UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingeniero de Sistemas

TEMA:
ANÁLISIS, DISEÑO, IMPLEMENTACIÓN Y SOCIALIZACIÓN DEL PLAN DE EMERGENCIA Y CONTINGENCIA PARA EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR, BASADOS EN LA NORMA ISO Y APOYADOS EN EL "FORMATO PARA LA ELABORACIÓN DE PLANES DE EMERGENCIA" QUE RIGE EN EL DISTRITO METROPOLITANO DE QUITO

AUTOR:
JORGE FERNANDO NUÑEZ ZAMBRANO

TUTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, febrero del 2020

CESIÓN DE DERECHOS DE AUTOR

Yo Jorge Fernando Nuñez Zambrano con documento de identificación N° 1711560886, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de titulación intitulado: "ANÁLISIS, DISEÑO, IMPLEMENTACIÓN Y SOCIALIZACIÓN DEL PLAN DE EMERGENCIA Y CONTINGENCIA PARA EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR, BASADOS EN LA NORMA ISO Y APOYADOS EN EL "FORMATO PARA LA ELABORACIÓN DE PLANES DE EMERGENCIA" QUE RIGE EN EL DISTRITO METROPOLITANO DE QUITO", mismo que ha sido desarrollado para optar por el título de: INGENIERO DE SISTEMAS, en la Universidad Politécnica Salesiana, quedando la Universidad faculta da para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, febrero del 2020

.....

JORGE FERNANDO

NUÑEZ ZAMBRANO

CI:1711560886

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, con el tema: ¨ANÁLISIS, DISEÑO,IMPLEMENTACIÓN Y SOCIALIZACIÓN DEL PLAN DE EMERGENCIA Y CONTINGENCIA PARA EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR, BASADOS EN LA NORMA ISO Y APOYADOS EN EL "FORMATO PARA LA ELABORACIÓN DE PLANES DE EMERGENCIA" QUE RIGE EN EL DISTRITO METROPOLITANO DE QUITO¨ realizado por Jorge Fernando Nuñez Zambrano, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, febrero del 2020

……

JORGE ENRIQUE LÓPEZ LOGACHO

CI: 1712082484

DEDICATORIA

El presente trabajo de titulación representa la etapa de culminación de mis estudios universitarios y como no dedicar el mismo primordialmente a mis padres cuya fortaleza y paciencia durante toda mi vida me llevaron a culminar esta etapa de estudios de la mejor manera.

También de manera especial a mi esposa e hijo que son la mayor inspiración para no rendirse y lograr cada uno de los objetivos que me eh prepuesto.

Y a cada una de las personas que a lo largo de mi carrera me supieron alentar y motivar para poder llegar hasta esta etapa.

Jorge Fernando Nuñez Zambrano

AGRADECIMIENTOS

Un agradecimiento infinito a la Universidad Politécnica Salesiana que durante toda mi carrera supo poner en mi camino a docentes y compañeros que contribuyeron para mi formación personal y profesional.

También un agradecimiento especial a mi tutor de tesis, que mediante su guía, directrices y consejos pudimos acabar el presente trabajo de la mejor manera.

Jorge Fernando Nuñez Zambrano

ÍNDICE

Contenido

ÍNDICE DE FIGURAS

Contenido

ÍNDICE DE TABLAS

Contenido

Resumen

El objetivo principal del siguiente proyecto es desarrollar un Plan de Emergencia y Contingencia que se aplicará en el Data Center de la Universidad Politécnica Salesiana Campus Sur, tomando en cuenta los riesgos que pueden causar una posible catástrofe ya sea natural o antrópica. Para eso se tomará como referencia el "Formato del Cuerpo de Bomberos del Distrito Metropolitano de Quito".

Mediante esta implementación se busca eliminar en lo posible pérdidas humanas y mitigar daños materiales, equipos e información importante para la universidad. La implementación se da con la capacitación al personal que usa las instalaciones del bloque D sean estos administrativos, docentes o alumnos. Teniendo en cuenta el plan a desarrollar con indicaciones de evacuación y respaldo de información. Para esto se considera el guiarse por políticas tecnológicas como las Normas ISO 22301 de Continuidad de Negocio. Identificando las vulnerabilidades, los riesgos que se pueden presentar y los elementos de emergencia con los que cuenta el bloque. Para el desarrollo de este plan se considera algunos conceptos tales como: en qué consiste un Data Center y qué es un Plan de Emergencia y Contingencia. En este plan se dará a conocer las medidas de acción que deben tener las personas que se encuentren en el momento de una catástrofe. Se usará la metodología llamada SCRUM que brinda la manera más indicada para llevar acabo el desarrollo de dicho plan. Por último, se brindarán medidas de contingencia y recomendaciones para evitar futuros siniestros o perdida de información del Data Center.

Abstract

The main objective of the following project is the development of the Emergency and Contingency Plan that will be applied in the Data Center of the Salesian Polytechnic University Campus South, considering the risks that can cause a possible natural or anthropic catastrophe. For that, it will be guided in "Formato de el Cuerpo de Bomberos del Distrito Metropolitano de Quito".

This implementation seeks to eliminate human losses and mitigate material damage, equipment and important information for the university. The implementation ends with the training of the administrator and technical operators who use the facilities of block D.

This plan will have evacuation indications and information backup. For this plan will be based technological standards such as the ISO 22301 Business Continuity Standards. Identifying the vulnerabilities, the risks that may arise and the emergency elements that the block has.

For the development of this plan, some concepts such as what is a data center? and what is an emergency and contingency plan? This plan will show actions that the people should follow at catastrophe´s time. The SCRUM methodology will be used for provide the best way to carry out the development of this plan. Finally, contingency measures and recommendations will provide to prevent future claims or loss of information from the Data Center.

CAPÍTULO I

1. Introducción

El presente proyecto de titulación busca implementar dentro del bloque D del Campus Sur de la Universidad Politécnica Salesiana un Plan de Emergencia y Contingencia (PE) para el Data Center de la carrera de Ciencias de Computación. Brindando una mejor herramienta para la prevención y mitigación de emergencias al momento de sufrir un siniestro ya sea el mismo provocado o natural, disminuyendo el riesgo de que suceda algún tipo de accidente o pérdida tanto material o como humana.

Dentro de cada empresa indistintamente cual sea su actividad o tamaño, se debe tener en cuenta un PE debido a que existen muchos eventos externos e internos a los cuales están expuestos sin excepción; estos eventos pueden tener un alto potencial para causar lesiones a las personas, impactos ambientales e inclusive daños a las propiedades.

Tomando en cuenta este precedente se procede a realizar un análisis, diseño, implementación y socialización de un PE para el Data Center de la UPS, este proyecto está basado en el conocimiento adquirido durante los años de estudio en Universidad Politécnica Salesiana apoyado por un extenso trabajo de investigación y la utilización de recursos tecnológicos innovadores.

El documento presentado contiene 4 capítulos, los cuales detallan paso a paso el proceso, materiales, recursos, etc., utilizados para la elaboración y cumplimiento del PE.

1.1. Antecedentes

Hoy en día se vive una era donde los cambios son notables, se han producido cambios basados en avances tecnológicos, optimización de recursos, cambios educativos todos en función de buscar un fin común que es la comodidad y buen vivir en la sociedad, pero existe un cambio que pocas veces es considerado por muchas personas, empresas, instituciones y son cambios naturales, los cuales influyen en comportamientos climáticos, ambientales, naturales, físicos etc.

Tomando en cuenta los cambios explicados anteriormente, aparece una consideración que se debe tomar en cuenta y es que estos cambios tienden muchas veces a provocar algún tipo de desastre, lo que ocasiona que tanto las personas como la infraestructura de los edificios donde se encuentran las empresas puedan sufrir algún percance, y no estén preparados o no sepan cómo actuar en ese momento para poner a salvo su vida y conservar en mayor parte su infraestructura.

La Universidad Politécnica Salesiana se caracteriza por siempre brindar los mejores servicios entre ellos está la innovación, creando espacios de aprendizaje óptimos y de vanguardia para sus alumnos y docentes.

1.2. Problema de Estudio

La UPS dispone de un Data Center (DC) en el cual se guarda y gestiona la información generada exclusivamente por el bloque D, junto con el monitoreo del alumnado y personal de éste bloque.

El problema se enfoca en la carencia de un PE para el Data Center, que permita tomar acciones ante cualquier tipo de desastre que pudiera presentarse, ya sea de tipo antrópico

o por desastre natural, poniendo en riesgo a las personas e infraestructura tecnológica que se encuentra en este lugar.

1.3. Justificación

En el Data Center de la UPS se evidencia la necesidad de plantear e implementar un proyecto que defina el PE, tomando como referencia la vulnerabilidad ante cualquier tipo de desastre natural, sin dejar a lado desastres que se puedan producir por fallas antrópicas netamente; por estos motivos se puede hablar sobre la importancia de tener un procedimiento o manual que permita reaccionar ante catástrofes.

Con este proyecto se pretende analizar los posibles riesgos internos y externos del Data Center y con ello preparar a todas las personas que trabajan en el mismo para dar una respuesta ante situaciones de evacuación, terremotos, incendios, así como eventos sociales y antrópicos que se podrían presentar en un determinado momento, esto con el fin de prevenir o mitigar al máximo los daños sociales, estructurales y de manejo de datos para asegurar que con estos procedimientos se pueda dar la continuidad del negocio en el que está inmerso el Data Center.

Todo esto basado en las normas, conductas y procedimientos dictadas por el máximo organismo de prevención de emergencias que para este caso específico es el Cuerpo de Bomberos del DMQ y dando seguimiento al Manual de Recuperación de Desastres que se encuentra implementado en el Data Center.

1.4. Objetivo General

Analizar, diseñar, implementar y socializar el Plan de Emergencia y Contingencia para el Data Center de la Carrera de Computación de la Universidad Politécnica Salesiana Campus Sur, basados en la Norma ISO y apoyados en el "Formato para la elaboración de Planes de Emergencia" que rige en el Distrito Metropolitano de Quito.

1.5. Objetivos Específicos

Analizar la información necesaria relacionada con infraestructura, seguridades y procesos que se ejecutan en el Data Center.

Identificar los riesgos y vulnerabilidades en los cuales se tenga que aplicar un PE.

Desarrollar el PE para el Data Center basado en el "Formato para la elaboración de planes de Emergencia", aprobada en la Resolución Administrativa No. 036-CG-CBDMQ-2009 que rige para el DMQ.

Desarrollar el Plan de Contingencia del DC para la Universidad Politécnica Salesiana.

Realizar la socialización del PE a los miembros del Comité de Emergencias del Data Center.

CAPÍTULO II

2. Marco Referencial o Institucional

2.1. Universidad Politécnica Salesiana (UPS)

La UPS es una obra de congregación Salesiana e institución de educación superior fundada el 5 de agosto de 1994, con sedes en las ciudades de Cuenca, Guayaquil y Quito respectivamente. La misma está dirigida de forma primordial a jóvenes de los sectores más indefensos de la población ecuatoriana. La misma posee una gran capacidad de investigación e innovación que la ayuda a sostenerse local y nacionalmente durante estos años.

"Según la información de la universidad entre las características más importante para esta institución es tener a bien resguardo la documentación que se maneja para garantizar el buen funcionamiento con eficiencia de los administradores, y tener el control interno de la institución y proteger el patrimonio documental entre otros" (Universidad Salesiana, 2019)

El Campus Sur ubicada en el sector de sur de la ciudad de Quito, es una Sede de la Universidad Politécnica Salesiana. La misma que está estructurada a su alrededor de parqueaderos, patio, áreas verdes. En esta sede se encuentra el bloque D donde está ubicado el Data center. Que a su vez se divide de la siguiente manera:

Primer Piso

- Laboratorios de Networking y Computación Avanzada.
- Baños.

Segundo Piso

- Auditorio José Carolo.
- Salida de Emergencia que dirige al patio principal de la Universidad.
- Ascensor para discapacitados.
- Laboratorio de interfaz humano-maquina.
- Data Center que se encuentra ubicado dentro del aula de laboratorio.

En ambos pisos se distingue señalética básica y elementos de emergencia ante posibles riesgos, cámaras de seguridad, no se observan rutas de evacuación con su respectiva señalética en caso de ser necesario.

En este campus se dictan varias carreras técnicas de tercer nivel como Ingeniería de Sistemas, Electrónica, Mecánica, entre otras. Por lo que existe un flujo considerable de alumnos y personal tanto docente como administrativo.

Bloque D UPS

Figura 1. Fotografías de la UPS Campus Sur, Bloque D Exterior e Interior, Elementos de Emergencia, Aula de Monitoreo, Laboratorio Interfaz Humano – Maquina.
Elaborado por: Jorge Nuñez

2.2. Marco Teórico

2.2.1 Data Center (DC)

Un DC como su nombre indica, es un Centro de Datos o Centro de Proceso de Datos (CPD). Los primeros DC se diseñaron siguiendo las arquitecturas clásicas de informática de red, en las que los equipos eran apilables en mesas, armarios o RACKS. Las necesidades de optimizar espacio físico junto a la capacidad de procesamiento, han permitido que los mismos evolucionen a equipos tan pequeños que son fácilmente ubicados en RACKS y en cuartos de dimensiones no. (¿Qué es un Data Center? - acens blog, 2008)

Data Center

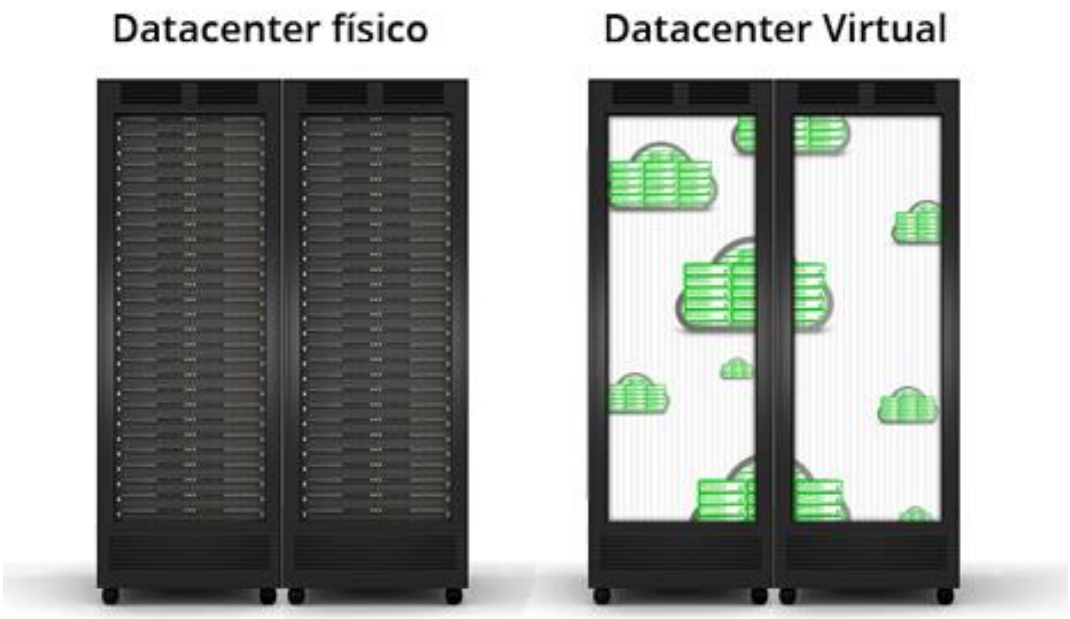


Figura 2. Gráfico de un Data center físico que puede alojar un Data Center Virtuales independientes. Con máximas garantías de seguridad, disponibilidad y flexibilidad. (Castellanos, 2008)
Elaborado por: Jorge Nuñez

Los primeros DC no estaban adecuados para ofrecer facilidades de red complejas, ni tampoco los requerimientos mininos de velocidad y ancho de banda como los de las arquitecturas actuales. La globalización y la propagación exponencial del internet obligaron a las empresas a requerir lugares seguros y concentrados donde se pueda manejar la información independientemente del giro de negocio que manejen, con el objetivo de salvaguardar la disponibilidad, integridad y confidencialidad de su información.

2.2.2 Diseños

Un Data center debe instalase en un cuarto o sala fria, a temperauras para de esta manera evitar sobrecalentamiento y con esta averia entre las mismas. Debe tener las medidas necesarias, la instalación de este centro se enfoca en dicersos puntos, los mismos que deben estar en un mismo equilibro, se deben tomar en cuenta los costos economicos, permisos legales, infraestructura alrededor ,instaleciones electricas, riesgos, entre otros.

2.2.3 División de un Data Center

- **Espacio de sala de informática**. - En este espacio se encuentran los Servidores, los equipos de Almacenamiento, redes LAN y WAN, la Infraestructura de Cableado, la Distribución de Energía, los Equipos de Refrigeración, Equipos de Vigilancia y Seguridad. (plagecons, 2018)

- **Espacio de soporte. -** En esta zona se encuentra la Sala de la planta eléctrica, la Sala de UPS, Sala de Baterías, la Sala de generador, Sala del Transformador, Sala de Planta Mecánica, Área Electromecánica, Zona de soporte de TI, Centro de operaciones, Almacén de Dispositivos de almacenamiento. Los estándares que recomiendan que los UPS mayores a 100 KW sean ubicados fuera del área de TI.

