Propuesta de Plan de Continuidad del Negocio (BCP) para la Universidad Don Bosco de El Salvador.

López Rodriguez Miguel Angel
CENTRO DE POSTGRADOS UNIVERSIDAD DON BOSCO
ANTIGUO CUSCATLAN, EL SALVADOR
miguel.lopez.sv@gmail.com

Resumen— Las instituciones de educación superior deben cuidar hoy en día su activo más importante: la información que posee. Siendo así, no es de extrañar que se le deba de proteger en caso de cualquier evento que pueda provocar una interrupción en su servicio, ya sea que se trate de errores humanos o de otros factores externos (tales como robo, desastres naturales o error de hardware), y consecuentemente se mire afectada la calidad de servicio y la rentabilidad. Si bien algunas universidades cuentan con plan de recuperación de desastres sencillo, todavía se desconoce las prestaciones de un plan de continuidad del negocio.

La presente investigación se basa en la propuesta de un proceso de gestión de continuidad del negocio para la Universidad Don Bosco.

Abstrac— The Institutions of higher education must take care today its most important asset: the information it holds. This being so, it is not surprising that he should protect in case of any event that may cause an interruption in service, whether in the case of human error or other external factors (such as theft, natural disasters or error of hardware), and consequently the quality of service and profitability you look affected. While some universities have simple Disaster Recovery Plan, the performance of a business continuity planning is still unknown.

This research is based on the proposal of a business continuity management process for Don Bosco University.

Índice de Términos— Authenticity, availability, business continuity plan, business impact analysis, disaster recovery plan, Maximum tolerance time, Risk matrix, Recovery time object, Recovery point object, security information.

I. INTRODUCCIÓN

A. Antecedentes institucionales

La Universidad Don Bosco (UDB) es una institución educativa de nivel superior, de utilidad pública, apolítica, de inspiración cristiana y sin fines de lucro. Forma parte de IUS, Instituciones Salesianas de Educación Superior, un organismo que agrupa a más de 60 universidades y estudios terciarios no universitarios en los cinco continentes.

Con una amplia oferta de carreras de pregrado y postgrado, cursos de especialización y formación continua e inspirada por el carisma salesiano, ha contribuido a la formación de profesionales integrales del más alto nivel.

Además, su modelo de vinculación Universidad – Empresa la ha llevado al establecimiento de servicios tecnológicos para formar parte activa en el mejoramiento de la calidad del sector productivo del país. [1]

B. Eventos de seguridad requeridos

Las universidades son cada vez más conscientes de la necesidad de estar preparadas para responder ante todo tipo de desastres y situaciones catastróficas.
Para la continuidad del negocio se debe definir un plan que especifique los objetivos y las prioridades a tener en cuenta por la organización en caso de un desastre que pueda afectar a la continuidad del negocio.

Para ello, es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento del sistema informático de la organización, así como recuperar los datos, aplicaciones y servicios básicos que se utilizan como soporte al negocio de la organización.

En la actualidad la importancia en la continuidad del negocio está más enfocada a las instituciones del sector bancario y financiero, como lo detallan las "Normas técnicas para la gestión de la continuidad del negocio" del Banco Central de Reserva como lo detallan sus artículos del 1 al 23. [2]

Sin embargo, la realidad es que muchas empresas no ven o no consideran que existan amenazas potenciales para su negocio hasta que el daño ya está hecho totalmente. Durante ese tiempo, el negocio puede llegar a un punto que no pueda recuperarse y el daño sea irreversible. [3]

C. Estructura del documento

El resto del documento está organizado de la siguiente manera:

En la sección 2, se presenta la metodología de trabajo donde se describe el planteamiento del Problema, Hipótesis, Objetivo General. Objetivos específicos. Alcance y Limitaciones.

En la sección 3 se presenta el marco conceptual, donde se describe la seguridad de la información, la gestión de riesgo, consecuencias de la falta de seguridad y los centros de respaldos y recuperación alternativos.

En la sección 4 se presenta el marco teórico, en el que describe el conocimiento de la organización, la planificación estratégica y el plan maestro.

En la sección 5 se presenta la estructura del plan de continuidad del negocio (BCP) en el que se detalla los componentes del BCP.

En la sección 6 se presenta los activos de información de la UDB y se describe el análisis de seguridad y riesgo y los resultados de cada activo de información.

En la sección 7 se presenta el análisis de impacto del negocio (BIA) en lo referente a su propósito, a los activos de información por nivel de riesgo y orden de prioridad, se mencionan los recursos requeridos para la restauración de información y los tiempos máximos tolerables de restauración.

En la sección 8, se presenta el plan de recuperación de desastres (DRP) y se describe el alcance, la organización y responsabilidades de los involucrados del DRP, la estructura en las etapas de inicio, respuesta, recuperación, reanudación y comunicación del DRP.

En la sección 9, se presenta el mantenimiento y mejora continua del BCP y describe el personal involucrado, las pruebas de activación, revisión de actualizaciones, cambios del BCP, concientización y capacitación.

En la sección 10, se presentan las conclusiones acorde a los objetivos específicos.
En la sección 11, se detallan todas las referencias
En la sección 12, se presenta una breve descripción del perfil del autor.

II. METODOLOGÍA DE TRABAJO

A. Planteamiento del Problema

La Universidad Don Bosco depende del personal, de sus recursos tecnológicos, y de las actividades que diariamente son ejecutadas para mantener la estabilidad funcional y seguridad operativa requerida. Como organización posee bienes tangibles, colaboradores, sistemas y tecnologías de información.

La información generada por la gestión académica y administrativa de la UDB se convierte en el activo más importante de la institución, por esa razón protegerla y poder recuperarla y dar continuidad ante desastres se convierte en una actividad primordial.

La universidad cuenta con procesos de respaldos y recuperación, identificados en el Centro de Tecnología Informática y comunicaciones (CTIC-UDB-Soyapango) y en el departamento de

Tecnología del Centro de Postgrado de la UDB-Antiguo Cuscatlán.

Aunque existen procesos se observa la necesidad de la elaboración de una propuesta de gestión de continuidad del negocio, que permita prevenir y minimizar el riesgo de la institución de no poder dar continuidad a las actividades de la universidad por causas disruptivas.

De esta forma la UDB puede disponer de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia, además el análisis correspondiente determinará los niveles de importancia de activos de información que deben incluirse, sus niveles de seguridad, riesgo y prioridad, información con la que actualmente no se cuenta.

B. Hipótesis

El desarrollo de una propuesta de gestión de continuidad del negocio para las aplicaciones y la información más sensible de la UDB, permitirá que la universidad posea un plan de contingencia ordenado y sistemático ante desastres y/o causas disruptivas que afecten la continuidad de sus operaciones.

De esta forma el proyecto de investigación contribuye al proporcionar un plan para la continuidad de los servicios más críticos y sensibles de las tecnologías de Información de la Universidad Don Bosco.

C. Objetivo General

Realizar un análisis de la situación actual de UDB en relación de los riesgos ante una pérdida de información en sus áreas más sensibles de operación, y proveer una propuesta de continuidad del negocio que permita a la universidad una guía para restablecer los servicios en un rango de tiempo aceptable para continuar con sus actividades.

D. Objetivos específicos

- Identificar los activos de información
- Identificar el nivel de prioridad por importancia.
- Identificar nivel de riesgo
- Realizar Análisis de impacto
- Definir plan de recuperación
- Definir plan de mejora continua
- Definir plan de capacitación y sensibilización

E. Alcance

Propuesta de gestión de continuidad del negocio, que identifique los principales activos de información, niveles de riesgo, análisis de impacto ante situaciones disruptivas, plan de recuperación de datos y mejora continua.

F. Limitaciones

El presente trabajo es una guía para la “Gestión de Continuidad del Negocio”, por consiguiente no incluye su implementación, será la institución quien desarrolle los mecanismos necesarios para ejecutar el plan de contingencia como un mecanismo preventivo, de verificación y de mejora continua, antelando de esta forma cualquier situación real de un hecho disruptivo en la UDB.

III. MARCO CONCEPTUAL

A. Seguridad de la Información

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, no obstante garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado.

El propósito de la seguridad de la información es, por tanto, garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el tiempo, el entorno y las tecnologías. [5]

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. [5]

Activo
Cualquier cosa que tenga valor para la organización.

Disponibilidad
La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Confidencialidad
La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados.

Integridad
La propiedad de salvaguardar la exactitud e integridad de los activos.

Seguridad de información
Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y Confiabilidad.

Evento de seguridad de la información
Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información
Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

B. Riesgo.

En base a la siguiente aseveración “Todas las actividades de una organización que implican un riesgo”, estos deben de gestionar mediante la identificación, análisis y evaluación con el objetivo de mitigarlo.

