Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

AUDIE RENÉ JUÁREZ NAJARRO
Asesorado por el Ing. Pedro Pablo Hernández

Guatemala, agosto de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACU**L**TAD DE INGENIERÍA
POR

AUDIE RENÉ JUÁREZ NAJARRO
ASESORADO POR EL ING. PEDRO PABLO HERNÁNDEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIA	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. César Augusto Fernández Cáceres
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PLAN DE CONTINUIDAD TI
EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha julio de 2010.

Audie René Juárez Najarro

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
ESCUELA DE CIENCIAS Y SISTEMAS

Ref: ASESOR 02-02

Guatemala, 29 de Enero de 2.011

Señores
Comisión de Revisión de Tesis
Carrera de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala
Guatemala, Ciudad

Respetables Señores:

El motivo de la presente es informarles que como asesor del estudiante **AUDIE RENE JUAREZ NAJARRO** con carne **2004-12978**, he procedido a revisar el trabajo de tesis titulado **PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA** y que de acuerdo a mi criterio el mismo se encuentra concluido y cumple con los objetivos definidos al inicio

He tenido reuniones periódicas con el estudiante y luego de haber revisado cuidadosamente el trabajo, considero que cumple con los requisitos de calidad y profesionalismo que deben caracterizar a un futuro profesional de la Informática.

Aprovecho para informarle que he leído detenidamente el documento Ref: ASESOR 01-02 y aplicando las recomendaciones que se dan en el mismo procedo a firmar de revisado el trabajo de tesis.

Sin otro particular me suscribo de ustedes,

Atentamente,

Ing. Pedro Pablo Hernández
Colegiado # 7240

Pedro Pablo Hernández Ramírez
Ingeniero en Ciencias y Sistemas
Colegiado 7240

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 9 de Febrero de 2011

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante AUDIE RENE JUAREZ NAJARRO carné **2004-12978,** titulado: **"PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL.: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"****, presentado por el estudiante AUDIE RENÉ JUÁREZ NAJARRO, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pèrez Turk
Director, Escuela de Ingeniería Ciencias y Sistemas

Guatemala, 12 de agosto 2011

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.285 2011

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por el estudiante universitario **Audie René Juárez Najarro,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, agosto de 2011

/cc

ACTO QUE DEDICO A:

Mis padres Audie y Miriam por todo esfuerzo, ejemplo y apoyo que sin condición me han brindado siempre. Con mucho amor dedico este trabajo en respuesta a su esfuerzo.

AGRADECIMIENTOS A:

Dios	Por prestarme la vida y los medios necesarios para llegar a este momento, ya que sin su voluntad todo esfuerzo humano fuera completamente vano.
Mis padres	Lic. Audie Juárez y Licda. Miriam Najarro por haberme dado la oportunidad de vida y de estudio, además de haberme enseñado valores morales a través de su ejemplo.
Mis abuelos	Julio Juárez, Alicia Sánchez, Ancelmo Najarro y Virgilia López por compartir su sabiduría y experiencia a través de sus consejos.
Mis hermanos	Steaven, Kevyn y Randy por compartir momentos indescriptibles.
Mis tíos	Por estar pendientes de mí y orientar mis pasos a través de sus consejos.
Mis primos	Por acompañarme en cada etapa de la vida.
Mi novia	Alejandra por los momentos que hemos compartido, por animarme y mostrarse comprensiva en el tiempo que llevamos de estar juntos.

Mis amigos	Por mostrarse sinceros con mi persona y familia.
La comunidad	Por compartir la formación profesional y con el deseo que coronen su esfuerzo.
Mi asesor	Ing. Pedro Pablo Hernández Ramírez por apoyarme en la elaboración de este documento y compartir sus conocimientos.
Mis compañeros de trabajo	Por compartir sus palabras de ánimo.
Biblioteca Central	Por brindarme las condiciones necesarias para desarrollar mis proyectos.
La Universidad de San Carlos de Guatemala y Facultad de Ingeniería	Por darme la oportunidad de formarme académica y laboralmente.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

.

Análisis de impacto (BIA - *Business Impact Assessment*): el propósito del BIA es crear un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular.

Análisis de riesgos (RA - *Risk Assessment*): metodología orientada a determinar la vulnerabilidad de la empresa. Con base en los diversos riesgos encontrados, se les asigna un valor específico, según la probabilidad de ocurrencia y de la cobertura del seguro contratado, con el fin de proponer alternativas para reducir el riesgo.

Backup Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información y exportarla a una unidad externa, los *backup* se realizan bajo demanda del interesado.

Baja de tiempo máximo (MTD - *Maximun Tolerable Downtime***):** es el periodo de tiempo máximo que una organización puede soportar para estar sin servicio y sin que esta deje de cumplir con sus objetivos.

Base de datos	Es un sistema de almacenamiento colectivo de las bibliotecas de datos que son requeridas y organizadas para cubrir sus requisitos de procesos y recuperación de información.
BCP	De sus siglas en ingles: *Business Continuity Plan.*
Cliente / Servidor	Sistema de organización de interconexión de computadoras (sistema de redes), se basa en la separación de las computadoras miembros en dos categorías, las que actúan como servidores (brindan información) y los clientes (receptores y usuarios de la información).
Cliente	Computadora o programa que se conecta a servidores para obtener información. Un cliente solo obtiene datos, no puede ofrecerlos a otros clientes sin depositarlos en un servidor. La mayoría de las computadoras que las personas utilizan para conectarse y navegar por internet son clientes.
Cracker	Persona que se especializa en violar medidas de seguridad de una computadora o red de computadoras, violando claves de acceso y defensas para obtener información que cree valiosa, el *cracker* es considerado un personaje sin honor a diferencia del *hacker*.

Dato	El término que usamos para describir las señales con las cuales trabaja la computadora es dato. Aunque los términos dato e información muchas veces son usados indistintamente, existe una diferencia importante entre ambas la cual radica en que los datos son individuales y sin ningún significado mientras que la información son los datos relacionados y que tienen un significado dentro de un contexto específico.
Default	Opción que un programa asume si no se especifica lo contrario. También llamado valores predeterminados.
Desastre	Cualquier evento mayor que afecte el funcionamiento normal de las operaciones de un negocio, puede ser de tipo natural, humano o técnico.
Diagrama de flujo	Es la representación gráfica de una secuencia de instrucciones de un programa que ejecuta un computador para obtener un resultado determinado.

Dirección Ip	Dirección numérica asignada a un dispositivo de *hardware* conectado a internet bajo el protocolo IP. La dirección se compone de cuatro números y cada uno de ellos puede ser de 0 a 255, las direcciones IP se agrupan en clases según el rango.
Editor	Es un *software* empleado para crear y manipular archivos de texto, tales como: programas en lenguaje fuente, listas de direcciones o instrucciones.
Encriptación	Método para convertir los caracteres de un texto de modo que no sea posible entenderlo si no es leído con la clave correspondiente asociada. Es utilizado para proteger la integridad de la información confidencial en caso de que sea interceptada.
Entorno gráfico	Sistema en el que la información que aparece en pantalla es representada en forma gráfica (imágenes).
Escalabilidad	Capacidad de crecimiento de la computadora.
Escáner	Dispositivo periférico que digitaliza información impresa mediante un sistema óptico de lectura.

Firewall	Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas.
Formateo	Proceso por el que se adapta la superficie magnética de un disco para aceptar la información bajo un sistema operativo determinado. En el proceso de formateado se colocan las marcas lógicas que permitirán localizar la información en el disco y las marcas de sincronización, además, de comprobar la superficie del disco.
Hacker	Experto técnico en algún tema relacionado con comunicaciones o seguridad, es también un gurú. Los *hackers* suelen dedicarse a violar claves de acceso por diversión o para demostrar fallas en los sistemas de protección de una red de computadoras.
Hardware	Componente físico de la computadora. El *hardware* por sí mismo no hace que una máquina funcione, pero si es posible que funcione con el *software* adecuado.

Información	Es el resultado de relacionar los datos y darles sentido, es el resultado final del procesamiento de datos.
Internet	Es la red de computadoras más extendida que conecta y comunica todo el mundo.
Intranet	Utilización de la tecnología de internet dentro de la red local (LAN) de una organización.
Ip	Protocolo de internet. Este provee un método para fragmentar y rutear la información. Es inseguro ya que no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.
ISO	*International standard organization*. En español es la organización de estándares internacional.
LAN	*Local área network* o red de área local. Red de computadoras interconectadas, distribuida en la superficie de una sola oficina o edificio no más de 100m. También son llamadas redes privadas de datos y su principal característica es la velocidad de conexión.

Linux	Versión *freeware* del conocido sistema operativo Unix, es un sistema multitarea multiusuario para computadoras personales de distribución gratuita.
Log	Archivo que registra movimientos y actividades de un determinado programa. Utilizado como mecanismo de control y estadística.
Lógica del *hardware*	Son los circuitos y chips que realizan las operaciones de control de la computadora.
Lógica del *software*	Lógica del programa es la secuencia de instrucciones en un programa.
Lógica	Es una secuencia de operaciones realizadas por el *hardware* o por el *software*.
Login	Proceso de seguridad que exige que un usuario se identifique con un nombre (*User-ID*) y una clave, para poder acceder a una computadora o a un recurso.
Mainframe	Nombre con el cual se designan a las grandes computadoras que funcionan en sistemas centralizados.

Menú Lista de comandos que aparece en la parte superior de las ventanas representadas por un nombre con una letra subrayada y que sirve para dar instrucciones a los programas o para comunicarnos con ellos por medio de estos.

Norma Conjunto de reglas sobre algún producto o servicio que garantiza uniformidad en todo el mundo, en cualquier sistema en el que se implemente. Existen dos tipos de normas: las estándar (o normada) que es generada por comités especiales y la de facto (o impuesta) que se acepta cuando un producto debido a su uso se convierte en universal. Los tres organismos más activos en el desarrollo de normas son: la ISO (*International Standards Organization*), la IEE (A*merican Institution of Electrical and Electronic Engineers*) y la CCITT (*International Telegraph and Telephone Consultative Comitee*). Las normas son la base de los sistemas abiertos.