Además de Sala de Impresión, Zona de Pruebas, Almacén de componentes de TI, Seguridad, Entrada de Mercancías, Instalación de entrada de telecomunicaciones, Sala de reuniones. (plagecons, 2018)

2.2.4 Data Center de la UPS

El Data Center se encuentra en el bloque D, subiendo al segundo piso del mismo, pasando el Auditorio Padre Carollo.

El Data Center comparte entrada con el Laboratorio de Interfaz Humano - Máquina, pero es un espacio completamente independiente.

Se compone de dos espacios físicos.

- Aula de Monitoreo

- Cuarto del Data Center.

Bloque D, Segundo Piso

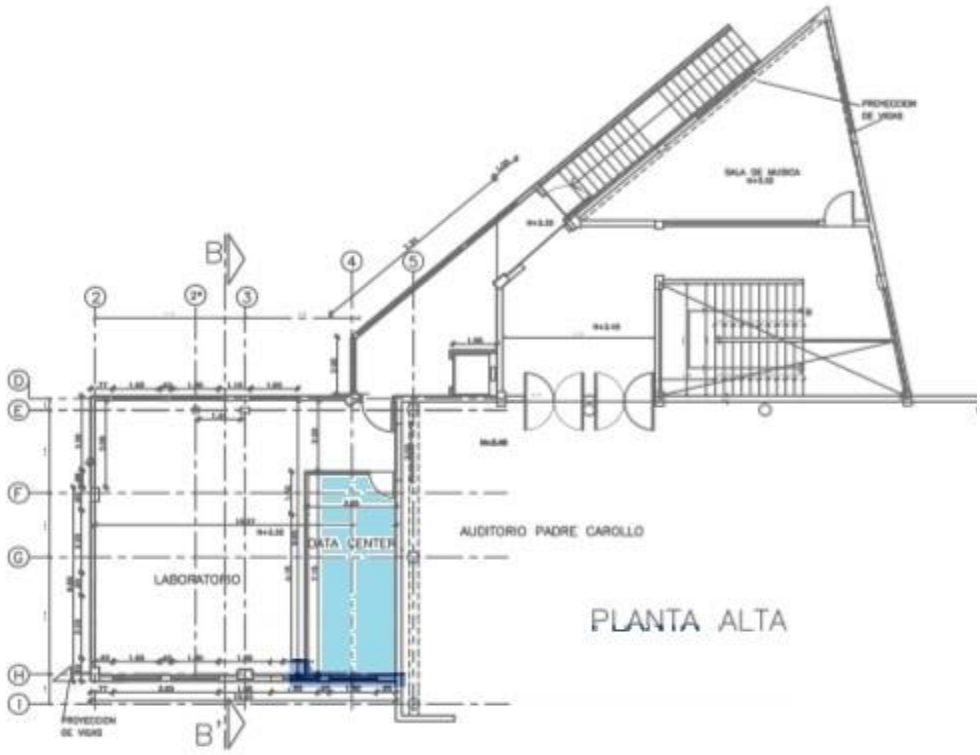


Figura 3. Plano de ubicación del Data Center
Elaborado por: Jorge Nuñez

De la misma manera la información que se controla en el Data Center de este Campus es considerable ya que se procesa todo tipo de información orientada a la academia, investigación y unidad de titulación, tanto de la carrera de Computación como el resto de carreras de la Universidad.

Data Center

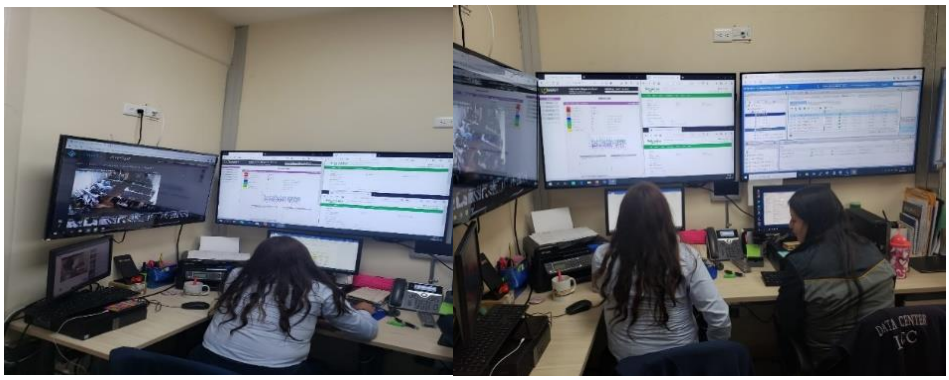


Figura 4. Aula de Monitoreo del Data Center
Elaborado por: Jorge Nuñez

El Data center está conectado a los laboratorios del bloque D anteriormente especificados.

Se detalla a continuación la topología lógica de la interconectividad de los mismos.

Topología de Laboratorios

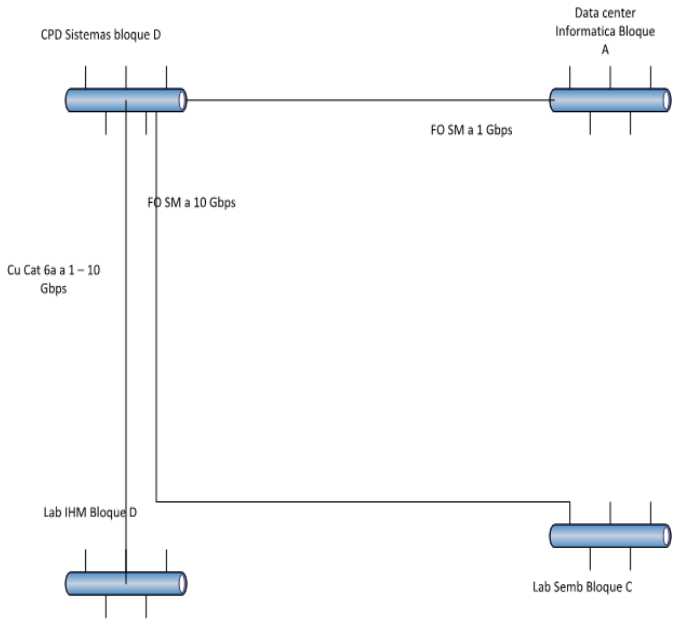


Figura 5. Ubicación y conexión de laboratorios del Campus Sur
Elaborado por: Jorge Nuñez

Conexión Lógica de Laboratorios

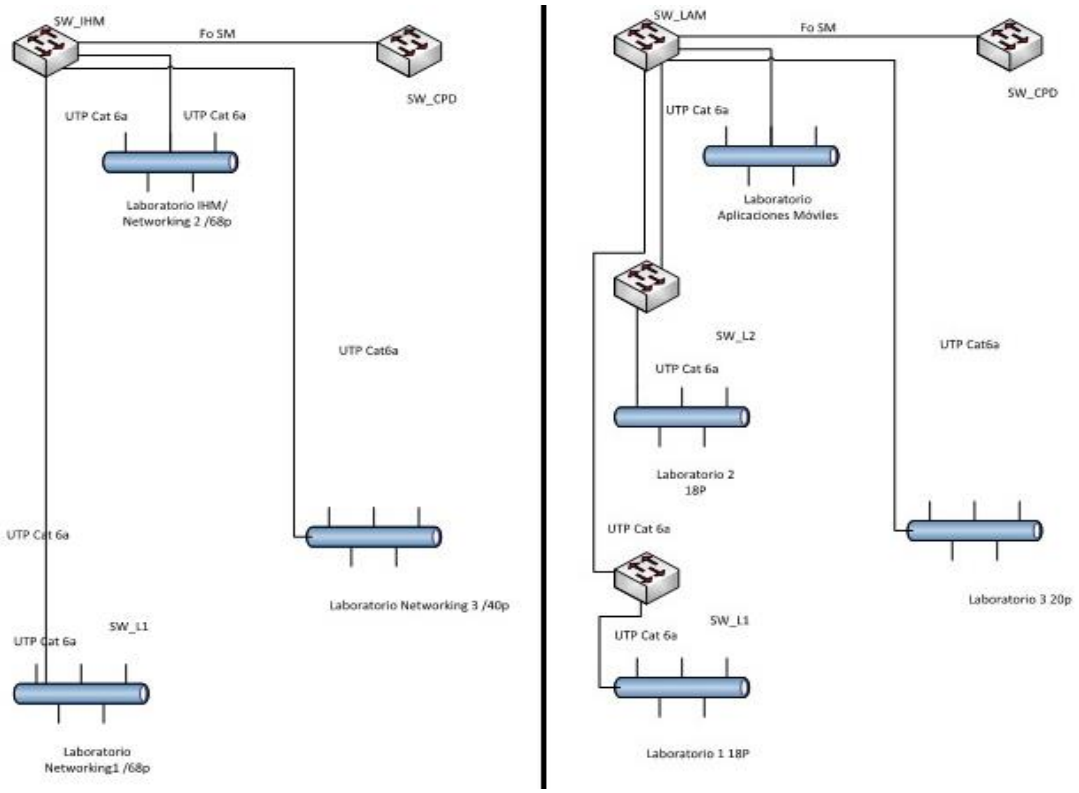


Figura 6. Conexión lógica del Data Center con los laboratorios incluido rediseño horizontal
Elaborado por: Jorge Nuñez

El Data Center está compuesto por 5 Servidores donde se lleva el control y procesamiento de toda la información. El aula de monitoreo cuenta con 3 pantallas con las que se puede monitorear el Data Center y también se lleva el control de las cámaras de seguridad de los laboratorios del bloque, posee sistema de climatización para darle la temperatura óptima para el adecuado para el correcto funcionamiento. Este centro la controlan tres personas autorizadas, el Ing. Jorge López como su Administrador, Ing. Marcela Gallegos como Técnico Operativo 1 y Ing. Thalia Ati como Técnico Operativo 2.

2.3. Plan De Emergencia y Contingencia (PE)

2.3.1. Concepto Plan De Emergencia y Contingencia

El plan de emergencia es la planificación y organización humana para la utilización óptima de los medios técnicos previstos con la finalidad de reducir al mínimo las posibles consecuencias humanas y/o económicas que puedan derivar ser la situación de emergencia; este plan integra un conjunto de estrategias que permiten reducir la posibilidad de ser afectados si se presenta la emergencia. El Plan de Emergencia persigue optimizar los recursos disponibles, por lo que su implantación implica haber otorgado previamente al establecimiento de reclusión de la infraestructura, de medios materiales o técnicos necesarios en función de las características propias de la instalación y de la actividad que él mismo realiza. Previamente se necesita haber realizado una identificación y análisis de los riesgos o deficiencias del establecimiento de reclusión, imprescindible para conocer la dotación de los medios de prevención protección que se precisan en el mismo. (ESCUELA POLITECNICA NACIONAL , 2015)

2.3.2. Objetivos del PE

El objetivo del PE es el de planificar y describir la capacidad para respuestas rápidas, requerida para el control de emergencias. Paralelo al plan se debe identificar los distintos tipos de riesgos que potencialmente podrían ocurrir e incorporar una estrategia de respuesta para cada uno, con algunos objetivos específicos:

- Establecer un procedimiento formal y por escrito que indique las acciones a seguir frente a determinados riesgos.
- Optimizar el uso de recursos humanos y materiales
- Un control adecuado para cumplir con las normas y procedimientos establecidos.

Para, Cesar Ortiz Los Planes de Emergencia y Contingencia son necesarios en todo sistema y no podría dejarse de lado en el tema de seguridad. (Cesar Ortiz, 2016)

2.3.3. Componentes del Plan de Emergencia y Contingencia

- Descripción de la empresa / entidad / organización.
- Identificación de factores de riesgos.
- Evaluación de riesgos detectados.
- Prevención y control de riesgos.
- Mantenimiento S.C.I. (Sistema de Comando de Incidentes)
- Protocolo de alerta y alarma de comunicación para emergencias
- Protocolos de intervención ante emergencias
- Evacuación
- Procedimientos para la implantación del plan de emergencia.

2.3.4. Marco Legal

2.3.4.1.Marco Legal de la Gestión de Riesgos del Ecuador

Constitución De La República Del Ecuador La gestión de riesgos en el Ecuador está direccionada en el siguiente marco legal:

Título V: Organización Territorial del Estado

Capítulo Cuarto: Régimen de competencias

Art 261. El Estado central tendrá competencias exclusivas sobre: ... (Numeral 8) "El manejo de desastres naturales."

Art 264. Los Gobiernos Municipales y de los Distritos Metropolitanos tendrán entre sus competencias exclusivas (numeral 13) "gestionar los servicios de prevención, protección, socorro y extinción de incendios". (Cesar Ortiz, 2016)

Sección Novena: Gestión del riesgo

Artículo 389. "El Sistema Nacional Descentralizado de Gestión de Riesgos está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras. (secretaria de gesión de riesgos, 2014)

Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.

Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.

Realizar y coordinar las acciones necesarias para reducir vulnerabilidades, prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

Ley de Seguridad Pública y del Estado

Capítulo 3, Artículo No. 11, Órganos Ejecutores. - "Los órganos ejecutores del Sistema de Seguridad Pública y del Estado estarán a cargo de las acciones de defensa, orden público, prevención y gestión de riesgos".

"La prevención y las medidas para contrarrestar, reducir y mitigar los riesgos de origen natural y antrópico o para reducir la vulnerabilidad, corresponden a las entidades públicas y privadas, nacionales, regionales y locales. La rectoría la ejercerá el Estado a través de la Secretaría de Gestión de Riesgos" (literal d). (secretaria de gesión de riesgos, 2014)

Código Orgánico de Ordenamiento Territorial, Autonomías y Descentralización (COOTAD)

Art. 140. Ejercicio de la competencia de gestión de riesgos. -La gestión de riesgos que incluye las acciones de prevención, reacción, mitigación, reconstrucción y transferencia, para enfrentar todas las amenazas de origen natural o antrópico que afecten al cantón se gestionarán de manera concurrente y de forma articulada con las políticas y los planes emitidos por el organismo nacional

responsable, de acuerdo con la Constitución y la ley. (secretaria de gesión de riesgos, 2014)

2.3.5. Norma ISO 22301

Es una norma basada en la BS 25999. Se cuenta con 106 requisitos que mandan en la implantación del plan de continuidad de negocio. La gestión de la continuidad del negocio ayuda a disminuir la posibilidad de ocurrencia de un incidente, y en caso de producirse, la organización se encuentra preparada para responder de manera adecuada y así reducir de forma drástica el daño del incidente. (blog de ISOTools Excellence, 2018)

Algunos beneficios de la gestión de continuidad del negocio son:

- Identificar y gestionar las amenazas actuales y futuras de la empresa.
- Método proactivo para minimizar el impacto de los incidentes.
- Operar funciones críticas durante los momentos del incidente.
- Mejorar el tiempo de reacción.

La norma ISO 22301 establece la metodología general para la continuidad de negocio. Dentro de la información documentada que se debe desarrollar:

- El alcance.
- La lista de requisitos legales, normativos y de otra índole.
- Política de la continuidad de negocio.
- Objetivos de la continuidad del negocio.
- Competencias del personal.
- Comunicación con las partes interesadas.

- Análisis del impacto en el negocio.
- Evaluar el riesgo.
- Estructura de la respuesta ante incidentes.
- Planes de continuidad del negocio.
- Procedimientos de recuperación.
- Resultados de acciones preventivas.
- Auditoría interna.
- Revisión de la dirección.
- Acciones correctivas.
- Mejora continua.

Se cuenta con la misma estructura de la norma ISO 9001, proporciona las bases para la gestión de negocios y demostrar el grado de confiabilidad de la empresa. La ISO 22301 refuerza la definición de los objetivos y su seguimiento, define de forma clara la responsabilidad de la dirección y la mejora de la planificación de todos los recursos para garantizar la continuidad del negocio. Su implantación es un gran beneficio y una forma de prevención antes de que ocurra un incidente.

La ISO 22301 es una norma basada en la BS 25999. Como parte de la gestión de la seguridad de la información es muy importante tener un plan de contingencia para garantizar la continuidad del negocio. El estándar es certificable y auditable según la norma ISO 22301, se puede utilizar como guía para establecer un modelo que garantice la seguridad de la información en caso de una emergencia. (blog de ISOTools Excellence, 2018)

CAPÍTULO III

3. Metodologías y Estudio de Factibilidad

De acuerdo a las normas se investiga un método para el desarrollo del plan y poder llevarlo a cabo, con la mayor facilidad posible en este caso se enfoca a dos métodos para hacer una comparación. De la factibilidad del método a utilizar.

3.1. Metodología Ágil SCRUM

Es una metodología para el desarrollo, se basó al principio en productos tecnológicos, pero también se puede emplear en sistemas que necesitan rapidez sobre todo flexibilidad.

Durante los últimos años la metodología SCRUM ha gozado de una gran popularidad dentro de la implementación y desarrollo de software, como referencias empresariales que utilizan esta metodología se puede citar a Google y Spotify dando resultados óptimos y fiables de sus productos y generando satisfacción por parte de sus clientes.