Según la ISO 31000, sobre la administración de riesgos, lo define como el efecto de la incertidumbre en los objetivos [7]

Riesgo = Probabilidad o frecuencia X el nivel de Impacto

Riesgo residual

El riesgo remanente después del tratamiento del riesgo

Aceptación de riesgo

Decisión de aceptar el riesgo

Análisis de riesgo

Uso sistemático de la información para identificar fuentes y para estimar el riesgo

Valuación del riesgo

Proceso general de análisis del riesgo y evaluación del riesgo

Evaluación del riesgo

Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

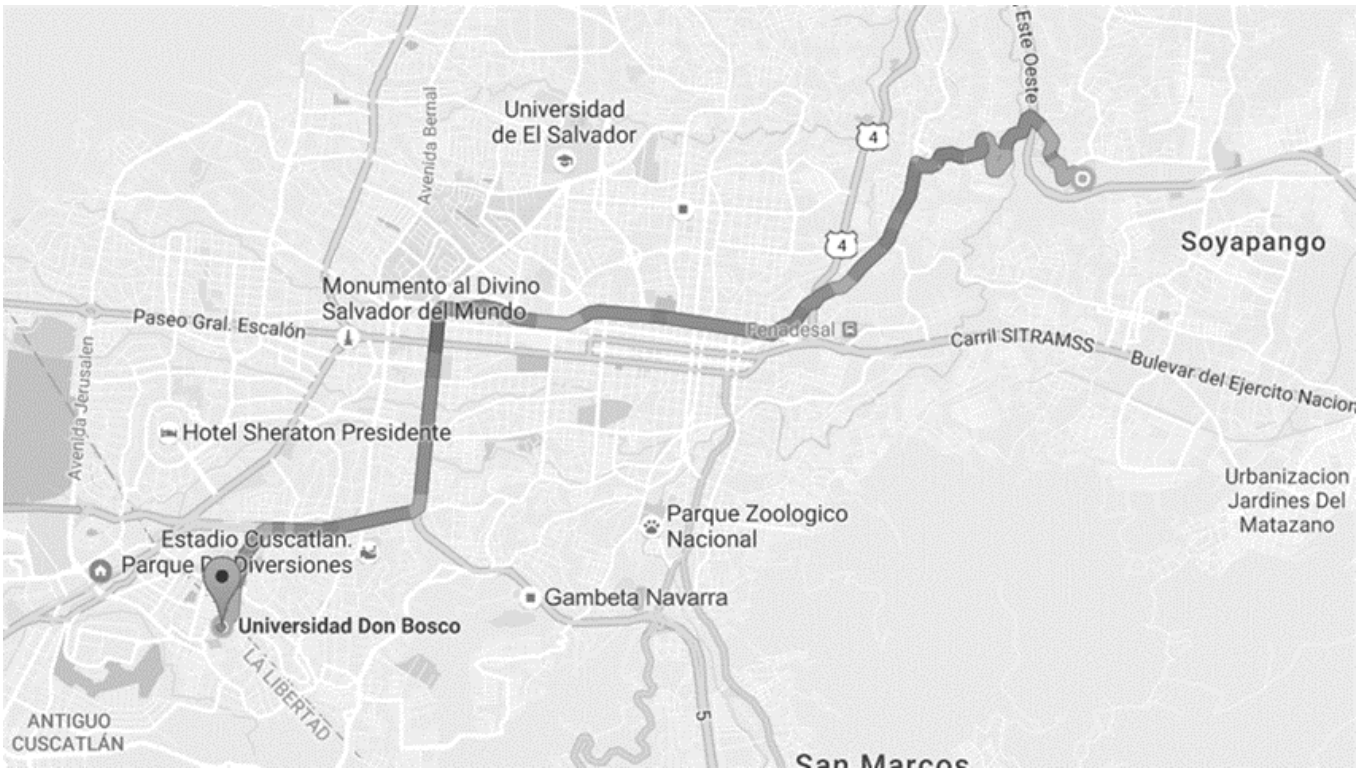

Figura 1, Ubicación de CTIC-UDB y Centro de Postgrados-UDB (32 km de distancia entre ambos campus)

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Tratamiento del riesgo

Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

C. Consecuencias de la falta de seguridad

En la actualidad el negocio y el desarrollo de las actividades de muchas organizaciones dependen de los datos e informaciones registradas en sus sistemas informáticos, así como el soporte adecuado de las Tecnologías de Información y las Comunicaciones para facilitar su almacenamiento, procesamiento, análisis y distribución.

A la hora de analizar las posibles consecuencias de la ausencia o de unas deficientes medidas de seguridad informática, el impacto total para la organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red, deberíamos tener en cuenta otras importantes consecuencias como resultados de una mala gestión de seguridad de la información.

D. Centros de respaldo y recuperación alternativos – UDB, Postgrado y nube

Se propone un Plan de Continuidad del Negocio (Business Continuity Plan - BCP), y la composición de un equipo asignado a esta actividad que se encuentre asignado el Centro de Tecnología de la Información y las Comunicaciones (CTIC), ubicado en la UDB.

Este equipo será el responsable de coordinar todas las actividades de ejecución del BCP frente a un desastre, esta labor deberá de realizarse tomando

como cede central de respaldos el CTIC, como plan de contingencia la Dirección de Tecnología del Centro de Postgrados de la UDB, y como opción alternativa algún servicio de respaldo en la nube.

Un elemento fundamental en la continuidad del negocio es la existencia de un centro alternativo, también conocido como centro de respaldo o centro de backup, si bien en la práctica sólo las grandes empresas podrán disponer de un local o edificio dedicado exclusivamente a esta misión.

Este centro tendría que estar equipado con los equipos informáticos adecuados y contar con copias de seguridad de los datos más críticos para el negocio suficientemente actualizadas.

E. Beneficios del BCP

Algunos de los beneficios que podrá obtener la UDB al hacer un "BCP", a parte de los ahorros del esfuerzo, tiempo y dinero, son los siguientes: [6]

- Mantener la continuidad de los servicios relacionados con las TIC del negocio.
- Proteger al negocio de fallas generales en los servicios informáticos.
- Minimizar los riesgos generados por la falta de servicios.
- Garantizar el acceso de la información de la Universidad.
- Mantener la disponibilidad de los recursos informáticos.
- Minimizar la toma de decisiones erróneas al presentarse algún desastre.
- Dar atención continua a los clientes, proveedores, accionistas, colaboradores.
- Tener capacidad de recuperación exitosa. [11]

IV. MARCO TEÓRICO

A. Conocimiento de la organización

Ideario de la UDB

La Universidad Don Bosco define el Ideario como el conjunto de ideas, principios y criterios que de manera organizada, conforman el "ideal" o el "deber ser" de una institución, organización o movimiento.

Creado en 2001 con los primeros esbozos del documento de la IUS, reúne la mística universitaria enraizada en los valores evangélicos, la flexibilidad del estilo educativo de Don Bosco y la preocupación por acompañar al joven en su proceso de madurez; así como el perfil del profesional que convoca.

El Ideario de la UDB nace de la rica experiencia pedagógica de más de un siglo heredada a los salesianos por Don Bosco, la cual se enriquece a través de los desafíos que surgen desde el contexto local (Soyapango) y nacional (El Salvador); de esta manera define el tipo de respuesta educativa según la naturaleza de la obra que, para nuestro caso, es una respuesta universitaria.

El Ideario de la Universidad va dirigido a toda la Comunidad Educativa (personal docente, administrativo y estudiantes), orientando y determinando todo su quehacer, permitiendo, así, la posibilidad de que toda la comunidad universitaria sea educadora desde un estilo concreto. [12]

Misión

Educamos, a la luz del Evangelio y fieles al carisma salesiano, para el desarrollo integral de la persona humana; promoviendo universitariamente, desde la ciencia y la tecnología, la construcción de una sociedad libre, justa y solidaria. [12]

Visión

Una universidad salesiana reconocida a nivel nacional e internacional por la innovación de sus carreras y servicios en función del entorno social y productivo, a partir de las competencias profesionales de sus graduados, un claustro docente de reconocido prestigio, la gestión del conocimiento, el mejoramiento continuo de la calidad y la infraestructura tecnológica para la formación integral de sus destinatarios. [12]

B. Planificación estratégica

Plan Estratégico

La planificación estratégica con un horizonte de diez (10) años, se consolida en los Objetivos Estratégicos basados por las cuatro perspectivas del FODA adoptadas en una relación causa y efecto.

Las perspectivas en referencia, constituyen líneas de Política para el decenio, que priorizan la visión de la UDB. El Plan puede ser revisado y actualizado en caso que las condiciones internas de la UDB, las nacionales e internacionales cambien de forma significativa.

Planificación Táctica

La ejecución de las estrategias institucionales se denomina Plan Maestro y es para un período de cinco (5) años. Su construcción hace uso del Cuadro de Mando Integral, para el seguimiento de indicadores y establece para los objetivos estratégicos, los indicadores, las metas, el inductor, el responsable y el periodo de ejecución.

Para garantizar la ejecución del Plan Maestro se definen Proyectos Estratégicos que se complementan con su plan de desarrollo.

Modelo de Planificación de la Universidad Don Bosco 2002-2006

A partir del año 1996 la Universidad adoptó un proceso de planificación en tres niveles: planificación estratégica, planificación táctica (Plan Maestro) y planificación operativa.

Esto dio como resultado la elaboración del Plan Estratégico para un período de diez años, el cual se concretizó a través de un Plan Maestro, para períodos de cinco años, (1997 – 2001); (2002 -2006) y (2007-2011), ejecutados por los planes operativos anuales desde 1997

Plan maestro estratégico 2007-2016

Perspectivas Adoptadas y sus Objetivos Estratégicos

La UDB ha adoptado cuatro perspectivas: Destinatarios, Financiera, Gestión e Innovación y Desarrollo Humano y Crecimiento, para construir el mapa estratégico con quince (15) Objetivos Estratégicos, distribuidos en cada perspectiva. Las perspectivas son como las líneas de política que orientarán el Plan Estratégico

1. **Perspectiva Destinatarios**

Constituyen a quienes se debe la Universidad Don Bosco y a quien ofrece servicios. Se consideran destinatarios a: estudiantes, padres de familia, empresas, organizaciones e instituciones que apoyan, público que hace de los servicios educativos, tecnológicos, profesionales y los de proyección social que desarrolla la Universidad Don Bosco. Son destinatarios prioritarios los miembros de la comunidad educativa de la Universidad Don Bosco.

