UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

PROPUESTA DE DESARROLLO DE UN PLAN DE RECUPERACION ANTE DESASTRES PARA LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD DON BOSCO

PARA OPTAR AL GRADO DE MAESTRO DE:

SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

MODALIDAD PROYECTO DE IMPLEMENTACIÓN

ASESOR:

Mg. LEONARDO CASTILLO

PRESENTADO POR:

ING GERSON QUINTANILLA

ING. ANDY OSEGUEDA

ANTIGUO CUSCATLÁN, LA LIBERTAD, EL SALVADOR, CENTROAMÉRICA
ENERO DE 2018

Tabla de Contenidos

Lista de figuras

Lista de tablas

Introducción

En la actualidad muchos de los riesgos que se ciernen sobre las empresas no son predecibles y siempre se está a merced de ser víctimas de algún suceso el cual pueda amenazar el funcionamiento normal de estas lo cual pueden traducirse en pérdidas económicas, de prestigio o en los casos más extremos forzar al cierre de estas, por lo que las organizaciones deben enfrentar la realidad y desarrollar sus propios planes para actuar frente a este tipo de situaciones como es el ataque de virus informáticos, intrusiones no autorizadas, interrupciones en las cadenas de abastecimiento o distribución o pérdida de personal clave; solo para mencionar algunos.

Estos planes deben partir de una adecuada evaluación de la situación de riesgos informáticos y operacionales de la organización, que permita definir un plan consistente con la realidad de la misma. Los planes deben, como mínimo, actualizar de manera permanente las direcciones y números de teléfono de los empleados clave, así como una adecuada documentación de las operaciones críticas, proveedores y suministradores de servicios contingentes.

En el presente documento se plantea la importancia de la implementación de controles y procesos los cuales garanticen la continuidad de funciones de la infraestructura de red de la Universidad Don Bosco, así mismo se presenta la estructura de la ISO 22301:2012, la cual es la base para la realización del análisis de las medidas a tomar en cuenta para garantizar el funcionamiento de la infraestructura de red ante un evento disruptivo, para este fin se ha realizado un análisis de la situación actual en la que está la Universidad y se propone un plan de recuperación ante desastres.

Se procederá a la entrega de documentos después del análisis los cuales serán la evaluación de riesgos de los activos de la Universidad y el plan de recuperación de desastres (DRP), el cual está compuesto de varias partes importantes como son contactos de las personas involucradas en el plan de recuperación, los líderes de equipos y los contactos de los proveedores en caso de ser necesario para restaurar los servicios de red que se definieron como críticos en la Universidad.

Este trabajo se enfoca en la problemática que tiene la Universidad en cuanto a los procesos necesarios para garantizar la recuperación de las funciones básicas ante un evento disruptivo, que si bien se ha comenzado a trabajar en este tema aún no se ha formalizado totalmente y lo que se pretende es que este documento sea de ayuda para la mejora de la recuperación de funciones en el área de informática de la Universidad y sus procesos.

OBJETIVOS

Objetivo General

Diseñar, implementar o complementar un plan de recuperación de desastres de la infraestructura de red de la Universidad Don Bosco mediante la identificación y clasificación de sus procesos críticos encontrados en conjuntos con las partes interesadas (negocio y TI), así como del análisis y tratamiento de los riesgos identificados.

Objetivos Específicos

- Diseñar un plan de recuperación de desastres (DRP) para los procesos de la infraestructura de red.
- Realizar la definición y clasificación de los procesos críticos del área de infraestructura de red en conjuntos con las partes interesadas (negocio y TI).
- Evaluar, clasificar y posteriormente tratar los riesgos críticos identificados a los que se encuentra expuesto el campus Soyapango que atenten con las funciones normales de la infraestructura de red.

Análisis del problema

En este momento la Universidad Don Bosco no cuenta con un Plan de Recuperación ante Desastres lo suficientemente robusto el cual provea de herramientas robustas que garanticen la continuidad de las operaciones ante un evento disruptivos, lo cual en este momento sería catastrófico tanto a nivel operacional como de imagen de la institución, cabe mencionar que en estos momentos se están tomando las medidas respectivas para tratar de mitigar las consecuencias ante un evento de esta naturaleza aún no se encuentra lo suficientemente maduro para garantizar una continuidad del negocio básica.

Alcance del proyecto

Este proyecto tendrá como alcance el análisis de riesgos y elaboración del DRP para los procesos críticos en la infraestructura de red de la Universidad Don Bosco (UDB) el cual será el entregable de este proyecto/investigación y quedara a la disposición de la Universidad si continuar con la mejora continua del proyecto entregado en esta investigación.

Limitantes

- Falta de planes conexos los cuales provean a la unidad de TI las herramientas ante el acontecimiento de eventos los cuales atenten el correcto funcionamiento de la infraestructura de red de la Universidad.
- Falta de procesos interrelacionados los cuales incluyan a todas las áreas (TI, contabilidad, financiera, auditoria y académica) interesadas y que garanticen la continuidad de negocio
- Falta de documentación de procesos de la operación
- Falta de documentación actualizada de los activos, diagramas y configuración de los equipos de la infraestructura de red

Justificación del proyecto

Dar o mejorar la base de continuidad de negocio en el área de IT de la Universidad don Bosco la cual a pesar de que ya posee cierto trabajo inicial en este aspecto, aún tiene trabajo por realizar y complementar en otras áreas, lo cual es la idea principal de este proyecto, complementar o generar conocimiento en algunas áreas de la infraestructura de la Universidad Don Bosco específicamente el área de informática.

En este proyecto se planteará un DRP (Disaster Recovery Plan) y una evaluación de riesgos para la Universidad Don Bosco específicamente para el área de infraestructura de redes, además se crearán unos procesos propuestos que son los que se someterán a aprobación, de ser necesario, a las autoridades de la Universidad posteriormente a la investigación por parte del área de informática de la Universidad.

Dentro de este contexto será necesario un análisis de frameworks entre los cuales se puede mencionar COBIT, ISO 22301, los documentos de ISACA: ESCENARIOS DE RIESGO. Usando COBIT 5 para Riesgo y Programa de Auditoría / Aseguramiento de la Gestión de Continuidad del Negocio; además se consultara información complementaria en diferentes

páginas y blogs en internet. La información de la situación actual de la Universidad en el área de informática será obtenida por medio de las autoridades siguientes: Vicerrector Académico, Director de infraestructura y Auditor interno.

CAPÍTULO I

Marco teórico

1.1 ISO 22301:2012 (Gestión de continuidad de negocio)

1.1.1 Que es la ISO 22301:2012

ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio creada en respuesta a la demanda internacional que obtuvo la norma británica original BS 25999-2. La norma identifica los fundamentos de un sistema de gestión de continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.

La norma proporciona un marco que permite a las organizaciones identificar sus amenazas y fortalecer su capacidad, para así disminuir la posibilidad de ocurrencia de un incidente disruptivo, y en caso de producirse, estar preparada para responder de forma adecuada, reduciendo drásticamente el daño potencial que ese incidente puede causar a la organización[1]. El objetivo es que la organización se mantenga en funcionamiento durante y después de una interrupción, garantizando de esta forma que los productos y servicios serán entregados a los clientes puntualmente.

Si la interrupción no es una opción para el negocio, la implementación de la norma ISO 223010 es el primer paso hacia un enfoque de buenas prácticas pues como todas las normas ISO no solo está orientada a los cumplimientos de estándares internacionales, sino también se enfoca en la mejora continua de sus procesos, esto mediante la implementación del ciclo PDCA.

[1] La norma 22301:2012 contiene no solamente temas de continuidad de negocio, sino prepara a las organizaciones a cómo proceder en caso de eventos disruptivos

Figura 1. Diagrama de ciclo PDCA orientada a la ISO 22301:2012.

1.1.2 ¿Para qué sirve la ISO 22301:2012?

Esta norma sirve poder proteger a la organización (lo más posible) de interrupciones o pérdidas de servicios o producción por un incidente fuera o dentro de la organización y poder recuperarlo en un tiempo determinado y definido por la naturaleza de la organización o empresa, cabe destacar que estas actividades deben de estar en continua revisión y actualización tal como se muestra en la figura 2 por las partes interesadas de forma que garanticen que cuando ocurra un evento disruptivo las consecuencias se disminuyan para la empresa.

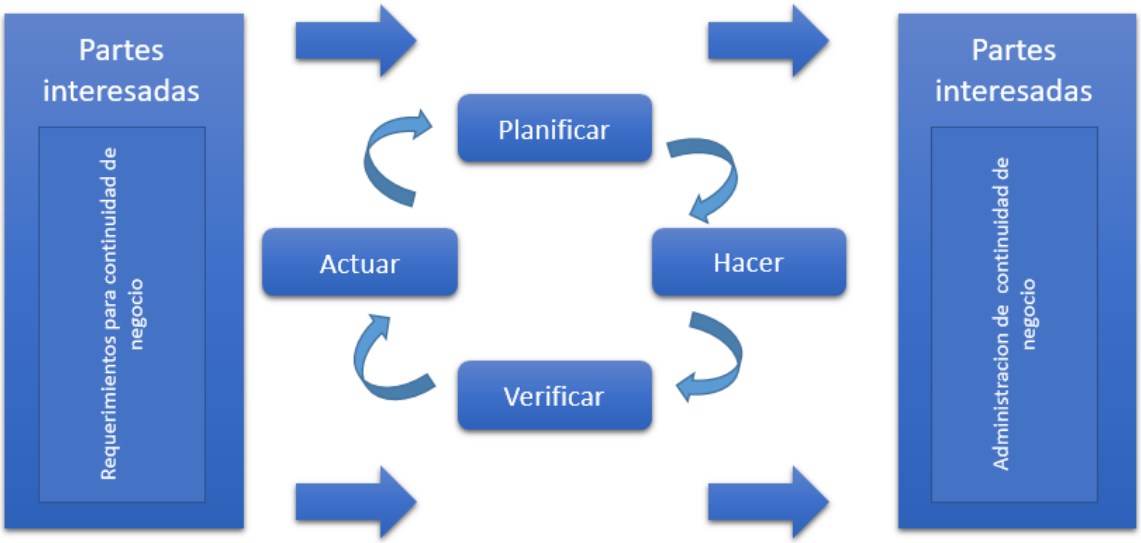

Figura 2. Diagrama de mejora continuidad de la ISO 22301:2012

1.1.3 Cuál es la importancia de la ISO 22301:2012

La implantación de la norma ISO 22301 permite a las organizaciones demostrar su capacidad para seguir funcionando con normalidad en caso de producirse una interrupción, minimizando sus debilidades y reforzando así sus fortalezas. La norma permite a las organizaciones:

- Establecer, implementar, mantener y mejorar los sistemas de gestión de continuidad de negocio.
- Cumplir con los requisitos de la política de continuidad de negocio.
- Proporcionar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente.
- Proporcionar un lenguaje común a organizaciones globales, especialmente a aquellas con una cadena de suministro larga y compleja.
- Protección de los empleados y reputación de la marca.

- Asegura la continuidad de negocio y de la comercialización de productos y servicios.
- Proporciona una base de entendimiento, desarrollo e implantación de la continuidad de negocio, aportando confianza tanto de negocio a negocio como de negocio a cliente.

La continuidad de negocio forma parte de la gestión general del riesgo dentro de una organización, por lo que tiene áreas y aspectos comunes con la gestión de la seguridad de la información.

1.1.4 Como está compuesta la ISO22301:2012.

La ISO 22301 se podría definir o componer en 17 pasos los cuales nos dan los requerimientos[3] que debemos tener para poder certificar nuestra organización o compañía como ISO22301, hay que aclarar entre líneas hay más pasos que se deben seguir para poder mantener e incluso implementar la ISO, pero estos son pasos sugeridos y definidos basados en el caso de estudio de esta investigación el cual consiste en la implementación del DRP a la infraestructura de red de La Universidad, hay que tener claro que la ISO22301 es genérica, pero, puede y debe aplicarse de manera distinta para cada caso u organización que quiera utilizar este marco de referencia.
Los pasos para la implementación de la ISO22301 se encuentran en la siguiente tabla:

#	Nombre.	Descripción.
1	Soporte de la administración.	Antes de empezar cualquier proyecto se debe tener el aval de la administración o gerencia ya que ellos darán las herramientas y recursos para poner a andar el proyecto y mantenerlo.
2	Identificar los requerimientos.	Antes de tomar cualquier paso concreto debemos estar seguros que vamos a poder cumplir todo lo que las partes interesadas quieren que se realice o se espera del plan. Y se deben definir y comunicar con cada parte interesada.
3	Objetivos y Política de la continuidad de negocio.	Gerentes y administradores necesitan definir las responsabilidades y reglas de la continuidad de negocio, por lo tanto se debe definir una política de continuidad de negocio y además se deben definir objetivos medibles que nos den una forma de medir que tanto el plan está llenando las expectativas definidas.
4	Soporte de documentos para la administración del sistema.	Esto se refiere a los procedimientos que se realizaron en documentos, auditorías internas, acciones correctivas entre otros documentos que sirven como evidencia del plan y sus etapas o sus activaciones/desactivaciones, esto nos ayudara para poder mantener y poner en marcha nuestro plan de manera más sencilla ya que tenemos antecedentes.
5	Evaluación y gestión de riesgos[2].	Se refiere a una de las partes más importantes del plan, la evaluación de riesgos que pueden suceder y afectar a la organización y además como poder gestionarlos,

		prevenirlos y/o mitigarlos.
6	Análisis de impacto de negocio.	El análisis de la evaluación de riesgos no puede estar solo sino más bien, debe estar acompañado de dos preguntas importantes y necesarias, 1) que tan rápido necesito recuperarme de una interrupción y (2) que necesito para que la recuperación sea exitosa, por lo tanto el análisis de impacto de negocio lo que busca es definir los recursos necesarios para recuperarse y el tiempo.
7	Estrategia de continuidad de negocio.	Dependiendo de las variables como RTO, recursos o incidentes, es necesario descifrar como lograr los objetivos planteados con el mínimo nivel de inversión. Esto puede llegar a ser difícil o complicado dependiendo de la naturaleza del negocio.
8	Plan de continuidad de negocio.	Hay varios tipos de planes de continuidad de negocio, como mínimo hay planes de respuesta a incidentes (son los que definen la primera reacción ante un incidente) y los planes de recuperación (que son activados cuando ocurre una incidencia). Todos estos necesitan estar basados en una estrategia para poder tener los recursos adecuados para poder solventar las interrupciones.
9	Entrenamiento y concientización.	Tener los planes y la documentación terminada no es suficiente si nadie sabe cuáles son los planes o no saben de su existencia. Es necesario definir empleados y gerentes (y demás personas incluidas en el plan) como realizar ciertos pasos cuando una interrupción sucede y además porque esto es importante en primer lugar.
10	Mantenimiento y actualización de la documentación.	Documentos escritos tienden a estar desactualizados fácilmente, si alguien deja la organización o nuevas personas entran a la misma, se cambian, agregan o quitan los procesos existentes y documentados. Cualquier cambio debe verse reflejado en la documentación especialmente los planes, sino se actualizan los planes no serán útiles cuando más se necesiten.
11	Ejercicios y pruebas del plan.	De cualquier manera, solo entrenamiento no va a ser suficiente para dominar y medir la eficiencia del plan, debemos realizar prácticas casi en situaciones reales para poder saber exactamente como estamos. Esto no implica que solamente el departamento de IT se vea involucrado, sino más bien que todas las partes interesadas practiquen el plan (gerentes, vendedores externos, outsourcing, etc.).
12	Revisiones después del incidente.	No importa que tanto intentemos, nunca vamos a poder prevenir incidentes al 100% lo que podemos hacer, sin embargo, es aprender de dichos incidentes. De un incidente se puede saber cómo reacciono la gente, que tan listos estaban, que mejoras necesita el plan, entre otras. ¿Y aún más importante se logró recuperar la operación en el tiempo

		estipulado? (RTO).
13	Comunicación de las partes interesadas.	Esto realmente es un "paso" que debería ir en cada una de las etapas del plan ya que la comunicación es parte fundamental del éxito del mismo. Se debe mantener a todas las partes interesadas informadas de los avances que hay y de cuál es el status de la interrupción o recuperación.
14	Medición de la evaluación.	La idea principal aquí es que no tiene sentido que hagamos algo a no ser que hayamos logrado lo que nos propusimos, los objetivos se definieron en el paso 3, pero debemos tener una o varias métricas para cuantificar la eficiencia. Aquí podemos utilizar el balance scorecard o simplemente ver el RTO si fue cumplido o no.
15	Auditoria interna.	Es imposible ser totalmente objetivo sobre su propio trabajo. Por lo tanto, alguien más debe revisar el trabajo realizado y sugerir mejoras, que es lo que pretender una auditoria interna. Las auditorías internas son muy útiles para poder ver la realidad de nuestro trabajo.
16	Acciones correctivas.	Todos nosotros hacemos mejoras diarias en lo que hacemos, pero la ISO 22301, quiere que seamos sistemáticos, la ISO obliga a la organización a encontrar porque sucedió la interrupción y garantizar que no suceda de nuevo (o al menos asegurar que no habrá una "no conformidad" en esa área nuevamente).
17	Revisión de la administración.	Cuando todos estos pasos han sido implementados la alta gerencia necesita evaluar y tomar algunas decisiones cruciales como actualizar los objetivos, proveer fondos, hacer mejoras grandes, entre otras. Al final la última responsabilidad de la organización es sobrevivir interrupciones.

Tabla 1 pasos para la implementación de la ISO22301

[2] La correcta evaluación, clasificación y tratamiento de riesgos permite la generación de una estrategia óptima que garantice una rápida recuperación ante eventos de interrupción de servicios.

[3] Los requerimientos para la aplicación de la norma en cada caso varían, sin embargo siempre mantienen el orden de los procesos y la lógica de implementación.

Figura 3. Pasos para la implementación de la ISO22301

1.2 COBIT

Figura 4. Estructura de COBIT

COBIT (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

Lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

Se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

1.2.1 MISIÓN

Buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.

1.2.2 BENEFICIOS

- Mejor alineación basada en una focalización sobre el negocio.
- Visión comprensible de TI para su administración.
- Clara definición de propiedad y responsabilidades.
- Aceptabilidad general con terceros y entes reguladores.
- Entendimiento compartido entre todos los interesados basados en un lenguaje común.
- Cumplimiento global de los requerimientos de TI planteados en el Marco de Control Interno de Negocio COSO.