Al ser una de las metodologías de desarrollo de mayor simpleza en su aplicación a un proyecto, se debe tomar en cuenta que requiere mucho trabajo y tino al momento de llevarla a cabo, debido a que esta metodología es cambiable es decir no se rige a seguir un protocolo sino más bien a adaptarse a las situaciones que se presenten durante el recorrido del proyecto.

Es una de las metodologías ágiles más óptimas y adaptables al negocio, como tal posee las siguientes características:

- Adaptable en lugar de predictible.
- Se enfoca a las personas no al proceso.
- Su estructura se basa en iteraciones y revisiones.
- Da prioridad a las funcionalidades y requisitos que pueden tomar menos tiempo de desarrollo.
- Define una visión general del producto.
- Cada iteración define un periodo de desarrollo el cual finaliza con la producción de un nuevo producto.

Se puede decir que las iteraciones son la base de la metodología ágil, para lo cual SCRUM se encarga de gestionar su avance mediante la aplicación de reuniones semanales cada una con un máximo de tiempo no superior a 60 minutos, en la que todo el equipo reunido revisa las actividades avanzadas durante el transcurso de la última reunión a la actual y se plantean las actividades para la siguiente revisión.

SCRUM no es la única metodología ágil que existe en el mercado, pero las más utilizadas y eficaces al momento de realizar un proyecto se tiene a la metodología EXTREME PROGRAMING Y SCRUM, por lo cual se realiza una comparación entre ambas para determinar la más óptima aplicable al presente proyecto (Tabla 1).

Tabla 1. SCRUM VS XP

SCRUM	EXTREME PROGRAMING (XP)
Cada iteración o Sprint tiene un periodo entregable de 4 semanas.	Entregables más rápidos pueden ir de una a tres semanas.
Cada tarea terminada entregada al cliente a satisfacción no se la puede modificar.	Las tareas son susceptibles a cambios durante cualquier etapa del proyecto.
La secuencia de las tareas puede ser modificada si el SCRUM Team lo cree conveniente.	Una vez definido las tareas, se sigue un orden estricto por lo cual no pueden ser modificadas.
Se basa en administración ordenada del proyecto.	Se centra en la creación de un producto.
Cada integrante del SCRUM Team trabaja individualmente.	Tiende a crear grupos de trabajo.

Nota: Comparación entre Metodología SCRUM Y XP

Dado el siguiente análisis entre ambas metodologías agiles, se opta por trabajar con SCRUM debido a que sus características de basarse en la administración de un proyecto mas no dedicarse solo a un desarrollo, permiten contemplar varios escenarios que se presentan durante la ejecución del proyecto y permite analizar su sustentabilidad a futuro.

3.1.1. Roles de la Metodología SCRUM

3.1.1.1. SCRUM Master

Esta es la persona líder del proyecto la cual tiene la función de asegurar que cada proceso sea usado debidamente y que cada regla establecida se cumpla a satisfacción, lo cual brinda una fluidez y jerarquía al proyecto en desarrollo.

Debido a lo expuesto anteriormente se toma la decisión de designar a Ing. Jorge López como líder del presente proyecto.

3.1.1.2. Equipo de Trabajo

Al tratarse de un proyecto de desarrollo de tesis aplicado a la UPS, una vez definido su alcance se determina que el presente proyecto tendrá una sola persona como desarrolladora y ejecutora, la misma que tiene la responsabilidad de elaborar el plan de emergencia además de cumplir con las capacitaciones al personal del DC y entregar un producto 100% eficiente.

3.1.1.3. Grupos de Interés

Durante el análisis de las especificaciones del Plan de Emergencia y su posterior ejecución dentro del DC, se han identificado los siguientes involucrados:

- Posee un Administrador y 2 Operadores Técnicos, quienes se encargan del monitoreo y del correcto funcionamiento, del ingreso de la información y otros. Los mismos que se encuentran 8 horas diarias dentro del Data Center.

- Los Docentes que reparten distintas cátedras en diferentes horarios son aproximadamente 10, que se dividen de acuerdo de su carga laboral en el Edificio D. (Ati, Horarios LAb Bloque D, 2019)

- Los alumnos son la mayor parte de la población que maneja el edificio D y el laboratorio contiguo al Data Center, no se puede llegar a un total exacto dado que cada semestre cambia horarios y número de estudiantes, sin embargo, se considera un aproximado mínimo de 150 alumnos diarios. (Ati, Horarios LAb Bloque D, 2019)

Se llega a la conclusión que aproximadamente se cuenta con 160 personas que recorren el establecimiento diariamente.

3.1.1.4. Iteraciones

Cada avance o iteración se realiza basados y coordinados con la disponibilidad de tiempo de los participantes del proyecto, en donde se estima tiempos de trabajo planificados de la siguiente manera:

- Lunes a viernes 2 horas diarias.
- Sábados 4 horas.

Empleando al máximo el tiempo disponible dando como resultado la resolución de un Sprint en un mes, cumpliendo a satisfacción los estándares establecidos por la metodología ágil SCRUM, obteniendo como resultado las siguientes iteraciones:

- Iteración 1: Como primer paso se comienza a recolectar información acerca de la situación actual de infraestructura del DC, a fin de conocer la ubicación exacta, identificar cada elemento tecnológico, operativo, administrativo y su importancia

dentro de sus actividades, de cada una de estos elementos evaluar su prioridad de aseguramiento al momento de sufrir algún tipo percance durante una catástrofe.

- Iteración 2: Se realiza un análisis del DC, tomando en cuenta varios aspectos como son ubicación geográfica, afectaciones climáticas que se pueden dar, que fenómeno natural esta propenso, sitios cercanos propensos a generar un desastre sea natural o provocado, también es de vital importancia identificar los diferentes accidentes laborales que existan y generen una emergencia dentro del DC, toda esta información obtenida se la registra y ordena con la finalidad de hacer un análisis a manera detallada de todas las vulnerabilidades que presenta.

- Iteración 3: Con los datos obtenidos del análisis de las vulnerabilidades y situación actual del DC, se procede a crear el PE contemplando todos escenarios que podrían darse, durante las diferentes catástrofes a las que está expuesto el DC, este PE está basado en las normativas y estándares regidas en la Norma ISO 22301, y las instrucciones del cuerpo de Bomberos Quito.

  Una vez realizado el Plan de Emergencia se procede a realizar las pruebas dentro del DC, con la finalidad de evaluar la fiabilidad del plan, obtener tiempos de respuesta tanto de las personas encargadas del DC como los otros beneficiarios de la implementación, en caso de presentarse una observación se deberá dar énfasis y buscar la solución más pronta a ese inconveniente.

- Iteración 4: Una vez realizadas las pruebas y con la aprobación de las personas participantes dentro del presente trabajo lo que sigue es la implementación del PE dentro del DC, logrando asegurar en un alto porcentaje la seguridad tanto de las personas como la infraestructura tecnológica del DC.

Diagrama de Tareas

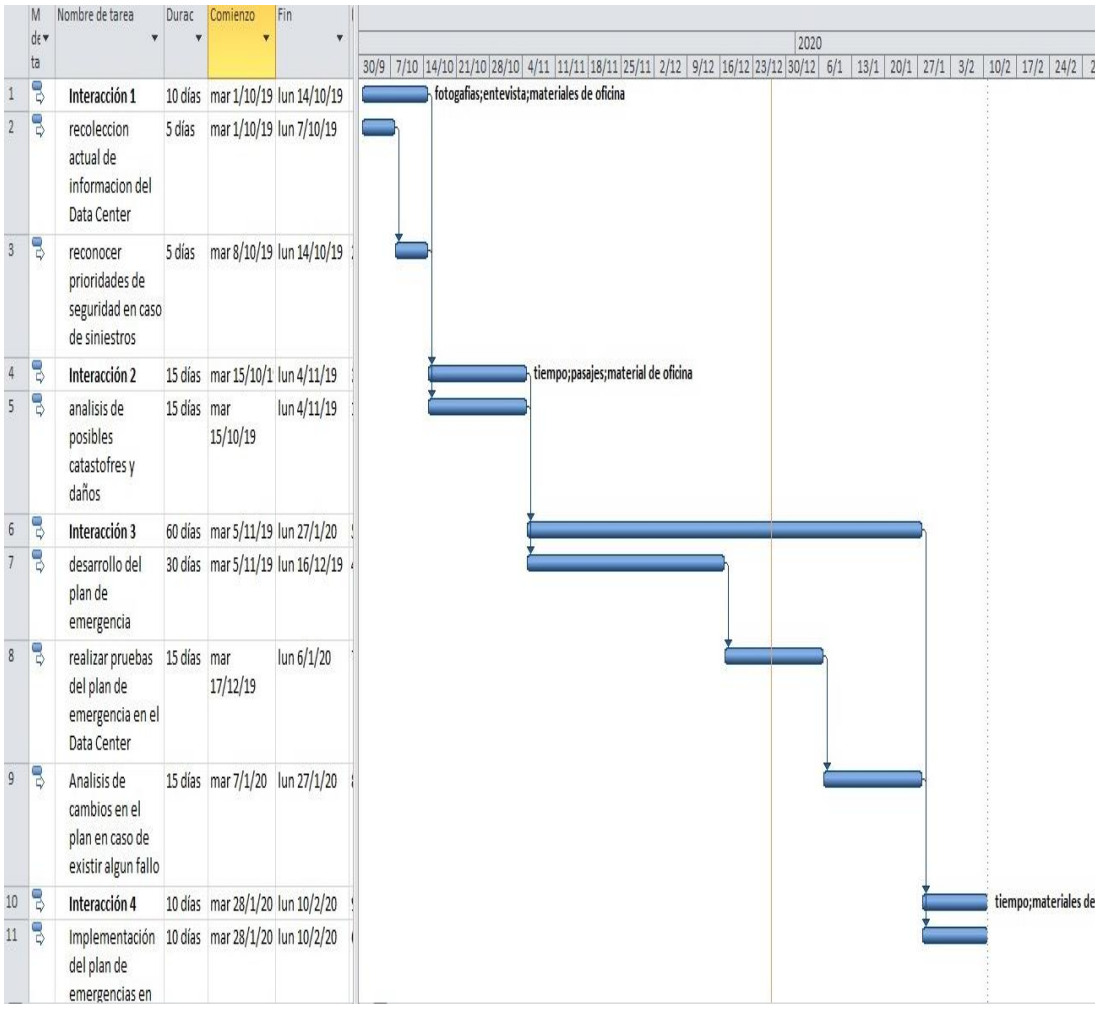


Figura 7. Diagrama de Gantt de tareas a realizar para la elaboración del proyecto.
Elaborado por: Jorge Nuñez

3.1.1.5.Diagramas

3.1.1.5.1. Procesos de Control del Data Center

Control de acceso. - El acceso a data center solo lo hacen personal calificado, quien se encuentra dentro de las mismas 8 horas diarias.

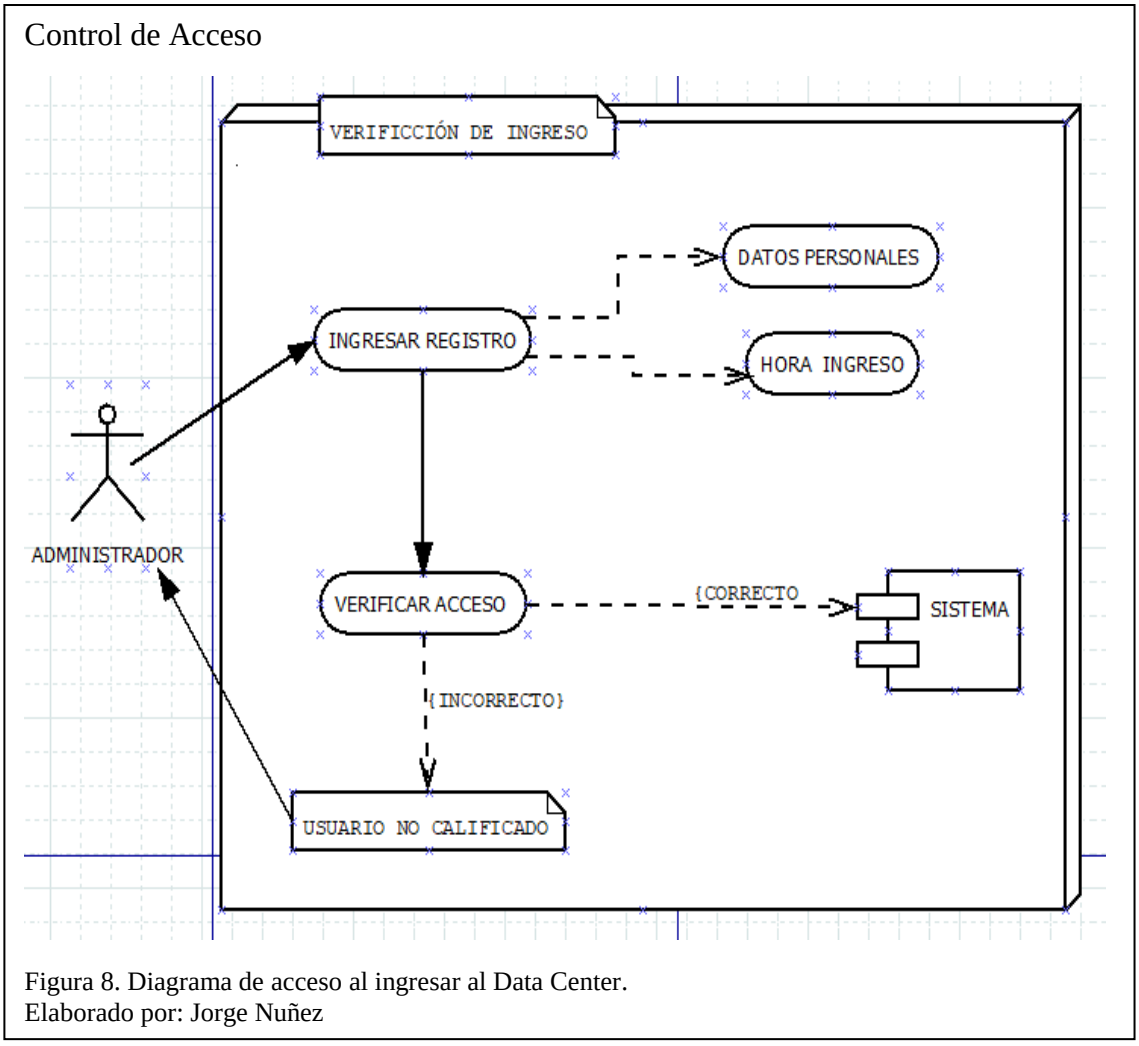


Figura 8. Diagrama de acceso al ingresar al Data Center.
Elaborado por: Jorge Nuñez

Proceso del control del ingreso del personal a laboratorios autorizados.

Para este proceso se aplica un enlistado llamado control de bitácoras donde los profesores hacen su registro manual de su ingreso.

Bitácora uso de Laboratorios

Estimado Docente, tenga la bondad de llenar la respectiva bitácora, en caso de existir alguna incidencia en los laboratorios

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR			DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN						
			FORMATO		BITACORA DE USO DE LOS LABORATORIOS				
					LABORATORIO DE NETWORKING 1				
					HORA		ACTIVIDAD		
FECHA	DOCENTE RESPONSABLE	FIRMA	MATERIA	GRUPO	INICIO	TERMINO	TEORIA	PRACTICA	OBSERVACIÓN

Figura 9. Formato de docentes al ingreso a laboratorios del bloque D. (Ati, Formato Ingreso Docentes Laboratorios BLoque D, 2019)
Elaborado por: Jorge Nuñez

Una vez realizado esto, se procede a legalizarlo por llamarlo de esta manera al finalizar el día, ingresándolo al sistema donde se registran los respaldos.

Proceso del préstamo de equipos y laboratorios del bloque D.

A continuación, se mostrará el flujo de procedimiento que debe seguir un estudiante para solicitar equipos o laboratorios en el bloque D, de la Universidad Politécnica Salesiana.