Paquete Elemento que sirve para organizar los distintos elementos de un diagrama.

Password Palabra utilizada para validar el acceso de un usuario a una computadora servidor.

Periféricos	Cualquier dispositivo de *hardware* conectado a una computadora.
Plan de comunicación de crisis	Al momento en que la empresa o institución tiene una crisis, el comité de comunicación debe saber cómo y a quién notificar para que haya comunicación y se sepa qué está sucediendo.
Plan de contingencia	Es un subconjunto de un plan de continuidad de negocio, que contempla cómo reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de *software* o *hardware*, errores humanos, intrusión, entre otros.
Plan de continuidad del negocio	(BCP – *Business Continuity Plan***)**: es un plan documentado y probado con el fin de responder óptimamente ante una emergencia, logrando así, el mínimo impacto a la operación del negocio.

Plan de emergencia de ocupantes (OEP)	El plan de emergencia de ocupantes es un documento que contiene los pasos a seguir en caso de que ocurra una emergencia con alguno de los ocupantes, siendo estos empleados: mantenimiento, administración o personas individuales.
Plan de recuperación de negocios (BRP)	Forma parte del plan de continuidad y su objetivo primordial es establecer los pasos a seguir para volver a la normalidad luego de haber abordado el plan de contingencia.
Plan de recuperación del desastre (DRP)	Es aquella parte del plan de contingencia y del plan de continuidad de negocio, que aborda aquellas contingencias que, por su gravedad, no permiten continuar prestando el servicio desde el centro local y se debe continuar con el servicio a partir de un nuevo centro. Este plan obliga contemplar la vuelta atrás cuando, tras arreglar las consecuencias del desastre, el servicio pueda ser reanudado en el centro local.

Plan de soporte de continuidad	Es una serie de pasos preestablecidos previamente para poder dar continuidad a las operaciones de la empresa o institución, entre estas se encuentran los comités de soporte, los equipos de implementación y toda la logística necesaria para continuar prestando servicio o produciendo.
Programa ejecutable	Los archivos de programa a menudo se denominan programas ejecutables, porque al teclear su nombre o al efectuar *click* sobre ellos el ícono que le corresponde en un entorno gráfico, logra que la computadora cargue y ejecute las instrucciones del archivo.
Programa	Sinónimo de *software*, conjunto de instrucciones que se ejecutan en la memoria de una computadora para lograr algún objetivo. Son creados por equipos de personas en lenguajes especiales de programación.
Programador de sistemas	En el departamento de procesamiento de datos de una organización, es el técnico experto en parte o en la totalidad del *software* de sistemas de computadora, tal como: el sistema operativo, el programa de control de red y el sistema de administración de base de datos.

Protocolo	Conjunto de reglas creadas para controlar el intercambio de datos entre dos entidades comunicadas. Pueden ser normadas o definidos por un organismo capacitado o por facto creadas por una compañía y adoptadas por el resto del mercado.
Red	Son dos o más computadoras conectadas para cumplir una función específica, compartir periféricos, información o comunicarse entre sí. Existen diferentes tipos de redes: según su estructura jerárquica se catalogan en redes cliente/servidor, con computadoras que ofrecen información y computadoras que reciben información. Redes *peer to peer* donde todas las computadoras ofrecen y consultan información simultáneamente. A su vez se pueden clasificar según el área geográfica estas son LAN, MAN o WAN.
Servidor	Computadora que pone sus recursos (datos, impresoras, accesos) al servicio de otras a través de una red.
Sistema operativo	Conjunto de programas que se encarga de coordinar el funcionamiento de una computadora, cumpliendo la función de interface entre los programas de aplicación, circuitos y dispositivos de una computadora.

Software	Componentes intangibles (programas) de las computadoras. Complemento del *hardware*. El *software* más importante de una computadora es el sistema operativo.
TCP/IP	Transmisión control protocol / *internet protocol* o protocolo de control de transmisión / protocolo internet. Usados para organizar computadoras en redes. Norma de comunicación en internet, compuesta por dos partes: el TCP/IP. El IP desarma los envíos en paquetes y los rutea mientras que el TCP se encarga de la seguridad de la conexión, comprueba que los datos lleguen completos y que se integren los paquetes íntegramente.
TCP	Protocolo de control de transmisión. Conjunto de protocolos de comunicación que se encargan de la seguridad y la integridad de los paquetes de datos que viajan por internet. Es un complemento del IP.
TI	Tecnologías de la Información, es el *hardware* y *software* que automatizan la recolección, procesamiento, distribución, almacenamiento y consulta de datos.
Unidad	Dispositivo físico de almacenamiento de los datos.

UPS	Por sus siglas en ingles *Uninterruptible Power Supply,* es un dispositivo de *hardware*, el cual utiliza baterías proporcionar energía eléctrica y regular el voltaje.
Usuario	Persona que interactúa con la computadora a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con la computadora a nivel profesional.
Virus	Pequeños programas de computadora que tienen la capacidad de auto duplicarse y residir en otros programas. Una vez que se difunden, los virus se activan bajo determinadas circunstancias y, en general, provocan algún daño o molestia.

RESUMEN

El plan de continuidad de operaciones es un plan de procedimientos alternativos a la forma tradicional de operar de la empresa o institución y constituye una herramienta que ayuda a que los procesos considerados como críticos en una organización continúen funcionando en una situación de desastre, aun cuando el desastre sea incontrolable en el entorno.

Para crear un plan de este tipo, se debe tener claro los recursos de información relacionados con los procesos críticos que dan funcionamiento a la empresa o institución, además, es imprescindible identificar el periodo de tiempo de recuperación crítico para cada uno de los recursos en el cual se debe establecer el procesamiento de las actividades que dan función a la organización antes de que se experimenten pérdidas significativas o aceptables.

Los beneficios de contar con este plan son múltiples, entre los que se pueden destacar:

- Proteger la marca y la lealtad de los clientes proactivamente evitando o atenuando los desastres

- Tener identificados los diversos eventos que podrían impactar sobre la continuidad de las operaciones

- Disminuir o prevenir las pérdidas en cuanto a tiempo, recursos y credibilidad para el negocio, en caso de desastre

- Tener una recuperación oportuna y eficaz de interrupciones del negocio

- Clasificar y categorizar los activos

El plan de continuidad puede ser implementado tanto para compañías u instituciones grandes como para las pequeñas. El tamaño no es impedimento para llevar a cabo el plan, naturalmente en una pequeña organización será más fácil el desarrollo del plan debido a que tiene pocos procesos mientras que en las grandes empresas será más complejo.

La creación del plan de continuidad está compuesta por cuatro etapas o fases definidas claramente, en cada una de ellas se encuentran identificados los entregables.

Fase 1: es el análisis obligatorio a la empresa u organización para conocer sus funciones, servicios, productos y manera en que opera. Es fundamental tener comunicación con los empleados para comprender sus puntos de vista acerca de los procesos que llevan a cabo.

Fase 2: es la selección de estrategias, esta está basada en dos aspectos fundamentales: la valoración de las diferentes alternativas y estrategias de respaldo y la corrección de vulnerabilidades detectadas, de esta manera se logra mitigar la probabilidad de ocurrencia.

Fase 3: en esta se desarrolla el plan, el cual involucra el progreso de los procedimientos y planes de actuación para las diferentes áreas y equipos creados, además, se organizan los equipos que intervendrán en cada una de las fases del plan. En esta etapa se debe tener una buena comunicación con los colaboradores debido a que la creación de equipos involucra a los mismos.

Fase 4: esta involucra la creación de un plan de pruebas que ayude a garantizar que el plan va a funcionar en caso de siniestros, también para identificar posibles problemas que se pueden suscitar, adicionalmente, se tiene el plan de mantenimiento, el cual debe garantizar que todos los procedimientos estén actualizados, para obtener máximos resultados.

Durante las fases de desarrollo la gerencia y administración pueden incurrir en los siguientes errores:

- Pensar que se trata de un plan puramente técnico
- Establecer un final para la elaboración del plan y no considerar las actualizaciones
- Considerar desastres totales y no tomar en cuenta los desastres parciales
- Pensar en políticas correctivas y no en preventivas
- Pensar que la empresa o institución está exenta a desastres

OBJETIVOS

GENERAL

Elaborar una guía para la creación de un plan que garantice la continuidad de las operaciones en la empresa o institución con base en aspectos de tecnología, capital intelectual y factores externos que representen una vulnerabilidad y riesgo, como caso de estudio Biblioteca Central de la Universidad de San Carlos de Guatemala.

ESPECÍFICOS

1. Detallar las etapas y aspectos fundamentales a tomar en cuenta para la elaboración de un plan de continuidad de operaciones dirigido a una empresa o institución.

2. Establecer los riesgos a los cuales están vulnerables las operaciones en Biblioteca Central de la Universidad de San Carlos.

3. Identificar las aplicaciones, los datos críticos y la infraestructura tecnológica que los soporta para diseñar medidas preventivas en Biblioteca Central.

4. Llevar a cabo la etapa de análisis de impacto, estableciendo tiempos máximos de interrupción para el caso de Biblioteca Central.

5. Clasificar los procesos y actividades según el grado de importancia para diseñar las medidas preventivas que permitan continuar brindando el servicio.

6. Presentar los antecedentes del plan de continuidad ante las autoridades de la Biblioteca Central para que comprendan los beneficios que aporta la implementación de este y cómo en un mercado competitivo, hace la diferencia aportando valor agregado al servicio.

INTRODUCCIÓN

En un mundo actualizado, competitivamente y agresivo como lo es el mercado de las empresas comerciales, se tiene que ser cada día más profesional prestando más y mejores servicios al cliente, dándole valor agregado al trabajo o producto.