1.2.3 ESTRUCTURA

La estructura del modelo COBIT[4] propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.
"La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

1.2.4 NIVELES

Se divide en 3 niveles, los cuales son los siguientes:

Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.

Actividades: Acciones requeridas para lograr un resultado medible.

---

[4] COBIT provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados

1.2.5 DOMINIOS

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

- PLANIFICACION Y ORGANIZACION: Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.
- ADQUISION E IMPLANTACION: Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
- SOPORTE Y SERVICIOS: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
- MONITOREO: Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

1.2.6 USUARIOS

- La Gerencia: Para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Los Usuarios Finales: Quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- Los Auditores: Para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
- Los Responsables de TI: Para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

1.2.7 CARACTERÍSTICAS

- Orientado al negocio.
- Alineado con estándares y regulaciones "de facto".
- Basado en una revisión crítica y analítica de las tareas y actividades en TI[5].
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

1.2.8 PRINCIPIOS

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

- Requerimientos de la información del negocio: Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos CRITERIOS:
- Requerimientos de Calidad: Calidad, Costo y Entrega.
- Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

1.2.9 COMPONENTES COBIT

Resumen Ejecutivo: Es un documento dirigido a la alta gerencia presentando los antecedentes y la estructura básica de COBIT Además, describe de manera general los procesos, los recursos y los criterios de información, los cuales conforman la "Columna Vertebral" de COBIT[5].

Marco de Referencia (Framework): Incluye la introducción contenida en el resumen ejecutivo y presenta las guías de navegación para que los lectores se orienten en la exploración del material de COBIT haciendo una presentación detallada de los 34 procesos contenidos en los cuatro dominios.

Objetivos de Control: Integran en su contenido lo expuesto tanto en el resumen ejecutivo como en el marco de referencia y presenta los objetivos de control detallados para cada uno de los 34 procesos[6].

---

[5] Es necesario una revisión y análisis integral de los procesos de la organización

[6] COBIT al plantear de forma clara objetivos de control permite que su seguimiento sea productivo y eficaz.

PLANEAR Y ORGANIZAR

- PO1 Definir el plan estratégico de TI.
- PO2 Definir la arquitectura de la información
- PO3 Determinar la dirección tecnológica.
- PO4 Definir procesos, organización y relaciones de TI.
- PO5 Administrar la inversión en TI.
- PO6 Comunicar las aspiraciones y la dirección de la gerencia.
- PO7 Administrar recursos humanos de TI.
- PO8 Administrar calidad.
- PO9 Evaluar y administrar riesgos de TI
- PO10 Administrar proyectos.
- PO11Administración de Calidad

ADQUIRIR E IMPLANTAR

- AI1 Identificar soluciones automatizadas.
- AI2 Adquirir y mantener el software aplicativo.
- AI3 Adquirir y mantener la infraestructura tecnológica
- AI4 Facilitar la operación y el uso.
- AI5 Adquirir recursos de TI.
- AI6 Administrar cambios.

MONITOREAR Y EVALUAR

- ME1 Monitorear y evaluar el desempeño de TI.
- ME2 Monitorear y evaluar el control interno
- ME3 Garantizar cumplimiento regulatorio.
- ME4 Proporcionar gobierno de TI.

PRESTACIÓN Y SOPORTE

- DS1 Definir y administrar niveles de servicio.
- DS2 Administrar servicios de terceros.
- DS3 Administrar desempeño y capacidad.
- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la seguridad de los sistemas.
- DS6 Identificar y asignar costos.
- DS7 Educar y entrenar a los usuarios.
- DS8 Administrar la mesa de servicio y los incidentes.
- DS9 Administrar la configuración.
- DS10 Administrar los problemas.
- DS11 Administrar los datos.

- DS12 Administrar el ambiente físico.
- DS13 Administrar las operaciones.

Para COBIT 5, contar con un plan de continuidad del negocio es de suma importancia, en el dominio que se refiere a entrega, servicio y soporte, dedica un proceso a la gestión del plan de continuidad (ISACA, 2017).

CAPÍTULO II

2.1 SITUACIÓN ACTUAL

2.1.1Contexto de la empresa

2.1.1.1 Descripción de la empresa.

La Universidad Don Bosco es una entidad educativa ubicada en Soyapango, San Salvador, inicio sus operaciones en 1996 y desde entonces a la fecha se ha enfocado en la planificación y estrategia de desarrollo siguiente:

- Compromiso social.
- Sostenibilidad institucional.
- Innovación académica.
- Generación y transferencia de conocimiento.
- Gestión del talento humano.
- Gestión de la infraestructura física y tecnológica.

La Universidad Don Bosco constituye una de las instituciones de estudios superiores más prestigiosas de El Salvador, sobre todo en el área técnica y tecnológica, ya que es la única en el país en ofrecer carreras como ingenierías en Biomédica, en Aeronáutica y Mecatrónica; así como en mantener convenios con la Sociedad Internacional de Prótesis y Ortesis (ISPO, por sus siglas en inglés), la cual otorgaba hasta 2016 a sus graduados en Ortesis y Prótesis la "Acreditación Internacional categoría I de ISPO".

En su Campus Central Soyapango ofrece 34 carreras en sus diferentes Facultades, para ello cuenta con tres pabellones de aulas, tres aulas magnas, un edificio administrativo, área de cafetería, salones de usos múltiples, una Biblioteca, una capilla, áreas de parqueo, zonas verdes y de recreación y además cuenta con el Centro de Investigaciones y Transferencia de Tecnología (CITT); las diferentes canchas deportivas son de uso común entre las diferentes entidades de la Ciudadela.

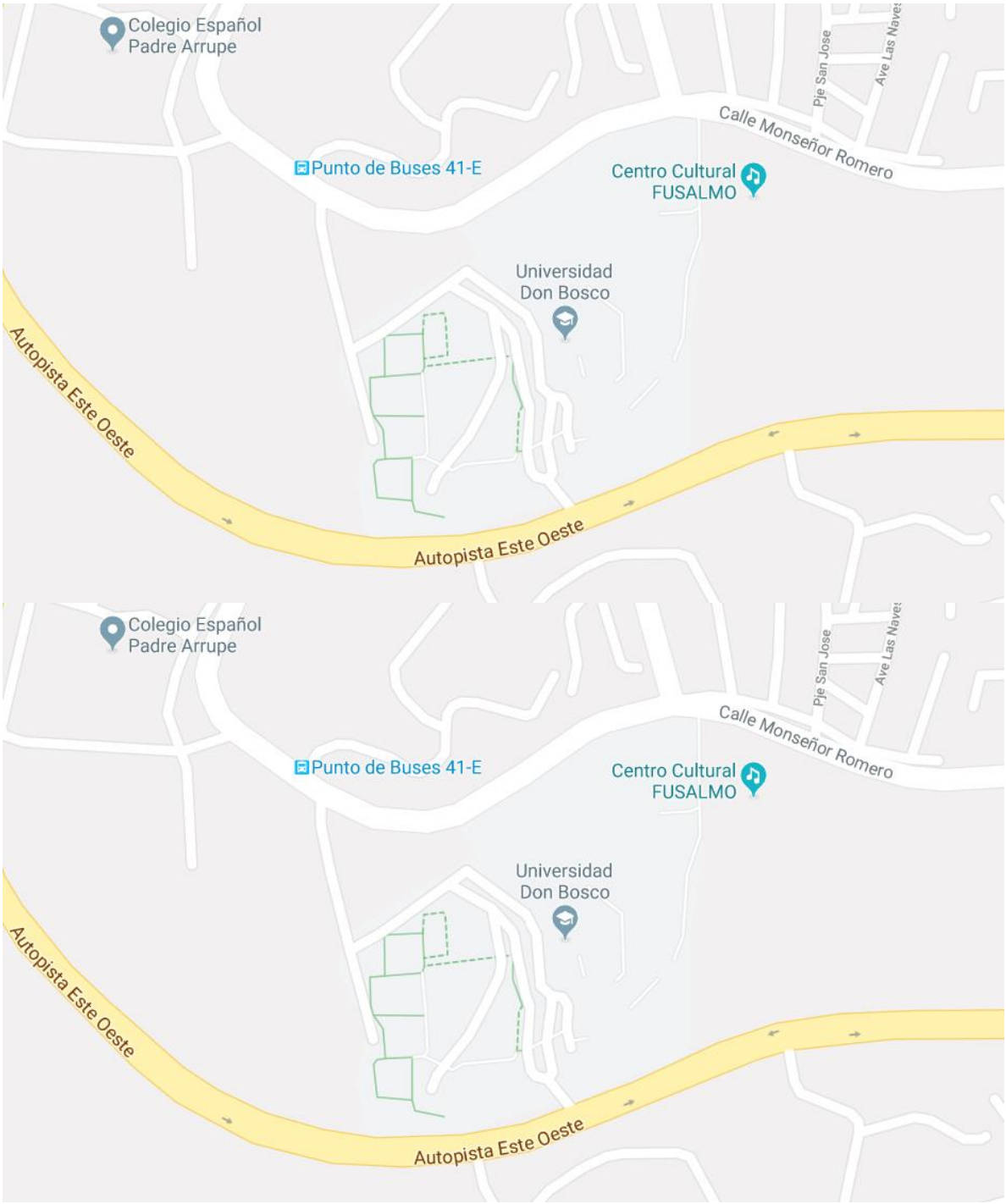

Figura 5. Ubicación del campus de la UDB en Soyapango

Además, cuenta con una locación en Antiguo Cuscatlán, La Libertad el cual es utilizado para sus estudios de post-grados donde cuenta con más de 20 carreras de post-grado entre maestrías doctorados, academia Cisco, escuela de idiomas y cursos libres en diferentes facultades. El Campus Antiguo Cuscatlán al igual que el campus Soyapango, cuenta con diferentes edificios

entre los cuales se pueden mencionar un salón de conferencias, edificios de aulas, área administrativa, biblioteca, cafetería, áreas verdes y parqueos que recientemente fueron expandidos.

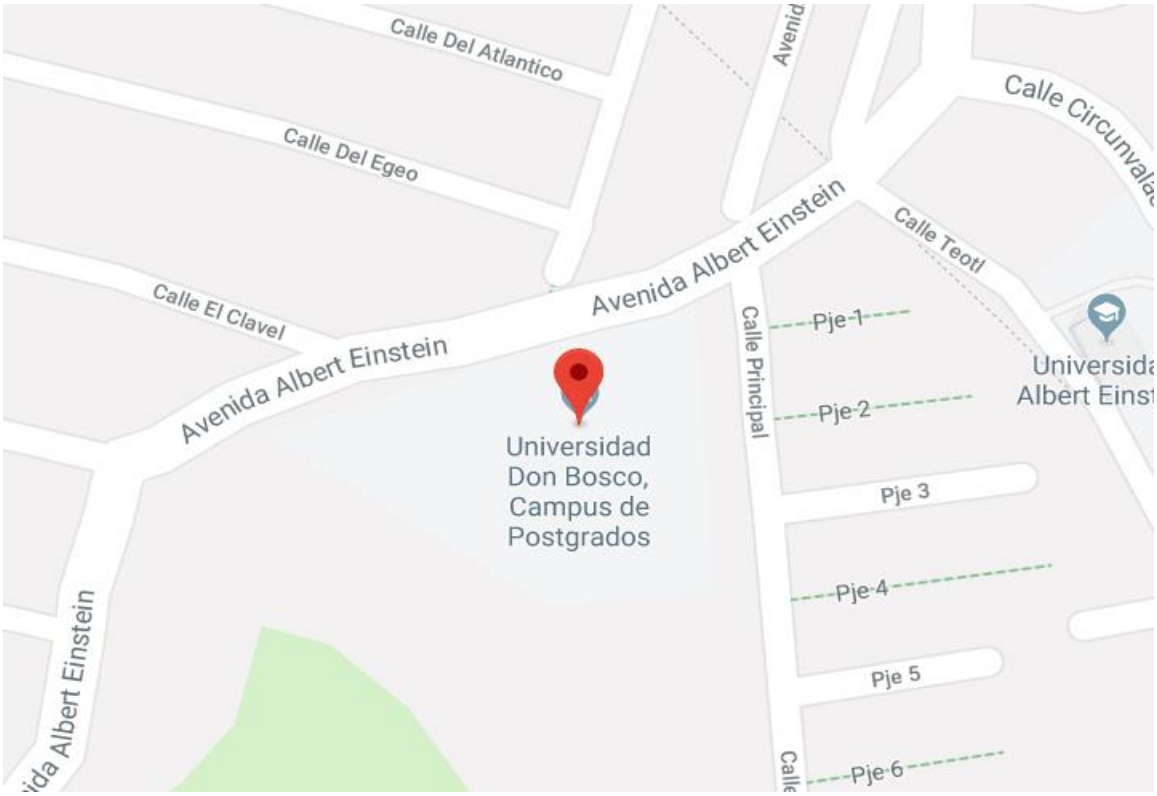

Figura 6. Ubicación del centro de postgrado de la UDB

2.1.1.2 Misión.

Somos una institución de Educación Superior con carisma salesiano dedicada a la formación integral de la persona humana, por medio de la investigación, la ciencia, la cultura, la tecnología, la innovación y el compromiso con la comunidad para la construcción de una sociedad libre, justa y solidaria.

2.1.1.3 Visión.

Una Universidad Salesiana, líder a nivel nacional y referente a nivel regional por su modelo educativo; reconocida por la innovación curricular; por el desarrollo profesional y la internacionalización de sus estudiantes, educadores y personal de gestión; por la ejecución de

proyectos de investigación, desarrollo e innovación; por sus publicaciones de impacto; por sus programas de grado y postgrado acreditados internacionalmente; por sus programas a distancia únicos e innovadores; por el mejoramiento continuo de la calidad y por la gestión de sus recursos físicos, tecnológicos y financieros para la sostenibilidad de la institución.

2.1.2 Estructura organizativa.

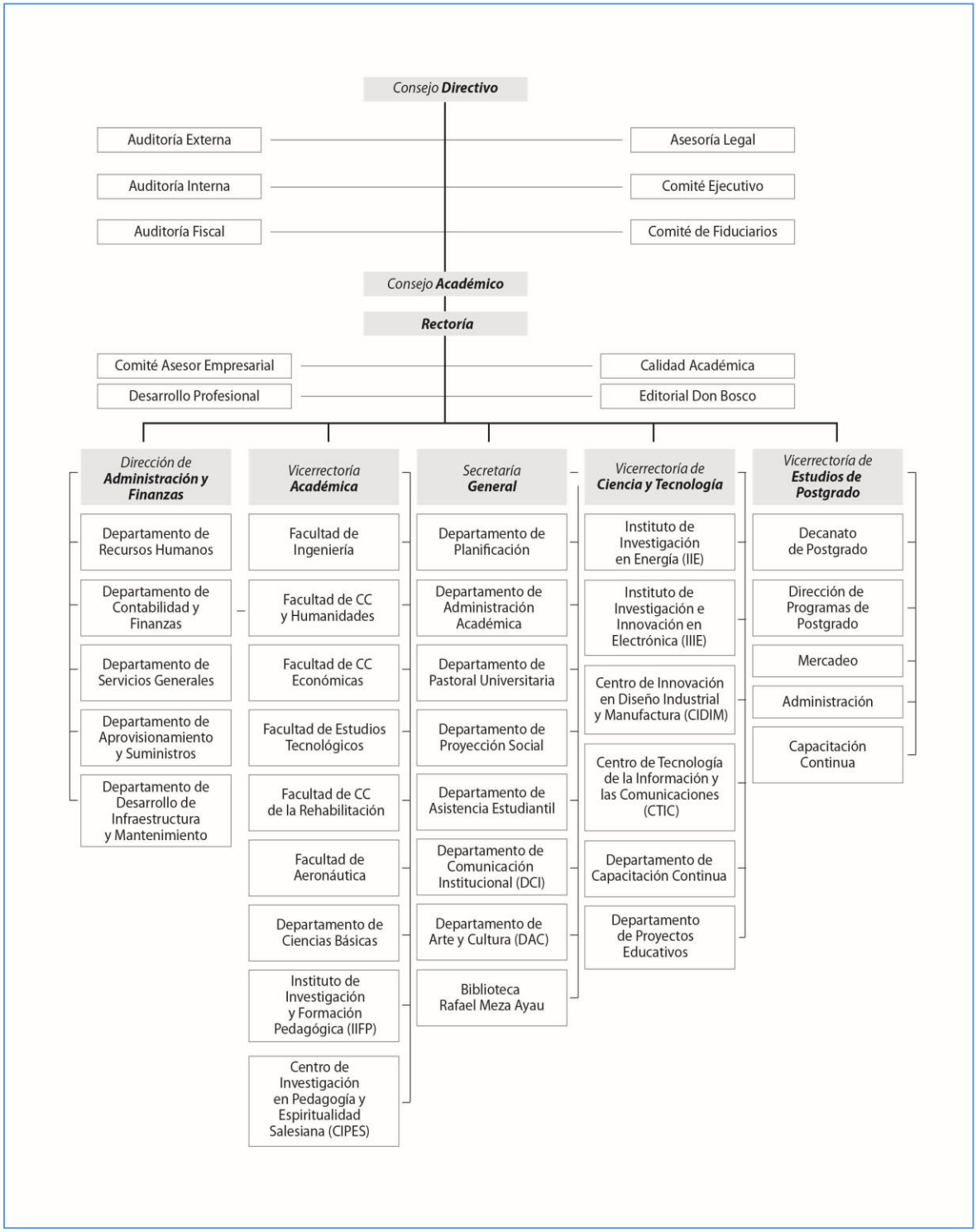

Figura 7. Estructura organizativa UDB oficial

2.2 Situación Actual.

Actualmente la Universidad don Bosco se encuentra trabajando en un DRP y en un BCP para sus procesos críticos de la infraestructura de red, para el presente estudio se realizaron una serie de entrevistas con las partes interesadas (Vicerrectoría, Auditoria y TI) en donde se establecieron los diferentes puntos en los que la universidad tiene fortaleza, puntos de mejora y necesidades que fueron expresadas en dichas entrevistas, estas reuniones se realizaron por medio de reuniones presenciales, video llamadas y conferencias de audio, producto de esto se identificó que en este momento no se cumple con lo requerido por la ISO 22301:2012 y en caso de la materialización de un evento disruptivo no se garantiza que la Universidad pueda continuar con las funciones básicas de operación.

