones**

8.2.1. Reporte de incidencia

En este se describe el dispositivo afectado el daño que presentó y la acción realizada para la recuperación del mismo.

Evento				
Tiempo de duración del evento:				
Fecha:				
Dispositivo	**Daño**	**Acción realizada**	**Tiempo de recuperación**	**Observaciones**