Por ello, el plan de continuidad toma un valor altamente significativo para las organizaciones, porque estar preparados para los tiempos difíciles significa la diferencia entre las empresas estables de las inestables.

En este estudio se presenta la forma estandarizada del departamento TI, apoyado en la alta gerencia y ejecutado por todo colaborador de la empresa o institución para lograr los objetivos propuestos, los cuales son dar continuidad a las operaciones, inclusive en situaciones de alto impacto donde no se tiene control.

“No podemos cambiar la dirección del viento, pero si podemos ajustar nuestras velas para llegar al objetivo”, con base en esta parábola, las empresas e instituciones no son responsables de muchos riesgos y vulnerabilidades que sufren hoy en día, sino son factores externos los que las ponen en riesgo, como por ejemplo: pandemias, desastres naturales, políticas gubernamentales, entre otros.

En estas situaciones es imprescindible estar preparados con procedimientos, políticas y planes que mitiguen el impacto, como consecuencia las operaciones y funciones pueden seguir adelante atendiendo el activo más importante como empresa o institución; los clientes.

Esta tesis describe una forma estandarizada de crear un plan de continuidad, el cual se puede, fácilmente, implementar en cualquier empresa pública o privada, sin importar el tamaño, sea esta pequeña, mediana o grande.

1. MARCO CONCEPTUAL

1.1. Antecedentes

La velocidad con la que se ejecutan las operaciones en las empresas y organizaciones es elevada, por lo cual una discontinuidad en las actividades por unas pocas horas de duración puede tener un impacto catastrófico en los resultados financieros y en la imagen de la organización que lo sufra.

En ese sentido, los servicios que prestan las empresas e instituciones tienen una íntima dependencia con los sistemas de información, lo cual exige que estos estén preparados para afrontar las múltiples amenazas que ponen en riesgo su operatividad y, en consecuencia, la continuidad de los negocios o servicios.

El incendio ocurrido en el Edificio Windsor en Madrid en el mes de febrero de 2005 o el Huracán Katrina en agosto de ese mismo año, son dos ejemplos que vienen a sumarse a sucesos, como los atentados del 11 de septiembre del año 2001 efectuados a Estados Unidos. Sin embargo, no es necesario un desastre de dimensiones parecidas a las de los mencionados anteriormente para poner en peligro no sólo la buena marcha de la organización sino su misma supervivencia; eventos como la irrupción de un virus o la instalación de un parche de seguridad pueden conducir a la inoperatividad temporal de los sistemas, la pérdida de información crítica o, en última instancia, la inutilización de las infraestructuras. [1]

[1] CNN Noticias en Español,www.cnn.com/español, 2008.

Además, existe otro tipo de riesgo que amenaza la continuidad como lo es la epidemia H1N1 que actualmente se está viviendo, esta situación podría prolongar y profundizar la crisis económica que se atraviesa, o bien detener o frenar la operación de algunas empresas.

Sumado a lo anterior y dada la tendencia humana de ver siempre el lado positivo a las cosas, muchos empresarios tienden a no hacer caso a la necesidad de prepararse ante una situación adversa, debido, principalmente, a que un desastre aparenta ser un acontecimiento inverosímil, a pesar de que la experiencia y las estadísticas demuestran lo contrario.

Actualmente, la infraestructura de TI se ha convertido en un pilar importante en la continuidad de los negocios ante la inminente necesidad de mantener la operación, reduciendo al máximo el impacto.

En todos los casos, el tiempo de recuperación es de alta importancia en las primeras 72 horas después de la interrupción, son vitales para saber si el negocio soportará o morirá debido a la contingencia que se presenta. Morir, no será un acto inmediato, sino que puede ser un proceso irreversible y lento porque no se tuvieron las respuestas inmediatas para adaptarse al entorno que se presenta.

1.1.1. Tipos de incidentes

Los incidentes o desastres no son solo los de tipo ambiental como los incendios, huracanes o inundaciones los que pueden causar daños adversos a una organización, sino aquellos que pueden tener impactos negativos para la empresa o institución de acuerdo al *disaster recovery guide*, como los que se describen a continuación:

- Los incidentes de seguridad en los sistemas con alto impacto, entre ellos se puede destacar los delitos cibernéticos, la pérdida de información, el robo de información sensible o su distribución accidental, los fallos en los sistemas TI, los errores de operación en los sistemas por parte de los usuarios o los colaboradores.

- Daños en las infraestructuras o en los servicios que dificulte el funcionamiento, tales como los fallos en: el suministro eléctrico, el suministro de agua, las comunicaciones, ausencia de servicios sanitarios o de limpieza.

- Los fallos en los equipos o en los sistemas incluyen los de las fuentes de alimentación y en los equipos de refrigeración, estos son aquellos desperfectos totales o parciales que tienen como consecuencia la imposibilidad de hacer uso del equipo.

- Las huelgas, robos masivos, guerras, actos de terrorismo o de sabotaje son daños deliberados que se salen del control de la organización, sin embargo, no por eso justifican la ausencia de servicio u operación de la empresa o institución.

Según las estadísticas extraídas del sitio web <http://www.thebci.org> instituto de continuidad BCI por sus siglas en ingles (*business continuity institute*) se tiene que:

- Un 50% de organizaciones tiene la experiencia de algún tipo de eventualidad o desastre.

- Sólo el 23% de las empresas a nivel mundial tiene un plan Integral de continuidad de negocios.

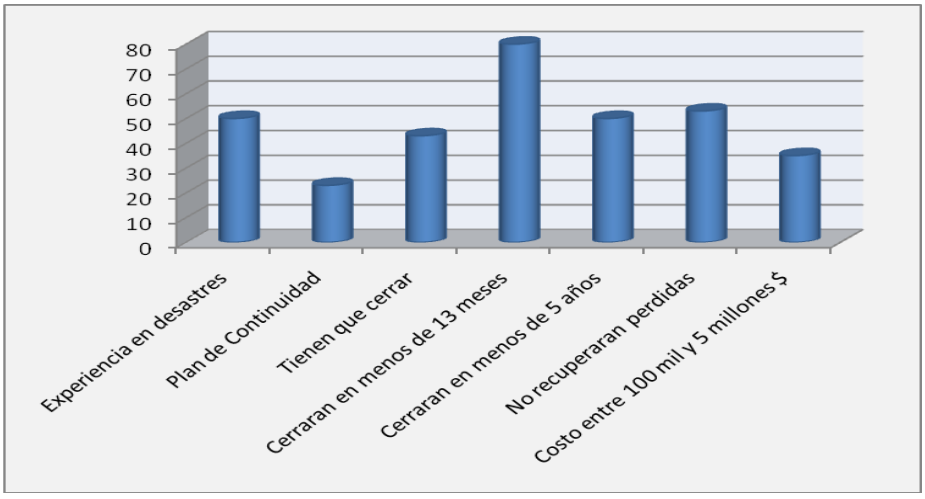
- Un 43% de las organizaciones, después de un accidente, no podrán continuar sus operaciones viéndose obligadas a cerrar.

- Un 80% tendrán que hacerlo en menos de 13 meses.

- Un 50% se verán forzadas a cerrar antes de cinco años después del desastre.

- Un 53% de los clientes de estas organizaciones no recuperarán las pérdidas causadas por los daños derivados.

Figura 1. **Estadística sobre desastres**



Fuente:http://www.ibermatica.com/ibermatica/integracioninfraestructuras/continuidadnegociobrs.

Los desastres impactan de forma diferente a cada organización, dependiendo de su tamaño y de su área de actividad, también importa la cultura y preparación de los directivos y de las medidas que tengan preparadas para esta situación, no siendo el tamaño una característica fundamental; las pequeñas y medianas organizaciones también pueden verse seriamente afectadas si no se encuentran adecuadamente preparadas.

Las consecuencias de estos acontecimientos adversos sobre las organizaciones que no tienen un plan de continuidad pueden llegar a ocasionar incluso, el cierre.

A pesar de que los efectos inmediatos de un desastre aparentemente son la pérdida de beneficios económicos por la pérdida de actividad puntual y la incapacidad para proveer servicios críticos, no son estos los efectos más perniciosos que un incidente de este tipo provoca, sino que el efecto mas perniciosos es el desprestigio de la marca.

Otros efectos derivados que pueden causar un gran impacto en la compañía son la pérdida de reputación de cara a los clientes, o la pérdida de ventaja competitiva con otras compañías.

1.2. ¿Qué es un plan de continuidad de negocios?

El plan de continuidad también conocido en sus siglas en inglés (BCP = *business continuity plan*) es un conjunto de procedimientos alternativos a la forma tradicional de operar de la empresa o institución y constituye una herramienta que ayuda a que los procesos considerados como críticos para la organización continúen funcionando en una situación de desastre, aun cuando este sea incontrolable en el entorno.

Para una organización contar con un plan de esta naturaleza significa que está totalmente preparada de forma correcta para cualquier eventualidad que pudiera surgir, continuando con sus operaciones mínimas e impactando, lo menos posible, la salud financiera de la empresa o institución.

Al tomar en cuenta que el plan de continuidad es encabezado y dirigido por el departamento de TI, significa tener madurez en cuanto a las tecnologías de la información.

Un BCP debe contemplar la continuidad de los procesos y servicios críticos de la empresa o institución y se integra bajo las dimensiones de organización (recursos humanos, materiales y líneas de mando), operaciones (políticas y procedimientos), tecnologías de la información e infraestructura de las instalaciones, todos estos aspectos analizados bajo el marco de referencia de la continuidad.

Las características que un plan de continuidad debe contemplar son:

- Claridad y realismo
- Ser de fácil entendimiento
- Todas las áreas de la organización (integral)
- Concreto y factible
- Ajustado y actualizado

El plan de continuidad es un documento para toda la organización y no debe descansar sólo en el nivel directivo o de alto mando, ya que los operarios son los que deben estar más inmersos en el entendimiento y aplicación del mismo.