Entre los aspectos más urgentes en el análisis se tiene:

2.2.1 Estructura actual de la red

Actualmente la Universidad cuenta con edificios designados para diferentes áreas específicas, algunas de ellas son, los laboratorios de computo, eléctrica, metrología, ortesis y prótesis, sus aulas magnas para usos varios y las aulas para las clases de diferentes materias y carreras. Actualmente el campus cuenta con 3 proveedores de internet, siendo su proveedor principal Columbus, el cual tiene publicado en internet sus direcciones publicas BGP, los proveedores, cada uno de ellos (Columbus, Claro y Telefonica) han dejado como equipo de última milla un Cisco ISR 2921 el cual se encarga de los enlaces metro Ethernet de cada proveedor y el enrutamiento hacia internet.

Se tiene un firewall Fortigate 1500D el cual soporta todo el enrutamiento interno de la redes soportadas por la Universidad, así como las reglas de acceso ya sea entre una o varias redes internas y cuáles pueden tener acceso a internet y cuáles no. El equipo que sirve para distribuir el internet es un Cisco Switch Catalyst 3550XL el cual hace la conexión hacia internet de la red interna donde están alojadas todas las operaciones.

La Universidad además, cuenta con una controladora de AP's (Access Point) Fortigate para el Wifi, el cual da acceso a internet inalámbricamente en todo el campus para alumnos, visitantes y empleados.

Todas las operaciones de TI se generan y residen en el Edificio 6 donde se encuentra el centro de cómputo, el cual recibe todos los proveedores de internet por medio de enlaces de fibra a 100mbps y aquí se encuentra el ODF (Optical Distribution Frame) que distribuye conectividad a todos los edificios por medio de fibras ópticas que corren alrededor del campus de la Universidad.

La granja de servidores se encuentra alocados en un Switch HP Gigabit, el cual es controlado por las políticas del Firewall, además estos están separados de todas las redes de los edificios y

solamente pueden tener acceso el área de redes y TI designada con permisos necesarios por los administradores.

Además posee un direccionamiento de red ya definido para cada edificio y propósito dentro de la Universidad, esto con el fin de proveer con internet a las diferentes áreas del campus, esta documentación se mantiene actualizada para poder tener un buen control de la información de red por áreas lo cual hace su mantenimiento más sencillo.

Toda esta información esta diagramada en las figuras 5, 6 y 7 los cuales fueron proporcionados por el Director de Infraestructura de la Universidad.

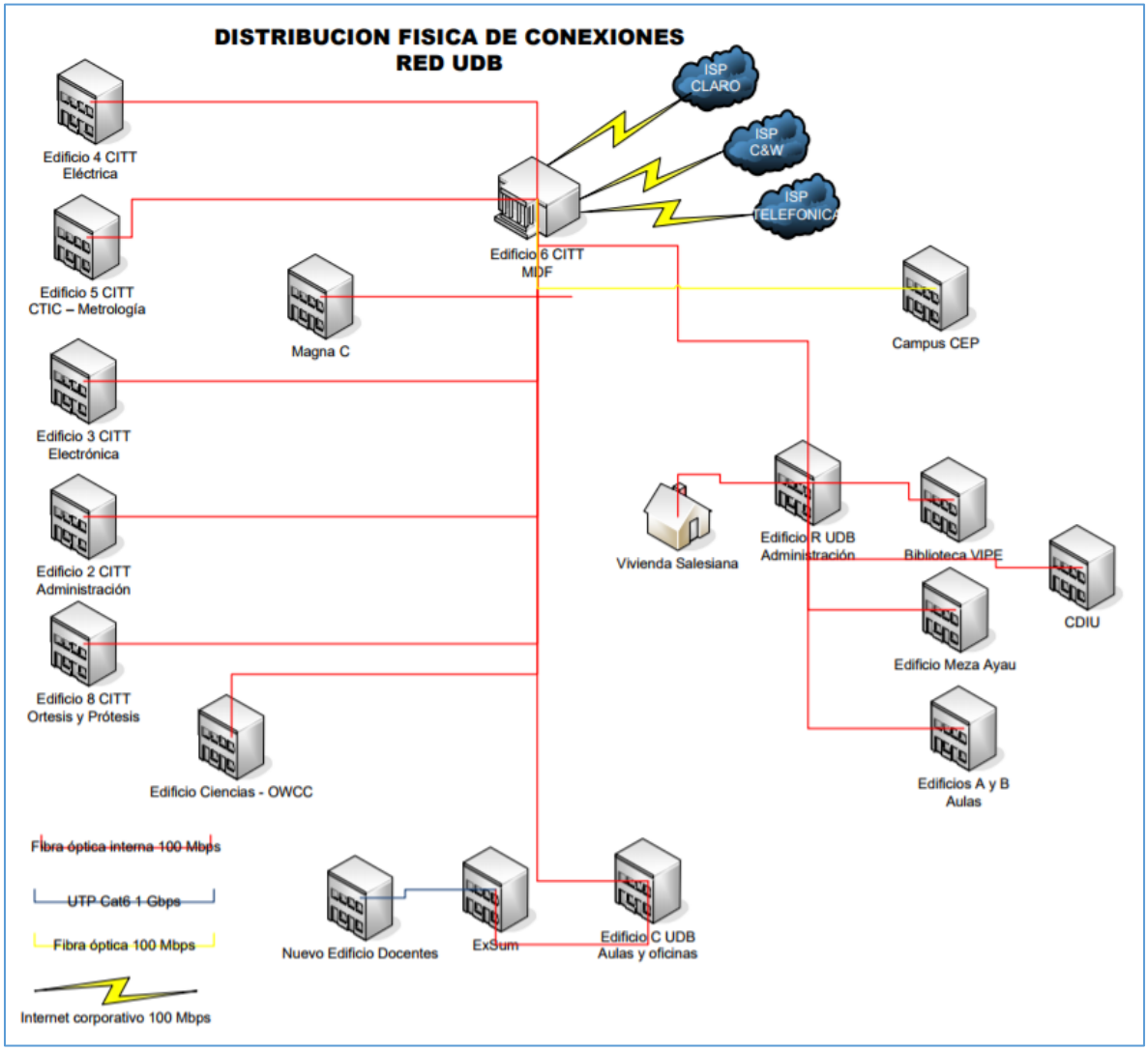

Figura 8. Distribución física de conexiones red UDB

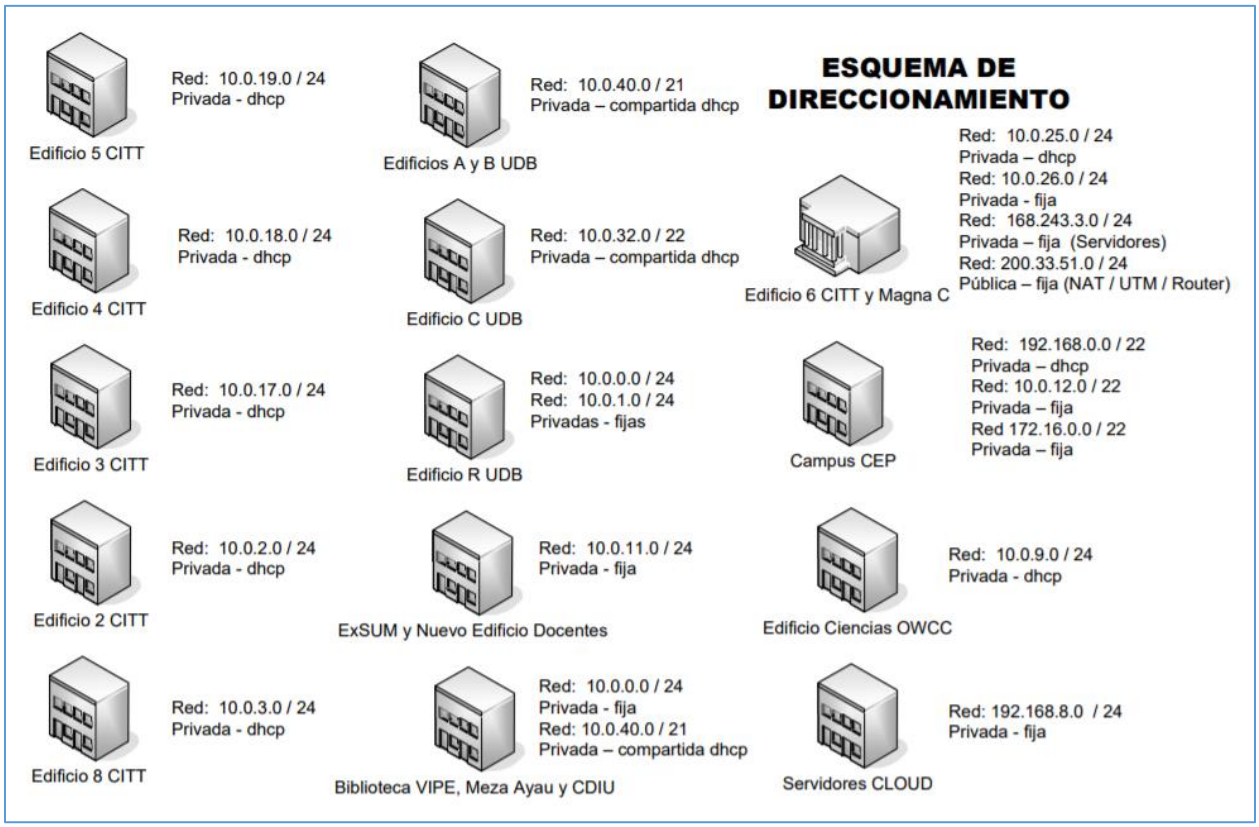

Figura 9. Esquema de direccionamiento de red de la UDB

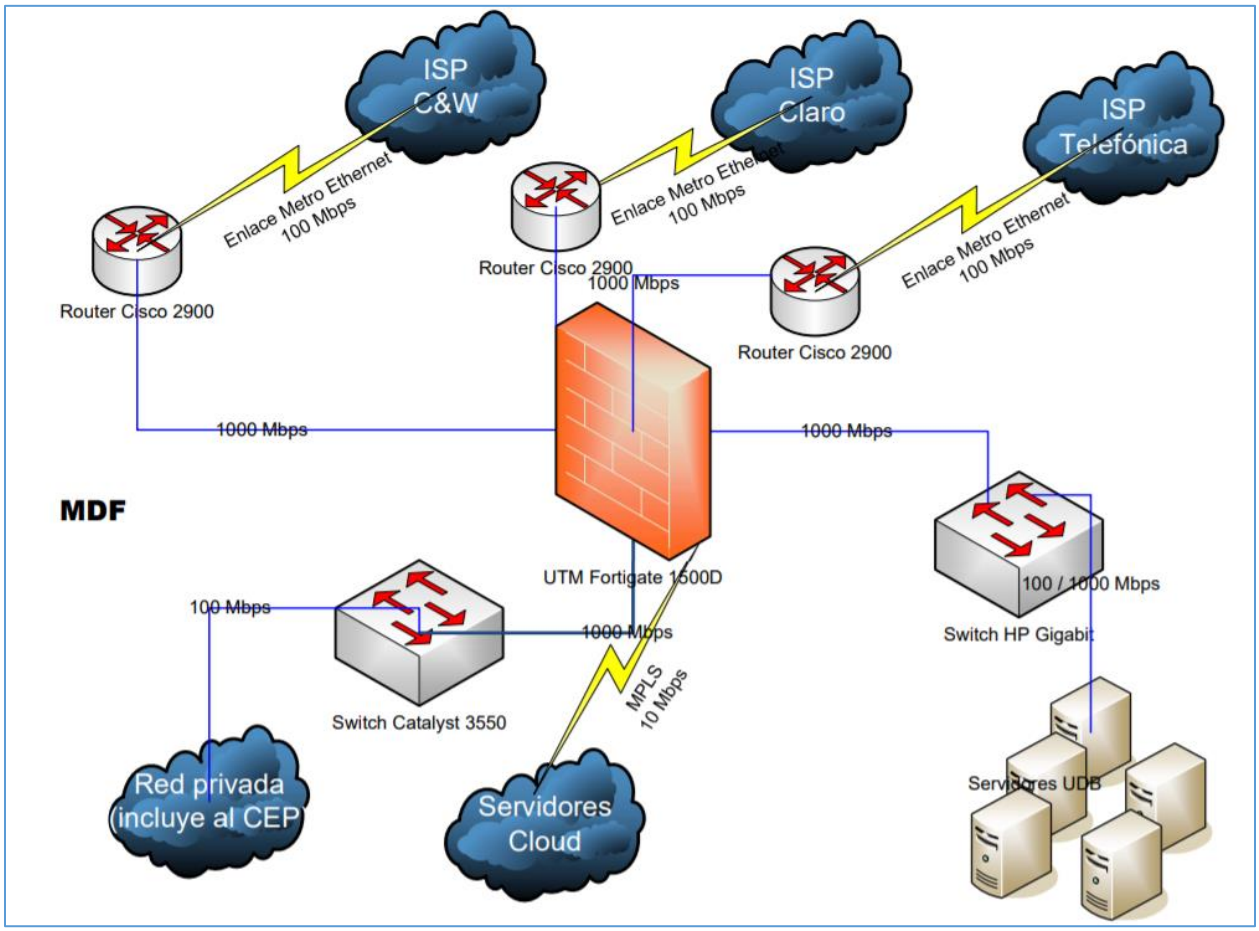

Figura 10. Diagrama de red lógico

2.2.2 Equipos de respaldo de energía eléctrica

Así también se analizó el aspecto de alimentación eléctrica en donde se planteó la necesidad de mejorar los diferentes equipos de back up de alimentación eléctrica, se encontró que actualmente se cuenta con lo siguiente:

- UPS APC Symmetra 40 KVA

Cuenta con dieciséis 16 módulos de baterías

Actualmente la carga (load) que implican todos los equipos en el área de servidores representa aproximadamente un 10% de la carga total. En condiciones normales el UPS también protege a las computadoras del Laboratorio de Informática que por ende representan el 90% restante de la carga, por lo que se encontró la necesidad urgente de contar con un UPS exclusivamente para los equipos críticos.

Se analizó el estado de la planta de emergencia, la cual tiene una potencia nominal 200 Kva, con un depósito de diésel de 100 galones (rellenable), cabe destacar que esta planta de emergencia da

servicio al área de Servidores, laboratorio de Informática, laboratorios de mecánica, metrología, Laboratorios de Servicios TIC (Edificios 5 y 6) entre otros, así mismo se encontró que en el momento del análisis no se habían realizado mantenimientos preventivos de la planta, lo cual se traduce en un riesgo importante, pues puede causar problemas tanto de poca alimentación o bien provocar cortocircuitos en los equipos conectados a ella.

Este hallazgo fue encontrado en la entrevista realizada con el Director de TI cuando se le consultó sobre los riesgos más importantes a los que está expuesta la operación de la infraestructura de red.

CAPÍTULO III

3.1 Análisis y diseño del plan.

Generalidades.

Para el diseño del plan se ha tomado como marco de referencia la ISO 22301:2012 si bien esta norma es para la continuidad de negocio, se utilizó como marco de referencia para el DRP al ser más robusto como norma y a su vez esto permite que la Universidad cuando desee adoptar un BCP sus planes conexos como el plan de recuperación ya se encuentre cimentado y fundamentado en la ISO22301, se ha adaptado el marco a las necesidades latentes que posee actualmente la Universidad Don Bosco campus Soyapango.

En la universidad Don Bosco aún no se cuenta con un BCMS (Business Continuity Management System) o Sistema de Gestión de Continuidad de Negocio (SGCN) ya establecido formalmente, sino más bien hay trabajo realizado para ciertas áreas definidos parcialmente o manejados solamente por el área involucrada sin tenerse un documento formal que soporte dicho avance o información, alguna de la documentación más importante que ya se tiene formalmente establecida y aprobada es el manual de procedimientos de TIC al igual que algunos procesos de auditoria realizados por el área de calidad.

Las partes más importantes que se tomaron cuando se definió el alcance y objetivos del proyecto son los que se mencionan a continuación, estos basados en la norma ISO22301:

a) Una política de continuidad o recuperación.
b) Personas responsables definidas.
c) Procesos de gestión relacionados con:
    i. Política de continuidad o recuperación.
    ii. Planeación.
    iii. Implementación.
    iv. Evaluación del desempeño.
    v. Revisión de la gestión.
    vi. Mejora continua.
d) Documentación que provea evidencia auditable
e) Cualquier proceso de gestión de continuidad del negocio relevante a la organización.

Algunos de ellos implementados parcialmente dentro de la Universidad y otros implementados de manera no formal.

Algo que se debe tomar muy en cuenta es la mejora continua dentro de la organización pero no solo planear sino implementar formalmente para las áreas a mejorar así como poder demostrarlo a las partes interesadas. Por eso mismo el estándar internacional utiliza el modelo "Planear – Hacer – Verificar – Actuar" (PHVA) para poder planear, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente la efectividad del sistema de gestión de continuidad del negocio.