Préstamo Laboratorios

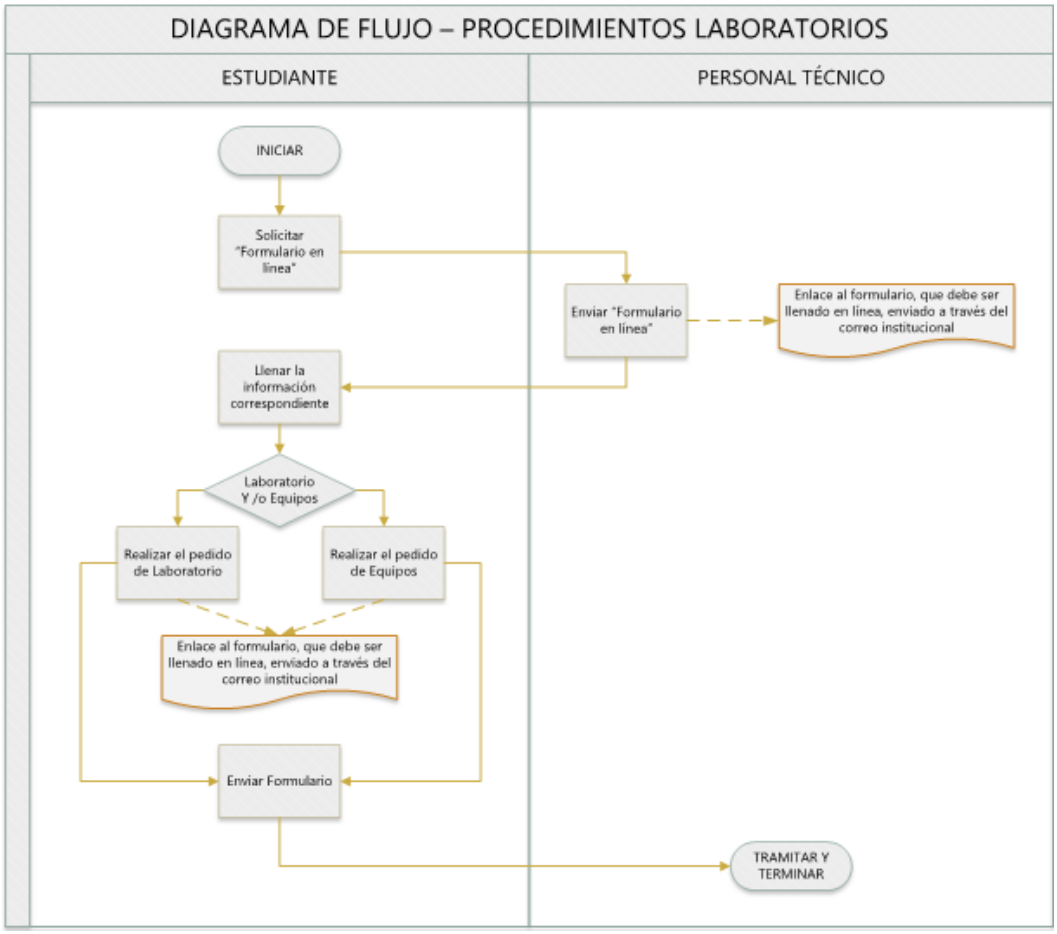


Figura 10. Diagrama de flujo para el préstamo de laboratorios del bloque D.
Elaborado por: Jorge Nuñez

3.1.1.6.Reuniones

Dado la disponibilidad de tiempo de todos los participantes de este proyecto, se toma la decisión de realizar reuniones semanales donde se registrarán los cambios y se evaluara el avance de cada iteración, las reuniones se llevarán a cabo de manera presencial, cada reunión tendrá una duración de 30 a 60 minutos según la complejidad a tratar, estas reuniones ayudaran a la toma de decisiones si se da el caso de presentarse algún inconveniente en la generación de la iteración.

3.2 Análisis de Factibilidad del Proyecto

3.2.1. Definición General

El análisis de factibilidad de un proyecto se basa en realizar una evaluación haciéndose referencia específicamente en los aspectos técnicos, tecnológicos, y financieros. Dando como resultado datos exactos los cuales brindan ayuda al momento de la toma de decisiones y definir la vialidad de implementación.

A continuación, se presenta el análisis de factibilidad del proyecto actual, se ha tomado en cuenta varios aspectos importantes que sustentaran las decisiones a tomar dentro del desarrollo, cada uno de los aspectos tiene una complejidad alta, debido a que presenta los recursos exactos con los que se cuenta al momento de implementar el proyecto.

3.2.2. Factibilidad Técnica y Operativa

El objetivo del análisis de la factibilidad operativa permite a determinar si el proyecto actual en este caso el desarrollo del Plan de Contingencia para el DC de la UPS se aplica de manera correcta por las personas involucradas en el DC, logrando obtener excelentes resultados y buena aceptación.

Las capacitaciones están destinadas tanto a encargados del DC como a alumnos, docentes, grupos de investigación, y personal administrativo del bloque D, con una duración de 4 horas.

Tabla 2. Tabla Socialización

CANTIDAD	DESCRIPCIÓN	HORA/TRABAJO
1	Capacitación Encargados DC	1
1	Capacitación Docentes	1
1	Capacitación Estudiantes	1
1	Capacitación Grupos de Investigación	1

Nota: Tabla de capacitaciones del PE.

Este proyecto al tratarse de un proyecto técnico - teórico, disminuye cualquier riesgo de sufrir algún daño o percance durante una posible catástrofe, contribuyendo a la seguridad y precautelarían de vidas y enceres del DC. Dando como resultado de este análisis, es factible.

3.2.3. Factibilidad Tecnológica y Humana

El estudio de la factibilidad tecnológica toma en cuenta todos los elementos a utilizar dentro del proyecto, tanto elementos de software como de hardware, define los requisitos que debe disponer para llevar un correcto desarrollo y ejecución del proyecto cumpliendo las necesidades y requerimientos del DC.

Con la finalidad de cumplir a satisfacción todos los requisitos necesarios que contempla este trabajo se realizan en las tablas 5 y 6 una descripción detallada de los componentes tecnológicos basados en avances actuales como facilidad de acceso a ellos, entre estas herramientas se tiene:

Tabla 3. Tabla Consultoría

CANTIDAD	DESCRIPCIÓN	HORA/TRABAJO	COSTO/HORA/TRABAJO	TOTAL
1	Consultor	20	50	1000
TOTAL				**1000**

Nota: Tabla de precios de consultoría en Quito (Salguero, 2019)

Tabla 4. Tabla Capacitaciones

CANTIDAD	DESCRIPCIÓN	HORA/TRABAJO	COSTO/HORA/TRABAJO	TOTAL
4	Capacitación involucrados	4	20	80
			TOTAL	**80**

Nota: Tabla de precios de consultoría en Quito (Salguero, 2019)

Tabla 5. Materiales

CANTIDAD	DESCRIPCIÓN	COSTO	TOTAL
1	Equipo Portátil	800	800
1	Impresora Laser	100	100
2	Extintor	50	100
	Depende el análisis se aumenta más materiales		
		TOTAL	**1000**

Nota: Tabla de equipos dentro del aula de monitoreo del Data Center

Tabla 6. Materiales

RECURSOS	COSTO
Costo Mano de Obra	1080
Recursos Materiales o Varios	1000
Otros Recursos	160
Imprevistos. 5%	215,5
TOTAL	**2455,5**

Nota: Tabla del costo total del proyecto

Una vez que se detallan todos los gastos que intervienen en el desarrollo del proyecto, se constata que la mayoría de elementos ya los contiene el DC. Además, debido a que el presente PE es un proyecto de titulación no incurre en todos los gastos expuestos anteriormente por lo cual la factibilidad económica es realizable cumpliendo con todos los ítems expuestos anteriormente.

3.2.4. Análisis Factores de Riesgo

Disponer de un PE dentro de una empresa o establecimiento es una responsabilidad muy alta debido a que es una herramienta de ayuda al momento de sufrir algún tipo de catástrofe, se puede tener un plan de emergencia técnicamente bueno, pero no sirve de nada no ponerlo en práctica y en conocimiento de cada uno de los miembros de la institución. Debe existir asesoramiento constante y un óptimo compromiso de las personas que están inmersas en la misma.

El apoyo junto con la participación de cada uno de los usuarios que conforman la institución es clave al momento de sufrir alguna catástrofe, y poder salvaguardar su vida como los bienes, maquinas, elementos etc., estos son los primeros en brindar primeros auxilios y métodos de seguridad antes de la llegada del personal especializado.

Antes del desarrollo de este plan dentro de una empresa se debe realizar varios análisis, tomando en cuenta ciertas consideraciones técnicas, las mismas que son de vital importancia, brindando la ayuda necesaria para identificar los diferentes tipos de vulnerabilidades que existen o pueden existir dentro del establecimiento.

Dentro de estas consideraciones se puede detallar:

- Datos generales de la institución.
- Ubicación

Tipos de Riesgos (Directos e Indirectos).

- Identificación de la amenaza
- Matriz de identificación de riesgos.

CAPÍTULO IV

4. Elaboración Del PE

DATA CENTER DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR.

Data Center

Figura 11. Fachada Principal del bloque D.
Elaborado por: Jorge Nuñez

DIRECCIÓN: Av. y Av. Rumichaca Ñan, Ave Moran Valverde, Quito

ADMINISTRADOR: Ing. Jorge López

Fecha de elaboración: Enero del 2020

Mapa y ubicación geográfica

Mapa Universidad Politécnica Salesiana

Figura 12. Mapa ubicación geográfica de la UPS, Campus Sur.
Elaborado por: Jorge Nuñez

El Centro de Datos donde se realiza el análisis para desarrollar el PE está ubicado en el bloque D, del campus sur de la institución antes mencionada, y con los siguientes puntos de referencia:

- Latitud: O78°31'29.82"
- Longitud; S0°13'47.46"

4.1. Descripción

4.1.1. Información general

Razón Social

Universidad Politécnica Salesiana

Dirección exacta

Se encuentra ubicada en la siguiente dirección Av. y Av. Rumichaca Ñan, Ave Moran Valverde, Quito

Administrador: Ing. Jorge López

Responsables de la seguridad del Data Center:

- Ing. Jorge López, (Administrador),
- Ing. Marcela Gallegos, (Técnico Operativo)
- Ing. Thalia Ati, (Técnico Operativo)

Actividad.

El Data Center es el centro encargado de guardar y procesar toda la información para el funcionamiento eficiente y eficaz de todos los procesos que maneja la Universidad junto con el monitoreo del alumnado y personal dentro del Edifico D para así tener seguridad de posibles riesgos.

Medidas de superficie y área útil del trabajo

Área de 21.14m2 aproximadamente.

Población

En el edificio se encuentra que existe variedad de alumnos en el área de laboratorios, por lo que se puede apreciar los siguientes datos aproximados.

- Posee un administrador y dos técnicos operativos, quienes se encargan de la administración, monitoreo y correcto funcionamiento, del ingreso de la información y otros. Los mismos que se encuentran 8 horas diarias dentro del Data Center.
- Personal docente que reparten distintas materias y diferentes horarios son aproximadamente 26, Considerando que diariamente asistirán entre 10 y 15.
- Alumnos que asisten normalmente a clases en el horario establecido, por lo que se considera que no se puede llegar a un total exacto, sin embargo, se considera un aproximado mínimo de 150 alumnos diarios entre hombres y mujeres. Se toma en cuenta que entre estos existen también, mujeres embrazadas y personas con discapacidad. (Ati, Horarios LAb Bloque D, 2019)

Se considera también las faltas del alumnado diariamente para realizar una estadística de alumnos por día, lo que nos da un aproximado de 160 personas que se encuentran diariamente en el bloque, a diferentes horas mientras se encuentran en horario de clases.

Fecha de implementación de elaboración: Febrero del 2020

Fecha de implementación del plan de emergencia. Febrero del 2020

4.2. Antecedentes

La UPS en su Campus Sur posee un Data Center (DC); ubicado en el bloque D, en el cual no consta con un PE ante cualquier tipo de siniestro que pueda presentarse ya sea provocado o un desastre natural, el cual se ha presentado en los últimos dos años, poniendo en riesgo al administrador y técnico operativos del DC; a los alumnos, docentes y a su vez a la infraestructura tecnológica posee el mismo.

4.3. Objetivos del PE

El principal objetivo del desarrollo de este plan es salvaguardar la seguridad de las personas presentes en el momento de un riesgo, y a su vez mitigar los daños a equipos donde es retenida la información de todos los procesos de la Universidad Politécnica Salesiana, provocando así que en momento que ocurra un riesgo de diversa índole este sistema siga funcionando sin problemas y sea un elemento de seguridad con respecto a información.

4.4. Responsable del desarrollo:

- Ing. Jorge López (Coordinación)
- Jorge Fernando Nuñez (Desarrollo)

4.5. Análisis de Factores de Riesgo

Estos son aquellos elementos físicos, naturales, eléctricos, etc. Que existen alrededor del Data Center y pueden ser los causantes de algún siniestro, accidente o catástrofe dentro o fuera del edificio D.

Dentro del presente plan se determina la existencia de dos tipos de Factores de Riesgo que son Directos e Indirectos, los mismos que se analizan a precisión a fin de tomar medidas de corrección y/o prevención.

4.5.1 Riesgos Directos

Al referirse a riesgos directos se hace un énfasis principal en aquellos elementos físicos (Hardware e infraestructura del bloque D) que al momento de un siniestro puedan caerse, inflamarse, fracturarse o afectar directamente al personal administrativo, docentes y alumnos que se encuentren en el bloque D.

Para ello se hace un inventario de toda la infraestructura y adecuación del lugar, a fin de realizar un análisis a detalle y tomar nuevas medidas de seguridad o reforzar las ya existentes.

Inventario Infraestructura Ocupacional

Tabla 7. Sofwtare del Data Center

Nombre de la aplicación	Crucial Yes / No	Activos fijos Yes / No	Ejecución
Vmware vSphere 6.5.0	Yes	Yes	Constante
Vmware vRealize 6.5.0	Yes	Yes	Constante
Vmware vRealize Log Insigth 4.3.0	Yes	Yes	Constante
Vmware ESXi 6.5.0	Yes	Yes	Constante
DHCP	Yes	Yes	Constante
DNS	Yes	Yes	Constante
Active Directory	Yes	Yes	Constante
Windows 10	No	Yes	Constante
pfSense-CE-2.4.3-AMD64	Yes	Yes	Constante
CACTIOS	No	Yes	Constante
ZKTeco 3.5.3	No	Yes	Constante
Milestone Xprotect 2018 2. 1a	Yes	Yes	Constante
GEIST Watchdog 3.16.3	Yes	Yes	Constante
HPE 3PAR SSMC	Yes	Yes	Constante

Nota: Software de control diario del Data Center

Detalle Infraestructura Eléctrica

Instalaciones eléctricas.

El DC tiene unas especificaciones técnicas las cuales cuentan con la instalación de dos acometidas eléctricas que provienen de estaciones eléctricas diferentes con sus respectivos generadores, que en caso de emergencia puedan asumir el control. Con su respectivo esquema eléctrico.

Diagrama Eléctrico Campus Sur

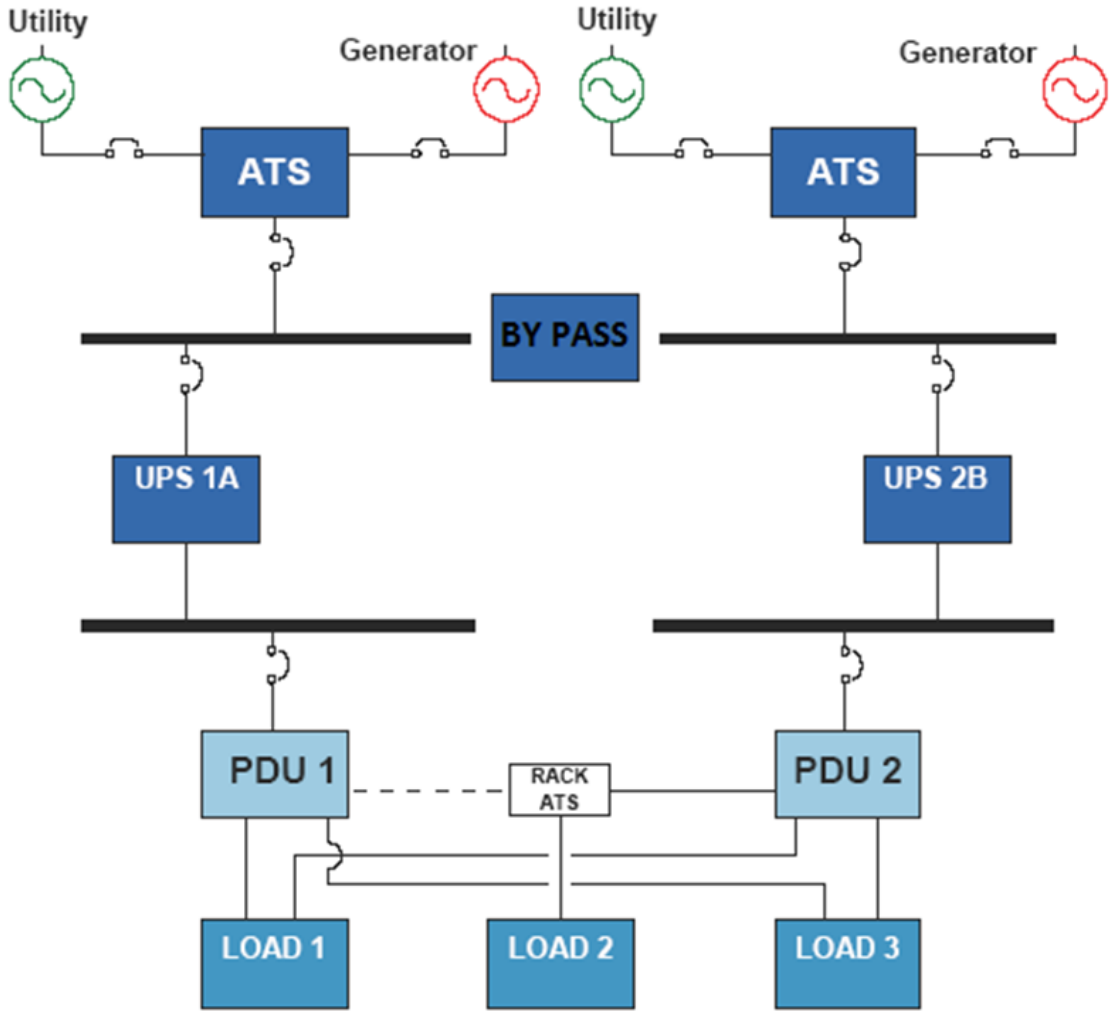


Figura 13. Mapa eléctrico del Campus Sur de UPS.
Elaborado por: Jorge Nuñez

Tabla 8. Distribución Eléctrica Campus Sur

TABLERO DE DISTRIBUCIÓN CENTRO DE COMPUTO TDCC			
PROTECCIÓN		PROPÓSITO	ACOMETIDA
# DE POLOS	CAPACIDAD		
3PH	125 A	ENTRADA LADO A	[(3 x1/0)+(1x#2)+ (1 x #4)] AWG Superflex para 3 fases + neutro + tierra
3PH	100 A	ENTRADA UPS A	[(2 x #4)+(1 x #4)+(1 x #4)] AWG Superflex para 2 fases + neutro + tierra
3PH	100 A	BYPASS UPS A	[(2 x #4)+(1 x #4)+(1 x #4)] AWG Superflex para 2 fases + neutro + tierra
3PH	100 A	SALIDA UPS A	[(2 x #4)+(1 x #4)+(1 x #4)] AWG Superflex para 2 fases + neutro + tierra
3 PH	60 A	TVSS	[(3 x #10)+(1 x #10)+(1 x #10)] THHN para 3 fases + neutro + tierra
3PH	125 A	ENTRADA LADO B	[(3 x#4)+(1x#6)+ (1 x #8)] AWG Superflex para 3 fases + neutro + tierra
3PH	100 A	ENTRADA UPS B	[(2 x #4)+(1 x #4)+(1 x #4)] AWG Superflex para 2 fases + neutro + tierra
3PH	100 A	BYPASS UPS B	[(2 x #4)+(1 x #4)+(1 x #4)] AWG Superflex para 2 fases + neutro + tierra
3PH	100 A	SALIDA UPS B	[(2 x #4)+(1 x #4)+(1 x #4)] AWG Superflex para 2 fases + neutro + tierra
3 PH	60 A	TVSS	[(3 x #10)+(1 x #10)+(1 x #10)] THHN para 3 fases + neutro + tierra