Bajo esta premisa, el capital humano tiene un peso importantísimo, ya que es el responsable de su aplicación y operación, por lo que debe existir un adecuado proceso de capacitación.

Las preguntas claves que se deben hacer con respecto al tema de continuidad son:

- ¿Cuáles son los recursos de información relacionados con los procesos críticos que dan funcionamiento a la empresa o institución?

- ¿Cuál es el periodo de tiempo de recuperación crítico para cada uno de los recursos de información en el cual se debe establecer el procesamiento de las actividades que dan función a la organización antes de que se experimenten pérdidas significativas o aceptables?

1.2.1. Beneficios

Los beneficios de implementar un plan de este tipo se describen a continuación de acuerdo a Gaspar Martínez, *El plan de continudad de negocios,* 2006:

- Proteger la marca y la lealtad de los clientes proactivamente evitando o atenuando los desastres.

- Conlleva tener identificados los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.

- Disminuye o previene las pérdidas en cuanto a tiempo, recursos y credibilidad para el negocio en caso de desastre.

- Tener una recuperación oportuna y eficaz de interrupciones del negocio.

- Clasifica y categoriza los activos para priorizar su protección en caso de desastre.

- Mejorar la capacidad de sobrevivir y de prosperar en el actual clima de negocio competitivo.

- Fomenta e implica a los recursos humanos de la compañía en las actividades de continuidad, logrando un clima colaborativo y de cooperación.

- Mejorar la eficacia y productividad del personal automatizando y simplificando procesos de recuperación.

Un plan de continuidad no es excluyente de un plan de contingencia, sino el segundo está dentro del primero. En ese sentido, el plan de continuidad para el negocio debe incluir los siguientes planes:

- De recuperación de desastres, el cual debe especificar la estrategia de un negocio para implementar procedimientos después de una falla.

- De reanudación, este especifica los medios para mantener los servicios críticos en la ubicación de la crisis.

- De recuperación, este especifica los medios para recuperar las funciones del negocio en una ubicación alterna.

- De contingencia, el cual especifica los medios para manejar eventos externos que puedan tener serio impacto en la organización.

- De retorno a la normalidad, es una serie de procedimientos que indican la forma en que se va a restaurar los procedimientos después de pasado el desastre.

- De pruebas, es el que va a verificar el correcto funcionamiento del plan antes de su implementación, para dar confiabilidad de su eficiencia.

- De mantenimiento, este sirve para mantener actualizadas las políticas del plan y para que a través del tiempo, no se deteriore.

Pero ¿cuál es la diferencia entre un plan de continuidad y uno de contingencia? Si estando en un estado de normalidad ocurre un desastre, lo que se debe realizar es reanudar con lo que se tenga para tratar de dar los servicios prioritarios. En paralelo hay un equipo que está tratando de recuperar lo que se dañó y una vez se haya concluido con esta labor, hay un ciclo en donde se restaura y se puede volver a la etapa de normalidad.

El plan de continuidad son todas las acciones que permiten mantener el negocio durante estos eventos y el plan de contingencia son los mecanismos que coadyuvan a la transición entre los diferentes estados de la continuidad; es decir, las estrategias que contribuyen a pasar de un desastre a la reanudación, de la reanudación a la recuperación y de la recuperación a la restauración.

1.2.2. ¿Quién debe tener un plan de continuidad?

Constantemente existen preguntas con respecto a si el tamaño de la organización influye en la implementación de un plan de continuidad, la respuesta es no.

El tamaño de la organización no tiene relación con la necesidad de tener un plan con medidas de continuidad, si la organización es extremadamente grande, con sucursales en varios países, edificios grandes, gran cantidad de empleados, movimientos millonarios de capital y ganancias elevadas, o por el contrario se trata de una micro o pequeña empresa con un par de empleados, en una pequeña oficina, ambas instituciones necesitan asegurar y respaldar la disponibilidad de sus actividades y procesos.

No obstante, debido a los escasos recursos y a las pocas opciones de respuesta ante un desastre que pueda enfrentar las pequeñas y medianas empresas, en algunos casos, sería más conveniente desarrollar un plan de recuperación para las pequeñas organizaciones que para las grandes corporaciones. [2]

1.3. El plan de continuidad en el mundo

Ante una tendencia empresarial e institucional en donde las entidades compiten a nivel mundial tal y como la que enfrentan hoy día. Los planes de continuidad están tomando un papel importante, principalmente, porque están enfocados a proteger la información (datos) y la infraestructura central de tecnologías de información (TI).[3]

[2] Vilchis, Xavier. *Business Continuity Plan ¿Ya lo tiene?,* 2009, p.32.
[3] International Standards for Business, http://www.iso.org/iso/home.htm, 2009.

A nivel mundial, la mayor parte de empresas e instituciones cuentan con un departamento enfocado en la TI, este ya es considerado como parte de su modelo organizacional dado a que uno de los activos más valiosos para las organizaciones, es la información.

La tecnología, principalmente las tecnologías de la información y comunicación TIC, están ayudando a disminuir las distancias físicas que existen y facilitar el acceso a la información sin dejar de considerar temas tan importantes como la seguridad y la disponibilidad de la misma.

Es muy importante destacar que uno de los activos que tienen mayor valor dentro de la organización, es la información. Por lo cual, el acceso a este recurso que resulta ser fundamental para la continuidad de las operaciones y servicios, se mantenga activo y funcional.

En la actualidad las empresas dedicadas a prestar servicios son las que dan prioridad a este plan, debido a que sus ganancias están estrechamente relacionadas con el tiempo de operación, por tal motivo, este sector económico a nivel mundial apunta a que sus trabajadores puedan monitorear y operar el sistema, inclusive, desde una ubicación fuera de la empresa, a esto se le conoce como operaciones remotas.

Desde este punto de vista, las organizaciones consideran al plan de continuidad como un documento importante para mitigar el impacto ante cualquier tipo de contingencia y de esta manera ser más competitivos, destacando que en un mercado globalizado como el que actualmente se esta viviendo, todos compiten utilizando los mejores recursos disponibles y las técnicas más especializadas para mejorar sus servicios, rendimiento y proyectar mejor imagen a sus clientes.

En ese sentido, un enfoque de calidad de servicio como el que certifican las normas ISO en sus diferentes categorías y niveles, es importante para dar valor agregado al servicio, tal es el caso de la norma ISO 27006 dedicada a certificar los aspectos de seguridad de la información, continuidad de operaciones y planes de restauración, esta norma ha sido nombrada por *"Internacional Ortanization for Standarization" como "Guidelines for information and communications technology disaster recovery services"*.

1.4. El plan de continuidad en Guatemala

El plan de continuidad, por su naturaleza, involucra aspectos tecnológicos como aspectos humanos, tal es el caso de la formación de equipos de continuidad, los cuales están encargados de poner en actividad el plan, partiendo de este punto, el elemento humano que van a estar interactuando con las políticas de continuidad y los criterios de funcionamiento, debe poseer un nivel de cultura de calidad de servicio.

Por lo cual, un aspecto fundamental es la cultura de calidad de servicio, sin embargo, el clima organizacional, también, juega un rol importante para disminuir la resistencia a utilizar, de forma efectiva, un plan de esta naturaleza.

En Guatemala, el plan de continuidad no está implementado en la mayoría de empresas ni instituciones, las organizaciones están adoptando las tecnologías de la información (TI) e implementando las mismas para tener control y manejo de la información, sin embargo, los niveles de seguridad no han sido explotados a tal nivel.

En las empresas privadas, de origen extranjero, tienen una visión diferentes a la visión de las nacionales en relación con los procesos de negocio, tal es el caso de los *call center*, en donde la continuidad de operaciones es vital, porque una interrupción impacta negativamente a nivel económico como a nivel del prestigio.

En las pequeñas y medianas empresas de capital guatemalteco, denominadas pyme, no cuentan con un plan de continuidad debido a que los directivos y trabajadores no tienen la visión ni la cultura de calidad de servicio, en ese sentido es importante mencionar que en este tipo de organizaciones el departamento de la TI es muy pequeño o no existe, esto es un impedimento potencial para la creación de este tipo de políticas.

En cuanto al aspecto institucional, es la burocracia que existe en las organizaciones tanto gubernamentales como no gubernamentales lo que hace difícil la implementación de un plan de continuidad. A pesar de este aspecto, ya se está logrando crear una cultura de servicio apoyada en las TI, por ello, es indispensable implementar políticas que garanticen la continuidad.

Por supuesto no se puede generalizar, en virtud que puede haber casos que sean la excepción, sin embargo, el patrón descrito anteriormente es el que predomina según la categoría de organización.

1.5. Importancia e impacto del plan de continuidad

Actualmente las TIC están contribuyendo, significativamente, a expandir los horizontes tanto de personas como de empresas e instituciones, así como, de tener alcance a nivel mundial con recursos relativamente bajos y velocidad elevada.

Por esta razón, el Internet, los negocios electrónicos, el comercio electrónico, los trabajos a distancias están tomando, día a día, auge. En ese sentido, las organizaciones hacen sus procesos dependientes de las TIC, por ello ha surgido la necesidad de contar con políticas que garanticen el resguardo de estos sistemas para brindar, realmente, solución a los incidentes que puedan suceder de manera efectiva, rápida y segura. Lo anterior fundamenta la necesidad de contar con un plan de continuidad en las instituciones.

Sin embargo, a mayor valor de la información almacenada en estos sistemas, mayor es la importancia de implementar políticas de seguridad y continuidad, no obstante el costo para la infraestructura de soporte en materia de seguridad, es más fuerte.

Naturalmente, el impacto que se logra en la organización cuando se implementa el plan de continuidad es positivo (tener como premisa principal el dar continuidad a las operaciones y procesos críticos que impacten la organización).