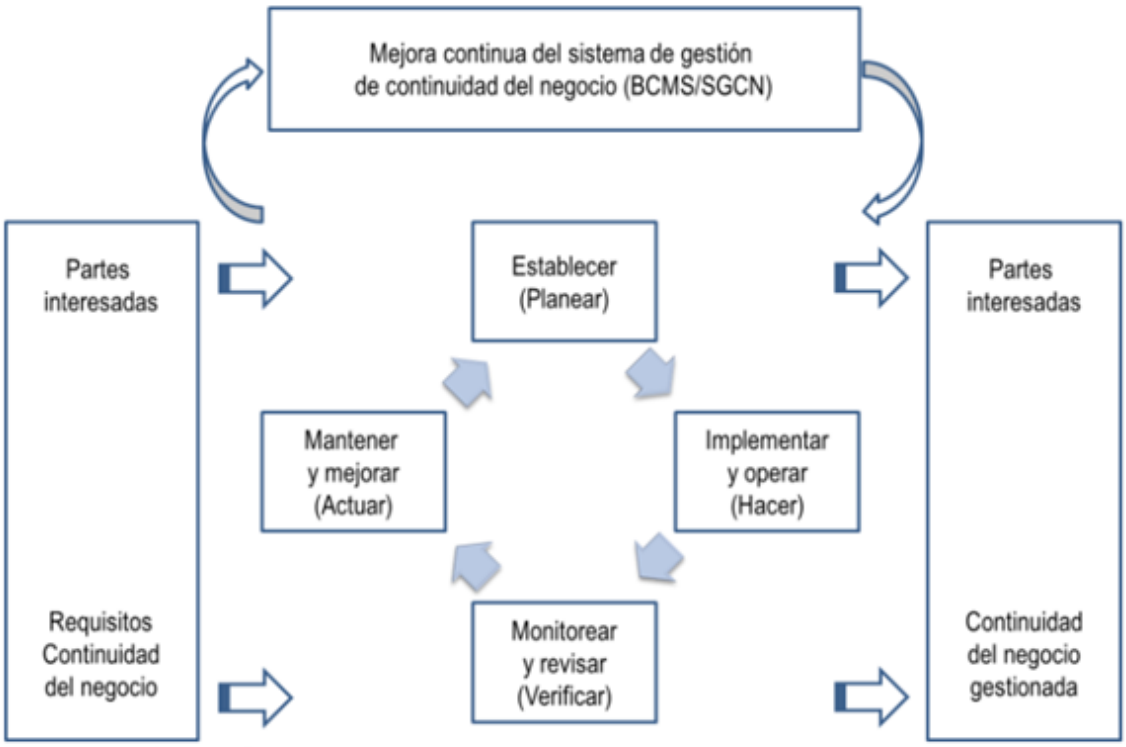

Figura 11. Modelo PHVA aplicado a procesos BCMS / SGCN.

La figura anterior ilustra cómo debería ser el ciclo de mejora continua del DRP, el cual estará dividido en diferentes partes las cuales se desarrollaran más adelante aplicados al escenario de la Universidad Don Bosco. La ISO está diseñada para que los requisitos necesarios sean genéricos para cualquier tipo de organización o partes de ellas sin importar el tamaño y la naturaleza de ellas.

3.2 Contexto de la organización.

Para conocer el contexto de la organización se realizaron entrevistas de campo, llamadas telefónicas y reuniones virtuales con las personas que se involucraron en el desarrollo de la mejora continua dentro de la Universidad, además se tomó en cuenta información encontrada en la página oficial de la organización y se corroboro con el personal responsable de la UDB la información obtenida.

Como la norma establece, para establecer el contexto de la organización se debe tomar en cuenta varios puntos, como lo son:

1) Articular los objetivos, incluyendo aquellos relacionados con la continuidad de negocio
2) Definir factores externos e internos que crean incertidumbre y dan lugar al riesgo.
3) Establecer el criterio de riesgo considerando el apetito de riesgo.
4) Definir el propósito del sistema de gestión de continuidad de negocio.

Para el análisis de estos puntos se tomó en cuenta los recursos actualmente existentes en la universidad basados en entrevistas con las personas en el área de TI y calidad, las personas más involucradas en esta parte son las siguientes:

Nombre	Cargo/Puesto
Ing. Erick Flores	Director de IT, Infraestructura y Soporte Técnico de la Universidad Don Bosco
Ing. Nery Marinero Alemán	Auditor interno de la Universidad Don Bosco
Ing. Henry Bladimir Flores Rivera	Director de Maestría en Seguridad y Riesgos Informáticos
Dr. José Humberto Flores M.	Vicerrector Académico Universidad Don Bosco

Posteriormente se procedió al análisis de las necesidades y expectativas basadas en las entrevistas que se tuvieron y se definió un alcance, objetivos y áreas de estudio con el que todas las partes interesadas estuvieran satisfechas. En este análisis se establecieron las partes de la organización incluidas en el plan, así como se establecieron los requisitos y se identificaron los productos y servicios de las actividades relacionadas dentro del alcance.

Una parte muy importante dentro del marco de referencia es el compromiso y apoyo de la dirección o gerencia, ya que esta deberá mostrar liderazgo y compromiso en relación con el plan de continuidad que se definió ya que ellos aprueban, revisan y mejoran el mismo.

Además la gerencia debe definir los roles y responsabilidades en la organización, esto, ya estaba como parte del trabajo inicial de la Universidad ya que ellos ya tienen las personas que se encargan de algunos procesos de continuidad de negocio (como es el backup de los servidores y

bases de datos) y también ya se tiene definido el rol de las personas en estos procesos, de esto se encuentra documentación varia que ya ha sido aprobada por la gerencia de la Universidad y están en uso actualmente como parte del trabajo que ellos han realizado.

3.4 Planeación o desarrollo de los requerimientos definidos.

Luego de haberse definido el alcance del proyecto por medio de las entrevistas se definió y planeo reducir el riesgo y fomentar la mejora continua en el área de Infraestructura de la Universidad Don Bosco campus Soyapango, esto con el fin de dar una base para la mejora continua en esta área y en el área de calidad de la Universidad. Aquí se consideraron los siguientes puntos importantes:

- La creación de un DRP (Disaster Recovery Plan o Plan de recuperación de Desastres).
- Una evaluación de riesgos.
- Definición de procesos críticos de la Universidad.
- Definición de procesos de recuperación para equipos críticos de infraestructura.
- Definición de personas responsables de activar el plan o procesos de recuperación dependiendo del escenario que se presente.

Además la dirección o gerencia deberá asegurar que se establezcan metas y objetivos de continuidad de negocio y estos deberían de considerar los niveles mínimos aceptables de productos y servicios para que la continuidad de negocio sea exitosa, además deben poder ser medibles y ser monitoreados y actualizados.

3.5 Soporte del plan y recursos.

La Universidad Don Bosco y las partes interesadas y responsables deberán proveer los recursos e información necesaria para establecer, implementar y mejorar el plan. Por lo tanto el plan no puede estar solo definido sino más bien debe poder ser utilizado y debe tener los recursos necesarios para funcionar.

Por esto mismo los recursos para la ejecución de este plan no son muy costosos y con esto nos referimos a que las personas que le darán soporte al mismo, son las colaboradores idóneos que han estado involucradas en planes anteriores en cuanto a mejora de áreas de TI o están actualmente trabajando en las partes que ya están definidas para el plan de continuidad de negocio, como es el caso del Jefe de Infraestructura y el Administrador de redes que actualmente trabajan en la Universidad.

También debemos tomar en cuenta que después de haberse definido los recursos necesarios queda a discreción de la Dirección de infraestructura, calidad y rectoría aprobar ya sea la adquisición de equipo o mejora de algunas partes de infraestructura que son tomadas dentro del alcance de este plan de continuidad (como son tener equipos de respaldo, cambiar equipos antiguos y otros que fueron definidos y/o mencionados en las entrevistas de los responsables de soportar el plan).

Uno de los objetivos que tiene este plan es generar conciencia en la importancia de tener un plan de continuidad o un DRP como se delimito en los objetivos tomando en cuenta los equipos, procesos y recursos críticos de la Universidad.
Esto y toda la información aquí presentada deberían ser comunicadas a todas las áreas de la organización por igual, para que todos estén enterados de las partes del plan, las personas involucradas, en que consiste y cuáles son las partes importantes del mismo.

Una de las partes que deben tener presentes es la documentación de este plan y todo lo referente a la continuidad de negocio, además se debe tomar en cuenta que, este, antiguo y futuros planes deben estar actualizados periódicamente para evitar que la información no sea la correcta a la hora de activar el plan de recuperación en una disrupción de alguna área critica de los servicios de la Universidad por lo tanto la información debe ser idónea y debe estar disponible cuando y donde sea necesaria.

3.6 Operación y control de operación.

Este DRP pretende implementar y controlar los procesos necesarios para llenar los requisitos definidos en el alcance y para reducir el riesgo de disrupciones en el área de infraestructura de la Universidad. Según lo definido en las entrevistas se implementaron procesos para la recuperación de ciertos equipos críticos de la infraestructura de red así como para recuperación de información de una estación de trabajo de administrador que ha fallado.

De igual manera cualquier cambio que se le realice al plan debe ser revisado y ver las consecuencias que tendrán esos cambios en el mismo para evitar mitigar un riesgo y dejar otro descuidado y no conforme a lo que se tenía inicialmente.

El plan de continuidad planteado incluye la creación y definición de un Análisis de Impacto de Negocio o BIA (Por sus siglas en inglés, Business Impact Analysis) el cual fue consultado con el director de Infraestructura y la encargada de Calidad de la Universidad Don Bosco. Inicialmente se habían definido unos procesos de negocio mucho más amplios de los que se obtuvieron al final, pero esto genero el cambio al enfoque del plan a el área de infraestructura de la Universidad solamente. Por lo tanto, luego de varias revisiones se definió el siguiente BIA con el jefe de infraestructura como responsable.

También como punto importante se realizó una evaluación de riesgos ya que por norma la organización debe tener un proceso formal para evaluar riesgos, el alcance de este plan incluye la evaluación de riesgos como parte del DRP, pero la actualización y mejora de este recaerá sobre la persona encargada de dicho parte del plan de continuidad.

Para poder completar la evaluación de riesgos como guía se puede utilizar la ISO 31000 (Risk Management o Gestión de riesgos), pero el alcance de este proyecto se limita a la entrega de este más no a la explicación del mismo.

Luego de la determinación del análisis de impacto y la evaluación de riesgos es donde se definirá y seleccionara la estrategia a utilizar en el plan ya que los anteriores son necesarios para poder determinar una estrategia adecuada para la Universidad, ya que esta es la que delimitara como proteger las actividades priorizadas, como estabilizar, continuar, reasumir y recuperar las actividades así como sus dependencias y recursos.

Finalmente esta nos dirá como mitigar, responder y administrar los impactos. La determinación de la estrategia es la que incluirá marcos de prioridad de tiempo para los diferentes recursos que se protegen de la infraestructura de red y la reanudación de las actividades.

Una de las partes más importantes para la delimitación de la estrategia es el establecimiento de los recursos, la organización deberá determinar los requisitos de recursos para implementar la estrategia seleccionada, algunos ejemplos de recursos que se deben tomar en cuenta para nuestro plan son los siguientes:

a) Personas.
b) Información y datos.

c) Instalaciones, equipos e insumos.
d) Sistemas de tecnologías de la información y las comunicaciones.
e) Transporte.
f) Finanzas.
g) Aliados y proveedores.

Todos estos están altamente Alineados entre si ya que son inter operativos entre ellos en algunos casos, por eso mismo dentro del plan que incluye el DRP se definen los contactos de todas las personas y proveedores que son el primer punto de contacto si en el caso de disrupción se tiene que reemplazar un equipo o alquilar uno por el tiempo que dura la disrupción o depende del escenario del desastre, pero todos ellos son necesarios con el fin de recuperar las operaciones lo más rápido posible y dentro del tiempo estipulado en la estrategia y en el BIA.

Además debemos tomar acciones proactivas para reducir la probabilidad de disrupción, acortar el tiempo de disrupción y limitar el impacto de disrupción en los servicios claves de la organización. Actualmente la Universidad ha migrado todos sus equipos a la nube y por esto mismo no dependen solamente de la infraestructura local, sino que tienen como sitio de backup la nube la cual aloja la mayoría de operaciones críticas de la Universidad, como son, el sitio web de la Universidad, El Aula Virtual, entre otros servicios críticos que ellos tienen ya como respaldo en la nube.

El único proceso crítico que aún no ha sido migrado es una VPN con el Banco Agrícola el cual aún esta localmente en el firewall de la Universidad, la desventaja de esto es que, como mencionaba el director de infraestructura al hacer el análisis, si el proveedor principal falla, ese túnel se viene abajo y se pierde conectividad con los recursos de banco y este afecta pagos y transacciones bancarias entre las instituciones. Debido a esto dentro de la parte de recomendaciones se plantea la configuración de BGP con los tres proveedores para poder tener una mejor y más estable conexión con el banco o en su defecto migrar a la nube al Webservice que la Universidad posee actualmente con el banco Credomatic.

Todo lo anterior está incluido en la implementación de los procesos de recuperación en caso de desastre ya que la organización debe ser vigilante de los mejores métodos para mitigar estos riesgos.

Una parte muy importante es la definición de la estructura de respuesta de incidentes, esta parte es la que identificara la tolerancia en el impacto que justifican iniciar una respuesta formal ante una amenaza o riesgo latente que puede ocurrir. Además evalúa la naturaleza y extensión de un incidente disruptivo y su impacto potencial.

Todas estas tareas recaen sobre el equipo de recuperación de desastres que en este caso está conformado por el Administrador de redes y el Director de Infraestructura de la Universidad ya que ellos son los que han sido definidos para la manipulación y recuperación de los servicios cuando estos estén siendo afectados por una disrupción.

La Universidad y su equipo deberán tener procedimientos o procesos de detección de incidentes, seguimiento de incidentes, comunicación de los mismos, entre otras tareas de monitoreo de

incidentes, esto está fuera del alcance de este plan, pero es un punto de partida para la implementación de documentación y procesos (ISO22301, 8.4.3)

El alcance de este plan llega a la documentación del DRP, BIA y evaluación de riesgos, pero para el correcto funcionamiento de este el plan debe continuar creciendo y definiendo roles para las personas que se verán involucradas en el mismo. Por lo tanto algunos puntos que se pueden tomar en consideración para el crecimiento de este plan son los siguientes:

a) Roles y responsabilidades definidas par personas y equipos con autoridad duran y luego de un incidente.
b) Uno proceso para activar respuesta.
c) Detallas para gestionar las consecuencias inmediatas de un incidente disruptivo.
d) Como la organización o equipo de trabajo continuara o recuperara sus actividades priorizadas dentro de un marco de tiempo predeterminado.
e) Un proceso para detenerse una vez finaliza el incidente.

Además la organización debe tener procedimientos documentados para recuperar y retornar las actividades de negocio al estado normal y también deberá realizar y probar procedimientos de continuidad de negocio para asegurar que están funcionando y son funcionales, en el caso de la Universidad semanalmente se hace un backup de las bases de datos y servicios y además son probados y certificados de que están en buen estado y pueden ser utilizados para recuperación de actividades o información perdida. La prueba de estos backup se realiza en un servidor de prueba que ellos poseen y además, las copias de los backup son llevadas a diferentes locaciones (Soyapango, Antiguo Cuscatlán y la nube).

3.7 Evaluación de desempeño.

La Universidad deberá definir que partes del plan deben ser monitoreados y medidos, cuales son los métodos que se utilizaran para asegurarse de tener resultados válidos, cuando se deberá realizar el monitoreo y la medición, cuando se deberá realizar el análisis y la evaluación del monitoreo y medición.

Se deben mantener información documentada apropiada como evidencia de los resultados y además deberán evaluar el desempeño y la efectividad del plan de gestión de continuidad.

Uno de los puntos más importantes de este plan la evaluación de procedimientos y las auditorías internas que se realizan[7], la Universidad actualmente ya posee un departamento de calidad el cual se encarga de mejorar ya sea procesos y/o procedimientos para la Universidad, inicialmente se incluyó trabajo para el área de TI de la Universidad, pero luego el departamento de calidad se fue enfocando un poco más en el área académica y otras funciones enfocadas a esta misma, por lo que el área de informática quedo parcialmente abandonada.

El área de calidad ya tiene algún trabajo realizado en el área de TI como son algunos procesos y procedimientos que ya han sido aprobados por la gerencia para ser puestos en marcha en periódicamente dentro de la Universidad. Este plan incluye procesos críticos que se definieron al principio de la investigación los cuales pueden y deben ser sujetos a revisión y aprobación de ser aceptados dentro del plan de la Universidad, algunos de los procedimientos aquí denotados son:

a) Proceso de recuperación de enrutador principal.
b) Proceso de recuperación de Switch principal.
c) Proceso de recuperación de firewall principal.
d) Proceso de recuperación de estación de trabajo de administrador.

Dado el alcance de este plan estos son algunos de los procesos más importantes dentro del área de infraestructura los cuales pueden ser tomados como base para mejora dentro del área de TI.

Como se mencionaba anteriormente el área de calidad ya tiene cierta experiencia en cuanto a auditorías internas la cuales deben estar enfocadas en que el área auditada llene los requisitos propios de la organización tanto como el marco de referencia que ellos utilizan dentro de la organización, este plan utiliza la ISO22301, la cual deberá ser tomada en cuanta a la hora de auditarlo y mejorarlo.

Finalmente este documento y otros deben ser revisados y aprobados por la gerencia o dirección de la Universidad luego de haber sido revisados por los encargados de la creación del plan de continuidad.

---

[7] La auditoría de los procesos es indispensable para asegurar la mejora continua

3.8 Mejora.

Como dicta el modelo PHVA (Planear – Hacer – Verificar – Actuar) una de las partes más importantes de todo este ciclo es la mejora continua por lo tanto cuando la madurez de este plan alcance la deseada, se debe tomar en cuenta que cuando ocurren no conformidades la organización debe:

a) Identificar la no conformidad.
b) Reaccionar a la no conformidad y dependiendo de la no conformidad se deben tomar acciones para controlarla, corregirla y tratar con las consecuencias de esta.
c) Evaluar las necesidades de acciones para eliminar la causa de la no conformidad para que no recurra u ocurra en otra parte.
d) Implementar cualquier acción necesaria.
e) Revisar la efectividad de cualquier acción correctiva tomada.
f) Realizar cambios o mejoras al DRP si es necesario[8].

Además debemos tomar en cuenta las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

Por lo tanto al igual que los auditores, los encargados del plan, la dirección y todas las partes interesadas de igual manera son responsables de la mejora continua de este plan y sus partes para que la efectividad de este vaya creciendo durante el tiempo y además de una mejor solución al problema, disrupción o no conformidad encontrada.

---

[8] Como parte de las mejoras a la norma 22701/22702 se encuentra una manera más ágil de cambios a procesos para su mejora

CAPÍTULO IV

4.1 DISEÑO DE LA SOLUCIÓN (DRP)

DISASTER RECOVERY PLAN (DRP)

Autores: **Gerson Quintanilla**
Andy Osegueda

Fecha:

Versión: **Versión 1.0**

Locación: **Universidad Don Bosco, Campus Soyapango.**

Firmas y aprobaciones.