Objetivos estratégicos:

1.1. Asegurar el posicionamiento de imagen de la UDB.

1.2. Fortalecer la vinculación social de la Universidad

2. Perspectiva Financiera

Es la que asegura los recursos financieros, y que permite continuar con el crecimiento y desarrollo de la Universidad en favor del logro de la MISIÓN y VISIÓN y de todos los objetivos de la UNIVERSIDAD, para garantizar el posicionamiento y la calidad educativa de la Universidad.

Objetivos estratégicos

2.1. Lograr el crecimiento económico financiero necesario que haga posible el dinámico desarrollo de la universidad.

2.2. Asegurar la consecución de recursos no reembolsables provenientes de diversas fuentes de cooperación.

3. Perspectiva Gestión e Innovación

Constituye todas aquellas iniciativas que servirán de base para el sostenimiento y desarrollo continuo de la Universidad, conlleva a la ejecución de proyectos para abrir camino de acuerdo a la Visión Institucional.

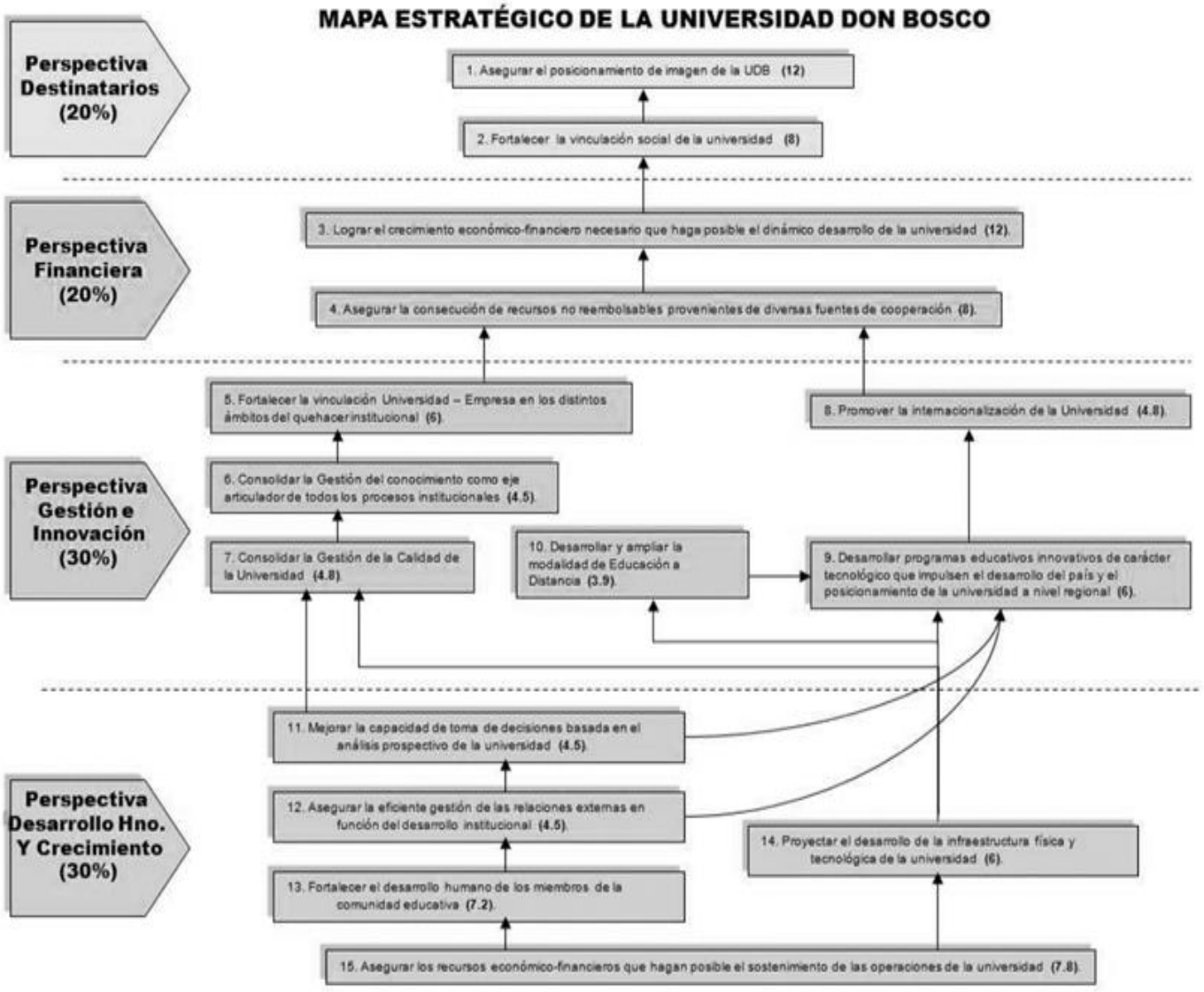

Figura 2, Mapa estratégico UDB 2007 - 2016

Objetivos estratégicos

3.1. Fortalecer la vinculación Universidad-Empresa en los distintos ámbitos del quehacer institucional.

3.2. Consolidar la gestión del conocimiento como eje articulador de todos los procesos institucionales.

3.3. Consolidar la Gestión de la Calidad de la Universidad.

3.4. Promover la internacionalización de la Universidad.

3.5. Desarrollar programas educativos innovativos de carácter tecnológico que impulsen el desarrollo del país y el posicionamiento de la universidad a nivel regional.

3.6. Desarrollar y ampliar la modalidad de educación a distancia.

4. Perspectiva Desarrollo Humano y Crecimiento

Constituye la base para que la Universidad Don Bosco cuente con los recursos humanos, físicos y financieros de funcionamiento de la Universidad, para potenciar el talento humano, contar con los recursos tecnológicos y los programas y proyectos de articulación con la sociedad.

Objetivos Estratégicos

4.1. Mejorar la capacidad de toma de decisiones basada en el análisis prospectivo de la Universidad.

4.2. Asegurar la eficiente gestión de las relaciones externasen función del desarrollo institucional.

4.3. Fortalecer el desarrollo humano de los miembros de la comunidad educativa.

4.4. Proyectar el desarrollo de la infraestructura física y tecnológica de la Universidad.

4.5. Asegurar los recursos económico-financieros que hagan posible el sostenimiento de las operaciones de la Universidad.

C. Plan Maestro

El Plan Maestro se ejecuta por proyectos, los cuales están agrupados en diez áreas temáticas. Los objetivos del Plan Estratégico2007-2016, agrupados por cada perspectiva, establecen el indicador, las metas, el inductor, el proyecto estratégico,

el responsable y el tiempo previsto para la ejecución. La Matriz de Planificación en la Perspectiva Desarrollo Humano y Crecimiento, a manera de ilustración. Las iniciativas o proyectos responden a los objetivos estratégicos, a la misión y la visión, y se distribuyen en las áreas temáticas siguientes:

- Mercadeo
- Innovación Curricular
- Gestión de la calidad
- Gestión del conocimiento
- Proyección Social
- Bienestar estudiantil
- Clima organizacional y Desarrollo Humano
- Relaciones Externas
- Infraestructura
- Desarrollo de unidades

V. ESTRUCTURA DEL PLAN DE CONTINUIDAD DEL NEGOCIO (BUSINESS CONTINUITY PLAN – BCP)

A. Componentes del Plan de Continuidad del Negocio (BCP)

De Gestión [4] [5]

1. Personas con responsabilidades definidas
2. Procesos de gestión relativos a:
3. Planeación
4. Desarrollo del BCP
5. Mejora Continua

Por norma, tiene los siguientes componentes

1 - Alcance
2 - Términos y definiciones
3 - Planear
4 - Implementar y operar
5 - Monitorear y revisar
6 - Mantener y mejorar

Contexto de la organización

1 Consideración del contexto interno y externo
2 Necesidades, requerimientos y alcance
3 Apetito del riesgo
4 Comunicación clara del alcance a partes internas y externas

Liderazgo

1 Resumen de los requerimientos específicos del rol de la alta gerencia
2 Designación de responsable del BCP

Soporte

1 Mayor énfasis en concientización
2 Mayor énfasis en comunicación
3 Más específico en requerimientos de control documental.

Operación

1 Requerimientos extendidos en estructura de respuesta a incidentes
2 Recuperación como un requerimiento totalmente nuevo

Evaluación del desempeño

1 Monitoreo, medición, análisis y evaluación
2 Auditoría interna
3 Revisión de la gerencia
4 Comunicar los resultados de la revisión de la gerencia a partes interesadas relevantes
5 Las entradas de las partes interesadas y los resultados de programas de concientización y entrenamiento no se consideran como entradas de la revisión.