Para las instituciones, a nivel interno, se logra un ambiente tranquilo porque los directivos tienen un plan para ejecutar en caso de imprevistos y los empleados cuentan con instrucciones claras y precisas de la respuesta que deben tomar ante ciertas situaciones difíciles.

A nivel externo, como organización, se logra buena imagen ante los clientes y confiabilidad ante otras empresas o instituciones que hacen uso de los productos y servicios de la institución, es decir, contar con un plan de continuidad refleja orden en los sistemas de información además de una alta cultura de servicio y calidad de atención al cliente.[4]

[4] Vilchis, Xavier. *Business Continuity Plan ¿Ya lo tiene?,* 2009, p.32.

1.6. Por dónde se inicia un plan de continuidad

Para dar inicio a la creación del plan de continuidad se debe conocer la empresa o institución desde el punto de vista de sus procesos, infraestructura tecnológica, proveedores, colaboradores, directivos y clientes.

Aunque la responsabilidad de los planes de continuidad del negocio debe ser de los directivos, puesto que involucran a toda la organización desde los altos mandos hasta los colaboradores de línea cada uno con un papel bien definido y delimitado, el área de tecnología e informática debe ser la responsable, principalmente, del desarrollo del plan.

Como no todas las empresas o instituciones tienen la misma estructura ni los mismos procesos de funcionamiento, es indispensable realizar un análisis completo de la institución que permita identificar y detallar claramente el funcionamiento de la organización, así como, las prioridades sobre los procesos que en ella se lleven a cabo y dan funcionamiento a su actividad.

El principal propósito de generar un plan de continuidad totalmente ajustado a la organización, radica en contar un mapa de acciones que reduzcan el tiempo de toma de decisiones durante las operaciones de recuperación, restauración de los servicios y procesos críticos, con el fin de obtener el funcionamiento del sistema lo antes posible, disminuyendo el coste y dando paso a la efectividad.

De acuerdo con Jiménez, Laura, Guia de desarrollo de un plan de continuidad de negocio, 2007. El plan de continuidad involucra 4 fases o etapas las cuales se detallan a continuación:

1.6.1. Fase I

El objetivo de esta fase es adquirir información sobre los objetivos de la organización, del funcionamiento y de los procesos que se consideran críticos.

Con base en la información obtenida, se procede a realizar un análisis de los riesgos asociados a los procesos identificados y se determina cuáles son las causas potenciales que pueden llegar a interrumpir el funcionamiento de la empresa o institución.

1.6.2. Fase II

En esta se seleccionan las estrategias y se basa en dos aspectos fundamentales:

- La valoración de las diferentes alternativas y estrategias de respaldo existentes en función a los resultados obtenidos en la fase de análisis y evaluación de riesgos (fase I), con base en la información se determina y selecciona la estrategia más adecuada a las necesidades de la organización.

- Corregir las vulnerabilidades detectadas en la fase de análisis y evaluación de riesgos (fase I), de esta manera se logra disminuir la probabilidad que ocurran desastres.

1.6.3. Fase III

En esta fase se desarrolla el plan, el cual involucra el tratamiento de los procedimientos y planes de actuación para las diferentes áreas y equipos creados, además, se organizan los equipos que intervendrán en cada una de las fases del plan.

En esta etapa del plan conviene que exista mucha comunicación con los colaboradores, ya que estos deberán ser organizados en equipos, para que de esta manera se lleven a cabo todas las actividades que ayuden a reducir la resistencia con apoyo de los altos mandos.

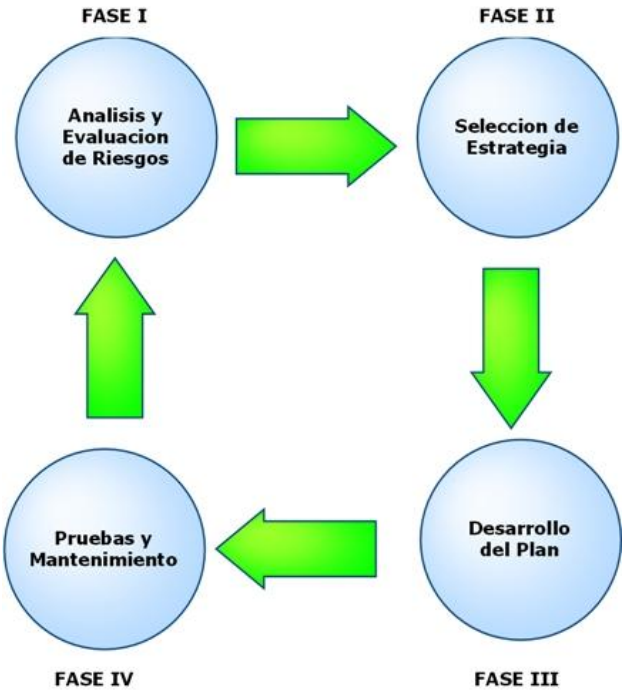
1.6.4. Fase IV

En esta etapa del plan es importante ponerlo a prueba bajo diferentes contextos para verificar que realmente funciona y es efectivo para la organización.

Es recomendable llevar a cabo las pruebas lo más realista posible, es decir, trasladar el contenido del documento a procedimientos prácticos.

Debido a que con el tiempo las empresas e instituciones cambian de políticas de administración como de procedimientos, es de carácter obligatorio el contar con un plan de mantenimiento con el objetivo de mantener actualizado el plan de continuidad, para que este siempre responda a las necesidades de la institución.

Figura 2. **Fases del plan de continuidad**



Fuente: elaboración propia.

Las 4 fases que involucran la creación del plan de continuidad son importantes. Por ello, estas etapas son consecuentes, es decir, que no se puede obviar ninguna de ellas, además se debe seguir el orden de las mismas para lograr un plan ajustado a la realidad de lo contrario el desorden y la falta de sincronización perjudicarían el desarrollo del plan.

Es importante destacar que cuando se llega a la fase número 4 se puede iniciar, nuevamente, la fase 1 para verificar el procedimiento o ejecutar otra iteración de este e ir ajustando con más detalle, el plan para lograr mayor exactitud.

2. EL PLAN DE CONTINUIDAD DE OPERACIONES

2.1. Fase I. Análisis del negocio y evaluación de riesgos

Para tener éxito en el desarrollo de un plan de continuidad, lo primero que se debe hacer es conocer y comprender bien cuáles son los procesos del negocio que son esenciales dentro de la empresa o institución para asegurar la continuidad de las actividades en caso de contingencia.

Para ello, se debe iniciar por abortar la visión respondiendo las siguientes preguntas:

- ¿Cuáles son las actividades más importantes para la organización?
- ¿Cómo afectaría económicamente una interrupción de los servicios a medida que va transcurriendo el tiempo sin reanudar estos?
- ¿Cuál sería la capacidad de operar de la empresa u institución a medida que pasa el tiempo?
- ¿Cuál es el plazo máximo para que cada actividad vuelva a la normalidad sin llegar a incurrir en graves pérdidas?
- ¿Cómo afectaría la interrupción de servicio a los clientes y a la imagen de la institución?

Las actividades y procesos que son de carácter vital dentro de una organización suelen ser, en su mayoría, los operacionales. Estos procesos interactúan de forma directa con los clientes o con otras organizaciones externas a la institución. Existe la posibilidad que estos procesos dependan de otros procesos internos que deben ser cubiertos en el análisis.

Para comprender las necesidades de la organización en cuanto a estrategias de continuidad, a continuación se describen dos formas de analizarlos:

- Análisis de riesgos (RA): este análisis tiene como objetivo identificar y clasificar los riesgos y los factores que potencialmente podrían afectar a las actividades que se quieren proteger. La evaluación de riesgos supone imaginarse lo que puede ir mal para poder estimar el impacto para la organización si el hecho ocurre. Se debe tener en cuenta la probabilidad de que sucedan cada uno de los riesgos identificados, de esta forma se pueden priorizar los riesgos y sus costos potenciales. Este análisis servirá para desarrollar un plan de acción adecuado y optimizado.[5]

- Análisis de impacto (BIA – *Business Impact Analysis*): este tipo de análisis permitirá identificar la prioridad de recuperación de cada proceso y actividad que de funcionamiento, a través de determinar el impacto en caso de interrupción. También, seleccionar cuál es la estrategia más adecuada para implementar.[6]

[5] Gaspar Martínez, *Plan de contingencia,* 2004, p.54.
[6] Gaspar Martínez, *El plan de continudad de ngocios,* 2006, p.25.

2.1.1. Análisis de riesgos (RA)

La base en un plan de continuidad de operaciones es, fundamentalmente, identificar los riesgos y ponderarlos según el impacto y la frecuencia en que estos ocurren, para ello se debe utilizar modelos probabilísticos y con base en una muestra, definir datos estadísticos que reflejen la importancia del riesgo.

El objetivo de un análisis de riesgos es establecer aquellas debilidades, vulnerabilidades, riesgos y amenazas actuales que por su situación o su importancia pueden poner en riesgo la marcha, antes de lo deseable, el Plan de recuperación de negocio. Este análisis debe centrarse en los procesos/actividades del negocio que se han considerado críticos, no obstante puede extenderse a aquellos que no lo son.

Es necesaria que las operaciones de la empresa o institución sean clasificadas con base en el impacto para la productividad de la organización y el valor que esta operación aporta para el servicio al cliente.

También se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas identificados. De esta forma se pueden priorizar los mismos y su coste potencial a través de desarrollar un plan de acción adecuado.

Existen diferentes metodologías para identificar y gestionar los riesgos, entre ellas están: NIST, MAGERIT, OCTAVE. No obstante para llevar a cabo la evaluación de riesgos es aconsejable responder las siguientes preguntas:

- ¿Qué se intenta proteger?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger y cuál es la probabilidad de ocurrencia?

2.1.1.1. Esquema del análisis de riesgos

Figura: 3. **Esquema del análisis de riesgos**

Fuente:http://intranet.ecu.edu.au/__data/assets/image/0006/129534/Business-Continuity-Planning-Process.jpg.