EL Plan de Recuperación de Desastres (DRP) es claro en las partes que el plan este firmado y aprobado por las partes interesadas:

Unidad de negocio de IT.

Nombre	Posición/Cargo	Firma
Erick Alfredo Flores Aguilar.	Director de Infraestructura.	
Eduardo Jose Ávila Portillo.	Administrador de Redes y Servidores.	

Gerencias.

Nombre	Posición/Cargo	Firma
Dr. Mario Rafael Olmos	Rector	
Dr. Humberto Flores	Vice Rector	

Revisiones.

Versión	Fecha de revisión.	Resumen de los cambios.	Preparado por:	Revisado por:	Aprobado por:	Fecha de aprobación:
1.1	02/04/2017	Todas las secciones y áreas involucradas en este documento.	Gerson Quintanilla Andy Osegueda.	Gerson Quintanilla Andy Osegueda.	Alta Gerencia y Gerente Infraestructura.	02/04/2017

Tabla de contenidos (Documento DRP).

1. Introducción.

Este Plan de recuperación del desastre (DRP) reconoce la dependencia operacional de los servicios de IT y direcciona los riesgos asociados con la pérdida de los sistemas, incluyendo la red de área Local (LAN), servidores de base de datos, Internet, Intranet, servicios estudiantiles, servicios financieros, correo electrónico, y las comunicaciones. La intención de un Plan de recuperación de desastres es proporcionar un plan escrito y probado que dirija el proceso de recuperación de servicios de infraestructura en el caso de una interrupción en la continuidad de los servicios, resultante de un desastre imprevisto o inesperado.

Nota: Gestión de continuidad del negocio (BCM) asegura la resistencia del negocio antes, durante y después de una interrupción operacional. BCM incluye gestión de proveedores, gestión de crisis, manejo de emergencias, administración de recuperación ante desastres (IT DRM), recuperación del negocio, planificación de contingencias y preparación. BCM no es parte de este documento.

Este documento está organizado de tal manera que no es necesaria una lectura palabra por palabra para entender las acciones apropiadas y actividades necesarias para la recuperación. En cambio, es una combinación de listas de comprobación y referencias a varios documentos que deben utilizarse cuando se presenta el incidente o disrupción de los servicios en el campus Soyapango de la Universidad Don Bosco.

Las secciones siguientes proporcionan los conceptos básicos de estrategia de recuperación, recursos y procedimientos requeridos durante la recuperación de los servicios de tecnología de la información y comunicaciones (TIC) de la Universidad Don Bosco campus Soyapango después de una interrupción que permita la continuidad de funciones críticas definidas por el personal de TI y por la gerencia de la Universidad Don Bosco después de una interrupción.

2.1 Plan de prueba.

Preparar un plan de prueba con diferentes escenarios de interrupción que se utilizará para poner a prueba la integridad y la efectividad del Plan de recuperación de desastres.

Plataforma	Fecha
Cambio de un Router.	Diciembre 2017.
Cambio de un Switch.	Diciembre 2017.
Cambio de un Servidor.	Diciembre 2017.
VPN contacto con los bancos.	Diciembre 2017.

Tabla 2.1 .Fechas de realización de pruebas a componentes

2.2 Revisión del plan y actualización.

Los resultados de las pruebas realizadas en el DRP ofrecen una comprensión del DRP propio y la capacidad del personal y planes para manejar situaciones de interrupción en diferentes escenarios, entendiendo que permitirá a Empresa alcanzar mejoras (mantenimiento y optimización) y actualizaciones según sea necesario.

2.3 Entrenamiento.

El entrenamiento es una actividad que debe llevarse a cabo al menos una vez por año calendario por Talento Humano principalmente para aquellos involucrados en el proceso de recuperación ya que esto aporta información para la adecuación del DRP e identifica los recursos necesarios. El entrenamiento facilita la asimilación de los procedimientos en caso de interrupciones en los servicios IT o del negocio.

3 Objetivos.

Este Plan de recuperación del desastre (DRP) proporciona una respuesta a las interrupciones o incidentes que puedan afectar las instalaciones físicas, infraestructura tecnológica, datos, aplicaciones y servicios críticos de la Universidad Don Bosco, Campus Soyapango tras la disrupción del algún elemento de la infraestructura de red de la misma.

El DRP detalla cómo se llevará a cabo la recuperación de procesos críticos en el área según la criticidad definido para ellos. El desarrollo, mantenimiento, prueba y continuo mantenimiento de este plan son responsabilidad de la Universidad Don Bosco, el Coordinador del DRP y los líderes de cada grupo.
El proceso de preparación de Plan de recuperación de desastres incluye varios pasos importantes como sigue:

1.
   - ♣ Identificar y mapear los servicios de IT hacia las funciones empresariales fundamentales (servicios críticos) categorizadas como se define en el análisis de impacto de negocio (BIA)
   - ♣ Determinar la estrategia de recuperación.
   - ♣ Documentar el equipo de recuperación, su organización y responsabilidades.
   - ♣ Desarrollar y documentar los procedimientos de recuperación.
   - ♣ Desarrollar y documentar los procedimientos de prueba de recuperación.

El responsable de la administración de este DRP es la Universidad Don Bosco será el gerente del área de infraestructura.

4 Alcance.

El DRP está diseñado para garantizar la restauración de las actividades regulares de tecnología de la información y las comunicaciones (TIC) en el caso de interrupción de servicios en el centro de datos de Universidad Don Bosco, Campus Soyapango, y su recuperación en el Sitio de recuperación de desastres de acuerdo con el Contrato actual incluido en el DRP.

El alcance de este DRP está limitado a la recuperación de los servicios identificados por La Universidad Don Bosco, como procesos de tecnología que apoyan procesos críticos definidos en el Análisis de impacto del negocio (Business Impact Analysis.)

A continuación se describen los servicios de IT incluidos en este DRP:

5 Suposiciones.

- Personal clave o sus suplentes identificados en el DRP están disponibles después del incidente
- Personal clave o sus suplentes tienen equipos de trabajo para conectar al sitio alterno y a los miembros del equipo DR.
- El sitio seleccionado alternativo, sitio de recuperación continuidad de negocios (BCRS) está disponible y puede ser utilizado en este esfuerzo de recuperación
- El personal encargado de la recuperación debe estar dispuesto a asumir responsabilidades más allá de las tareas diarias, compromiso y responsabilidad como parte del equipo
- No sólo los recursos críticos incluidos en el DRP están disponibles, pero también vendedores / proveedores
- Equipos y software serán previamente definidos y estandarizados en orden para asegurarse que los datos se restauran funciona adecuadamente.
- <proveedor de telecomunicaciones> debe tener un plan de contingencia (o recuperación de conectividad con internet y firewall) en caso de que el circuito principal esté fuera de servicio.

6 Acrónimos.

Acrónimos.	**Definición.**
BCRS	Business Continuity Recovery Site (Sitio de recuperación de continuidad del negocio)
BIA	Business Impact Analysis (Análisis de impacto del negocio)
BU	Business Unit (Unidad de Negocio)
DR	Disaster Recovery (Recuperación de desastres)
DRP	Disaster Recovery Plan (Plan de recuperación de desastres)
ITC	Information Technology and Communications (Tecnología de información y comunicaciones)
RPO	Recovery Point Objective (Punto objetivo de recuperación)
RTO	Recovery Time Objective (Tiempo objetivo de recuperación)

7 Organización y responsabilidades.

El primer punto de contacto es el director de TI de la Universidad Don Bosco quien será el encargado de realizar el árbol de llamadas (call tree) hacia todas las personas que ya están definidas en el plan, para que puedan involucrarse oportunamente cuando se active el plan de recuperación de una disrupción o desastre.

7.1 Unidad de negocio: director de IT.

El responsable de la administración de este DRP es el gerente de infraestructura.

- Durante un desastre / interrupción, él / ella debe:
  • Liderar el departamento a través de respuesta a desastres, recuperación del negocio y actividades de reanudación
  • Comunicar la situación (status) y o problemas periódicamente al equipo de gestión de Crisis
- Antes y después de un desastre / interrupción, él / ella debe:
  • Asegurar una formación adecuada y las pruebas del plan al menos una vez por

año calendario
• Asegúrese de DRP es mantenido y actualizado periódicamente con los cambios en el entorno técnico, personal y proveedores

7.2 Unidad de negocio: Líder de recuperación.

Las tareas del líder de recuperación son las siguientes:

Antes de un desastre / interrupción, debe:
• Asegurar la disponibilidad de recursos para la recuperación (documentación, copias, etc.).
• Garantizar las condiciones de disponibilidad del sitio de recuperación de continuidad de negocios (BCRS)

Durante un desastre / interrupción, debe:
• Durante un desastre tiene autoridad para adoptar decisiones
• Establecer dirección, estrategias y pasos a seguir para el personal
• Comunicar las actualizaciones, estatus o problemas periódicamente al BU es líder
• Liderar el departamento a través de respuesta a desastres, recuperación del negocio y actividades de reanudación
• Ser responsable del mantenimiento periódico y actualizaciones del DRP

Después de un desastre / interrupción, debe:
• Elaborar un reporte con la información de la recuperación y rendimiento
• Participar en la identificación e implementación de mejoras para el DRP
• Documentar y llevar a cabo sesiones de las lecciones aprendidas con los ejecutivos.

7.3 Coordinador de Recuperación

- **Antes de un desastre / interrupción, debe:**
  • Participar en el análisis de impacto en el negocio
  • Contribuir en el análisis y diseño de los procedimientos de recuperación
  • Tener a mano una copia actualizada de los procedimientos de recuperación y DRP disponibles
  • Asegurar que se entrene a los equipos de recuperación

  Durante un desastre / interrupción, debe:
  • Administrar y proporcionar directrices a los equipos de recuperación
  • Comunicar las actualizaciones, estatus o problemas periódicamente con el líder de la

recuperación
• Servir de enlace entre los equipos de recuperación y el líder de recuperación.
• Coordinar con otros coordinadores de recuperación
• Comunicarse con proveedores / terceros
• Seguimiento de personal.

Después de un desastre, debe:
• Dirigir los equipos de recuperación para restablecer las operaciones al sitio principal
• Colaborar en la labor de restablecer el sitio principal
• Participar en la identificación e implementación de mejoras para el DRP
• Participar en el desarrollo de las lecciones aprendidas

7.4 Equipos de recuperación.

Los miembros del equipo son responsables de trabajo definido en los procedimientos de recuperación. Estos son sus responsabilidades:

Antes de un desastre / interrupción, deben:
• Apoyar el desarrollo de procedimientos de recuperación y mantenimiento continuo
• Participar en la formación

Durante un desastre / interrupción, deben:
• Realizar trabajos de recuperación según el Plan de recuperación y los procedimientos de recuperación
• Documentar y reportar cualquier desviación de los procedimientos documentados

Después de una situación de desastre deben:
• Soporte para regresar a la Página principal
• Colaborar en la actualización del plan de DRP y procedimientos para implementar mejoras
• Participar en el desarrollo de las lecciones aprendidas

8 Etapas de la recuperación de desastres y procesos.

8.1 Activación del plan.

El oficial encargado de declarar la interrupción o disrupción es el director TI el cual crea una junta de emergencia con los coordinadores de recuperación ya definidos y estos, además dependerán de la gravedad de la disrupción o interrupción de servicio. Luego esta junta es la encargada de colaborar y coordinar el desarrollo de la recuperación estratégica basado en las circunstancias extraordinarias que están sucediendo. El plan de recuperación

debe incluir los equipos de recuperación que necesitan ser activados en la parte de recuperación de los sistemas. Un ejemplo de un diagrama de activación es el que se encuentra en la figura 12.1

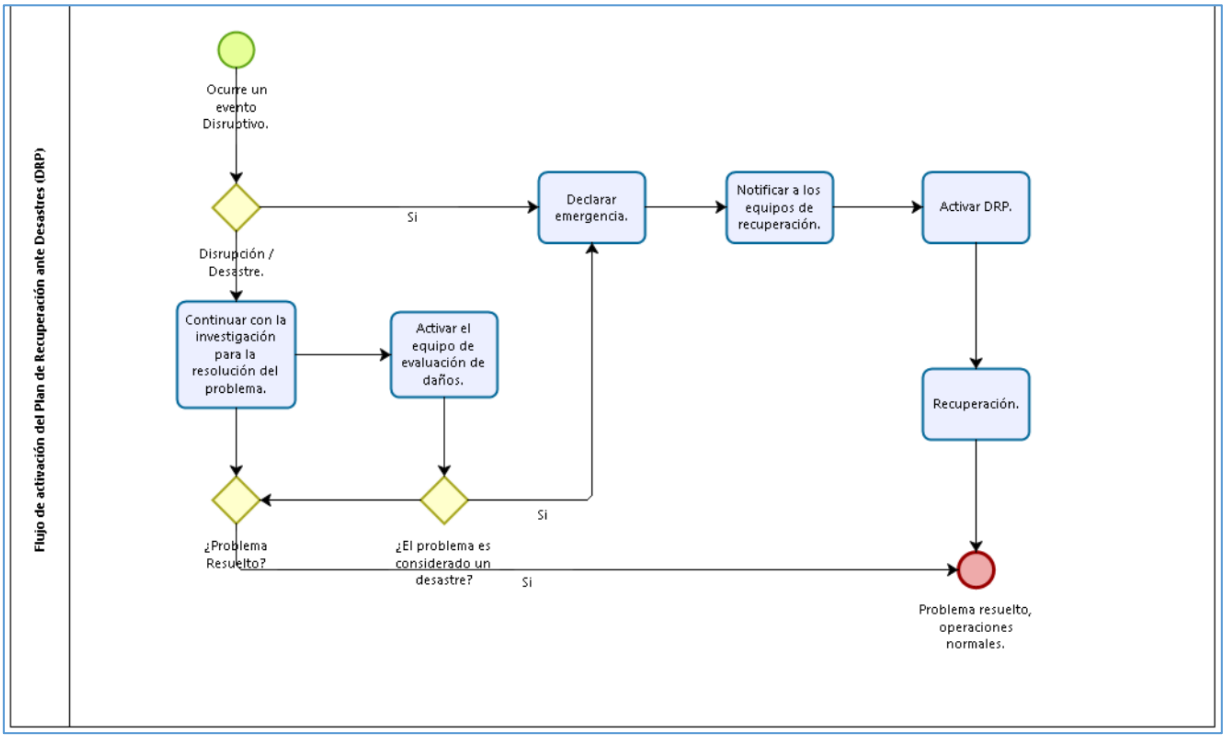

Figura 12.1 Activación del plan de continuidad.

8.2 Activación y equipos de recuperación.

El coordinador de recuperación debería usar la información de contacto localizada en "staff e información de locaciones" para contactar sus miembros del equipo y reportar la situación.

Además, los líderes de recuperación deben:

1. Llevar el control del documento de "Control de locaciones del personal".
2. Explicar la situación actual a los miembros del equipo, considerando:
   - 2.1. Evaluación inicial de daños.
   - 2.2. Duración esperada de la disrupción.

2.3. Objetivos y estrategias que utilizar.

2.4. Cualquier consideración de seguridad especial.

2.5. Procedimiento de contacto de todo el personal de recuperación.

2.6. Designación del lugar para la recuperación.

2.7. Establecer mecanismos para manejar llamadas externas referentes a la disrupción.

2.8. Mantener comunicación con el líder de recuperación.

9 Etapa de respuesta.

La evaluación inicial de la interrupción/disrupción es hecha por el líder de la unidad de negocios de IT de la Universidad Don Bosco en una reunión con los coordinadores de recuperación, para medir y saber la magnitud y el impacto de la disrupción. El plan de recuperación incluye equipos de recuperación que necesitan ser activados al principio de la etapa de recuperación, así como sitios alternos que puedan ser utilizados para la restauración de los procesos.

9.1 Etapa de recuperación.

En esta etapa los coordinadores de recuperación activan el plan de recuperación propuesto anteriormente y se realizan las siguientes acciones:

- Activar e implementar el plan de recuperación.
- Activar los equipos de recuperación.
- Activar el sitio de recuperación (si existiera)
- Coordinar con los proveedores externos para poder restaurar servicios.
- Identificar la data recuperada del almacenamiento de emergencia.
- Comunicar actualizaciones y otros problemas que aparezcan.

9.2 Comunicación.

Los canales de comunicación deben ser bien manejados durante el desastre, el líder de IT es el encargado de reportar estatus y actualizaciones. Las comunicaciones a usuarios finales deben ser coordinadas y conducidas por la unidad de soporte.

10 APENDICES.

Apéndice.	**Nombre.**
A1	Información del staff.
A2	Información de locaciones.
A3	Información de sitios externos.
A4	Proveedores y números de contacto.
A5	Información de sitios de recuperación.
A6	Proveedores y contactos detallados.
A7	Control de staff por área de trabajo.
A8	BIA/Servicios críticos
A9	Diagrama de recuperación (secuencia)
A10	Inventario de procedimientos de recuperación.
A11	Procedimientos de recuperación.

Tabla 2.2 Lista de apéndices

10. 1 APENDICE A1: Información del staff.