VI. Activos de Información

A. Análisis de seguridad y riesgo [6]

Es necesario definir los instrumentos para el análisis del riesgo de los activos de información de la UDB, en este sentido en base a la ISO 31010 que define el riesgo como: [8]

Riesgo = Probabilidad o frecuencia X el nivel de Impacto

Se propone para el instrumento de recopilación de datos las siguientes escalas:

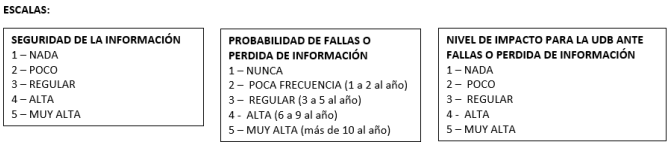

Figura 3, Escalas para levantamiento de información

CODIGO

FECHA D/M/A ____/____/____

UNIVERSIDAD DON BOSCO – PROYECTO CONTINUIDAD DEL NEGOCIO
Cuestionario sobre la seguridad y el riesgo de los activos de información

Nombre: _____ **Departamento:** _____ **Cargo:** _____

Estimado colaborador, favor de tomar en cuenta las siguientes escalas y colocar el número en las casillas correspondientes de cada activo de información, adicionar los activos y comentarios que considere pertinentes. Gracias por su colaboración. Lic. Miguel Angel López

ESCALAS:

SEGURIDAD DE LA INFORMACIÓN
1 – NADA
2 – POCO
3 – REGULAR
4 – ALTA
5 – MUY ALTA

PROBABILIDAD DE FALLAS O PERDIDA DE INFORMACIÓN
1 – NUNCA
2 – POCA FRECUENCIA (1 a 2 al año)
3 – REGULAR (3 a 5 al año)
4 - ALTA (6 a 9 al año)
5 – MUY ALTA (más de 10 al año)

NIVEL DE IMPACTO PARA LA UDB ANTE FALLAS O PERDIDA DE INFORMACIÓN
1 – NADA
2 – POCO
3 – REGULAR
4 - ALTA
5 – MUY ALTA

EJEMPLO

No	Activos de información (sistemas)	Seguridad de la información				Probabilidad	Impacto	Prioridad	Comentarios
		Confidencialidad	Integridad	Autenticidad	Disponibilidad				
1	Evaluación docente	5	5	5	3	3	5		Este sistema debe estar activo 7X24 para docentes de pregrado y post grado
2	Portafolio académico	5	5	5	3	3	5		Este sistema debe estar activo 7X24 para docentes de pregrado y post grado

CUALQUIER CONSULTA ESCRIBIR A miguel.lopez.sv@gmail.com

1

ESCALAS: 1- NADA, 2 – POCO, 3 – REGULAR, 4 – ALTA, 5 – MUY ALTA

Figura 4, Formato para la recopilación de datos de seguridad, riesgo y prioridad de activo de información

En base a las escalas aplicadas a la seguridad, riesgo y prioridad de activos de la información se define el siguiente instrumento para la recopilación de datos.

B. Identificación de Activos de Información UDB

Como parte de la metodología de investigación y con la colaboración de la jefatura del CTIC, se identificaron los activos de información UDB. [5]

TABLA 1

FORMATO PARA LA RECOPILACIÓN DE DATOS DE SEGURIDAD

EJEMPLO

No	Activos de información (sistemas)	Seguridad de la información			
		Confidencialidad	Integridad	Autenticidad	Disponibilidad
1	Evaluación docente	5	5	5	3
2	Portafolio académico	5	5	5	3

TABLA 2

FORMATO PARA LA RECOPILACIÓN DE DATOS DE RIESGO Y PRIORIDAD POR ORDEN DE IMPORTANCIA DE LOS ACTIVOS DE INFORMACIÓN

EJEMPLO

No	Activos de información (sistemas)	Probabilidad	Impacto	Prioridad	Comentarios
1	Evaluación docente	3	5		Este sistema debe estar activo 7X24 para docentes de pregrado y post grado
2	Portafolio académico	3	5		Este sistema debe estar activo 7X24 para docentes de pregrado y post grado

TABLA 3

LISTADO DE ACTIVOS DE INFORMACIÓN

No	Activos de información
1	Evaluación docente
2	Portafolio académico
3	Auditoria de documentos procesos académicos
4	Tutoría estudiantil
5	Estudio de satisfacción
6	Becas
7	Bolsa de trabajo
8	Administración de horas sociales
9	Administración de estudio socioeconómico
10	Expediente académico del alumno pregrado y posgrado
11	Planes de estudio
12	Inscripciones académicas
13	Compras
14	Inventarios
15	Requisiciones de personal
16	Acciones de personal
17	Expedientes de empleados
18	Planilla
19	Contabilidad
20	Módulo de cheques
21	Módulo financiero
22	Modulo de proyectos
23	Modulo de activo fijo
24	Sistema de administración general
25	Sistema de gestión de la información para el análisis institucional
26	Sistema de gestión de la planificación institucional
27	Configuraciones de equipos de comunicación
28	Configuraciones de servidores
29	Base de datos
30	Programas fuentes
31	Respaldos
32	Documentación técnica, administrativa f. electrónico

C. Seguridad de los activos de información

ESCALAS:

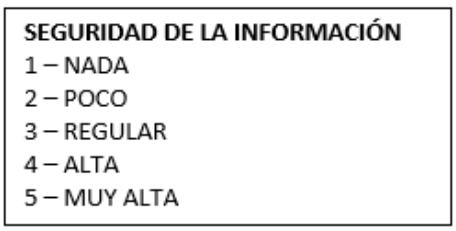

Figura 5, Escalas para identificar el nivel de seguridad en los activos de información.

TABLA 4

NIVEL DE SEGURIDAD EN LOS ACTIVOS DE INFORMACIÓN

No	Activos de información	Seguridad de la información				
		Confidencialidad	Integridad	Autenticidad	Disponibilidad	Promedio
1	Evaluación docente	4	5	5	5	4.75
2	Portafolio académico	5	5	5	5	5.00
3	Auditoria de documentos procesos académicos	4	4	5	5	4.50
4	Tutoría estudiantil	4	5	5	5	4.75
5	Estudio de satisfacción	5	4	5	5	4.75
6	Becas	5	5	5	5	5.00
7	Bolsa de trabajo	4	4	5	5	4.50
8	Administración de horas sociales	5	5	5	5	5.00
9	Administración de estudio socioeconómico	5	5	5	5	5.00
10	Expediente académico del alumno pregrado y posgrado	5	5	5	5	5.00
11	Planes de estudio	4	4	5	5	4.50
12	Inscripciones académicas	5	5	5	5	5.00
13	Compras	5	5	5	5	5.00
14	Inventarios	5	5	5	5	5.00
15	Requisiciones de personal	4	5	5	5	4.75
16	Acciones de personal	5	5	5	5	5.00
17	Expedientes de empleados	5	5	5	5	5.00
18	Planilla	5	5	5	5	5.00
19	Contabilidad	5	5	5	5	5.00
20	Módulo de cheques	5	5	5	5	5.00
21	Módulo financiero	5	5	5	5	5.00
22	Modulo de proyectos	4	5	5	5	4.75
23	Modulo de activo fijo	4	5	5	5	4.75
24	Sistema de administración general	4	4	5	5	4.50
25	Sistema de gestión de la información para el análisis institucional	4	4	5	5	4.50
26	Sistema de gestión de la planificación institucional	5	4	5	5	4.75
27	Configuraciones de equipos de comunicación	4	4	4	5	4.25
28	Configuraciones de servidores	4	4	4	5	4.25
29	Base de datos	4	4	4	5	4.25
30	Programas fuentes	4	4	4	5	4.25
31	Respaldos	4	4	4	5	4.25
32	Documentación técnica, administrativa f. electrónico	4	4	4	5	4.25

En base a los datos obtenidos referente a los atributos de seguridad de los activos de información, el promedio en temas de confidencialidad, integridad, autenticidad y disponibilidad de la información se

encuentran entre 4 y 5, lo que en relación a la escala de evaluación es alto y muy alto.

Aclarando que el enfoque de la investigación es el plan de la continuidad del negocio, y no los aspectos de seguridad, razón por la que no aplicaron métodos de verificación al respecto.

D. Matriz de riesgo

Se utilizará como herramienta de medición una matriz de riesgo, por ser una forma sencilla pero eficaz para identificar los riesgos más significativos inherentes a los activos de Información de la UDB, siendo un instrumento válido para mejorar el control de riesgos y la seguridad de una organización.

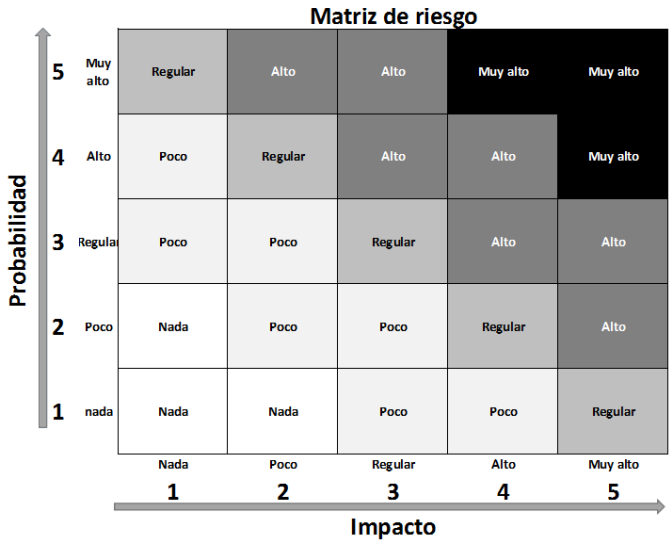

Figura 6, Escala de matriz de riesgo

La verdadera utilidad de la matriz de riesgos radica en que ofrece la posibilidad de tener una idea general de los riesgos, por este motivo, la representación de la matriz debe ser en forma de tablas no demasiado complejas donde aparezcan los riesgos, probabilidad de ocurrencia, gravedad de los mismos.