Nota: Tablero de Distribución del Centro de Computo

Como parte de TDCC se incluye en su interior 2 distribuidores de energía monofásico de dos hilos de 12 posiciones para alimentación de cargas eléctricas reguladas UPS A y UPS B. Dos distribuidores trifásicos de 12 posiciones para distribución de energía normal (lado A, lado B) en la figura siguiente se muestran al TDCC. Cuenta con acrílicos para cubrir las barras, evitando algún peligro en la manipulación.

El TDCC posee dos Supresores de Transitorios Marca CPT 100 KVA, incorporado en las barras principales del tablero eléctrico a través de su respectiva protección termo magnética, que se alimenta con cable # 10 AWG.

El TDCC posee un distribuidor de energía regulada por cada UPS, con este antecedente se realizan extensiones eléctricas, con el objetivo de alimentar a los diferentes racks del Data Center. Así también se realizan las alimentaciones desde estos distribuidores hacia el control de accesos y panel de incendios.

Para el rack de comunicaciones R1 se realiza 2 extensión L5-20 para la conexión del PDU vertical con conectores Nema L520R, con cable # 12 por medio de anillado BX sellado y caja de aluminio.

También se realizan 2 extensiones, de 220 V / 20 A con conectores Nema L620R, con cable # 12 por medio de anillado BX sellado y caja de aluminio, y 2 extensiones, de 220 V / 30 A con conectores Nema L630R, con cable # 10 por medio de anillado BX sellado y caja de aluminio.

Para el Data Center de inicio, se requiere una potencia de 8 KVA, por lo que para un crecimiento en relación a la demanda se instaló dos UPS para el Data Center el cual es redundante y modular.

UPS Symmetra LX.

UPS Monofásico marca APC modelo SYA8K16P se alimentan desde el TDCC y las protecciones son mediante un breaker de 3 Polos de 100 A. Los UPS son de 8 KVA con opción de crecimiento a 16 KVA redundante.

La energía eléctrica para todos los equipos a ser conectados al UPS es acondicionada, filtrada y regulada en línea tanto en voltaje como en frecuencia. Los UPS APC instalados son de operación continua con tecnología ON-LINE y con características que garantizan máxima confiabilidad, de calidad mundial.

Adicionalmente los equipos UPS´s instalados son capaces de manejar comunicaciones en red y de notificaciones remotas sobre su estado y operación. Los UPS incluyen puerto RS232 y tarjeta de comunicaciones vía Web y SNMP para monitor.

Además, para una mejor maniobra de los UPS y control, en el TDCC se tiene breakers de Bypass de UPS A y UPS B, que garantiza el cambio de energía normal a regulada o viceversa sin necesidad de realizar un apagado general de la carga; aprovechando la topología y tecnología del UPS APC.

Infraestructura Tecnológica

Para el análisis de esta estructura se recopila la siguiente información de equipos tecnológicos que conforman el Data Center y laboratorios.

Dispositivos	Descripción
Rack 1	Servidor HP Proliant DL38067
Rack 2	5 servidores HPE APOLLO
Rack 3	2 ODF
1 switch	Cisco 500 Series
2 switch	Cisco 550 Series
Watchdog	Monitoreo de variables ambientales
Switch de núcleo	Cisco 9300 Series

En los siguientes gráficos se aprecian cuál es la arquitectura de procesamiento en topología lógica y física.

Arquitectura Data Center

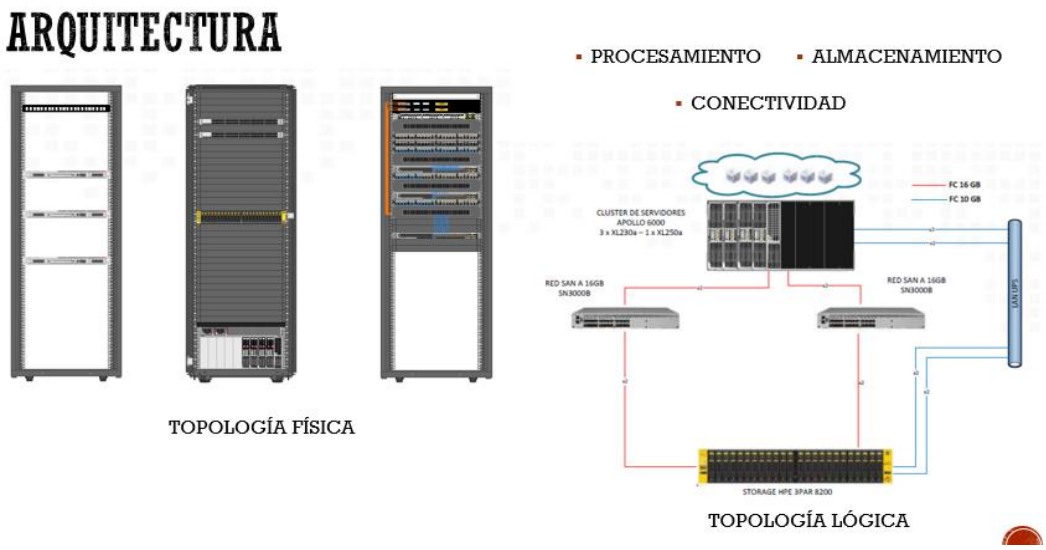


Figura 14. Descripción física y Lógica los equipos del Data Center.
Elaborado por: Jorge Nuñez

Arquitectura Procesamiento Data Center

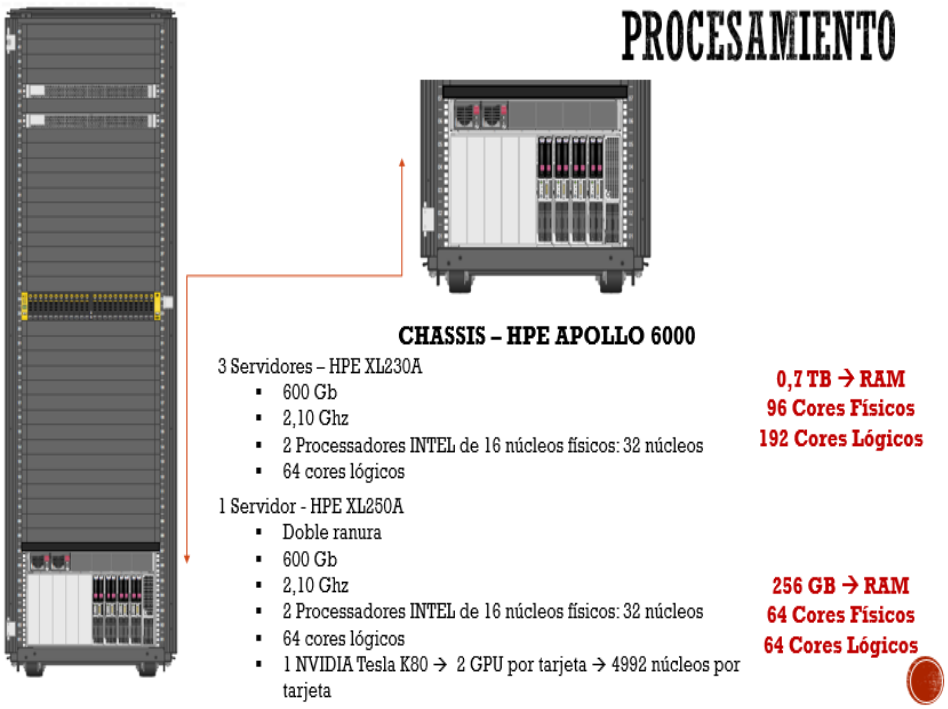


Figura 15. Descripción de los servidores de proceso del Data Center.
Elaborado por: Jorge Nuñez

Arquitectura Almacenamiento Data Center

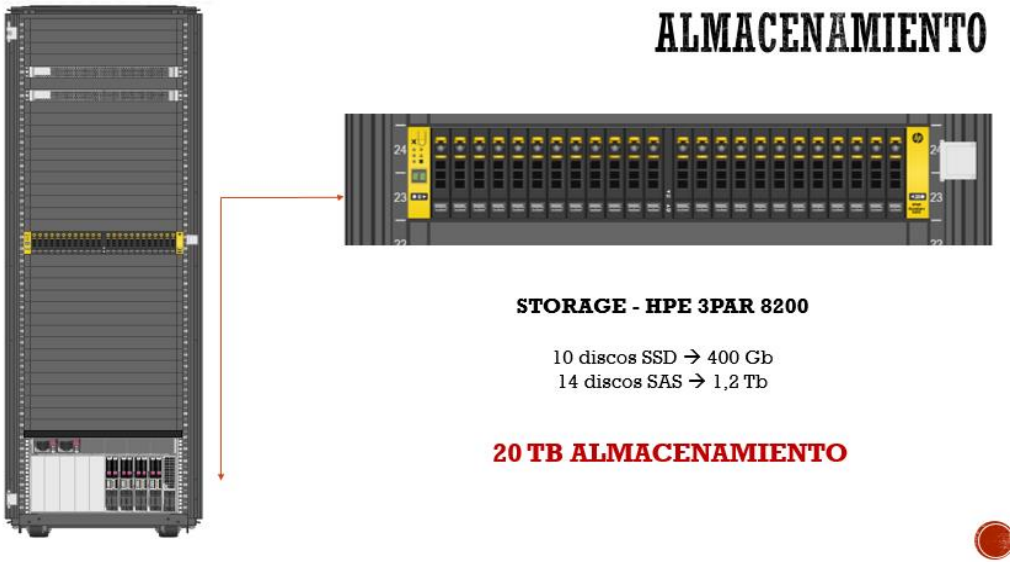


Figura 16. Descripción de equipos de almacenamiento del Data Center.
Elaborado por: Jorge Nuñez

Arquitectura Comunicación Data Center

Figura 17. Descripción de equipos de comunicación del Data Center.
Elaborado por: Jorge Nuñez

En los laboratorios encontramos los siguientes equipos, los mismos que pueden tener algún tipo de riesgo cuando suceda algún siniestro.

Tabla 9. Inventarios descriptivos de CPUs

CPU						
NÚMERO	**CÓDIGO UPS**	**SERIAL FÁBRICA**	**MARCA**	**PROCESADOR**	**MEMORIA GB**	**DISCO GB**
1	SCA	F3ZFBY1	DELL	Core I7	8GB	500GB
2	80042000605324	F34GBY1	DELL	Core I7	8GB	500GB
3	80042000605325	F41FBY1	DELL	Core I7	8GB	500GB
4	80042000605326	F30DBY1	DELL	Core I7	8GB	500GB
5	80042000605327	CNTFBY1	DELL	Core I7	8GB	500GB
6	80042000605328	CP0GBY1	DELL	Core I7	8GB	500GB
7	80042000605323	CN9FBY1	DELL	Core I7	8GB	500GB
8	80042000605322	F2XFBY1	DELL	Core I7	8GB	500GB
9	80042000605321	F30GBY1	DELL	Core I7	8GB	500GB
10	80042000605320	F40DBY1	DELL	Core I7	8GB	500GB
11	80042000605319	F3VDBY1	DELL	Core I7	8GB	500GB
12	80042000605314	F2SDBY1	DELL	Core I7	8GB	500GB
13	80042000605315	CNPGBY1	DELL	Core I7	8GB	500GB
14	80042000605316	F4GFBY1	DELL	Core I7	8GB	500GB
15	80042000605317	CNPFBY1	DELL	Core I7	8GB	500GB
16	80042000605318	F2YDBY1	DELL	Core I7	8GB	500GB
17	80042000605309	F50DBY1	DELL	Core I7	8GB	500GB
18	80042000605310	CNQCBY1	DELL	Core I7	8GB	500GB
19	80042000605311	F47DBY1	DELL	Core I7	8GB	500GB
20	80042000605312	CNQDBY1	DELL	Core I7	8GB	500GB
21	80042000605313	CNNFBY1	DELL	Core I7	8GB	500GB
22	80042000605304	F43FBY1	DELL	Core I7	8GB	500GB
23	80042000605305	CN6DBY1	DELL	Core I7	8GB	500GB
24	80042000605306	F38FBY1	DELL	Core I7	8GB	500GB
25	SCA	F42FBY1	DELL	Core I7	8GB	500GB
26	80042000605308	CP4FBFY1	DELL	Core I7	8GB	500GB
27	SCA	F2ZFBY1	DELL	Core I7	8GB	500GB
28	SCA	F48DBY1	DELL	Core I7	8GB	500GB
29	80042000605302	F32DBY1	DELL	Core I7	8GB	500GB
30	80042000605303	CN3DBY1	DELL	Core I7	8GB	500GB
31	SCA	F45GBY1	DELL	Core I7	8GB	500GB
32	80042000605307	F3SCBY1	DELL	Core I7	8GB	500GB
33	80042000609175	3024942	DELL	Core I7	8GB	500GB
34	80042000609183	30H5942	DELL	Core I7	8GB	500GB
35	80042000609178	30N4942	DELL	Core I7	8GB	500GB
36	80042000609166	2Y74942	DELL	Core I7	8GB	500GB
37	80042000609177	2Y63942	DELL	Core I7	8GB	500GB
38	80042000609179	3034942	DELL	Core I7	8GB	500GB
39	80042000609176	2Z66942	DELL	Core I7	8GB	500GB
40	80042000609174	30S3942	DELL	Core I7	8GB	500GB
41	80042000609172	2YG2942	DELL	Core I7	8GB	500GB
42	80042000609169	3047942	DELL	Core I7	8GB	500GB
43	80042000609173	30X5942	DELL	Core I7	8GB	500GB
44	80042000609180	2Z67942	DELL	Core I7	8GB	500GB

45	80042000609165	2Z37942	DELL	Core I7	8GB	500GB
46	80042000609171	2Y53942	DELL	Core I7	8GB	500GB
47	80042000609168	2Z73942	DELL	Core I7	8GB	500GB
48	80042000609170	3004942	DELL	Core I7	8GB	500GB
49	80042000609167	2ZJ5942	DELL	Core I7	8GB	500GB
50	80042000609164	31Z5942	DELL	Core I7	8GB	500GB
51	80042000609182	2Z65942	DELL	Core I7	8GB	500GB

Nota: CPUs que se encuentran en el bloque D.