Rol	Nombre	Teléfono Oficina.	Teléfono Celular.
Director Infraestructura/IT/Seguridad	Erick Alfredo Flores Aguilar.	22518200 ext. 1729	7924-6922 / 7028-3268
Administrador de Redes y Servidores.	Eduardo Jose Ávila Portillo.	22518200 ext. 1729	7237-2480

10.2 APENDICE A2: Información de locaciones.

Lugar.	Responsable.	Dirección.	Teléfono 1.	Teléfono 2.
Universidad Don Bosco, Soyapango.	Erick Flores Aguilar	Calle Plan del Pino, Cantón Venecia, Soyapango, San Salvador.	UDB. Tel. 2251-8200 ext. 1620	Secretaria General. Tel. 2251-8209 ext. 1728

Tabla 2.3 Apéndice A2

10.3 APENDICE A3: Información de Sitios externos.

Place	Responsable	Dirección.	Teléfono 1.	Teléfono 2.
Centro de estudio de postgrados	Erick Alfredo Flores Aguilar / Henry Bladimir Flores Rivera	Centro de estudios de postgrado, Final Av. Albert Einstein No. 233 Colonia Jardines de Guadalupe, La Libertad.	Postgrados Antiguo Cuscatlán. 2251 8200	Postgrados Antiguo Cuscatlán. 2251 8200

Tabla 2.4 Apéndice A3

10.4 APPENDICE A4: Proveedores y números de contacto.

Lugar.	Responsable.	Dirección.	Teléfono 1.
JmTelcom	Director de IT	Col Roma 67 Av Sur No 2-D San Salvador, El Salvador	2247-3000
STB Computer	Director de IT	57 Av. Norte Alameda Roosevelt #2940, San Salvador	2121-8190
ASIT	Director de IT	Condominio Torremolinos Local No.15, San Salvador	2555-9420
ETS Consulting	Director de IT	Edificio Vitorria, Calle El Mirador 4814, San Salvador	2206-6916
CXTEC	Director de IT	New York, Estados Unidos.	(315) 479-1070
C&W (Columbus)	Director de IT	Edificio Avante, Urbanización Madre Selva 3, Calle Llama del Bosque Poniente, Pje. S, L-15 y 17, Antiguo Cuscatlán, La Libertad, El Salvador	2536-8528
Claro, El Salvador	Director de IT	Complejo Telecom Roma, Edificio "F", 1er Nivel, Calle Liverpool y Final Calle el Progreso, Colonia Roma	2271-7010
Telefonica, El Salvador	Director de IT	64 Av. Sur. Centro Financiero Gigante, Torre D, 1er Nivel (Edificio de estacionamiento) Dpto. de San Salvador	2211-2000

Tabla 2.5 Apéndice A4

10.5 APENDICE A5: Información de sitios de recuperación.

Sitio de recuperación del plan de continuidad de negocio.	
Dirección:	Centro de estudios de postgrado, Final Av. Albert Einstein No. 233 Colonia Jardines de Guadalupe, La Libertad.
Encargado:	

Contacto.	
Nombre:	Henry Bladimir Flores Rivera
Teléfono:	2251-8200
E-mail	hflores@udb.edu.sv

Sitio para almacenamiento de Backup.	
Sitio:	Amazon Drive Cloud Storage.
Dirección:	Seattle, Washington, USA
Teléfonos:	No aplica se crea un de ticket en el portal web.

Contacto.	
Name:	Amazon NOC.
Teléfono NOC:	801 5566998877
Email:	NOC@amazon.com

Sitio para almacenamiento de Backup.	
Sitio:	Universidad Don Bosco, Campus Antiguo Cuscatlán.

Dirección:	Prolongación Avenida Albert Einstein, #233, Colonia Jardines de Guadalupe, Antiguo Cuscatlán, La Libertad
Teléfonos:	2251-8200

Contacto.

Nombre	Henry Bladimir Flores Rivera
Tel. Oficina.	2251-8200
E-mail	hflores@udb.edu.sv

Sitio para almacenamiento de Backup.

Sitio:	Universidad Don Bosco, Campus Soyapango.
Dirección:	Calle Plan del Pino, Cantón Venecia, Soyapango, San Salvador
Teléfonos:	2251-8200

Contacto.

Nombre:	Erick Alfredo Flores Aguilar
Tel. Oficina	2251-8200 (1729)
E-mail	eflores@udb.edu.sv

10.6 APENDICE A6: Proveedores y números de contactos detallado.

Compañía.	**JmTelcom**			
Servicios Soportados.	Cableado/equipos de red/servidores			
Servicios existentes.	Cableado/equipos de red/servidores			
Teléfono de contacto.	**2246-6000**			
Dirección:	67 Avenida Sur, Colonia Roma, San Salvador, El Salvador			
E-mail	**info@jmtelcom.com**			
Contactos.	E-mail	Teléfono.	Celular.	Locación.
-	**info@jmtelcom.com**	2246-6000	-	San Salvador, El Salvador

Compañía	**STB Computer**			
Servicios Soportados.	Cableado/equipos de red/equipos de computo			
Servicios existentes.	Cableado/equipos de red/equipos de computo			
Teléfono de contacto.	**2121-8190**			
Dirección:	57 Av. Norte Alameda Roosevelt #2940, San Salvador			
E-mail	mercadeo@stbgroup.com			
Contactos	E-mail	Teléfono.	Celular.	Locacion.
Yanira Monterrosa.	ymonterrosa@stbcomputer.com	2121-8190	7877-2799	San Salvador, El Salvador

Compañía	**ASIT**
Servicios Soportados.	Cableado/equipos de red/equipos de computo
Servicios existentes.	Cableado/equipos de red/equipos de computo
Teléfono de contacto.	**2555-9420**

Dirección:	Condominio Torremolinos Local No.15, San Salvador			
E-mail	-			
Contactos	E-mail	Teléfono.	Celular.	Locación.
-	-	2555-9420	-	San Salvador, El Salvador

Compañía	**ETS Consulting**			
Servicios Soportados.	Cableado/equipos de red/equipos de computo			
Servicios existentes.	Cableado/equipos de red/equipos de computo			
Teléfono de contacto.	**2206-6916**			
Dirección:	Edificio Vitorria, Calle El Mirador 4814, San Salvador			
E-mail				
Contactos	E-mail	Teléfono.	Celular.	Locación.
-	-	2206-6916	-	San Salvador, El Salvador

Compañía	**CXTEC**			
Servicios Soportados.	Equipos de red (internacional).			
Servicios existentes.	Equipos de red (internacional).			
Teléfono de contacto.	**(315) 479-1070**			
Dirección:	-			
E-mail	international@xctec.com			
Contactos	E-mail	Teléfono.	Celular.	Locación.
-	international@xctec.com	(315) 479-1070	-	New York, Estados Unidos.

Compañía	**Columbus (C&W)**			
Servicios Soportados.	Enlace de internet principal y publicación BGP			
Servicios existentes.	Enlace de internet de 100mbps			
Teléfono de contacto.	**(503) 2536-8528**			
Dirección:	Edificio Avante, Urbanización Madre Selva 3, Calle Llama del Bosque Poniente, Pje. S, L-15 y 17, Antiguo Cuscatlán, La Libertad, El Salvador			
E-mail	gumontoya@cwc.com / jumartinez@cwc.com			
Contactos	E-mail	Teléfono.	Celular.	Locación.
SID Project Manager: Gustavo Montoya Specialist Engineer: Juan S. Martinez	gumontoya@cwc.com jumartinez@cwc.com	(503) 2536-8528 57-315-222-9416	- -	El Salvador Colombia

Compañía	**Claro Telecom, El Salvador**			
Servicios Soportados.	Enlace de internet			
Servicios existentes.	Enlace de internet de 100mbps			
Teléfono de contacto.	**(503) 2271-7010**			
Dirección:	Complejo Telecom Roma, Edificio "F", 1er Nivel, Calle Liverpool y Final Calle el Progreso, Colonia Roma			
E-mail	Milton.diaz@claro.com.sv			
Contactos	E-mail	Teléfono.	Celular.	Locación.
Ingeniero de Proyectos. Milton Gabriel Díaz Ramírez	Milton.diaz@claro.com.sv	2271-7452	7855-1485	El Salvador, San Salvador.

Compañía	**Telefonica, El Salvador**			
Servicios Soportados.	Enlace de internet			
Servicios existentes.	Enlace de internet de 100mbps			
Teléfono de contacto.	**(503) 2211-2000 opción 2**			
Dirección:	64 Av. Sur. Centro Financiero Gigante, Torre D, 1er Nivel (Edificio de estacionamiento) Dpto. de San Salvador			
E-mail	ricardo.zelaya@telefonica.com			
Contactos	E-mail	Teléfono.	Celular.	Locación.
Jefatura N2 Ricardo Zelaya	Ricardo.zelaya@telefonica.com	2211-2000 opción 2	7833-0563	El Salvador, San Salvador.

10.7 APENDICE A7: Control del staff por área de trabajo.

Objetivo Mantener control centralizado de la locación de los empleados.

Procedimientos para líderes de equipos.

- Hacer y enviar copias de esta lista de contactos.
- Completar después de la activación del plan de recuperación para tener control.
- Revisarlo a medida avanza el plan de recuperación.

Códigos de locación.

0. Empleado no contactado, se dejó un mensaje.
1. Empleado en sitio trabajando.
2. Empleado fuera del sitio de trabajo.
3. Empleado sugerido para ayudar en caso de que se active el plan de recuperación.
4. Empleado en el sitio alterno.
5. Empleado sugerido de permanecer en sitio hasta próximo aviso.

Fecha: Diciembre 2017

NOMBRE DE CONTACTO.	TELÉFONOS.	CÓDIGO DE LOCACIÓN.	FECHA.
Director de IT / Director Depto. Seguridad Informática / Director Infraestructura / Director Soporte Técnico.	2251-8200 ext. 1729 7924-6922 7028-3268		DICIEMBRE 2017
Administrador de Redes.	2551-8200 ext. 1729 7237-2480		Diciembre 2017

10. 8 APENDICE A8: BIA / Servicios Críticos de infraestructura.

Los siguientes datos fueron obtenidos mediante las entrevistas a las partes interesadas (Auditoria interna y Dirección de infraestructura) y análisis de ellas

Nombre de la aplicación.	Departamento.	Descripción del proceso crítico.	RTO	RPO	Responsable
Gestión de enlaces de comunicación	Departamento de TI	Sistema que lleva el control de los diferentes enlaces que se poseen y el monitoreo de los mismo	1 hora	1 hora	Ing. Erick Flores.
Servidores y comunicación	Departamento de TI	Encargado de la comunicación total de todos los aplicativos dentro y fuera de la Universidad, este mismo guarda la información que se ingresa de los diferentes aplicativos	2 horas	2 horas	Ing. Erick Flores
Plataformas educativas	Departamento de TI	Es una herramienta física-virtual que brinda la capacidad de interactuar con uno o varios usuarios con fines pedagógicos para poder facilitar la educación a todos los estudiantes.	4 horas	4 horas	Ing. Erick Flores.
Conexión con ISP	Departamento de TI	Enlace entre ISP y la Universidad.	1 hora	1 hora	Ing. Erick Flores

10.9 APENDICE A9: Diagrama de recuperación (secuencia)

Secuencia de recuperación.	Recursos.	Servicios soportados.	Locación.	Alternativa.
1	Router	Internet Última Milla	Centro de Datos	Cambio de proveedor
2	Firewall	VPN's, Internet, Enrutamiento	Centro de Datos	Cambio de equipo
3	Switch	Distribución Interna de Red	Centro de Datos	Cambio de equipo

10.10 APENDICE A10: Inventario de procedimientos de recuperación.

Nombre del procedimiento.	Descripción.
Recuperación de enrutador principal.	Pasos que seguir para la recuperación del enrutador principal ya sea por falla parcial o total del activo.
Recuperación switch principal.	Pasos que seguir para la recuperación del Switch principal ya sea por falla parcial o total del activo.
Recuperación Firewall principal.	Pasos que seguir para la recuperación del Firewall principal ya sea por falla parcial o total del activo.
Recuperación Estación de Trabajo de Administradores.	Pasos a seguir para la recuperación de la estación de trabajo de los administradores principal ya sea por falla parcial o total del activo.

Tabla 2.6 Apéndice A10

10.11 APENDICE A11: Procedimientos de recuperación.

	Procedimientos de recuperación.	Archivos.
1	Recuperación Enrutador Principal.	Buscar repositorio de archivos con nombre <RecuperacionRouter.docx> o su copia física en oficina de IT.
2	Recuperación Switch Principal.	Buscar repositorio de archivos con nombre <RecuperacionSwitch.docx> o su copia física en oficina de IT.
3	Recuperación Firewall Principal.	Buscar repositorio de archivos con nombre <RecuperacionFirewall.docx> o su copia física en oficina de IT.
4	Recuperación de Estación de Trabajo de Administradores.	Buscar repositorio de archivos con nombre <RecuperacionEstacion.docx> o su copia física en oficina de IT.

Tabla 2.7 Apéndice A11

Procesos de recuperación

	Recuperación de firewall principal.	Código Proceso:
		Versión: 0.1
UNIVERSIDAD DON BOSCO, DEPARTAMENTO DE IT.		
Elaborado por:	Revisado por:	Aprobado por:
Fecha:	Fecha:	Fecha:

1. Recuperación del firewall principal.

Paso.	Responsable.	Descripción.	Frecuencia.	Recurso.
1	Director de CTIC	Jefe de CTIC debe definir quiénes son los encargados de la recuperación de equipos en una lista con sus contactos y posiciones dentro de la Universidad.	Cada 6 meses o cuando existan cambios.	
2	Jefe de infraestructura	Jefe de infraestructura debe declarar que el equipo necesita ser reemplazado cuando el firewall presenta fallas parciales o totales en sus componentes.	En demanda.	
3	Jefe de infraestructura	Se debe reemplazar el equipo declarado por el Jefe de Infraestructura sino hay en existencia se debe contactar a los proveedores correspondientes.	En demanda.	Lista de proveedores.docx o lista de proveedores DRP UDB.
4	Jefe de infraestructura	Se debe obtener la última configuración del equipo del repositorio para poder recuperar las operaciones tan pronto el equipo este en sitio o si ya está en sitio restaurar la configuración rápidamente.	En demanda.	Repositorio de respaldos de configuraciones.
5	Jefe de infraestructura	Después de la recuperación probar que todas las operaciones	En demanda.	

		estén restauradas al igual que la VPN y otros recursos de internet.		
6	Jefe de infraestructura	Si el equipo que fallo se encuentra en garantía, hacerla efectiva con el proveedor correspondiente.	Lo más pronto posible.	Lista de proveedores.docx o lista de proveedores DRP UDB.
7	Jefe de infraestructura.	Hay que declarar que todas las operaciones han sido restauradas y crear un informe del equipo que fallo y las razones.	Una semana después del incidente.	

Tabla 2.8 Recuperación del firewall

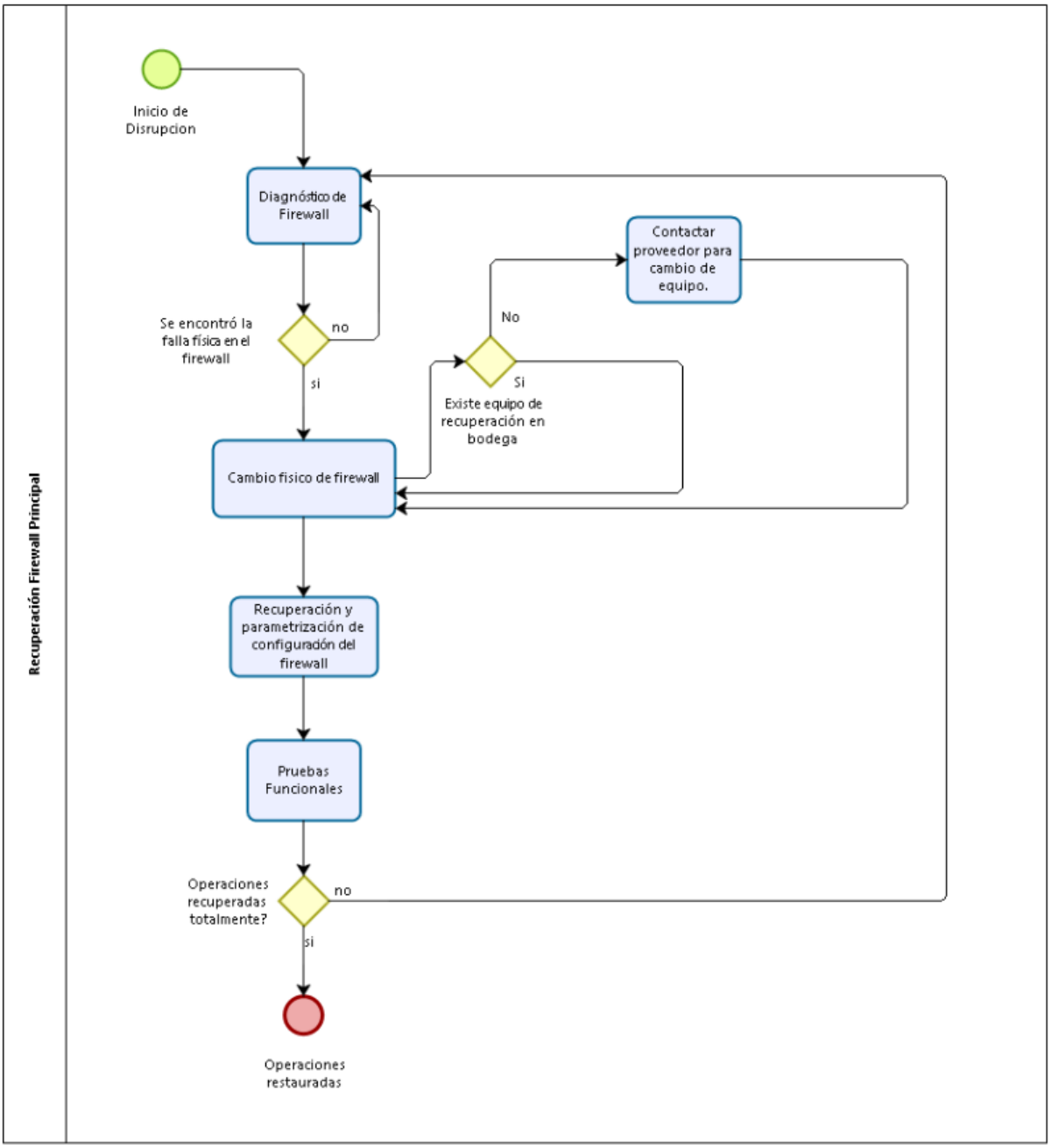

Figura 12.2 Recuperación de firewall principal.