Tomando como base la escala de la matriz de riesgo se aplica la probabilidad y el impacto a los activos de información de la Universidad Don Bosco.

TABLA 5

NIVEL DE RIESGO EN BASE A LA PROBABILIDAD DE FALLA Y EL NIVEL DE IMPACTO,

No	Activos de información	Probabilidad	Impacto	Nivel de riesgo
31	Respaldos	Regular	Muy alto	Alto
3	Auditoria de documentos procesos académicos	Regular	Muy alto	Alto
16	Acciones de personal	Regular	Muy alto	Alto
27	Configuraciones de equipos de comunicación	Regular	Muy alto	Alto
28	Configuraciones de servidores	Regular	Muy alto	Alto
6	Becas	Regular	Alto	Alto
7	Bolsa de trabajo	Regular	Alto	Alto
11	Planes de estudio	Regular	Alto	Alto
22	Modulo de proyectos	Regular	Alto	Alto
5	Estudio de satisfacción	Regular	Alto	Regular
1	Evaluación docente	Poco	Muy alto	Alto
2	Portafolio académico	Poco	Muy alto	Alto
10	Expediente académico del alumno pregrado y posgrado	Poco	Muy alto	Alto
12	Inscripciones académicas	Poco	Muy alto	Alto
13	Compras	Poco	Muy alto	Alto
14	Inventarios	Poco	Muy alto	Alto
15	Requisiciones de personal	Poco	Muy alto	Alto
17	Expedientes de empleados	Poco	Muy alto	Alto
18	Planilla	Poco	Muy alto	Alto
19	Contabilidad	Poco	Muy alto	Alto
21	Módulo financiero	Poco	Muy alto	Alto
25	Sistema de gestión de la información para el análisis institucional	Poco	Muy alto	Alto
26	Sistema de gestión de la planificación institucional	Poco	Muy alto	Alto
29	Base de datos	Poco	Muy alto	Alto
30	Programas fuentes	Poco	Muy alto	Alto
4	Tutoría estudiantil	Poco	Alto	Regular
8	Administración de horas sociales	Poco	Alto	Regular
9	Administración de estudio socioeconómico	Poco	Alto	Regular
20	Módulo de cheques	Poco	Alto	Regular
23	Modulo de activo fijo	Poco	Alto	Regular
24	Sistema de administración general	Poco	Alto	Regular
32	Documentación técnica, administrativa formato electrónico	Poco	Alto	Regular

VII. ANALISIS DE IMPACTO DEL NEGOCIO – BUSINESS IMPACT ANALISYS (BIA)

A. propósito

El Análisis de Impacto al Negocio (BIA) se desarrolla como parte del proceso de planificación de contingencia para Universidad Don Bosco enfocado a los activos de información identificados en la etapa de gestión de riesgos. [15]

El propósito de la BIA es identificar y priorizar los activos de Información de mayor importancia para la misión del negocio, y utilizar esta información para caracterizar el impacto en el proceso de las actividades de la universidad si estos no están disponibles. [15]

Determinar los activos de información para la misión de la institución así como la criticidad de recuperación. Además se debe identificar los sistemas CORE de la UDB, estimar el impacto de una interrupción de los servicios junto con el impacto de interrupciones y el tiempo de inactividad estimado. El tiempo de inactividad debe reflejar el máximo que la UDB puede tolerar sin dejar de mantener la misión. [15]

Identificar las prioridades de la recuperación de los recursos del sistema.

En base a los resultados de las actividades anteriores, los recursos del sistema con mayor claridad se pueden vincular a los procesos de la misión / los procesos críticos de negocio. Los niveles de prioridad pueden ser establecidas para las actividades de recuperación de secuenciación y recursos. [15]

Ejemplos de recursos que deben ser identificados incluyen instalaciones, personal, equipo, software, archivos de datos, componentes del sistema y los registros vitales. [15]

B Activos de Información por nivel de riesgo y orden de prioridad

TABLA 6

PRIORIDADES DEL BIA DE LOS ACTIVOS DE INFORMACIÓN

No	Prioridad BIA	Activos de información	Nivel de riesgo	Prioridad por importancia
2	1	Portafolio académico	Alto	Muy Alta
3		Auditoria de documentos procesos académicos	Alto	Muy Alta
10		Expediente académico del alumno pregrado y posgrado	Alto	Muy Alta
12		Inscripciones académicas	Alto	Muy Alta
13		Compras	Alto	Muy Alta
14		Inventarios	Alto	Muy Alta
15		Requisiciones de personal	Alto	Muy Alta
16		Acciones de personal	Alto	Muy Alta
17		Expedientes de empleados	Alto	Muy Alta
18		Planilla	Alto	Muy Alta
19		Contabilidad	Alto	Muy Alta
21		Módulo financiero	Alto	Muy Alta
25		Sistema de gestión de la información para el análisis institucional	Alto	Muy Alta
26		Sistema de gestión de la planificación institucional	Alto	Muy Alta
27		Configuraciones de equipos de comunicación	Alto	Muy Alta
28		Configuraciones de servidores	Alto	Muy Alta
29		Base de datos	Alto	Muy Alta
30		Programas fuentes	Alto	Muy Alta
31		Respaldos	Alto	Muy Alta
23	2	Modulo de activo fijo	Regular	Muy Alta
24		Sistema de administración general	Regular	Muy Alta
1	3	Evaluación docente	Alto	Alta
6		Becas	Alto	Alta
7		Bolsa de trabajo	Alto	Alta
11		Planes de estudio	Alto	Alta
22		Modulo de proyectos	Alto	Alta
4	4	Tutoría estudiantil	Regular	Alta
5		Estudio de satisfacción	Regular	Alta
8		Administración de horas sociales	Regular	Alta
9		Administración de estudio socioeconómico	Regular	Alta
20		Módulo de cheques	Regular	Alta
32		Documentación técnica, administrativa formato electrónico	Regular	Alta

C. Identificar los recursos para la restauración

Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cálculo o centro de datos, por su equivalente en inglés: data center.

Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, servidores y redes de comunicaciones.

Aunque cuando se mencionan los CPD por lo general se piensa en lugares de gran infraestructura normalizados, en la realidad se deben considerar aquellos que tengan las condiciones necesarias para para el proceso de restauración, en la Universidad Don Bosco se debe contemplar las siguientes modalidades:

1. La UDB cuenta con dos lugares que pueden alternarse como CPD, el CTIC y el departamento de Tecnología del Centro de Postgrados, estos lugares deben de realizar respaldos y restauraciones en las siguientes modalidades:
    a. En situ, con la infraestructura y medios digitales adecuados.
    b. En la nube, arrendando espacios virtuales con empresas que proporciones soporte en línea (NAS, DAS, etc.)
2. Con una empresa que proporcione el servicio de CPD, lugar al que se pueda trasladar el equipo de restauración de la UDB para realizar el proceso de recuperación y opere hasta nivelar los servicios prioritarios.

D. Identificar los tiempos máximos tolerables de restauración de los activos de información

El tiempo de inactividad máximo tolerable (MTD) *Maximum Tolerable Downtime*

Un análisis de impacto de negocio proporciona como resultado la diferenciación entre las funciones o actividades críticas y no críticas de la organización. Una función es considerada crítica si las implicaciones del daño a los afectados son inaceptables.

El tiempo de inactividad máximo tolerable (MTD) por la Institución (*Maximum Tolerable Downtime*, MTD) o la interrupción máxima tolerable (*Maximum Tolerable Outage*, MTO), es decir, el período máximo de no disponibilidad para las actividades, activos o procesos, antes de que la organización deje de operar.

La DMT representa la cantidad total de tiempo que están dispuestos a aceptar por interrupción de procesos del negocio, la interrupción e incluye todas las consideraciones de impacto.

La determinación de MTD es importante porque podría dejar planificaciones de continuidad con la dirección imprecisas al no seleccionar un método de recuperación adecuado, otro punto importante es la profundidad de detalle que se requiere en el desarrollo de los procedimientos de recuperación, incluyendo su alcance y contenido. [15]

Tiempos de recuperación por activo de información (RTO) Recovery Time Objetive

Objetivo de Tiempo de Recuperación (RTO). Define la cantidad máxima de tiempo que un recurso del sistema puede permanecer no disponible antes de que haya un impacto inaceptable en otros recursos del sistema, procesos de la UDB.

La determinación del sistema de información de recursos RTO es importante para la selección de tecnologías apropiadas que son los más adecuados para el cumplimiento de la DMT. [15]

El RTO es un tiempo objetivo para la reanudación de los servicios después de un desastre. Un negocio que ha establecido reanudar sus operaciones totalmente en una semana antes de ser plenamente operativo de nuevo no tiene por qué invertir demasiado dinero en la preparación de la recuperación de desastres a diferencia de otra empresa que necesita estar operando a las dos horas.