2.1.1.2. Identificar activos

Para cada uno de los procesos críticos de la organización es fundamental realizar un inventario de los activos involucrados en el proceso. Los activos se definen como los recursos de una empresa o institución que son necesarios para la consecución de sus objetivos de negocio. Ejemplos de activos de una organización pueden ser:

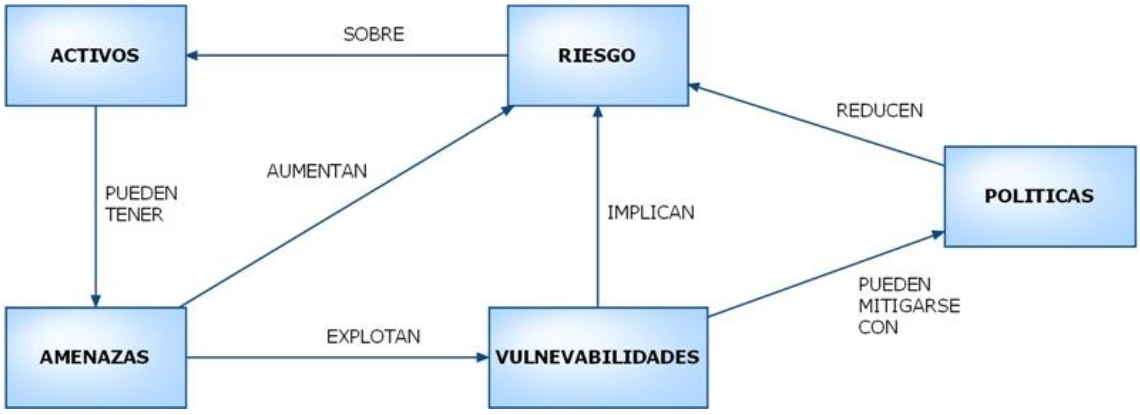
- Información
- Equipamiento
- Conocimiento
- Sistemas

Cada activo de la organización tendrá unos costes asociados. En algunos casos estos pueden ser cuantificados con un valor económico (activos tangibles) como el *software* o el *hardware* y, en otros casos, es más complicado cuantificar el activo con valores monetarios (activos intangibles) tales como: el prestigio o la confianza de los clientes.

Es fundamental elaborar un inventario de activos para identificar, claramente, su propietario y su valor para la organización, así como, su localización actual.

En el siguiente esquema se destacan los diferentes elementos que intervienen en el análisis de riesgo y cómo estos están relacionados unos con otros.

Figura 4. **Relación entre activos y vulnerabilidades**



Fuente: elaboración propia.

Bajo los lineamientos descriptivos de Jiménez, Laura*, Guia de Desarrollo de un Plan de Continuidad de Negocio*,2007.

2.1.1.3. Identificar procesos

Los procesos de negocio son todas aquellas actividades fundamentales que están íntimamente asociadas al tipo de empresa o institución, es decir, dan sentido y razón de ser a la organización.

Por los procesos de negocio que las empresas e instituciones pueden generar ganancias ya sea por la transformación de materia prima en producto terminado o por utilizar recursos con la finalidad de prestar servicios.

Según la definición formal de proceso de negocio, este "… es un conjunto de tareas relacionadas lógicamente llevadas a cabo para lograr un resultado de negocio definido. Cada proceso tiene sus entradas, funciones y salidas.[7]"

Existen metodologías para identificar los procesos de negocio, entre ellas están los casos de uso de negocio establecidos por RUP (*Rational Unified Process*)[8].

Otra de ellas es la que se basa en las metas y objetivos del negocio o de la institución, es decir, apoyarse en la planificación estratégica en donde se encuentran las bases de cómo lograr los objetivos (los procesos de negocio).

Los procesos de negocio tienen las siguientes características:

- Pueden ser medidos y están orientados al rendimiento
- Tener resultados específicos y concretos
- Entregan resultados a clientes o "*stakeholders*"
- Responden a alguna acción o evento especifico
- Las actividades deben agregar valor a las entradas del proceso

[7] http://es.wikipedia.org/wiki/Proceso_de_negocio, Noviembre 2010.
[8] http://es.wikipedia.org/wiki/Caso_de_uso, Noviembre 2010.

2.1.1.4. Identificar amenazas

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios.

Cuando se analizan los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

La siguiente ilustración clasifica las distintas amenazas a los sistemas.

Figura 5. **Tipos de amenazas**

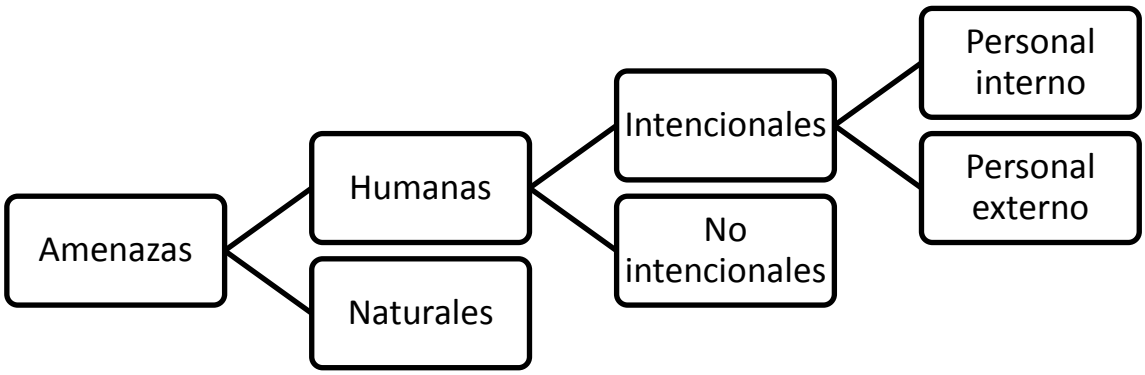


Figura: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.16.

Dependiendo de la organización y el proceso analizado, serán aplicables distintos tipos de amenazas. Las amenazas tendrán una probabilidad de ocurrencia que dependerá de la existencia de una vulnerabilidad que pueda ser explotada, para materializarse en un incidente.

Por ejemplo una amenaza de tipo de desastre natural como un terremoto, tendrá una mayor probabilidad de ocurrencia en una empresa con oficinas en Japón, donde los terremotos ocurren con mayor frecuencia, que en España. Por lo tanto, a priori se puede inferir que el riesgo de daño por terremoto en una empresa o institución situada en Japón es mayor que el de una situada en España.

Al momento de valorar la probabilidad de ocurrencia de una amenaza, resulta más complicado estimar las amenazas humanas (ataques maliciosos, robos de información, etc.), que las naturales.

A continuación se presenta una tabla con valores a escala de 1 a 5, donde 1 es una amenaza que no es probable mientras que el nivel 5 corresponde a amenazas altamente probables de suceder.

Tabla I. **Niveles de amenazas**

Nivel	Definición
Alta = 5	*La amenaza esta altamente motivada y es suficientemente capaz de llevarse a cabo.*
Media-Alta =4	*La amenaza está fundamentada y es posible.*
Media = 3	*La amenaza es posible.*
Media-Baja = 2	*La amenaza no posee la suficiente capacidad.*
Baja = 1	*La amenaza no posee la suficiente motivación y capacidad.*

Fuente: http://www.acis.org.co/fileadmin/Conferencias/ConferenciaBCP.pdf, pagina 37.

En el componente humano existen dos factores a tener en cuenta:

amenaza = capacidad x motivación

La motivación es una característica humana que es difícil de valorar, sin embargo es un factor a considerar: empleados descontentos, ex-empleados, etc

Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de *software* que determinan vulnerabilidades a nivel del sistema operativo y *firewall*:

Seguridad física.

- Monitoreo ambiental
- Control de acceso
- Desastres naturales
- Control de incendios
- Inundaciones
- Seguridad en las conexiones a Internet
- Políticas en el *firewall*
- VPN
- Detección de intrusos

Seguridad en la infraestructura de comunicaciones.

- Routers
- *Switches*
- *Firewall*
- *Hubs*

Seguridad en sistemas operativos (Unix, Windows).

- Correo electrónico
- Seguridad en las aplicaciones criticas

Se debe definir las aplicaciones que son críticas para la organización y por cada una de ellas se obtendrá una matriz de riesgo. Es importante considerar que las aplicaciones están soportadas por:

- Sistemas operativos
- *Hardware* servidor
- Redes LAN y WAN
- Centro de cómputo

También con el fin de realizar una correspondencia con los datos obtenidos por medio de las listas de verificación, se cuenta con el uso de herramientas de *software* especializadas, las cuales identifican vulnerabilidades en los sistemas operativos. A continuación se muestran algunas de las características de este tipo de herramientas:

- Búsqueda de vulnerabilidades en su red (Windows y Linux)
- Directorios compartidos, puertos abiertos, cuentas no usadas
- Revisión de actualizaciones aplicadas en los sistemas operativos
- Detección de dispositivos USB

2.1.1.5. Evaluar vulnerabilidades

Las vulnerabilidades son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves en una organización. Las vulnerabilidades en sí mismas no causan daño alguno,

sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo.

Para identificar las vulnerabilidades que pueden afectar a una empresa o institución se debe responder a la pregunta:

¿Cómo puede ocurrir una amenaza?

Para responder a esta pregunta se coloca como objetivo la amenaza y se define las distintas situaciones por las que puede ocurrir la misma, se evalúa si dentro de la organización puede darse esa circunstancia; es decir, si el nivel de protección es suficiente para evitar que se materialice la amenaza. Por ejemplo: si la amenaza es robo de datos estratégicos de la organización, se puede establecer, entre otros, los siguientes escenarios:

Tabla II. **Evaluación de vulnerabilidades**

ESCENARIOS	NIVEL DE PROTECCIÓN
1. Entrada no autorizada a los datos a través del sistema informático.	¿Existe un control de acceso a los datos?
2. Robo de datos de los dispositivos de almacenamiento magnético.	¿Están los dispositivos de almacenamiento protegidos y controlados de forma adecuada?
3. Robo de datos mediante accesos no autorizados.	¿Existen perfiles adecuados de acceso a los datos?