	Recuperación de enrutador principal.	Código Proceso:
		Versión:
UNIVERSIDAD DON BOSCO, DEPARTAMENTO DE IT.		
Elaborado por:	Revisado por:	Aprobado por:
Fecha:	Fecha:	Fecha:

1. Recuperación del enrutador principal.

Paso.	Responsable.	Descripción.	Frecuencia.	Recurso.
1	Director de CTIC	Jefe de CTIC debe definir quiénes son los encargados de la recuperación de equipos en una lista con sus contactos y posiciones dentro de la Universidad.	Cada 6 meses o cuando existan cambios.	
2	Jefe de infraestructura	Jefe de infraestructura debe declarar que el equipo necesita ser reemplazado cuando el enrutador falla.	En demanda.	
3	Jefe de infraestructura	Se debe reemplazar el equipo declarado por el Jefe de Infraestructura sino hay en existencia se debe contactar a los proveedores correspondientes.	En demanda.	Lista de proveedores.docx
4	Jefe de infraestructura	Se debe obtener la última configuración del equipo fallando del repositorio para poder recuperar las operaciones tan pronto el equipo este en sitio o si ya está en sitio solo restaurar la configuración.	En demanda.	Repositorio de respaldos de configuraciones.
5	Jefe de infraestructura	Después de la recuperación probar que todas las operaciones estén restauradas.	En demanda.	
6	Jefe de	Si el equipo que fallo se	Lo más pronto	

	infraestructura	encuentra en garantía, hacerla efectiva.	posible.	
7	Jefe de infraestructura.	Hay que declarar que todas las operaciones han sido restauradas y crear un informe del equipo que fallo y las razones.	Una semana después del incidente.	

Tabla 2.9 Recuperación del enrutador

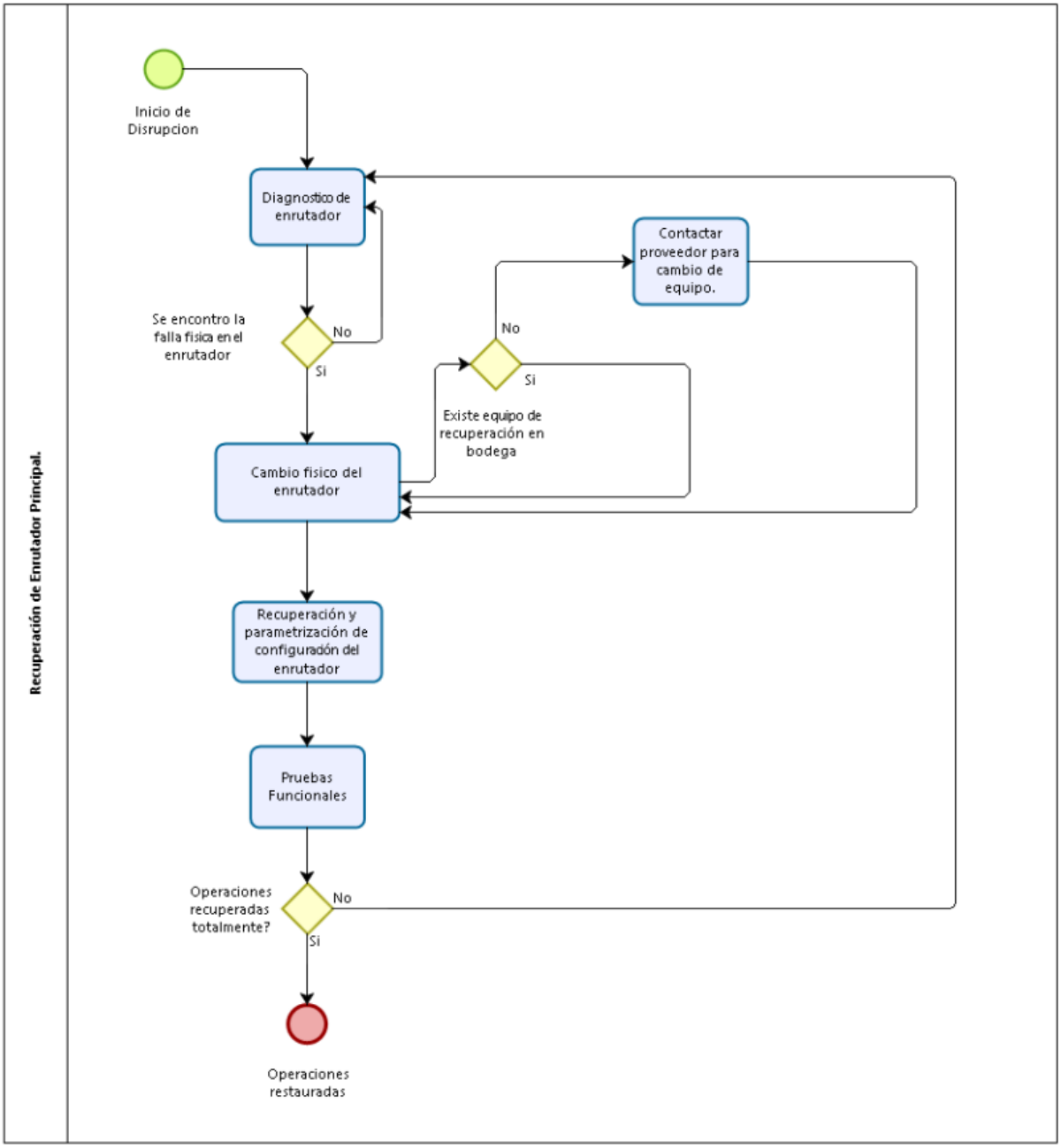

Figura 12.3 Recuperación de enrutador principal.

	Recuperación de Switch principal.	Código Proceso:
		Versión:
UNIVERSIDAD DON BOSCO, DEPARTAMENTO DE IT.		
Elaborado por:	Revisado por:	Aprobado por:
Fecha:	Fecha:	Fecha:

1. Recuperación del Switch principal.

Paso.	Responsable.	Descripción.	Frecuencia.	Recurso.
1	Director de CTIC	Jefe de CTIC debe definir quiénes son los encargados de la recuperación de equipos en una lista con sus contactos y posiciones dentro de la Universidad.	Cada 6 meses o cuando existan cambios.	
2	Jefe de infraestructura	Jefe de infraestructura debe declarar que el equipo necesita ser reemplazado cuando el Switch falla parcial o totalmente y afecta las operaciones normales del sitio en cuestión.	En demanda.	
3	Jefe de infraestructura	Se debe reemplazar el equipo declarado por el Jefe de Infraestructura sino hay en existencia se debe contactar a los proveedores correspondientes.	En demanda.	Lista de proveedores.docx o lista de proveedores DRP UDB.
4	Jefe de infraestructura	Se debe obtener la última configuración del equipo del repositorio para poder recuperar las operaciones tan pronto el equipo este en sitio o si ya está en sitio restaurar la configuración. Como nota este proceso se puede seguir para los equipos que también son de capa 2 los cuales solo necesitan ser conectados directamente a la red sin ningún o mayor configuración requerida.	En demanda.	Repositorio de respaldos de configuraciones.
5	Jefe de infraestructura	Después de la recuperación probar que todas las	En demanda.	

		operaciones estén restauradas.		
6	Jefe de infraestructura	Si el equipo que fallo se encuentra en garantía, hacerla efectiva.	Lo más pronto posible.	Lista de proveedores.docx o lista de proveedores DRP UDB.
7	Jefe de infraestructura.	Hay que declarar que todas las operaciones han sido restauradas y crear un informe del equipo que fallo y las razones.	Una semana después del incidente.	

Tabla 2.10 Recuperación del Switch

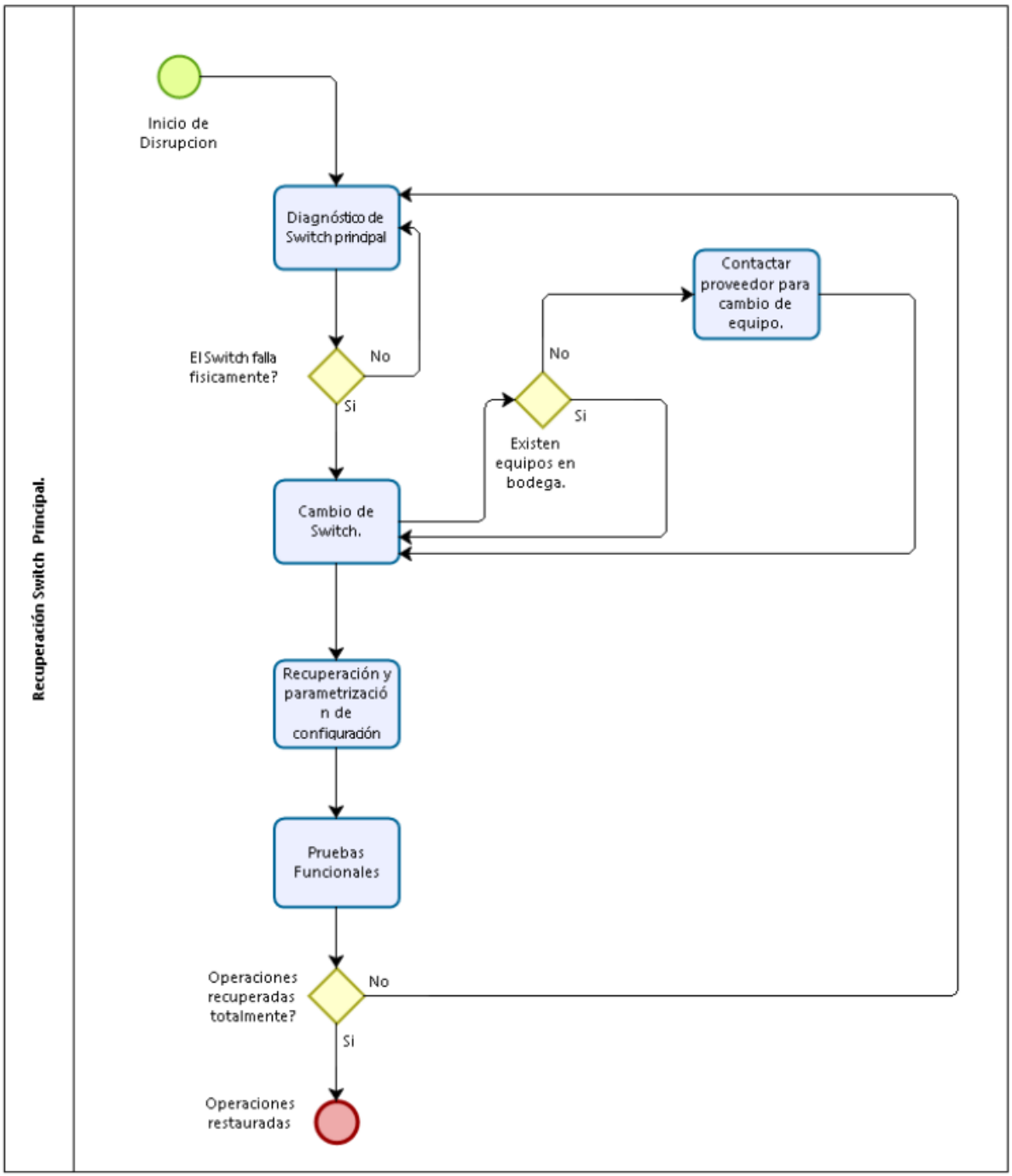

Figura 12.4 Recuperación de switch principal.

	Recuperación de Estación de Trabajo de Administrador.	Código Proceso:
		Versión:
UNIVERSIDAD DON BOSCO, DEPARTAMENTO DE IT.		
Elaborado por:	Revisado por:	Aprobado por:
Fecha:	Fecha:	Fecha:

1. Recuperación de estación de trabajo de administrador.

Paso.	Responsable.	Descripción.	Frecuencia.	Recurso.
1	Director de CTIC	Jefe de CTIC debe definir las computadoras que estarán bajo el uso de los administradores las cuales por la naturaleza de su trabajo poseen y almacenan información importante para el área.	En demanda.	
2	Técnico soporte.	Quincenalmente se debe hacer un backup de todos los archivos críticos que poseen las máquinas de los administradores de los sistemas para evitar o minimizar cualquier pérdida de información en caso de fallo del equipo.	Quincenal.	
3	Técnico de soporte.	Dependiendo del fallo del equipo puede variar entre partes como la fuente de energía, el disco duro, la tarjeta madre entre otros componentes vitales para el funcionamiento de la estación de trabajo, después de la detección del problema se debe proceder a cambiar la parte que falla.	En demanda.	Lista de proveedores.docx o lista de proveedores DRP UDB.
4	Administrador.	En caso la falla sea en el disco duro, se debe	En demanda.	Repositorio respaldos de

		proceder a verificar los documentos que se han perdido o dañado para luego ser recuperados y ver si la información en este esta actualizado.		información de las estaciones de trabajo.
5	Técnico Soporte.	Si la parte cambiada en el equipo estaba en existencia en bodega, se debe llenar una bitácora con el componente utilizado y el componente reemplazado, en caso de ser disco duro, el disco duro debe perforarse para evitar que alguna información pueda ser recuperada después de ser desechado.	En demanda.	Formato bitácora de equipos reemplazados.

Tabla 2.11 Recuperación de estación de trabajo de administrador

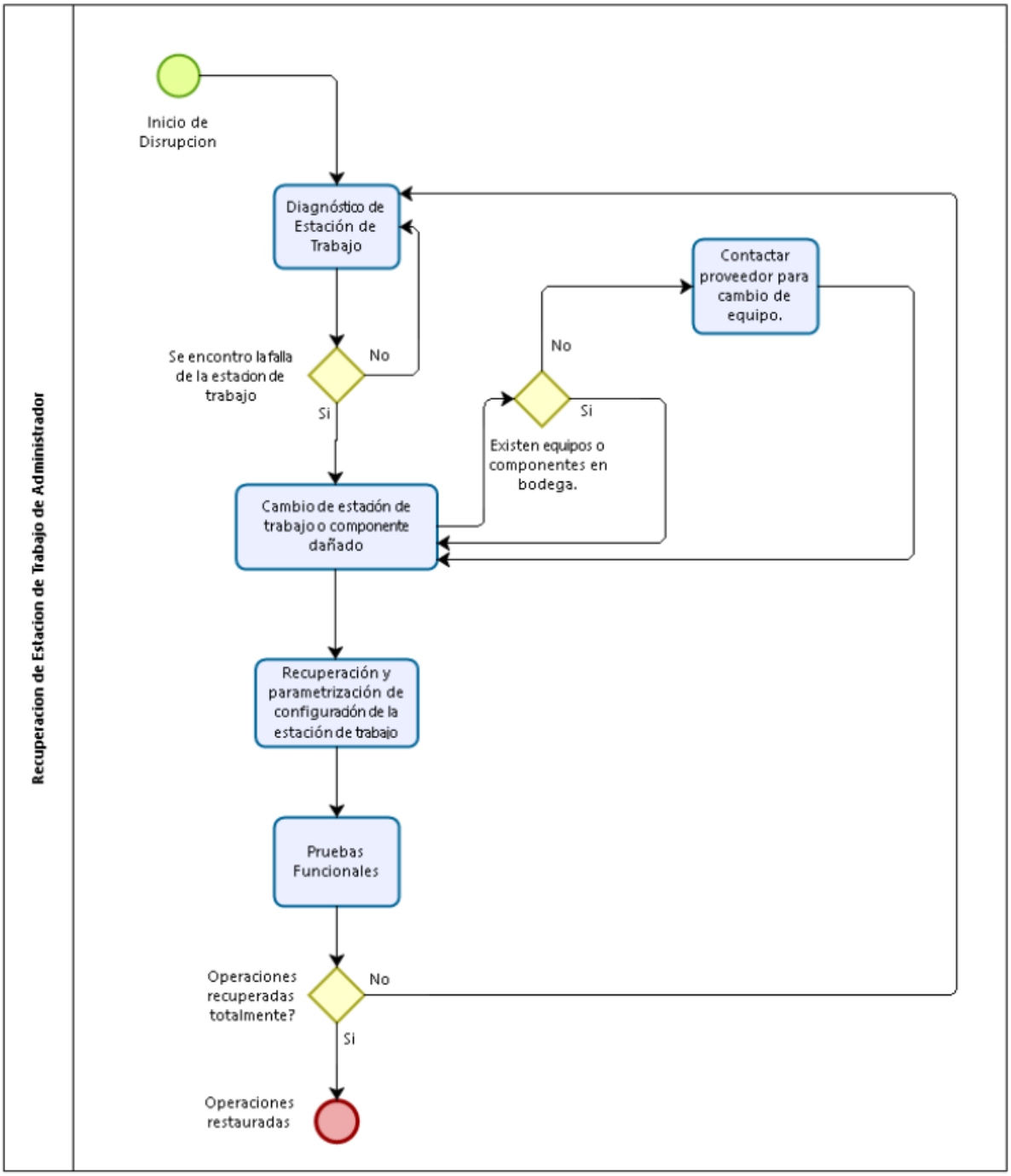

Figura 12.5 Recuperación de la estación de trabajo principal.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1) En este momento la Universidad se encuentra vulnerable en el contexto de protección a la continuidad y recuperación de sus procesos de infraestructura de red ante eventos disruptivos, lo cual en caso que se materialice causara graves consecuencias a nivel operativo como a nivel de imagen de la institución.

2) El contar con procedimientos bien definidos en el marco de la recuperación de desastres es fundamental para garantizar una recuperación básica de funciones en un tiempo adecuado sin que afecte en gran medida a las operaciones de la institución en caso del acontecimiento de eventos que atenten al normal funcionamiento de las funciones de la institución.

3) Como se pudo observar en el capítulo III de este documento, se debe tomar en cuenta que una vez se establezcan los controles y medidas de recuperación, es imperativo darle el respectivo seguimiento para asegurar mantener el DRP lo más actualizado para hacer frente a nuevos métodos de ataques y eventos los cuales amenacen la normal operación de la Universidad.

5.2 Recomendación

1) Los equipos de recuperación deben utilizarse solo para la tarea que se ha definido de recuperación de desastres y no para otra tarea diaria dentro del funcionamiento de los sistemas de la Universidad.
2) Se debe tener un equipo de recuperación o respaldo para el firewall o tener un proveedor que pueda dar un equipo nuevo en un periodo corto de tiempo.
3) Tener los respaldos de las configuraciones de los equipos críticos actualizados y con copias probadas y en diferentes locaciones.
4) Acomodar el campus antiguo Cuscatlán para poder ser un sitio de contingencia si ocurre algún desastre en el campus Soyapango.
5) Configurar todos los proveedores de internet con el bloque BGP público que la Universidad posee para no depender solamente de un proveedor de internet, esto específicamente para algunas VPN’s que se ven afectadas cuando el proveedor principal falla.