Si una empresa ha definido que tiene un tiempo muy corto de RTO, entonces debe invertir fuertemente en

sistemas de recuperación de desastres, inclusive considerar tener un site de contingencia. Este site de contingencia podría mantener una copia de seguridad completa del sistema con estaciones de trabajo, que permitan mantener la operación del negocio a niveles aceptables mientras se ejecuta el plan de continuidad del negocio.

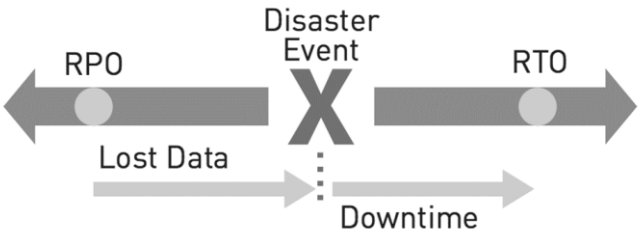

Figura 7, Máximo tiempo de recuperación del negocio

Punto de Recuperación Objetivo (RPO) Recovery Point Objetive

Punto Objetivo de Recuperación (RPO). Representa el punto en el tiempo, antes de un corte de interrupción de sistema, El punto de partida en que los proceso de negocio deben ser recuperados (por lo general es la más reciente copia de seguridad de los datos) después de un incidente. [15]

El RPO está relacionado tanto con la copia de seguridad de los datos, como de la réplica de los mismos. Considerando una empresa que mantiene un servicio X para sus clientes. Si ocurre un desastre este servicio o sus datos pueden degradarse o desaparecer.

Como parte del plan de continuidad, la empresa debe de saber cuánto tiempo puede permitir la no disponibilidad de este servicio y la cantidad de información que se puede asumir como perdida, antes de que falle el negocio, se pierda la reputación o los clientes se vayan a la competencia.

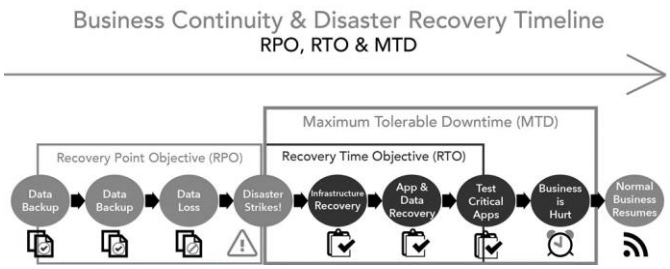

Figura 8, Punto objetico de recuperación del negocio ante fallas.

En función de este valor, definiremos las réplicas o las copias de seguridad.

En resumen, el RPO es el tiempo máximo establecido desde la última copia de seguridad o la cantidad de datos (en tiempo) que nos podemos permitir perder en el caso de desastre.

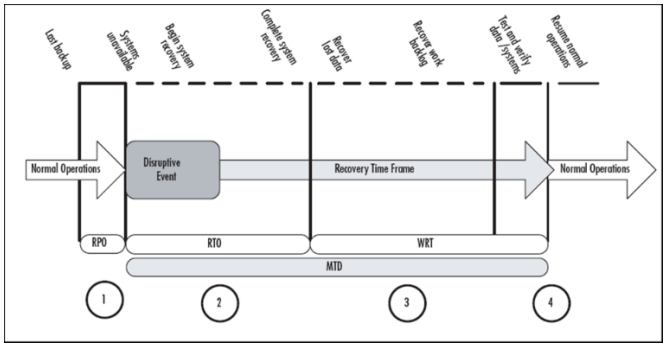

Figura 9, Tiempo de inactividad máxima aceptable

Para el Plan de Continuidad del negocio de la UDB, debido a la diversidad de activos de información y los tipos de respaldos, se propone rangos de tiempo de horas en base al siguiente cuadro.

Prioridad BIA UDB	RPO Horas Máximas	RTO Horas Máximas	MTD Horas Máximas
1	24	36	48
2	24	36	48
3	36	48	72
4	36	48	72

Tabla 10, Tabla RPO, RTO y MTD para UDB

VIII. Plan de Recuperación de Desastres (DRP) Disaster Recovery Plan

El Plan de recuperación del desastre (DRP) proporciona una respuesta a las interrupciones o incidentes que puedan afectar las instalaciones físicas, infraestructura tecnológica, datos y aplicaciones.

El DRP detalla cómo se llevará a cabo la recuperación de procesos críticos en el área según la criticidad definido para la UDB.

El desarrollo, mantenimiento, prueba y continuo mantenimiento de este plan son responsabilidad de Universidad Don Bosco, el coordinador del BCP y los líderes de cada grupo. [16]

El proceso de preparación de Plan de recuperación de desastres incluye varios pasos importantes que se detallan a continuación:

Identificar y mapear los servicios de IT hacia las funciones de recuperación del DRP.

- Determinar la estrategia de recuperación

Documentar el equipo de recuperación, su organización y responsabilidades

A. 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 la CTIC-UDB oficina central.

El alcance de este DRP está limitado a la recuperación de los servicios identificados por el CTIC como procesos de tecnología que apoyan procesos críticos de la UDB definidos en el Análisis de impacto del negocio (Business Impact Analysis.) [16]

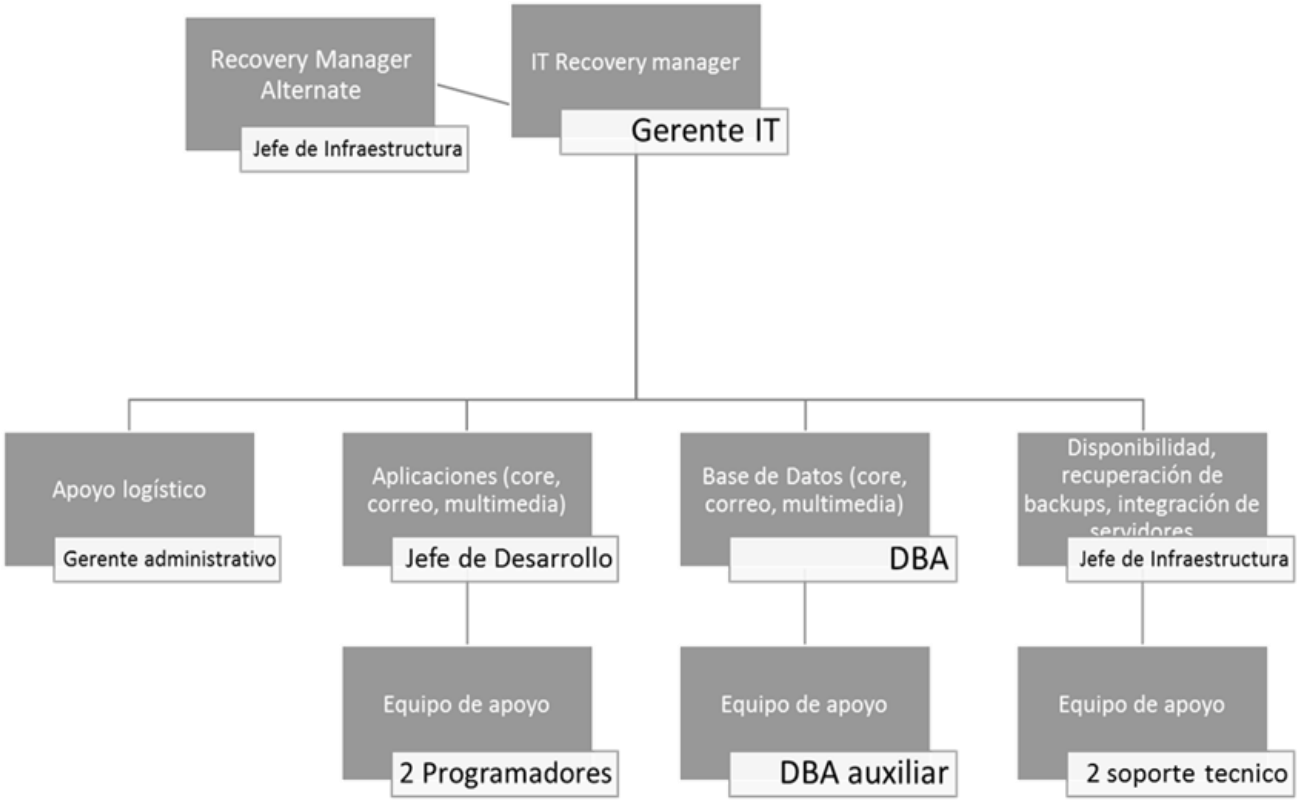

Figura 11, Organización del DRP

- Desarrollar y documentar los procedimientos de recuperación
- Desarrollar y documentar los procedimientos de prueba de recuperación

El responsable del CTIC-UDB define el coordinador del DRP [16]

B. Organización y Responsabilidades

Para que el proceso de recuperación arranque apropiadamente, la organización del DRP, incluyendo roles y responsabilidades debe ser formalizada. [16] En base a consulta con el Director del CTIC indico no colocar nombres a los equipos y referenciar únicamente roles.