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.18.

Si no se responde afirmativamente a las preguntas de “Nivel de Protección”, es porque existen vulnerabilidades que podrían utilizarse de tal manera que la amenaza se convierta en un incidente real y causar daños importantes en la organización.

2.1.1.6. Evaluación del impacto

Todos los incidentes causan un impacto dentro de la organización, que también deberá tomarse en cuenta a la hora de calcular los riesgos. La valoración del impacto puede realizarse de forma cuantitativa, estimando las pérdidas económicas, o de forma cualitativa, asignando un valor dentro de una escala (alto, medio, bajo).

Por ejemplo, el robo de información confidencial de la organización puede causar un impacto alto si ésta cae en malas manos.

Otro caso, se puede estimar las pérdidas económicas de equipos tangibles valorando el coste de reposición y puesta en marcha nuevamente.

2.1.1.7. Evaluación del riesgo

El Riesgo es la posibilidad de que se produzca un impacto determinado en la organización. El riesgo calculado es simplemente un indicador ligado a la par de valores calculados de vulnerabilidad y de impacto, ambos unidos a su vez de la relación entre el activo y la amenaza a la que el riesgo calculado se refiere.

Probabilidad de incidencia = amenaza X vulnerabilidad
Riesgo = probabilidad de incidentes X impacto

Existen niveles de riesgo y clasificación de operaciones estándares los cuales, con base en los criterios de impacto, han sido clasificados según Marcombo, Alexander. Sistemas de gestion de seguridad de informacion, 2007, de la siguiente manera:

2.1.1.7.1. Críticos o alto

- Sus funciones no pueden ser ejecutadas a menos que sean remplazadas por recursos idénticos
- No se pueden utilizar métodos manuales
- El costo de interrupción es muy alto

2.1.1.7.2. Vitales o medio

- Sus funciones pueden ser ejecutadas manualmente durante un periodo corto
- Mayor tolerancia a las interrupciones
- El costo de interrupción es bajo si la caída es menor a 3 días

2.1.1.7.3. Sensitivos o bajo

- Sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo
- Mientras se hace manualmente requiere personal adicional
- Costos de interrupción medios

2.1.1.7.4. No críticos o sin riesgo

- Sus funciones pueden ser interrumpidas durante un periodo relativamente largo, con poco o ningún costo

- El riesgo suele expresarse en términos cualitativos (Alto, Medio, Bajo). A continuación se muestra un ejemplo de una matriz de probabilidad/impacto:

Tabla III. **Evaluación de riesgos**

Probabilidad				
	Alto	Riesgo medio	Riesgo alto	Riesgo alto
	Medi	Riesgo bajo	Riesgo medio	Riesgo alto
	Bajo	Riesgo bajo	Riesgo bajo	Riesgo medio
		Bajo	Medio	Alto
Impacto				

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.19.

Cuanto más baja sea la probabilidad de ocurrencia (no existan vulnerabilidades) y el impacto sobre la organización sea también bajo, se estará en un nivel de riesgo bajo.

Sin embargo, si existen vulnerabilidades que aumenten la probabilidad de ocurrencia o el impacto del incidente sea alto para la organización, se estará en unos niveles de riesgo medio-alto. Para ejemplificar el análisis de riesgo se muestra la siguiente tabla:

Tabla IV. **Análisis de riesgos**

Descripción	Probabilidad	Impacto	Riesgo
Terremoto en ciudades situadas fueras de fallas sísmicas.	Baja	Medio	Bajo
Terremoto en ciudades situadas sobre fallas sísmicas.	Alta	Medio	Alto
Robo de información en compañías con control y autentificación de acceso.	Baja	Alto	Medio
Robo de información en compañías sin control y autentificación de acceso.	Alta	Alto	Alto

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.20.

Una vez que se han evaluado los riesgos, queda decidir qué se hace con ellos. Se pueden llevar a cabo diferentes acciones, entre ellas se encuentran:

- Transferir el riesgo a través de seguros o subcontratando la gestión del riesgo a terceras empresas

- Aceptar el riesgo (posicionamiento aprobado por la dirección de la organización)

- Reducir el riesgo con controles que los mitiguen

- Eliminar el riesgo (eliminando la causa o el foco del riesgo)

2.1.2. Análisis de impacto (BIA)

El análisis de impacto es de importancia elevada para establecer las estrategias de recuperación, que en un inicio son las encargadas de dar continuidad a las actividades críticas y posteriormente al resto de actividades si es posible y factible.

Una actividad dentro de una organización tiene un nivel determinado y medible de criticidad, el cual es posible cuantificar en función de lo dependiente que es la actividad con los objetivos de la organización y de lo que repercutiría su indisponibilidad.

Desde el punto de vista económico esta valoración tiene lugar al dar respuesta a la pregunta, ¿cuánto perdería la organización si la actividad o proceso no estuviera disponible?

Para llevar a cabo el análisis de impacto se debe realizar las siguientes actividades que ayudaran a:

- Identificación de la relación de procesos: establecer los procesos de negocio que se llevan a cabo dentro de la organización y cómo estos interactúan entre sí.

- Identificación de la relación de aplicaciones: establecer la relación que existe entre las aplicaciones, cómo manejan la información que soporta los procesos de la organización.

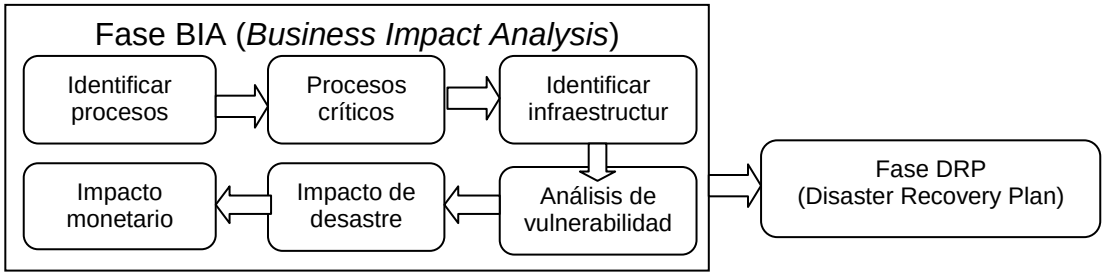
- Relación de departamentos y usuarios: establecer la relación de aplicaciones que soportan los procesos de la compañía desde el punto de vista de los usuarios y el agrupamiento de departamentos.

- Determinar cuáles son los procesos críticos: la valoración se puede dar bajo dos aspectos diferentes, uno basado en la importancia que tenga el proceso en la organización, cuya ausencia tendría un impacto alto en la actividad de la compañía (valoración cualitativa). La otra, se referiría a las pérdidas económicas por período debido a la ausencia de los procesos (valoración cuantitativa).

- Período máximo de interrupción: la sumatoria de las pérdidas suele ir creciendo linealmente a medida que pasan el tiempo y las actividades están interrumpidas. No obstante, a partir de un momento determinado que se llama período máximo de interrupción, las pérdidas sufren un aumento significativo y las funciones no podrían ser reasumidas.

En los casos en que la organización radique en varias sedes geográficamente distantes, será necesario establecer un alcance geográfico.

Figura 6. **Análisis de impacto (BIA)**



Fuente: elaboración propia.

2.1.2.1. Relación de departamentos y usuarios

Los procesos de la organización están gestionados por los usuarios los cuales están agrupados en departamentos con un rol definido. Dentro del inventario de procesos es necesario conocer al personal involucrado en los mismos. Esta información puede obtenerse de las mismas entrevistas donde se recoge la información de los procesos existentes y de los elementos (*hardware*, *software*, etc.) que lo conforman.

2.1.2.2. Relación de procesos

Para poder tener la información acerca de los procesos y las aplicaciones que hacen funcionar a la empresa o institución, es esencial la participación activa de las personas directamente responsables de los mismos dentro de la organización y de los colaboradores que conocen detalladamente los mismos.

Para lograr el mencionado objetivo se puede utilizar entrevistas personales y cuestionarios para obtener información sobre los procesos críticos del negocio.

Los procesos se pueden en dos áreas: los operativos y los de soporte:

- Los procesos operativos son aquellos que guardan una relación directa con el cliente (comercial, facturación, almacenaje, atención al cliente, etc.);

- Los procesos de soporte, son aquellos que facilitan los “recursos” para realizar los procesos operativos (recursos humanos, gestión financiera, etc.).

2.1.2.3. Relación de aplicaciones

En esta actividad se identifica y organiza el inventario de los recursos tecnológicos que soportan los procesos de la organización, a fin de establecer aquellos que den soporte directo a los servicios críticos.

Los tipos de recursos que se deben analizar según Gaspar Martínez, Plan de contingencia, 2004, son:

- *Hardware*, identificando cada uno de los elementos tecnológicos computacionales que soportan los sistemas de información de la organización.

- *Software* base, son todos aquellos componentes de *software*, incluido los asociados al sistema operativo, indispensables para el funcionamiento y optimización del Sistema de Información de la organización.

- *Software* de aplicaciones, inventariando las aplicaciones de gestión que son utilizadas en la empresa o institución, estos pueden ser de desarrollo propio para la funcionalidad requerida (*software* a la medida).

- Sistemas de infraestructura, considerando aquellos elementos o componentes que sin disponer de una tecnología enfocada propiamente al tratamiento de la información sí son requeridos para garantizan la operatividad del servicio.

2.1.2.4. Determinar los procesos críticos

En esta actividad se debe evaluar los impactos económicos y operacionales sobre el negocio en caso de no disponer de la función analizada. La valoración de pérdidas no es una ponderación sencilla o al azar, ya que pueden concurrir aspectos intangibles, tales como la imagen de la organización ante sus clientes.