6) Limitar la carga en el UPS principal del centro de cómputo ya sea quitando ciertas áreas del centro informático u obteniendo otro UPS para las estaciones de trabajo y así extender el tiempo que el UPS soportara la carga del centro de datos.
7) Cambio de switches capa 2 por switches administrables y tener capacidades de vlaning para tener una mejor segmentación de la red de la Universidad.

Glosario

Palabra.	**Significado.**
Actividades (Conforme a COBIT)	Acciones requeridas para lograr un resultado medible.
Análisis de Impacto	El Análisis de Impacto BIA tiene por objeto analizar los impactos a los que la organización puede enfrentarse ante la discontinuidad de sus operaciones.
Auditoria interna	La auditoría interna es un sistema de control interno de la empresa y consiste en el conjunto de medidas, políticas y procedimientos establecidos en una organización concreta para proteger su activo, minimizar riesgos, incrementar la eficacia de los procesos operativos y optimizar y rentabilizar, en definitiva, el negocio.
BCRS	Se puede definir también como una compilación de procesos que permiten identificar y evaluar los riesgos potenciales que podrían interrumpir la actividad normal en la organización
BIA	Business Impact Analysis, es la parte del DRP que identifica los sistemas afectados durante una disrupción y además cuantifica económicamente el impacto.
Continuidad de Negocio.	Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre
COBIT (Marco de referencia)	Por sus siglas en ingles "Control Objectives Control Objectives for Information and related Technology".
Cortafuegos/Firewall	Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios
Dominios (Conforme a COBIT)	Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional
DRP	Por sus siglas en inglés "Disaster Recovery Plan", es un plan estructurado que posibilite la recuperación de los sistemas IT.
Evaluación de Riesgos	La evaluación de riesgos busca identificar y eliminar riesgos presentes en el entorno de trabajo así como la valoración de la urgencia de actuar.

Evaluación de gestión de riesgos	Evaluar riesgos es un proceso por el cual una organización identifica amenazas, evalúa el nivel de riesgo asociado con esas amenazas, y determina formas de evitar altos riesgos (high-risks hazards). Una evaluación de riesgos debería ser llevada a cabo antes de que las políticas para el manejo de riesgos sean creadas, y antes de que un proyecto comience.
Estructura organizativa	La estructura organizacional es fundamental en todas las empresas, define muchas características de cómo se va a organizar, tiene la función principal de establecer autoridad, jerarquía, cadena de mando, organigramas y departamentalizaciones, entre otras.
Enrutador/Router	Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red o un switch), y que por tanto tienen prefijos de red distintos.
Frameworks/Marco de referencia.	Es una base que determina teorías, antecedentes, regulaciones o límites de un proyecto, investigación, programa o procesos. Algunos ejemplos son las ISO, COBIT, ISACA, ITIL, entre otros.
Infraestructura	Todos aquellos elementos básicos e imprescindibles para cualquier institución organización pública o privada (empresa, oficina o industria) que precise todos o algunos de os siguientes servicios de telecomunicaciones: teléfono, fax, ordenador, escáner, impresoras, TPV, cámaras de control y vigilancia, control de accesos, datafonos, climatización, incendio, etcétera.
ISO	International Organization for Standardization, organización encargada de desarrollo de la estandarización y las actividades con ella relacionada en el mundo con la mira en facilitar el intercambio de servicios y bienes, y para promover la cooperación en la esfera de lo intelectual, científico, tecnológico y económico.
ISO 22301	Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio
ISACA	Information Systems Audit and Control Association, organización que ayuda a los profesionales en diferentes áreas de la cyberseguridad.
IT	La tecnología de la información (TI, o más conocida como IT por su significado en inglés: information technology) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas
Norma	Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
NOC	Network Operation Center o centro de control de red, es donde se monitorea, manipula y controlan las redes de computadoras de una o varias organizaciones.

Procesos (Conforme a COBIT)	Conjuntos o series de actividades unidas con delimitación o cortes de control.
Riesgo	Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufran perjuicio o daño.
RTO	Recovery Point Objective: Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.
RPO	Recovery Time Objetive: RPO se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. ¿Las transacciones de cuánto tiempo estamos dispuestos a perder, o a tener que reintroducir al sistema?
Switch	Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta
TIC	Tecnología de Información y comunicación.
UPS	Uninterruptible power supply: O baterías de respaldo para equipos informáticos ya sea computadoras o equipos de infraestructura.

Referencias bibliográficas

[1] Dejan Kosutic. (2017). Título del artículo. ISO 27001 vs ISO22301 Matrix. Recuperado de http://www.advisera.com/27001academy/

[2] Rhand Leal. (2017). Título del artículo. Business Impact Analysis Toookit Preview. Recuperado de http://www.advisera.com/27001academy/

[3] Ing. Juan Carlos Angarita C (2012). Título del artículo. ISO 22301:2012 Societal security -- Business continuity management systems Requirements. Recuperado de http:// www.iso.org/standard/50038.html

[4] ISACA (2012). Título del artículo. COBIT 5 Spanish. Recuperado de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

[5] Miguel Angel Mendoza (2015). Título del artículo. COBIT para la seguridad en las organizaciones. Recuperado de http://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

[6]Sarah K. White (2017). Título del artículo. COBIT para la seguridad en las organizaciones. Recuperado de http://www.networkworld.es/archive/que-es-cobit-un-marco-para-la-alineacion-y-la-gobernanza

[7] Daniel Soto (2016). Título del artículo. ¿Que es COBIT y para qué sirve? Recuperado de http://www nextech.pe/que-es-cobit-y-para-que-sirve/

[8] Paloma Garcial Lopez (2013). Principales Novedades de la ISO 22701/22702?. Recuperado de http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf

ANEXOS

ANEXO 1: BIA de procesos de la estructura de red

Business Impact Assessment						
Entity	UNIVERSIDAD DON BOSCO					
BU	**Proceso crítico del negocio**	**Descripción**	**Responsable**	**RTO**	**Comentarios RTO**	**RPO**
PROCESOS DE INFRAESTRUCTURA DE RED						
VICERECTORÍA DE CIENCIA Y TECNOLOGÍA	Gestión de enlaces de comunicaciones	Sistema que lleva el control de los diferentes enlaces que se poseen y el monitoreo de los mismos.	Ing. Erick Flores, Coordinador de TI UDB	1 hora	Sistema de alta criticidad para el control de las comunicaciones y enlaces utilizados por la Universidad.	1 hora
	Servidores y comunicaciones	Encargado de la comunicación total de todos los aplicativos dentro y fuera de la Universidad este mismo guarda la información que se ingresa de los diferentes aplicativos.		2 horas	Sistema de alta criticidad que necesita estar disponible debido a la alta tasa de transacciones manejado por el mismo.	2 horas
	Plataformas educativas	Es una herramienta física-virtual que brinda la capacidad de interactuar con uno o varios usuarios con fines pedagógicos para poder facilitar la		4 horas	Sistema utilizado tanto por personal administrativo, docentes y alumnos con fines pedagógicos, es de alta criticidad y debe estar	4 horas

		educación a todos los estudiantes.			disponible en poco tiempo luego de una interrupción.	
	Conexión con ISP	Enlace entre ISP y la Universidad		1 hora	El enlace entre ISP y la Universidad debe ser lo más constante posible, puesto que muchos sistemas dependen del mismo.	1 hora

Tabla 3 BIA de procesos críticos de la infraestructura de red

ANEXO 2: Análisis de riesgos a procesos críticos de la infraestructura de red

Riesgo ID	Descripción de riesgos	Responsable actual	Fecha levantamiento de riesgo	Probabilidad Inherente	Impacto inherente	Proximidad	Contramedida/s (Responsable)	Probabilidad residual	Impacto residual	Outline Contingency Plan	Estatus actual
1	Existe el riesgo de pérdida de funcionalidad en los procesos llevados en la Universidad al no contar con un servicio de Internet adecuado	Ing. Erick Flores, Coordinador de TI UDB	Diciembre 2017	M	H	En cualquier momento	Contratación de un servicio de internet secundario totalmente independiente de modo que si hay una caída de servicio el enlace secundario entre a trabajar de inmediato	L	M	Contratación de un enlace secundario de internet	Abierto
2	Existe el riesgo de caida de operaciones de la infraestructura de red al haber un corte de energia y que la planta electrica no funcione adecuadamente por falta de mantenimiento preventivo	Ing. Erick Flores, Coordinador de TI UDB	Diciembre 2017	H	H	En cualquier momento	Contar con un plan de mantenimiento preventivo efectivo para la planta eléctrica, el cual asegure un funcionamiento óptimo en caso de cortes eléctricos, Coordinador de TI	M	M	Mantener en óptimas condiciones las planta auxiliar de modo que si cae el servicio eléctrico no afecte la operatividad	Abierto
3	Riesgo de interrupciones de servicios y procesos debido a ataques DOS	Ing. Erick Flores, Coordinador de TI UDB	Diciembre 2017	M	H	En cualquier momento	Implementación de técnicas de mitigación para ataques informáticos (Firewall, IDS, IPS), Coordinador de TI	L	M	Implementación de medidas (hardware y software) de mitigación ante ataques DOS	Abierto

4	Existe riesgo de Perder la conectividad de la Red interna y puede suceder por algún problema interno o externo	Ing. Erick Flores, Coordinador de TI UDB	Diciembre 2017	M	H	En cualquier momento	Mantener un constante monitoreo del estado de la red de la universidad así como la definición de mantenimientos constantes y la elaboración de procedimientos para hacer frente a cualquier inconveniente, Coordinador de TI	L	M	Contar con un plan de redundancia de conexiones	Abierto
5	Existe el riesgo de caída de los enlaces dedicados a los bancos receptores de pagos	Ing. Erick Flores, Coordinador de TI UDB	Diciembre 2017	H	M	En cualquier momento	Contratación de un enlace secundario el cual garantice que la conectividad no se vea interrumpida, Coordinador de TI	M	L	Disponer de procedimientos los cuales puedan activarse cuando el enlace VPN principal falle	Abierto
6	Existe el riesgo de falla en la conectividad (core) del campus principal	Ing. Erick Flores, Coordinador de TI UDB	Diciembre 2017	M	H	Períodos de construcción y remodelaciones	Implementación de un sitio alterno ante desastres el cual provea la capacidad de operatividad básica, Coordinador de TI	L	M	Traslado de las operaciones básica de la universidad al sitio alterno definido	Abierto

Tabla 4 Análisis de riesgos de los procesos de la infraestructura de red

ANEXO 3 Evidencias de entrevistas

EVIDENCIAS PREGUNTAS DEPARTAMENTO DE CALIDAD.

Buenas tardes Inga Nery.

Como le comentaba el Ing. Flores mi compañero y yo nos encontramos en el desarrollo de nuestro trabajo de graduación y como parte de este se encuentra el análisis del estado actual de los procesos concernientes a la continuidad de negocio de la universidad, por lo que quisiéramos concertar con usted una sesión ya sea presencial o bien por conferencia de modo que podamos completar la retroalimentación la cual ya comenzamos con el área de tecnología y tener un panorama claro sobre si los objetivos y puntos de vista de las áreas están alineados. Como parte de la reunión nos parece conveniente tocar puntos específicos, lo cuales nos ayudaran a realizar el diagnostico actual de los procesos de continuidad de negocios de la universidad, los cuales quisiéramos compartírselos de antemano a fin de obtener una retroalimentación más efectiva de los temas, a continuación le comento lo que tenemos en mente consultarle:

- La Universidad tiene una metodología y procedimiento de Administración del riesgo?

- La universidad tiene alguna Estrategia para la recuperación de desastres (y si está documentado, tales como pasos para levantar los componentes de TI entre ellos servidores, routers, aplicaciones, etc)

- Se cuenta con un plan de contingencia en caso de un evento disruptivo que garantice la continuidad de negocio, además si los planes son conexos con otros planes que se estén llevando

- En base a las diferentes auditorias desarrolladas cual es el estado de preparar ración del personal de TI en cuanto al conocimiento de tratar la continuidad de negocio y si las distintas personas claves de la universidad están alineadas a los procedimientos correspondientes

- Conocer si se tiene la iniciativa de parte de la universidad de adoptar normas orientadas al aseguramiento de la continuidad de negocio entre las cuales podríamos mencionar COBIT (que objetivos y procesos de COBIT tiene implementados como el proceso DSS 04), normas ISO

- En el marco del gobierno de TI, conocer si el área en este momento está alineada a los objetivos estratégicos de la universidad y si se han detectado oportunidades de mejora en este sentido

Tal como le comentaba nuestro objetivo es obtener su apreciable retroalimentación tratando de afectar lo mínimo sus actividades diarias, por lo que si se le hace más factible realizar esta sesión con una llamada estamos en la disposición de adaptarnos en esta modalidad, también por el tema de los permisos en nuestros propios lugares de trabajo, por lo que quedamos pendiente del día y la forma de realizar la sesión.

De antemano agradezco su valiosa ayuda.

Saludos.

Atte. Andy Osegueda/Gerson Quintanilla

EVIDENCIAS PREGUNTAS DEPARTAMENTO DE INFRAESTRUCTURA.

Buenos Tardes Erick,
Dada la aprobación del Nuevo enfoque del Proyecto, queríamos saber que tan factible podría ser que nos ayude con cierta información y si fuera posible tener una reunión vía internet.
Estos son algunos de los puntos que más nos interesan:

1) Diagrama de red.
2) Equipos Críticos de red.
3) Procedimientos implementados de recuperación.
4) Procesos de recuperación
5) Proveedores de internet.
6) Proveedores de equipos.
7) Equipos de recuperación o backup.
8) Enlaces con los bancos.
9) Backup de configuraciones existentes y locación de los mismos.
10) Personas encargadas de la configuración y mantenimiento de los equipos de red.
11) Organigrama interno del área de infraestructura.
12) Contacto de las personas involucradas en el área de infraestructura.
13) Procesos y/o procedimientos críticos para el área de infraestructura (backups, cambios de equipos, cambio de configuraciones)
14) Contingencia para equipos eléctricos en caso existiera.
15) Contactos de los encargados de los suministros eléctricos.

Quedo a la espera de sus comentarios y hora para tratar de tener la reunión vía internet de ser posible.

Evidencias:

Contactos de encargados IT UDB:

Nombre: Erick Alfredo Flores Aguilar
Cargo: Jefe del Depto. de Seguridad Informática / Infraestructura de TI / Soporte Técnico
Teléfono oficina: 2251-8200 ext. 1729
Teléfono celular: 7924-6922 / 7028-3268
Dirección de residencia: Metrópolis San Gabriel Nte. Cluster 5, Pol. 3 #14, Apopa

Nombre: Eduardo José Ávila Portillo
Cargo: Administrador de Redes y Servidores
Teléfono oficina: 2251-8200 ext. 1729
Teléfono celular: 7237-2480

Dirección de residencia: San Bartolo del Norte, Calle los lirios, Polígono 7, casa #1. Junto a casa Comunal, Ilopango

Equipos de Recuperación.

Especificaciones de servidor de recuperación (también utilizado para la certificación de los respaldos semanales de servidores locales)

Servidor HP Proliant ML350 Gen9
Doble procesador Xeon E5-2620 2.4 Ghz
RAM 32 Gbytes
Almacenamiento: Discos SATA 2 Terabytes
Red: Adaptador HP Gigabit 331i (4 puertos)

Proveedores de equipos:

STB Computer
PBX: 2121-8190
57 Av. Nte. Alameda Roosevelt #2940
San Salvador, El Salvador, C.A.

ASIT
Condominio Torremolinos Local No. 15
San Salvador
2555 9420

Equipos de Networking (enrutamiento, wireless y seguridad perimetral)

JMTelcom
67 Avenida Sur, Colonia Roma, San Salvador, El Salvador
PBX El Salvador: (503) 2246-6000

ETS Consulting
Edificio Vittoria, Calle El Mirador 4814, San Salvador.
+503 22066916

Proveedor internacional (networking)

CXTEC
Telefono: (315) 479-1070
Correo Electronico: international@cxtec.com

Proveedores de internet:

C&W (Columbus)
- BW: 100 Mbps
- Contacto local:
Gustavo Montoya
SID Project Manager
+503 2536-8528
gumontoya@cwc.com
- Contacto Colombia:
Juan S. Martínez
Specialist Engineer
57-315-222-9416
jumartinez@cwc.com

Claro
- BW: 100 Mbps
- Contacto local:
Milton Gabriel Díaz Ramírez
Ingeniero de Proyectos
Gerencia de Productos Corporativos
Teléfonos: M(503) 7855-1485 / F(503) 2271-7452
milton.diaz@claro.com.sv

Telefónica:
- BW: 100 Mbps
- Contacto local:
Ricardo Zelaya
Jefatura N2
ricardo.zelaya@telefonica.com
+503 2211-2000 opción #2
+503 7833-0563

Diciembre 1ro del 2017.

Reunión preliminar Proyecto de graduación Maestría en Seguridad y Gestión de Riesgos informáticos

El propósito de la reunión fue para dar a conocer los objetivos y alcances de la investigación para el proyecto de graduación de la maestría en seguridad y gestión de riesgos informáticos, la reunión se llevó a cabo con Erick Flores, director IT e infraestructura de la Universidad Don Bosco campus Soyapango.

Los puntos a tocar fueron:

- Objetivos del proyecto.
- Alcance del proyecto.
- Necesidad de la universidad en cuenta a la continuidad de negocio.
- Procesos, proyectos y documentación que actualmente poseen en cuanto a continuidad de negocio.
- Procesos críticos de la Universidad.
- Planes de continuidad de negocio.

Además, se delimito el proyecto a la creación de:

- Evaluación de riesgos para los siguientes procesos críticos:
    - Servicios Financiero.
    - Sitio web de la Universidad.
    - Sistema de Biblioteca.
    - Aula virtual.
    - VPN contacto con los bancos.
- Creación de un DRP para los procesos mencionados anteriormente.

Además, se gestionará el permiso para poder observar la documentación existente y posiblemente tener un video llamado con las personas encargadas, especialmente del área de calidad, para poder gestionar la creación de los planes deseados acorde a la metodología que se utiliza en el área de calidad con la ayuda del Ing. Erick Flores.

Se agradece la ayuda de las personas involucradas antes, durante y después del proyecto.

Gracias y saludos.