Líder DRP

Director CTIC (UDB), apoyo alterno (Director de Administración y Finanzas) [17]

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 [16]

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. [16]

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. [16]

Coordinador de Recuperación

El IT Recovery Manager verifica la magnitud del desastre y se apoya inicialmente con el recovery manager alternative y se dividen el contactar a los coordinadores de los equipos de recuperación para ahorrar tiempo. [16]

- Aplicaciones - jefe de Sistemas
- Base de datos – Administrador de base de datos
- Disponibilidad, configuraciones, respaldos – jefe de infraestructura
- Apoyo logístico. Director administrativo[16]

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[16]

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 [16]

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. [15]

Unidad de Recuperación

Se cuenta con tres equipos que accionan según el tipo de recuperación, se identifica como importante adicionar un cuarto equipo de logística que este bajo el liderazgo del Director administrativo financiero.

- Equipo de aplicación
- Equipo de base de datos
- Equipo de infraestructura
- Equipo de Logística

Estos puede trabajar de forma independiente o integrados con el resto de equipos según sea el caso, cada equipo es responsable de la verificación de buen funcionamiento después del proceso de recuperación.

Los miembros del equipo son responsables de trabajo definido en los procedimientos de recuperación.

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.

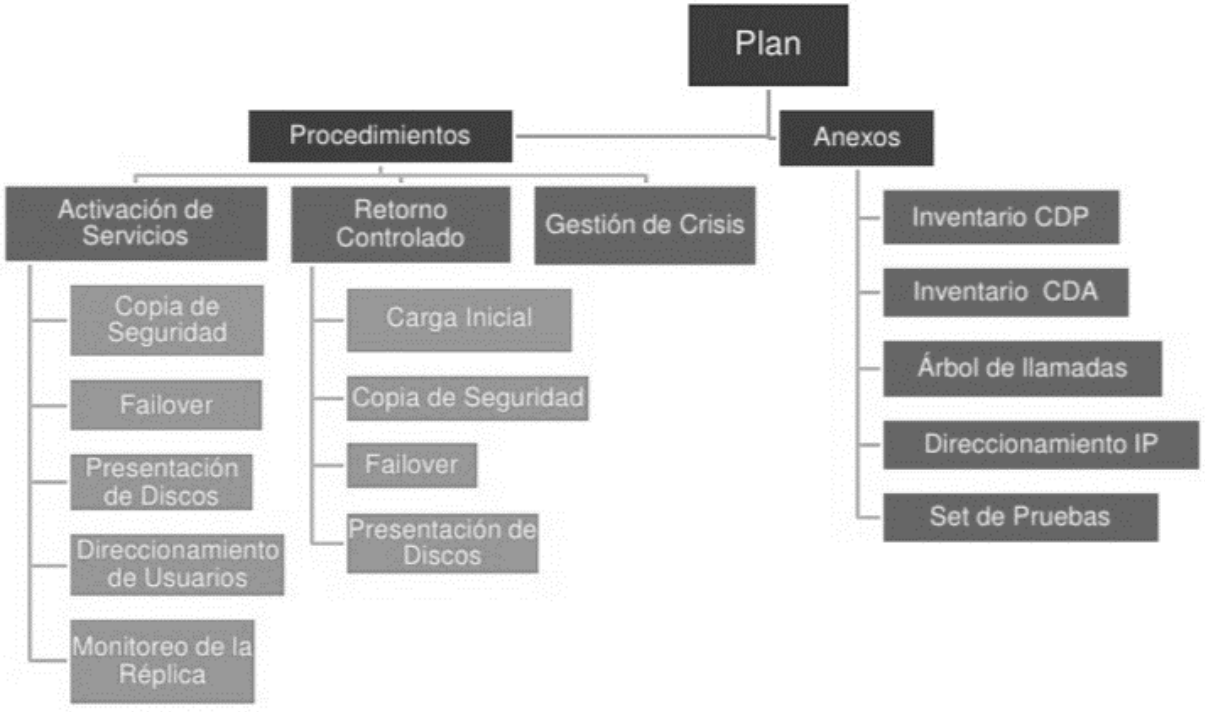

Figura 12, Estructura del DRP

- Participar en el desarrollo de las lecciones aprendidas

C. Estructura del plan DRP

La declaración oficial de un evento de interrupción es hecha por el líder de la unidad de negocio de TI que llama a una reunión con los coordinadores de recuperación para evaluar la magnitud y el impacto de la interrupción.

Los coordinadores de recuperación colaboran para desarrollar una estrategia de recuperación y el plan en base a las circunstancias particulares del caso.

El plan de recuperación incluye los equipos de recuperación que necesitan ser activados para comenzar la etapa de recuperación.

Secuencia de llamada

El Coordinador de recuperación debe usar la información de contacto ubicada en el Informe "El personal y los Puntos de Información" (véase el apéndice A1) para ponerse en contacto con los miembros de sus equipos e informar de la situación.

Se toma como parte de esta actividad que los miembros del DRP deben reportar si cambian

Número de contacto para actualizar sus datos en el DRP. Esta es la secuencia de llamadas:

Además, los coordinadores de recuperación deben:

1. Mantenga un registro de personal a través de "Control de Localización Personal".

2. Llevar a cabo una reunión informativa para explicar la situación actual a los miembros del equipo, teniendo en cuenta:
   - Los resultados iniciales de evaluación de daños.
   - La duración prevista de la interrupción.
   - Objetivos y estrategias para ser usados.
   - Cualquier consideración especial de seguridad.
   - Procedimientos de contacto de todo el personal de apoyo y la recuperación.
   - Ubicación para realizar un trabajo de recuperación designado.
   - Los canales de comunicación establecidos entre la estación de trabajo y la otra ubicación equipos (si un centro de procesamiento alternativo se activa).
   - Recordar al personal de no hacer declaraciones "públicas" o "fuera de registro" a cualquier representante de los medios de comunicación, público u otras entidades.

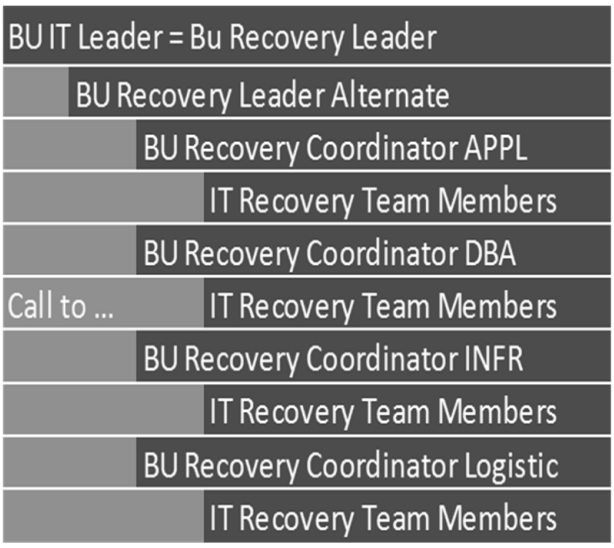

Figura 13, Plan de activación, secuencia de llamada del DRP

3. Establecer un mecanismo para manejar las llamadas entrantes externas, para lo cual deberá:
   - Utilizar los datos proporcionados en la declaración oficial (si está autorizado para proporcionar información).

- Desarrollar un registro para documentar todas las llamadas entrantes.
- Informar de que se le devolverá la llamada cuando la información requerida está disponible.
- Consulte las preguntas críticas al Líder de recuperación para la resolución
-

4. Mantener la comunicación con el líder de la recuperación:
   - El líder de Recuperación envía una lista de las personas en contacto y no contacto
   - Realizar ninguna declaración adicional solicitada por la EMT o Líder de recuperación.

Fase de respuesta

El plan de recuperación incluye los equipos de recuperación que necesitan ser activados para comenzar la etapa de recuperación.

- Comunicar el plan de recuperación para Líderes de gestión de crisis y la unidad de negocio.
- Identificar el lugar (s) de trabajo para el personal de recuperación.
- Organizar un horario de trabajo y la rotación basado en la carga de trabajo, recursos y personal disponibles.

Etapa de recuperación

En esta etapa, los Coordinadores activan a los equipos de recuperación para implementar el plan preparado en la etapa anterior.

- Activar y poner en práctica el plan de recuperación.
- Activar los Equipos de Recuperación.
- Activar el sitio de recuperación.
- Coordinar con los proveedores externos para restablecer los servicios.
- Identificar los datos de copia de seguridad para ser recuperados del almacenamiento.
- Identificar los cambios de conexión para los usuarios del sitio de recuperación.
- Ejecutar a través del proceso de recuperación hasta que la recuperación efectiva de todos los sistemas críticos.
- Comunicar las actualizaciones de estado y los problemas.
- Realizar un seguimiento de lo que salió bien y áreas de mejora.

Etapa de reanudación

Una vez que la recuperación de todos los sistemas críticos de negocio se ha completado, el Coordinador de recuperación se centrará en un plan de reanudación para las operaciones en el sitio principal.

Cuando el sitio principal esté disponible, los equipos de recuperación se activan para reanudar funciones.

- Activar el sitio principal.
- Coordinar con los proveedores externos para restablecer los servicios al sitio principal.
- Identificar los datos de copia de seguridad para ser recuperados de almacenamiento.
- Activar y poner en práctica el Plan de Reanudación.
- Comunicar los cambios de conectar los usuarios al sitio principal.
- Ejecutar a través del proceso de reanudación hasta la reanudación efectiva de todos los Sistemas.
- Comunicar las actualizaciones de estado y los problemas.

- Eliminar todos los datos del sitio alternativo.
- Desactivar sitio alternativo.
- Realizar un seguimiento de lo que salió bien y áreas de mejora.