Tabla 10. Inventario de Monitores y Mouse

MONITOR			MOUSE	
NÚMERO	**CÓDIGO UPS**	**SERIAL FÁBRICA**	**CÓDIGO UPS**	**SERIAL FÁBRICA**
1	SCA	CN-OR16JC-72872-37V-A8HM	SCA	CN-09RRC7-48729-374-03BS
2	SCA	CN-OR16JC-72872-37U-AG7M	SCA	CN-09RRC7-48729-481-0MTG
3	SCA	CN-OR16JC-72872-37O-APPB	SCA	CN-09RRC7-48729-374-07VF
4	SCA	CN-OR16JC-72872-37V-A5GM	SCA	CN-09RRC7-48729-372-0NWV
5	SCA	CN-OR16JC-72872-37V-AFVM	SCA	CN-09RRC7-48729-372-062D
6	SCA	CN-OR16JC-72872-37V-A5JM	SCA	CN-09RRC7-48729-374-03BR
7	SCA	CN -OR16JC-72872-37U-AFKM	SCA	CN-09RRC7-48729-374-19YH
8	SCA	CN-OR16JC-72872-37U-AEHM	SCA	CN-09RRC7-48729-371-1KT1
9	SCA	CN-OR16JC-72872-37V-ARDM	SCA	CN-09RRC7-48729-379-0CY4
10	SCA	CN-OR16JC-72872-37V-A8TM	SCA	CN-09RRC7-48729-374-079V
11	SCA	CN-OR16JC-72872-37V-A8KM	SCA	CN-09RRC7-48729-36U-0CEU
12	SCA	CN-OR16JC-72872-37O-ANPB	SCA	CN-09RRC7-48729-374-03BG
13	SCA	CN-OR16JC-72872-37V-AP2M	SCA	CN-09RRC7-48729-374-03RT
14	SCA	CN-OR16JC-72872-37U-AFLM	SCA	CN-09RRC7-48729-374-07VJ
15	SCA	CN-OR16JC-72872-37U-AE5M	SCA	CN-09RRC7-48729-372-0CF8
16	SCA	CN-OR16JC-72872-37V-A5YM	SCA	CN-09RRC7-48729-38U-19UW
17	SCA	CN-OR16JC-72872-37U-AFHM	SCA	CN-09RRC7-48729-488-0RUL
18	SCA	CN-OR16JC-72872-37V-A98M	SCA	CN-09RRC7-48729-36U-0DWK
19	SCA	CN-OR16JC-72872-37U-AG2M	SCA	CN-09RRC7-48729-374-03QJ
20	SCA	CN-OR16JC-72872-37V-AP9M	SCA	CN-09RRC7-48729-374-03A7
21	SCA	CN-OR16JC-72872-37V-ARFM	SCA	CN-09RRC7-48729-374-0401
22	SCA	CN-OR16JC-72872-37O-ANAB	SCA	CN-09RRC7-48729-372-064R
23	SCA	CN-OR16JC-72872-37V-ALTM	SCA	CN-09RRC7-48729-374-03RD
24	SCA	CN-OR16JC-72872-37V-A9HM	SCA	CN-09RRC7-48729-371-1KQY
25	SCA	CN-OR16JC-72872-37V-A5KM	SCA	CN-09RRC7-48729-374-07UT
26	SCA	CN-OR16JC-72872-37V-A9MM	SCA	CN-09RRC7-48729-37A-03RK

27	SCA	CN-OR16JC-72872-37U-AFGM	SCA	CN-09RRC7-48729-374-07VG
28	SCA	CN-OR16JC-72872-37V-A58M	SCA	CN-09RRC7-48729-372-08CV
29	SCA	CN-OR16JC-72872-37V-ARKM	SCA	CN-0C639N-71616-374-0HXB
30	SCA	CN-OR16JC-72872-37O-AP3B	SCA	CN-09RRC7-48729-373-0T6K
31	SCA	CN-OR16JC-72872-37V-A8RM	SCA	CN-09RRC7-48729-37A-03RM
32	SCA	CN-OR16JC-72872-37U-AF9M	SCA	CN-09RRC7-48729-36U-0CCN
33	80042000609355	CN-04FF47-64180-4BU-O8KI	SCA	CN-09RRC7-48729-488-0RUN
34	80042000609333	CN-04FF47-64180-4BS-1H3I	SCA	CN-09RRC7-488-0RT3
35	80042000609367	CN-04FF47-64180-4BS-12MI	SCA	CN-09RRC7-48729-485-177T
36	80042000609325	CN-04FF47-64180-4CD-2SKB	SCA	CN-09RRC7-48729-488-0RF4
37	80042000609342	CN-04FF47-64180-4BS-1GTI	SCA	CN-09RRC7-48729-488-0RTB
38	80042000609326	CN-04FF47-64180-4BS-12HI	SCA	CN-09RRC7-48729-486-0D6A
39	80042000609358	CN-04FF47-64180-4CD-2RQB	SCA	CN-09RRC7-48729-488-0RT6
40	80042000609375	CN-04FF47-64180-4BS-1EYI	SCA	CN-09RRC7-48729-371-1KRF
41	80042000609329	CN-04FF47-64180-4BS-135I	SCA	CN-09RRC7-48729-488-0S75
42	80042000609328	CN-04FF47-64180-4BS-2QYI	SCA	CN-09RRC7-48729-486-0D5T
43	80042000609335	CN-04FF47-64180-4CC-OF5B	SCA	CN-09RRC7-48729-488-0RFY
44	80042000609334	CN-04FF47-64180-4BS-12SI	SCA	CN-09RRC7-48729-481-0MUY
45	80042000609341	CN-04FF47-64180-4BS-1ECI	SCA	CN-09RRC7-48729-485-0D8P
46	80042000609339	CN-04FF47-64180-4BS-1EKI	SCA	CN-09RRC7-48729-485-178L
47	80042000609353	CN-04FF47-64180-4BS-114I	SCA	CN-09RRC7-48729-487-0LR7
48	80042000609372	CN-04FF47-64180-4BS-2PCI	SCA	CN-09RRC7-48729-488-0RTK
49	80042000609387	CN-04FF47-64180-4BU-09BI	SCA	CN-09RRC7-48729-487-0LR5
50	80042000609340	CN-04FF47-64180-4BS-123I	SCA	CN-09RRC7-48729-374-03ZR
51	80042000609343	CN-04FF47-64180-4BS-12QI	SCA	CN-09RRC7-48729-488-0S5S

Nota: Monitores y mouse que se encuentran en el bloque D.

4.5.2 Riesgos Indirectos

Para este proceso se consulta cuáles son los tipos y riesgos indirectos que se pueden presentar en el Data Center tomando como referencia los siguientes:

- **Derrame de líquidos.** Puede existir goteras dentro del Data Center lo que ocasiona que los equipos se dañen y dejen de funcionar, la existencia de goteras se debe a canales rotos, o mal puesto y/o fracturas en la estructura del techo dadas por movimientos telúricos espontáneos en la ciudad.

- **Perdida de clima**. - Un Data Center debe tener equipos de refrigeración de temperatura que va de acuerdo con el medio ambiente por lo que su refrigeración debe ser la adecuada y se debe poder regularla ya que este se puede perder por varios motivos.

- **Mala manipulación de los equipos**: En ocasiones por falta de conocimiento o descuido los operadores pueden hacer mal uso de los equipos como por ejemplo ocasionar un apagado no planificado.

- **Contaminación del aire:** En este caso se toma en cuenta la presencia de polvo o contaminación excesiva dentro del Data center.
- **Incendios. -** El fuego es el principal enemigo de un Data Center. Este se puede dar por el constante funcionamiento de los equipos.
- **Humedad**: puede ocasionar relativamente daños en los equipos, como por ejemplo la humedad excesiva puede derivar a una destilación a diferencia de la humead relativa baja, puede ocasionar corrientes estáticas. Por lo que los dos tipos de humedad son perjudiciales para el Data center.
- **Suministro eléctrico**: El fallo de una instalación eléctrica o de algún conector eléctrico, una mala conexión, un tipo de cableado mal estructurado, pueden provocar desastres graves en un Data Center
- **Robo:** Existen personas mal intencionadas que en un acto vandálico pueden apoderarse de los equipos y ocasionar grandes pérdidas.

- **Perdida de información-** Esto se puede dar debido al robo de información o a su vez mal manejo y control de los sistemas, así como también la falta de un antivirus, ya que las amenazas de virus son muy frecuentes.

Infraestructura Externa

Se hace referencia la Estructura del bloque D. que está conformado de 2 pisos divididos de la siguiente manera.

Bloque D, Segundo Piso

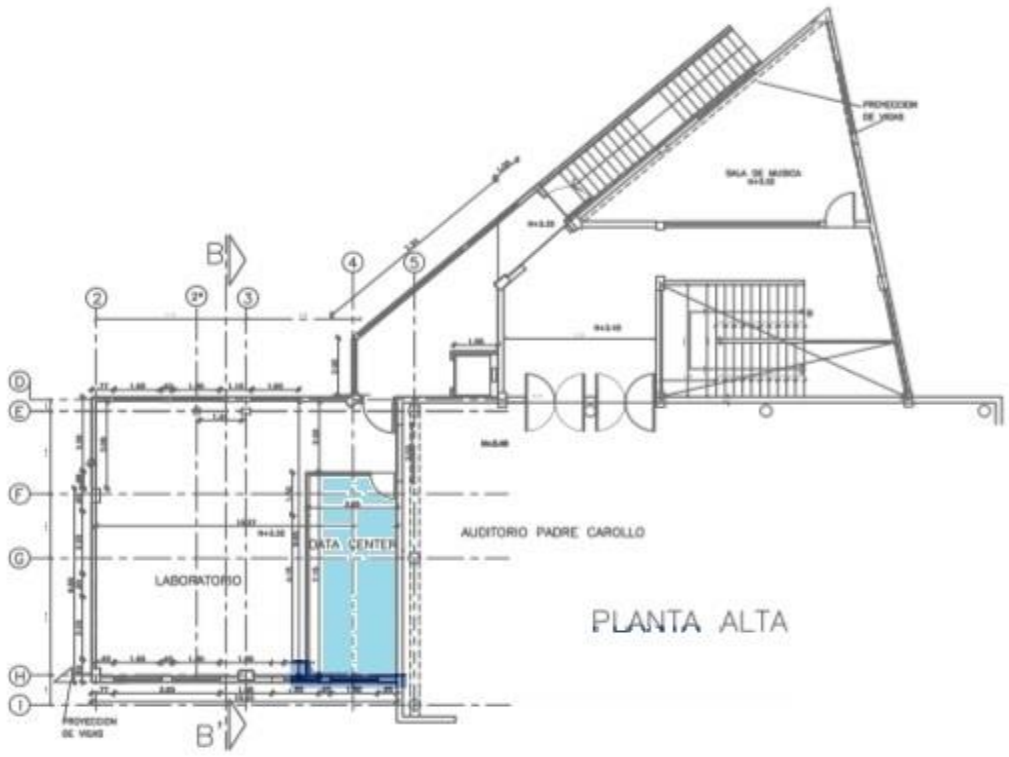


Figura 19. Plano de ubicación del Data Center
Elaborado por: Jorge Nuñez

Figura 18. Plano de ubicación del Data Center
Elaborado por: Jorge Nuñez

Riesgos Naturales

Este tipo de riesgos son los que más daño pueden causar y a los que mayor interés se les debe dar al momento de elaborar un plan de emergencia, para lograr salvaguardar las vidas y proteger los equipos en un alto porcentaje.

Se han identificado varios tipos de riesgos naturales a los cuales esta propenso a sufrir el DC, entre ello definimos los más importantes:

- Vulcanismo.
- Sismicidad
- Inestabilidad
- Inundaciones

En estos casos cualesquiera de estos desastres naturales van de la mano ya que provocan derrumbes, y colapso de los equipos, así como también daños humanos y económicos.

4.6. Evaluación de los riesgos

Tomando en cuenta que los Data Centers deben estar preparados para continuar con su función normalmente a pesar de cualquier situación que se presente.

Esto se puede lograr con la implementación de conexiones, elementos, áreas o servicios redundantes. Por lo que a continuación se realiza el análisis de los riegos mencionados. Tomando en cuenta los daños que se efectúan de acuerdo a los riesgos citados anteriormente. Así mismo se considera que los activos fijos que hay que proteger en caso de una eventualidad, considerando que los siguientes puntos son los valores a analizar.

- La interrupción del servicio (IS).
- Interrupción del monitoreo y gestión (Adm).
- Seguridad de la información (SI).

- Alteración de la información (AI).
- Fuga de información (FI).

A estos se tomará valores entre 1 el valor más bajo y 5 valor más alto.

Para este propósito se analizan tres aspectos fundamentales de los datos como la disponibilidad, confidencialidad e integridad, para determinar los activos graves que deben ser valorados y protegidos. Para esto se aplicará una fórmula matemática de los mismos que tengan un valor de 10. Como se muestra a continuación:

$$Disponibilidad = IS\ (10) + Adm\ (10) + IS\ (10) = 30$$

$$Confindencialidad = SI\ (10) + A\text{l}\ (10) + (10) = 30$$

$$Integridad = IS\ (10) + Adm\ (10) + AI\ (10) = 30$$

De lo que se obtiene un resultado de:

$$Total = Confindencialidad\ (10) + Integridad\ (10) + Disponibilidad\ (1) = 30$$

Para la ponderación se ocupará un rango de 1 a 10 así:

$$Ponderado = (Total * 10) / 30$$

$$\text{P}onderado = (10 * 10) / 30$$

$$Ponderado = 10$$

Es decir, el nivel de gravead que tiene cada uno de los activos mencionados es el ponderado:

Tabla 11. Equipos a proteger

Activo	IS	Adm	SI	AI	FI	Conf.	Int.	Disp.	Total	Ponderación
Servidores	10	10	10	5	5	30	30	30	30	10
Almacenamiento	10	10	10	5	5	30	30	30	30	10
Switch SAN	5	10	10	5	5	30	30	30	30	10
Core	5	6	6	2	2	10	18	22	50	6
Gestión	5	5	4	2	2	6	22	22	50	6
Acceso a Activos	5	3	4	2	2	6	18	18	42	4
Monitoreo	4	4	4	2	2	6	14	20	34	4
Energía	10	4	4	2	2	6	20	14	26	6
Clima	10	2	4	2	2	6	14	30	34	4
Software de administración y gestión	10	5	5	5	4	14	30	18	88	10
Software de Monitoreo	8	4	4	2	3	12	18	6	50	6
Varios	2	2	2	2	2	6	6	20	18	2

Nota: Ponderación de equipos a proteger de bloque D. (Ati, https://dspace.ups.edu.ec/handle/123456789/15904, 2018)

De esta manera se obtiene los resultados acerca de los componentes que hay que salvar en caso de algún riesgo, indicando que el valor máximo es 15, el mismo que se usa para una ponderación dentro de un rango de 1 a 5

Para la evaluación de los riesgos que, del Data Center, se considera:

- Aspectos geográficos del bloque.
- Materia estructural del bloque.
- Vulnerabilidades.
- Amenazas.
- Componentes del bloque.

Estos riesgos has sido analizado con valores de 7 características determinadas por las Normas ISO 27005, donde se encuentra detallado los valores para poder realizar la evaluación de los desastres.

Mediante una investigación se tomaron los valores de 1 a 5, de manera cuantitativa para esta evaluación, donde 1 es bajo y 5 alto. Con esto lo que realizamos una operación de suma en cada resultado obtenido en cada escenario, es decir el valor máximo es 35 y el mínimo es 7.

A continuación, se muestra los riesgos desde el más alto hasta el más bajo, Determinados de acuerdo al análisis realizado.

Tabla 12. Tabla de Impacto

Riesgo s / Parámetro	Suministro eléctrico	Inundación	Sismo	Viento Fuerte	Incendio	Tormenta Eléctrica	Erupción volcánica	Manifestaciones civiles violentos	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

Nota: Riesgo de impacto que causa estos desastres y sus porcentajes de gravedad donde 1 es poco riesgo con rango del 1% al 20%, 2 riesgos medio con rango de 21% al 40%, 3 medio con rango de 41% a 60%, 4 medio alto con rango del 61% al 80% y 5 alto con rango de 81 al 100%.

(Ati, https://dspace.ups.edu.ec/handle/123456789/15904, 2018)

De la tabla anterior se puede apreciar los porcentajes de riesgo que se resalta en cada uno de los rangos que se presentan obteniendo que el factor de ataques informáticos es el más grave con un 83% valor 5 y siendo el menos grave el factor de inundación con un 29% valor 3.

Para el análisis del impacto de riesgos lo que se hace es identificar tanto los proceso como procedimientos de los servicios principales para que por más crítico que sea el impacto, los servicios sigan funcionando normalmente. Los procedimientos y recursos se los clasificara de acuerdo a su prioridad.

Con ello podemos medir el tiempo máximo que se puede dejar de ejecutar una actividad sin que esto desenlace en una pérdida de información y también perdida económica, provocando molestias, penalizaciones entre otros.

Para lo cual se realiza la evaluación colocando los activos de mayor gravedad a menos gravedad.

Tabla 13. Valoración de activos

Riesgo / Activo	Ataque informático	Sismos	Suministro eléctrico	Tormenta eléctrica	Incendios	Erupciones volcánicas	Negligencia	Climatización	Atentados terroristas	Vientos fuertes	Manifestaciones civiles violentas	Inundaciones
Servidores	*2*	*24*	*2*	*0*	*N/d*	*24*	*1*	*1*	*N/d*	*2*	*2*	*1*
Almacenamiento	*2*	*24*	*2*	*0*	*N/d*	*24*	*1*	*1*	*N/d*	*2*	*2*	*1*
Switch SAN	*2*	*24*	*2*	*0*	*N/d*	*24*	*1*	*1*	*N/d*	*2*	*2*	*1*
Software de administración y gestión	*2*	*24*	*2*	*0*	*N/d*	*24*	*1*	*N/A*	*N/d*	*N/A*	*N/A*	*N/A*
Hipervisor	*2*	*24*	*2*	*0*	*N/d*	*24*	*1*	*N/A*	*N/d*	*N/A*	*N/A*	*N/A*
Core	*2*	*24*	*2*	*1*	*N/d*	*N/A*	*2*	*5*	*N/d*	*N/A*	*N/A*	*2*
Sistema de energía continua	*N/A*	*24*	*2*	*0*	*N/d*	*1*	*1*	*N/A*	*N/d*	*2*	*2*	*1*
Software de Monitoreo	*8*	*N/A*	*4*	*N/A*	*N/d*	*N/A*	*5*	*N/A*	*N/d*	*N/A*	*N/A*	*N/A*
Sw administración	*2*	*24*	*2*	*0*	*N/d*	*N/A*	*1*	*5*	*N/d*	*N/A*	*N/A*	*2*
Climatización	*N/A*	*24*	*1*	*0*	*N/d*	*1*	*1*	*1*	*N/d*	*1*	*1*	*1*
Equipo de monitoreo	*N/A*	*24*	*2*	*1*	*N/d*	*3*	*2*	*3*	*N/d*	*N/A*	*N/A*	*1*
Sw acceso	*4*	*24*	*2*	*1*	*N/d*	*N/A*	*2*	*5*	*N/d*	*N/A*	*N/A*	*2*
Varios	*N/A*	*24*	*4*	*4*	*N/d*	*N/A*	*5*	*N/A*	*N/d*	*N/A*	*N/A*	*N/A*

Nota: Tabla Cuantitativa de los activos en riesgo en caso de una eventualidad que atente con la continuidad de las operaciones. Siendo 1 No Perceptivo, 2 Bajo, 3 Normal ,4 Alto y 5 Emergencia **(Ati, https://dspace.ups.edu.ec/handle/123456789/15904, 2018)**

Analizando la tabla anterior se evidencia que frente a un ataque informático todos los activos de servicios seguirán brindando, almacenando o compartiendo información en orden de gravedad. En ese caso serán los últimos en almacenarse teniendo en cuenta que se puede provocar perdida de información.

A los activos de energía continua, climatización y varios se obtuvo valor de 1 por lo cual serán los primeros en almacenarse.

Lo que se espera que el resultado sea el total respaldo de todos los activos sin que exista perdidas y a su vez no sea necesario recuperarlas de forma exhausta permitiendo que el Data Center siga funcionando con normalidad.

Tomando en cuenta que el Data Center se mantiene en funcionamiento las 24 horas durante los 7 días de la semana esto lo hace automáticamente manteniendo un nivel bajo, en horas en la noche, y el día, Es decir en horario donde existe grupos grandes funciona de manera más rápida asegurando el buen resguardo de información. Debido en que en ese tiempo existe embotellamiento por la candad de respaldos que hay que guardar, debido a eso se considera identificar el rango de espacio en tiempo que existe para seguir almacenando información respaldándola sin que ningún desastre pueda ocasionar algún tipo de perdida. Lo mencionado anteriormente se podría describir a continuación:

Tabla 14. Tiempos máximos de respaldos en caso de una catástrofe

Riesgo / Activo	Ataque informático	Sismos	Suministro eléctrico	Tormenta eléctrica	Incendios	Erupciones volcánicas	Negligencia	Climatización	Atentados terroristas	Vientos fuertes	Manifestaciones civiles violentas	Inundaciones
Servidores	2	24	2	0	Ind	24	1	1	ind	2	2	1
Almacenamiento	2	24	2	0	Ind	24	1	1	ind	2	2	1
Switch SAN	2	24	2	0	Ind	24	1	1	ind	2	2	1
Software de administración y gestión	2	24	2	0	Ind	24	1	N/A	ind	N/A	N/A	N/A
Hipervisor	2	24	2	0	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	Ind	1	1	N/A	ind	2	2	1
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	Ind	N/A	1	5	ind	N/A	N/A	2
Climatización	N/A	24	1	0	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

Nota: Tabla que describe de los tiempos que se tardaría en dejar de funcionar cada activo pendiendo del desastre que se presente.

(Ati, https://dspace.ups.edu.ec/handle/123456789/15904, 2018)

Se toma en cuenta que los espacios que la tabla presenta es también para el mantenimiento que de sebe dar al Data center además de analizar algún tipo de corrección para su correcto funcionamiento. Estos deben hacerse constante y anticipadamente de tal manera que si se presenta alguna amenaza estos deben seguir funcionando guardando los respaldos

4.7. Prevención y Control de riesgos.

El bloque D de la UPS campus sur cuenta con recursos señaléticas de evacuación, y sistemas de alarma, así como también con equipos de emergencia que se encuentran distribuidos de la siguiente manera

- **Piso 1:**

Bloque D

Figura 20. Señalética y sistema de emergencia del primer piso bloque D.
Elaborado por: Jorge Nuñez

- ***Piso 2:***

Bloque D

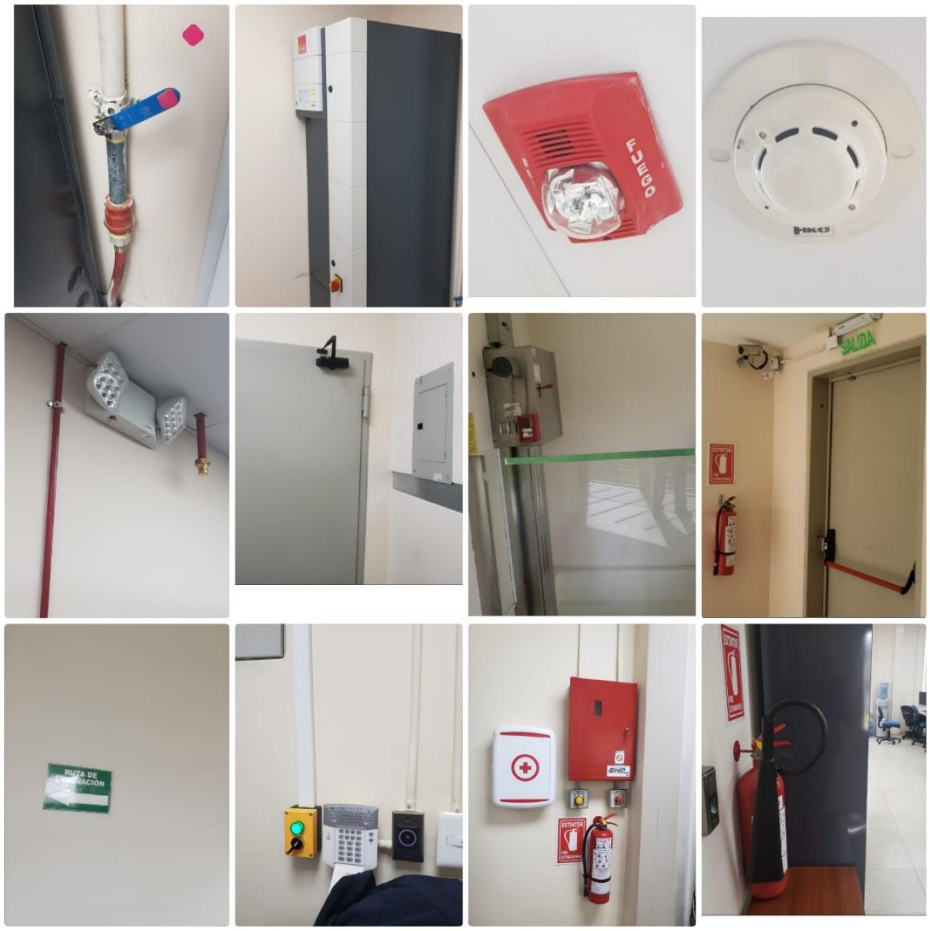


Figura 21. Señalética y sistema de emergencia y seguridad del segundo piso bloque D.
Elaborado por: Jorge Nuñez

Según lo recopilado se describe que se cuenta con:

- 4 extinguidores
- 1 sistema corta fuego
- 1 ruta de evacuación

- 1 rampa para discapacidad con su señalización
- Sistemas de seguridad

4.8. Protocolos de intervención ante emergencias

En caso de unas emergencias debe organizar con anterioridad brigadas las mismas que deben cumplir con sus funciones antes durante y después del suceso.

Mapa de asignaciones y brigadas

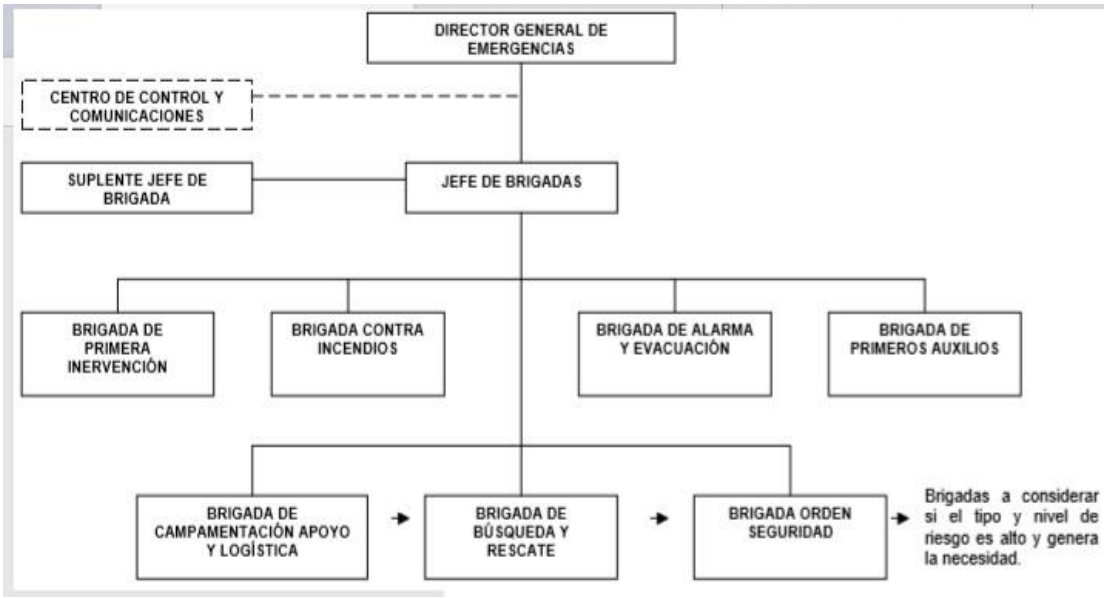


Figura 22. Mapa de asignaciones y brigadas tomado de (Cuerpode bomberos del distrito metropolitano de Quito, 2009)

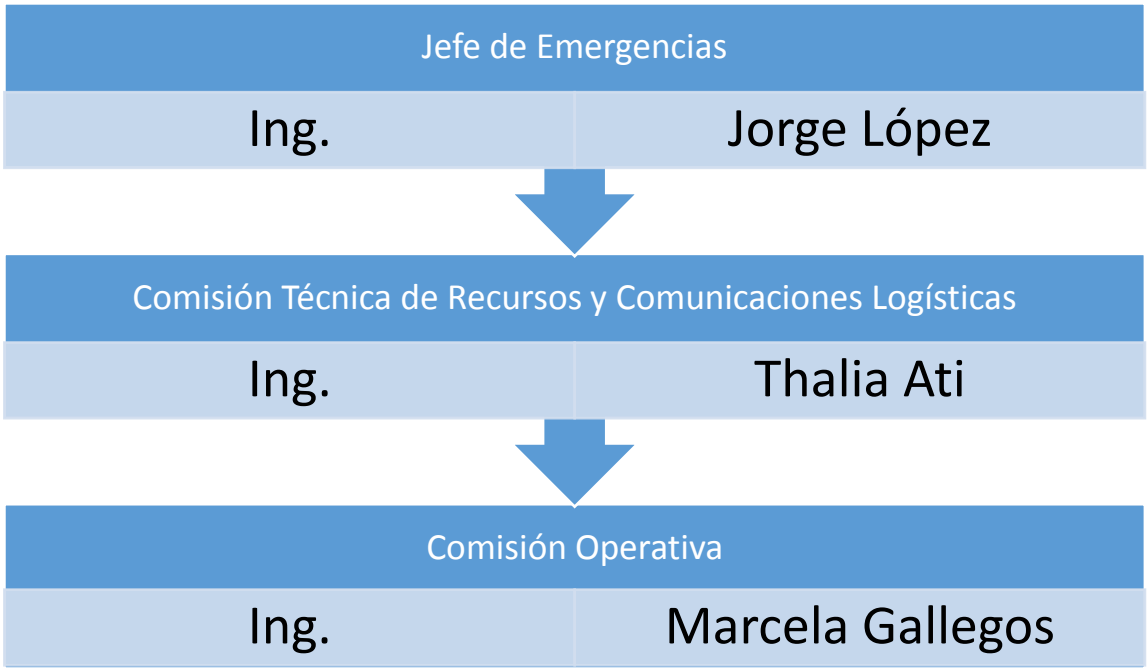
Elaborado por: Jorge Nuñez

4.9. Funciones de las Brigadas de Alarma y Evacuación

4.9.1. Comité de Emergencias (CE):

Son responsables de coordinar y administrar las actividades preventivas, correctivas y durante una emergencia. Para el análisis de las amenazas, vulnerabilidades y diseño de las estrategias del Plan de Emergencias son los administradores del DC.

El comité de emergencias para el DC está organizado de la siguiente mañera:



4.9.1.1.Funciones del Jefe de Emergencias:

Responsable: Ing. Jorge López

Funciones preventivas

- Coordinación y evaluación de las acciones de las comisiones.
- Establecer comunicación constante con las directivas de la UPS.
- Establecer presupuestos recurrentes para el buen funcionamiento del PE.
- Coordinar las responsabilidades del CE.
- Organizar reuniones periódicas con el CE.
- Dar reportes a las autoridades sobre todo los aspectos que contempla el PE.

Funciones durante la emergencia:

- Dictar estado de emergencia.
- Coordinar decisiones durante la emergencia.
- Establecer comunicación en el CE.
- Recolectar la información de la emergencia suscitada.
- Coordinar las decisiones extraordinarias no contempladas en el PE.
- Dictar la finalización del estado de emergencia.

Funciones correctivas:

- Coordinar las acciones de PE guiador por el Plan de Continuidad de Negocio. (Ati, https://dspace.ups.edu.ec/handle/123456789/15904, 2018)

- Evaluar las acciones y procedimientos realizados durante la emergencia.
- Pedir informes a cada uno de los integrantes del PE.

Para esto el jefe emergencias debe tener en cuenta lo siguiente:

- Tener lista de teléfonos internos y externos. (Anexo E, Anexo F)
- Tener lista de recursos.
- Tener Planos y Mapas del bloque D del Campus Sur de la Universidad. (Figura 18, Figura 19).
- Tener medio de comunicación (Teléfonos, radios portables, celular, entre otros)
- Conocer íntegramente le PE.
- Conocer las funciones del CE.

4.9.1.2.Comisión Técnica de Recursos y Comunicaciones Logística

Responsable: Ing. Thalia Ati (Técnica Operativa)

Objetivo: Su función principal es coordinar que se cuente con todos los recursos y activos que se necesitan durante una emergencia.

Funciones preventivas:

- Conocer las causas y efectos de las vulnerabilidades que posee el DC.
- Coordinar la prevención de las vulnerabilidades y riegos del DC.
- Coordinar acciones de prevención de los diferentes riesgos.
- Realizar informes de activos y equipos necesarios para contener los riesgos y mitigar las vulnerabilidades.

- Brindar mantenimiento a los diferentes recursos materiales y físicos del DC y en general del bloque D.
- Actualizar las tablas de control del PE.
- Informar a los demás miembros del comité de emergencias sobre cualquier cambio en las instalaciones de la Universidad
- Mantener actualizado un plan de contingencia para el control en las áreas más críticas del bloque D.

Funciones durante la emergencia:

- Analizar el comportamiento del riesgo, ubicar el sitio específico donde está sucediendo y cuantificar las posibles consecuencias de no informar oportunamente al Jefe de Emergencia.
- Mantener una relación permanente con el personar interno y externo de DC, para poder dar una adecuada directriz para el control del riesgo.
- Comunicarse con las instituciones de emergencia. (Anexo F)
- Aplicar Plan de Contingencia detallado en el Capítulo IV.
- Analizar y determinar las causas internas y externas que generaron la emergencia.

Funciones correctivas:

- Evaluar la causa – efecto de un siniestro y dar seguimiento al Plan de Contingencia.
- Realizar correctivos para mitigar en lo posible que vuelva a ocurrir la misma emergencia.

- Brindar informes técnicos causa – efecto al Jefe de Emergencia.
- Coordinar recursos que se podrían utilizar para futuros siniestros o emergencias.

4.9.1.3.Comisión Operativa

Responsable: Ing. Marcela Gallegos (Técnica Operativa)

Objetivo: Dirigir y controlar el Plan de Emergencia y Contingencia del Data Center

Funciones preventivas

- Proponer realizar simulacros constantes de emergencia en el DC.
- Actual alizar periódicamente el inventario de recursos del Plan de Emergencia.
- Garantizar que el PE funcione en su totalidad en tiempo real.
- Incentivar y promover en la Comunidad Salesiana la participación en el Plan de Emergencia.