Comunicación

Los canales de comunicación tienen que ser bien administrado durante un desastre. El líder de TI es responsable de informar las actualizaciones de estado para los líderes de gestión de crisis y de negocios.

El Coordinador de recuperación es responsable de comunicar y coordinar con otros coordinadores de recuperación, los proveedores de servicios de terceros y mantener el flujo de información entre los equipos de recuperación.

Toda la comunicación con los usuarios finales será coordinada y llevada a cabo por los equipos de Mesa de Negocios unidades de servicio.

IX. Mantenimiento y Mejora Continua

Debido al constante cambio de los procesos, al avance tecnológico y al nacimiento de nuevas amenazas principalmente relacionados con estos aspectos, es importante que el plan de continuidad del negocio permanezca siempre actualizado acorde a las necesidades de la universidad.

Es necesario que se efectúen revisiones periódicas que determinen la validez en la aplicación de los planes de continuidad, promoviendo permanentemente actualizaciones que garanticen que se encuentran totalmente vigentes y ejecutables en base a la realidad y acorde a las amenazas tanto internas como externas posibles de presentarse. [16]

A. Personal Involucrado

Como es comprensible la revisión debe efectuarse en función de los posibles cambios principalmente en los siguientes elementos participantes: [16]

- Personal
- Direcciones, números telefónicos del personal
- Plan estratégico de la UDB
- Ubicación, instalaciones y recursos

B. Pruebas de activación

Todo plan de continuidad del negocio necesita de la respectiva calibración, representando esta los ajustes necesarios para que pueda ser ejecutado de manera adecuada. [16]

Las pruebas se relacionan a ejercicios que el personal cumple con el objetivo de conocer los procedimientos, sus responsabilidades y la manera de interacción con otras personas o recursos.

La activación del plan se da cuando las pruebas han alcanzado un desarrollo oportuno y disponen de un nivel apto para poder ser implementado, contando con las suficientes garantías para alcanzar los beneficios citados. [16]

C. Revisión y actualizaciones

Todo plan de continuidad del negocio deberá ser permanentemente monitoreado a fin de que sus acciones estén acorde a la realidad y necesidad del BEV en total conformidad a las posibles amenazas y riesgos que se puedan presentar. [16]

La actualización se basa en hacer que las acciones y actividades sean modificadas si el caso lo requiere, con el objetivo que su ejecución permita brindar todas las garantías necesarias.

Es importante señalar que la revisión y actualización del plan de continuidad del negocio

es un proceso continuo para lo cual se deberán establecer equipos pertinentes que ejecuten esta responsabilidad. [16]

D. Cambios en el BCP

Si es necesario, deberán establecerse cambios en los diferentes procesos existentes dentro del BCP, conforme a una política de mejoramiento continuo y en busca de mejores alternativas para minimizar las amenazas posibles a presentarse y de esta manera evitar interrupciones que generen riesgos y pérdidas a la institución. [16]

Es importante que se establezcan las aprobaciones requeridas para que su ejecución sea eficiente y permita beneficiar al BCP. [16]

E. Concientización y capacitación

Para desarrollarse adecuadamente deberá establecer cronogramas de capacitación, basados en temas puntuales con la participación de todo el personal debidamente clasificado en función de sus Responsabilidades.

Los programas de capacitación deberán ser respaldados con material impreso estratégicamente ubicado y distribuido a fin de que siempre esté al alcance de los involucrados.

- Que comunicar
- Cuando comunicar
- Con quien comunicarse

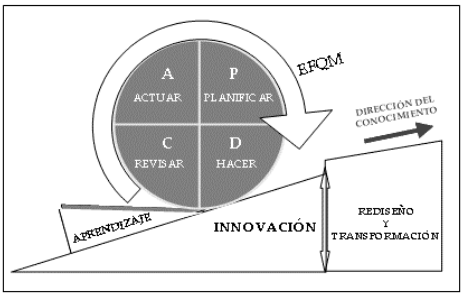

Figura 14, Ciclo de Mejora Continua

X. CONCLUSIONES

• El concepto de activos de información no debe limitarse únicamente a los datos e información de los sistemas, deben incluirse además los programas fuentes de los sistemas, las configuraciones de los servidores y equipos de comunicación, routers y switcs), base de datos (estructura y datos), y archivos en formato electrónico.

• El análisis realizado identifica un nivel de seguridad muy aceptable, entre la escala alto y muy alto, pero y el 40% de sus activos de información en un nivel de importancia muy alta, lo que significa es importante que verifique los procesos de recuperación con el objetivo de constatar que se están realizando correctamente y que el tiempo RPO no sea mayor al RTO

• El análisis de gestión de riesgo identifica los respaldos en niveles de poco y bajo riesgo ante fallas, no obstante la mayoría de los activos de información se encuentran con una probabilidad baja de impacto de alto o muy alto ante una falla disruptiva. Lo anterior indica que más del 70% de los activos de información son de alto impacto, por lo que se debe verificar los procesos de respaldo y recuperación.

• El BIA identificó como mejor opción de respaldo el CTIC de la UDB, y como CPD alternativo el Centros de Postgrado ubicado en Antiguo Cuscatlán, pero se recomienda utilizar otros métodos alternativos como la nube.

• El DRP es un instrumento operacional muy importante que contribuye a identificar las operaciones y servicios considerados críticos dentro de la entidad, que contribuyen a restablecer en el menor tiempo posible los servicios y operaciones con el apoyo de un plan de continuidad del negocio, es importante que la gerencia del CTIC realice la creación del comité DRP lo que permitirá en base al plan de activación y continuidad, dar inicio a las

operaciones más importantes en el menor tiempo posible y de una forma sistemática y ordenada.

• La falta de una programación de verificación de procesos críticos y la validación de respaldos y recuperación ha generado vulnerabilidades y amenazas en los procesos actuales, por esa razón en el BCP, se incluye un plan de mejora continua que será responsabilidad del CTIC, y se sugiere como minio dos revisiones semestrales al año.

• Por último y no menos importante, incluir un plan de capacitación y sensibilización a las áreas, comisiones y personal involucrado, haciendo énfasis en la importancia del BCP y cómo reaccionar ante los desastres e incidente de falta de servicios de información, este plan de capacitación permitirá accionar con mayor rapidez y seguridad ante casos fortuitos.

XI. REFERENCIAS

Recursos en línea:

[1] U.D.B. El Salvador, «www.udb.edu.sv,» [En línea]. Disponible, última fecha de comprobación de disponibilidad 6/febrero/2017 http://www.udb.edu.sv/udb/index.php/pagina/ver/quienessomos_institucional

[12] U.D.B. El Salvador, «www.udb.edu.sv,» [En línea]. Disponible: última fecha de comprobación de disponibilidad 6/febrero/2017

http://www.udb.edu.sv/udb/index.php/pagina/ver/ideario_mision_vision

[14] Biblioteca digital, Gráficos estadísticos, Frecuencias absolutas y relativas, última fecha de comprobación de disponibilidad octubre/2016

http://148.206.107.15/biblioteca_digital/capitulos/210-3487dvu.pdf

Normas:

[2] Banco Central de Reserva, Normas Técnicas para la Gestión de la Continuidad del negocio, publicación del 30 de junio de 2015

[3] Provititi, Guide to Business Continuity Mangement, Third edition, 2014

[4] International Organization for Standarization, ISO/IEC 22301 – Estándar Internacional de la Continuidad del negocio, 2012

[5] International Organization for Standarization, ISO/IEC 27001 - Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos, 2013

[6] International Organization for Standarization, ISO/IEC 27005 – Information technology – Security techniques – Information Security risk management, 2008

[7] International Organization for Standarization, ISO/IEC 31000 - Risk management — Principles and guides, 2009

[8] International Organization for Standarization, ISO/IEC 31010 - Risk management — Risk assessment, 2009

[9] International Organization for Standarization, ISO/IEC 22317 – Business Impact Analisys, Draft technical specification or tecchnical report, 2015

Reportes técnicos:

[10] University of Arizona, EEUU Tucson Arizona, Guidelines for Generating a Disaster Recovery Plan, 2002

[11] Continuidad del Negocio y Recuperación de Desastres. ISACA, 2011

[15] NIST, Computer Security Publications, SP-800-34, Rev 1, Template BIA, 2010

[16] University of Arizona, EEUU Tucson Arizona, Guidelines for Generating a Disaster Recovery Plan, 2012

[17] San Jose University, Business Continuity Plan, Master Plan, 2012

Publicaciones Periódicas:

[13] U.D.B. El Salvador, Planeación Estratégica UDB 2007-2016, síntesis, 2013

XII. Acerca del Autor

Licenciatura en Ciencias de la computación, Universidad Francisco Marroquin, Guatemala.
Master en Seguridad y Gestión de Riesgos Informáticos del Centro de Postgrados de la Universidad Don Bosco de El Salvador.
Bussines process Management, (BPM), Aharón Ofri, Israel/Jerusalén
Certification Microsoft Office Specialist Expert, Microsoft, El Salvador
25 años de experiencia como Project manager (PM) y Director de proyectos a nivel centroamericano, ocho años de experiencia aplicando metodología Project Management Professional (PMP), 10 años de experiencia como Director IT y consultor.
Docente, PM de proyectos de Investigación, facilitador de Seminarios Especialización en la Universidad Don Bosco y facilitador de diplomados de gestión empresarial en el Centro de Postgrados de la UDB.