Funciones durante la emergencia

- Comunicarse constantemente con el Jefe de Emergencia, para coordinar el manejo correcto de la emergencia.
- Velar por que se de primeros auxilios a todas las personas involucradas en la emergencia.

- Listar las personas que resulten lesionadas, especificando su estado de salud y coordinando el lugar donde fueron enviados, así como también los equipos del Data Center
- Garantizar el cumplimiento del Comité de Emergencia.
- Solicitar y coordinar el apoyo externo.
- Coordinar las rutas de evacuación. (Anexo B, Anexo C, Anexo D)

Funciones después de la emergencia

- Determinar e implementar las acciones correctivas resultantes de la evaluación.
- Mantener relación constante con lugares de salud para tener un mapa actualizado de la ubicación de los mismos.
- Velar por la reposición de recursos utilizados en la emergencia.
- Brindar un informe de actividades realizadas al Jefe Emergencias constantemente.

4.10. Evacuación

Para la evacuación también se dirige por medio de una brigada para lo cual se puede seguir los siguientes lineamientos:

Antes de la emergencia:

- Conocer integrante el PE y las rutas de evacuación que constan en los anexos de este trabajo, tanto la ruta de evacuación principal como la alterna, e inspeccionarlas periódicamente, En caso de no tener suficientes señaléticas sugerir la implementación de las mismas a la administración del campus.

- Listar periódicamente las personas que laboran en el DC.
- Informar anomalías al Jefe de Emergencias para prevenir siniestros.
-

Durante la emergencia:

- Si se escucha la sirena de emergencia, primeramente, chequear el área afectada cuantas personas están involucradas y brindar información sobre una posible evacuación.
- Si encuentra una novedad como presencia de humo, paquete sospechoso u otro factor que pueda desencadenar una emergencia debe notificar al jefe encargado.

En caso de alarma de evacuación:

- Evacuar e indicar las rutas de evacuación a las personas que estén involucradas el momento de una emergencia. (Anexo B, Anexo C, Anexo D).
- Inspeccionar rápidamente todas las áreas asignadas.
- Asegurarse de dejar las puertas de las salidas de emergencia sin seguro o llave.
- Impedir que cualquier persona no autorizada regrese al lugar del siniestro.
- Controlar las aglomeraciones o desordenes sociales que den origen al pánico en la zona de emergencia.
- Ayudar a las personas que presenten impedimentos físicos para la evacuación.
- Coordinar cuando la ruta principal de evacuación este cerrada se use la ruta secundaria.
- Cuando por algún motivo no se pueda usa ninguna de las rutas de evacuación, buscar un lugar seguro para llevar a las personas involucradas en la emergencia.
- Siempre mantener la calma y gritar frases como: “no corran”, “conserven la calma”, “circulen por la derecha”, etc.

- Dar instrucciones al personal de su área de permanecer en el lugar específico y en completo orden y silencio para facilitar el conteo.
- En el punto de encuentro, verificar que todas las personas que se encontraban en el edificio este a salvo.
- Informar anomalías al Jefe de Emergencias para prevenir siniestros.

Después de la emergencia:

- Solo el Jefe de Emergencia podrá autorizar el regreso al bloque D, siempre siguiendo los parámetros y recomendaciones del PE.
- Ayudar a la coordinación de las actividades para agilizar el restablecimiento a la normalidad.

4.11. Plan de Contingencias

Conforme al análisis de riesgos y vulnerabilidades realizada, se puede sugerir procedimientos para combatir potencialmente que un siniestro netamente antrópico pueda repetirse y así precautelar la perdida de información, daño de equipos o poner en peligro a estudiantes, docentes y administradores dentro del bloque D.

El Plan de Contingencia para el Data Center plantea algunas recomendaciones para en lo posible mitigar la incidencia de siniestros causados por el personal inmerso en él.

Las recomendaciones son las siguientes:

4.11.1 Recomendaciones A Nivel Físico

Se recomienda realizar lo siguiente, frente a este riesgo potencial.

- Primero, el Data Center no tiene que ser accesible físicamente a cualquier persona que no sean Personal Autorizado, Administrador o Técnicos Operativos del mismo.
- Segundo, es primordial que exista un lugar físico donde esté ubicado el Data Center, el acceso a este debe concederse únicamente al Personal Autorizado, y el espacio físico deberá cumplir con especificaciones puntuales y adecuadas que conlleve a su funcionamiento óptimo, por ejemplo, climatizador ambiental adecuado, aislamiento del lugar físico contra polvo y gases.
- Tercero, siempre debe existir lugares expuestos y de fácil acceso donde se encuentren visibles los números telefónicos de emergencia. (Anexo E, Anexo F)
- Cuarto, el bloque D, así como todos los bloques que componen el campus sur de la UPS deberá tener los siguientes elementos para protección y acción en caso de una emergencia:
    - Sistema contra incendios.
        - Extintores (Usar Anexo G)
        - Sensores de humo.
        - Botón de pánico.
        - Luces electrobioscopias.
        - Sirena de emergencia.
    - Botiquín de primeros auxilios.
    - Plan de Emergencia del Data Center.

- Información visual de planes de evacuación y rutas de escape
- Información de puntos de encuentro.

4.11.2 Recomendaciones A Nivel Lógico

Tener habilitado un cortafuego que evite ingresos no deseados de redes fuera del perímetro del campus sur hacia el sistema de cámaras de seguridad y red del Data Center. Para llevar a cabo esto se puede seguir las siguientes directrices:

- Primero, se recomendaría configurar adecuadamente el firewall dentro de la red del Data Center.
- Segundo, se recomienda que todos los activos de hardware posean en sus características de fabrica la implementación de un cortafuegos.
- Tercero, instalar un sistema que permita la detección de intrusos y permita monitorear los accesos no autorizados a la red y al sistema del Data Center.
- Cuarto, capacitar a los técnicos operativos y administrador del Data Center para el manejo correcto de contraseñas que contenga unos estándares mínimos de seguridad, por ejemplo, no usar contraseñas básicas o fáciles de ser descifradas.
- Quinto, solo se permitirá la instalación de software con fines educativos o de índole administrativo en las computadoras de los laboratorios del bloque D y del área de monitoreo del Data
- Por último, se recomienda la tener contraseñas del BIOS y de acceso de usuario en todas las maquinas del área de monitoreo del Data Center.

Pueda que estas recomendaciones aumentarían relativamente los costos en materia de seguridad, pero al final se verán justificados los mismos cuando exista una expansión en el Data Center.

4.11.3 Recomendaciones para prevenir fallas en los equipos

- Primera, se recomienda designar a uno o a ambos técnicos operativos como las personas que coordinen el mantenimiento correctivo y también el preventivo a todos los equipos del Data Center y del área de monitoreo.
- Segundo, se recomienda contratar los servicios de alguna empresa que brinde mantenimiento físico y lógico a todos los activos de los diferentes laboratorios del bloque D.
- Tercero, se recomienda la utilización de un sistema de alimentación ininterrumpida o sus siglas en ingles UPS para que cuando ocurra un corte eléctrico los equipos puedan funcionar normalmente por un lapso de tiempo determinado y no existan sobrecargas en los mismos.

De igual manera estas recomendaciones pueda que incurran en costos de seguridad, pero de igual manera se verán justificados a medida que el Data Center crezca en activos y manejo de información, este tipo de mantenimientos se deberán realizar al menos dos veces al año.

4.11.4 Recomendaciones contra el robo de datos y fraude

El informarse de métodos actuales de vandalismo podrán guiar a los administradores del Data Center a estar conscientes de posibles problemas. Para defenderse de este tipo de desastres se puede recomendar lo siguiente:

- Publicar la Política de Seguridad de la Universidad si esta estuviese vigente.
- Siempre tratar de formar un criterio de responsabilidad y buena fe en los administradores, docentes y estudiantes que estén inmersos en todo el campus de la UPS.
- Poseer botones de pánico en todos los laboratorios y aulas dentro del bloque D.
- Una entrevista correcta y revisión de referencias a los aspirantes a trabajar en el Data Center podrá dar un mejor criterio de contratación de los mismos.
- Tener sistemas de cierres automáticos en todas las puertas del bloque D.
- Un ambiente limpio y ordenado de trabajo siempre es importante.
- El liderazgo del administrador es indispensable como ejemplo a seguir de los técnicos operativos.

4.11.5 Recomendación de protección para el correo corporativo

Recomendamos usar herramientas que permita implementar infraestructura de clave pública para la protección de la comunicación por correo electrónico la misma que implique el envío de información confidencial.

4.11.6 Recomendaciones para Respaldos o Backups de Información en el Data Center

El Data Center deberá obtener periódicamente copias de seguridad de información que se maneja ahí, así como de todos los activos y sistemas que aseguren el óptimo funcionamiento del DC y de las funciones que realiza en la Universidad.

Por ellos se recomienda tener:

- Respaldos del Sistema Operativo.
- Respaldos de los Datos que se procesan dentro del mismo:
    - Bases de Datos
    - Índices
    - Etc.
- Respaldos del Hardware, se puede contar con equipos respaldo por si alguno sufriera algún daño en un siniestro se pueda seguir con el procesamiento de datos dentro del Data Center.
- Respaldos en la nube, contratar el servicio de servidores web que permitan alojar ahí la información periódica e importante del Data Center.

4.11.6.1 Volumen de información a copiar

Existen varias estrategias que se pueden recomendar para la realización de respaldos o backups en el Data Center, a continuación, se mencionará las más importantes que se podría usar.

- **Backups sólo de los datos**: esta es una estrategia poco recomendable, ya que, en caso de siniestro, será necesario la recuperación de todo el entorno que proporciona el software para restaurar los mismos, esta estrategia ayuda poco al plan de recuperación de destres del DC.
- **Backups completos**: esta estrategia es recomendable, si se tiene espacio y el tiempo de respaldo no influye con el comportamiento normal del Data Center.
- **Backups incrementales**: en esta estrategia solo se respalda los cambios realizados desde la última vez que se realizó un backup por lo que es necesario el anterior backup para restaurar el sistema.
- **Backups diferenciales**: es esta estrategia tal como la incremental se guardan los últimos cambios realizados pero esta vez de todos los ficheros modificados, igualmente se necesita la copia de seguridad previa.

4.11.6.2 Tiempo disponible para realizar Backups

El respaldo de información es una media de contingencia de las más importantes pero el mismo tiempo se deberá evaluar la estrategia que más convenga para el funcionamiento continuo del Data Center, debido a que este proceso de respaldo puede durar minutos u horas y hay que tener en cuenta que mientras dura este proceso pueda que se necesite acceder a información que está siendo respaldada, por este motivo se recomienda que estos procesos se los realice fuera del horario laboral del administrador y técnicos operativos del Data Center.

4.11.6.3 Frecuencia de realización de copias de seguridad

Realizar backups en el DC está ligado directamente al literal anterior, y a la estrategia escogida la realización del backup.

4.11.6.4 Responsable del proceso

El Administrador o Jefe de Seguridad del Data Center deberá delegar al técnico responsable de las copias de seguridad del mismo.

CONCLUSIONES

Mediante el análisis y desarrollo del PE, se puede analizar las vulnerabilidades y riesgos que posee el DC de la UPS y con ello llevar a cabo acciones que permitan mitigar posibles daños o afectaciones que se puedan dar durante una emergencia en el mismo.

Con los resultados de los estudios de factibilidad se encontró que es completamente aplicable el Plan de Emergencia y Contingencia dentro del Data Center.

Se deberá realizar estudios constantemente para encontrar nuevas vulnerabilidades del Data Center producto del funcionamiento continuo del mismo, se debe realizar periódicamente el mantenimiento de todos los sistemas de alarmas, y protección que posee el Bloque D.

Una metodología SCRUM es completamente adaptable para el desarrollo del PE y Continencia, debido que al ser una metodología ágil nos permite optimizar tiempos y recursos para mediante iteraciones llevar a cabo este plan en el tiempo establecido.

El administrador y técnicos operativos del Data Center tienen el suficiente conocimiento del mismo para poder seguir los protocolos que plantea el Plan de Emergencia y Contingentica.

Es importante que la Universidad Politécnica Salesiana posea un espacio físico donde se aloje el DC para no tener servidores alojados en cada bloque de la misma y con ello facilitar el procesamiento y respaldos de la información.

Mediante la socialización del Plan de Emergencia y Contingencia se pudo formar comités Emergencia y dar responsabilidades a cada una de las personas encargadas de los mismos, para estar en lo posible lo mejor preparados ante una catástrofe o emergencia.

RECOMENDACIONES

Se recomienda tomar en cuenta los procesos de evacuación, los roles del Comité de Seguridad asignado en caso de riesgos o emergencia, para que de esta manera haya una mejor planificación para las medidas de acción.

También se recomienda tomar en consideración el Plan de Contingencia para poder activar el proceso de respaldo automático de información, así como planteamientos que procuren a la mejora continua de manejo de activos e información del Data Center.

Este proyecto no tendría sentido sin la socialización del mismo al personal que administra y opera el Data Center, así que después de implantado se debe dar la capacitación del mismo.

Por último, una actualización periódica del Plan de Emergencia y Continencia a fin de tomar en cuenta todos los cambios de activos, infraestructura, personal administrativo, docentes, estudiantes y de más involucrados en el Data Center.

LISTA DE REFERENCIAS

¿Qué es un Data Center? - acens blog. (23 de abril de 2008). Obtenido de acens blog: https://blog.acens.com/acens/que-es-un-data-center/

ARUS. (09 de julio de 2018). evolucón de los data center. Obtenido de https://www.arus.com.co/la-evolucion-de-los-data-center/

Ati, T. (08 de 2018). https://dspace.ups.edu.ec/handle/123456789/15904. Obtenido de http://dspace.ups.edu.ec/handle/123456789/15904

Ati, T. (2019). Formato Ingreso Docentes Laboratorios BLoque D. Quito, Pichincha.

Ati, T. (2019). Horarios LAb Bloque D. Quito.

blog de ISOTools Excellence. (12 de Abril de 2018). Blog especializado en Sistemas de Gestión. Obtenido de https://www.pmg-ssi.com/2018/04/iso-22301-plan-continuidad-negocio/

Camacho, M. (2017). Obtenido de INSTALACIÓN DEL CENTRO DE PROCESAMIENTO DE DATOS EN LA SEDE DE LA: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4956/51224%20-%20Camacho%20Suarez%20Manuel%20Gerardo...pdf?sequence=1

Castellanos, I. (23 de Abril de 2008). Acens Blog. Obtenido de https://blog.acens.com/que-es-un-data-center.html

Cesar Ortiz, A. (2016). FOROS DE SEGURIDAD. Obtenido de http://www.forodeseguridad.com/artic/discipl/4132.html

Cloud Magna. (5 de junio de 2016). Obtenido de https://cloudmagna.com/blog/que-es-un-data-center/

Consultores Tecnologicos Empresariales. (Septiembre de 2019). plan de Continuidad de negocio. Obtenido de https://www.cte.net.pe/plan-de-continuidad-de-negocio/

Copyright 2019 Tangient LLC. (1 de febrero de 2019). PROCESOS DE SOFTWARE. Obtenido de : https://procesosdesoftware.wikispaces.com/METODOLOGIA+SCRUM

Cuerpode bomberos del distrito metropolitano de Quito. (15 de junio de 2009). manual de plan de contigencias. 3.

ESCUELA POLITECNICA NACIONAL . (2015). SEGURIDAD DE INSTALACIONES. Obtenido de http://epn.gov.co/elearning/distinguidos/SEGURIDAD/45_plan_de_emergencias.html

Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica. (Septiembre de 2015). Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información. (P. Hidalgo, & V. Enriqez, Edits.) Obtenido de https://revistapolitecnica.epn.edu.ec/images/revista/volumen36/tomo1/MetodologiadeValuaciondeRiesgos.pdf

FUNDACIÓN FINE. (2012). Fundación para la Integración del Niño Especial. Obtenido de https://fineecuador.wordpress.com/2012/09/15/hello-world/

Grupo GT servicios integrales. (28 de junio de 22016). Obtenido de https://gt-grupo.com/normativas-aplicables/reglamento-de-instalaciones-de-proteccion-contra-incendios/

Lampre Formacion. (s.f.). Oferta Formativa. Obtenido de Plan de emergencia y autoprotección: https://www.lanpreformacion.com/planes-de-emergencia/

plagecons. (2018). INFRAESTRUCTURA PARA TECNOLOGÍA INFORMÁTICA. 25,26,27. (M. P. Quinga , Ed.) Recuperado el noviembre de 2019

Salguero, A. (4 de 12 de 2019). Costos Capacitaciones. (J. Nuñez, Entrevistador)

secretaria de gesión de riesgos. (mayo de 2014). manual el comite de gestion de riesgos. Obtenido de http://www.competencias.gob.ec/wp-content/uploads/2017/06/MANUAL01.pdf

Universidad Politecnica Salesiana. (18 de diciembre de 2019). Razon de Ser. Obtenido de Universidad Politecnica Salesiana: https://www.ups.edu.ec/razon-de-ser

Universidad Salesiana. (18 de diciembe de 2019). gestion documental de archivo. (L. Alvares, & J. Juncosa, Edits.) Obtenido de https://www.ups.edu.ec/web/guest/gestion-documental-archivo