Algunos criterios que pueden ayudar a valorar las eventuales pérdidas pueden ser:

- Costo de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante
- Ingresos económicos dejados de percibir
- Penalizaciones por incumplimiento de contratos con clientes
- Sanciones administrativas por incumplimiento de leyes debido a la falta de control en situación de desastre
- Gastos financieros

Para simplificar la tarea de valoración de los procesos se puede establecer una clasificación numérica, asignando mayor prioridad (1) a aquellos procesos que se consideren más críticos y menor prioridad (3) a los que se consideren menos críticos.

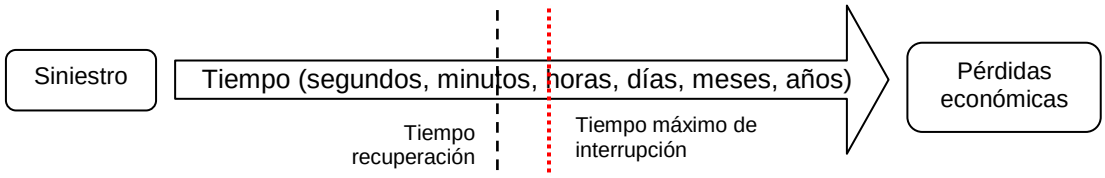
2.1.2.5. Periodo máximo de interrupción

Cuando se tiene la visión clara del negocio, de los procesos que lo componen y de la criticidad de cada uno de ellos, se debe establecer los tiempos de recuperación.

Como el objetivo del plan es dar continuidad al negocio tras un incidente o contingencia grave con las menores pérdidas económicas posibles para la compañía, se deben estimar, para cada uno de los procesos que se han considerado críticos, el tiempo a partir del cual las pérdidas económicas afectarían de forma grave a la compañía *(*tiempo máximo de interrupción*)*. Esta estimación es importante para seleccionar la estrategia de respaldo adecuada a las necesidades de recuperación.

Pueden existir procesos en los que el tiempo de recuperación es muy pequeño (horas), por ejemplo, el servicio de banca electrónica de un banco, y otros procesos como la facturación a clientes en una empresa de servicios, pueden tener un periodo de recuperación mayor (días o semanas).

Figura 7. **Tiempo de recuperación**



Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.13.

En síntesis, el análisis de criticidad brinda una visión de los procesos, actividades y recursos a proteger con la prioridad de recuperación de cada uno de ellos, junto con los tiempos objetivo de puesta en marcha tras un incidente.[9]

[9] International Standards for Business, http://www.iso.org/iso/home.htm, 2009.

2.1.2.6. Evaluar contramedidas

Para reducir riesgos se utilizan los denominados controles o medidas de seguridad. Estos se pueden clasificar en:

- Controles preventivos
  - Identifican potenciales problemas antes de que ocurran
  - Previenen errores, omisiones o actos maliciosos
    - ✓ Realizar copias de seguridad de los archivos
    - ✓ Contratar seguros para los activos
    - ✓ Establecer procedimientos / políticas de seguridad
    - ✓ Establecer control de acceso a la información
    - ✓ Establecer control de acceso físico

- Controles para la detección
  - Identifican y reportan la ocurrencia de un error, omisión o acto malicioso ocurrido
    - ✓ Monitorización de eventos
    - ✓ Auditorías internas
    - ✓ Revisiones periódicas de procesos
    - ✓ Censores de humo
    - ✓ Detección de virus (antivirus)

- Controles correctivos
  - Disminuyen el impacto de una amenaza
  - Solucionan errores detectados por controles detectivos
  - Identifican la causa de los problemas con el objeto de corregir errores producidos

- Modifican los procedimientos para reducir futuras ocurrencias del problema.
    - Parches de seguridad
    - Corrección de daños por virus
    - Recuperación de datos perdidos

Las medidas seleccionadas para mitigar riesgos deben mantener una proporción entre el esfuerzo y costo necesarios para su implantación y el riesgo que mitigan (evaluación del costo-beneficio).

Uno de los objetivos del plan de continuidad es evitar, en la medida de lo posible, que se produzcan incidentes que hagan necesaria su ejecución. Por ello, es importante que la organización conozca sus riesgos e implemente las medidas adecuadas para corregir el mayor número de vulnerabilidades que puedan provocar un incidente grave.

La evaluación de riesgos debe ser periódica y de acuerdo con el modelo de gestión de riesgos de la organización y en función de la evolución del negocio (crecimiento), de cambios importantes en la organización (procesos internos), nuevas obligaciones legales.

2.2. Fase II. Estratégias de respaldo

En esta fase se establecen políticas preventivas que ayuden a prevenir incidentes que ocasionen una discontinuidad en las operaciones de la empresa o institución, no obstante estas políticas son fundamentales ya que constituyen la base para la fase de recuperación. Las políticas seleccionadas deberán garantizar la restauración de los procesos afectados por el incidente tratando de estar dentro del rango de tiempo determinado por el análisis de impacto.

2.2.1. Respaldo a servidores

Las fallas en los servidores es uno de los principales causantes de inactividad en las empresas e instituciones provocando grandes pérdidas por falta de servicio.

Los factores pueden ser diversos, tales como: la saturación del servidor por numerosas transacciones, procesamiento de tareas muy pesadas e inclusive factores de orden físico como lo son los cortes de energía eléctrica entre otros, para ello las siguientes medidas de respaldo.

2.2.1.1. *Cluster* de alta disponibilidad

Un *cluster* es un arreglo de servidores que responden como si fueran un mismo y único servidor, dando servicio con la mayor disponibilidad posible.

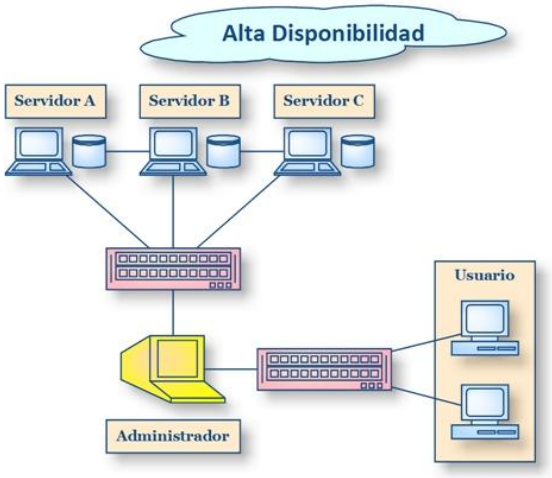
En un *cluster*, se tiene un arreglo de 2 o más servidores, los cuales están configurados para responder como si se tratara de un solo servidor, de esta manera se debe incorporar un equipo administrador que es el servidor que se encarga de distribuir y coordinar el trabajo a realizar entre los servidores del arreglo.

El *cluster* de alta disponibilidad trabaja para dar una respuesta a las peticiones, es decir, existe un servidor principal encargado del procesamiento de datos y el administrador continuamente verifica si este responde a las peticiones, en caso deje de responder, el servidor administrador lo detecta como fallo e inmediatamente lo saca de línea y coloca al servidor que esta replicado como principal mientras el otro que no responde es atendido por el departamento técnico.

Entre los servidores del arreglo deberá existir la replicación de datos, la cual permite, que sea cual sea el servidor que está respondiendo la información, esta siempre esta actualizada.

Un *cluster* es importante para el plan de continuidad porque con su implementación se logra tener respuesta por parte de los servidores, inclusive si uno de ellos deja de funcionar.

Figura 8. **Servidores tolerantes a fallos**



Fuente: elaboración propia.

Alta disponibilidad: responde el servidor B, hasta que el administrador detecta que el servidor A no responde.

Esta política ofrece un funcionamiento continuo sin pérdida de datos de manera que sus aplicaciones y datos comerciales están siempre disponibles cuando se necesitan, ya se trate de una semana laboral de siete días interrumpidos o de un entorno empresarial 12/5 ó 23/6.

Un servidor de copia de seguridad con una réplica actual de su entorno de aplicaciones siempre está disponible para la conmutación por error o el cambio con el fin de reemplazar su servidor de producción con un objetivo de tiempo de recuperación de segundos a minutos y un objetivo del punto de recuperación de cero.

La alta disponibilidad reduce de forma significativa el riesgo y los costes de las interrupciones de las actividades comerciales.

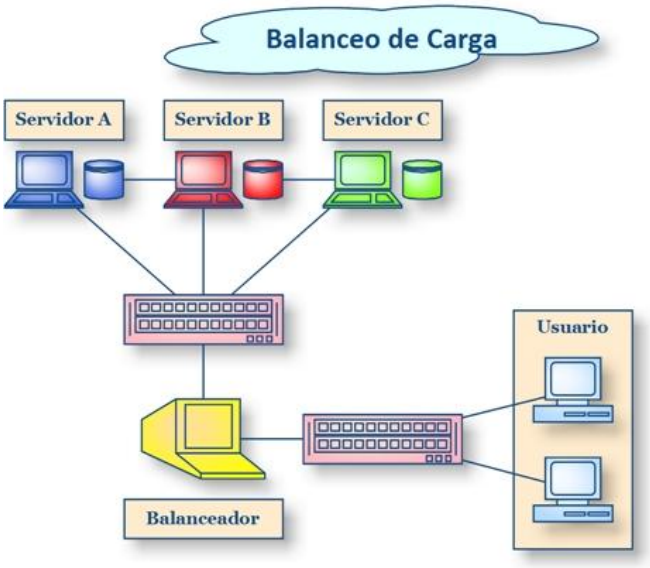
Además, las innovaciones recientes en automatización y la inclusión de capacidades de protección de datos continua han agilizado y facilitado enormemente la gestión de la estrategia para garantizar la continuidad de la empresa.

2.2.1.2. *Cluster* de balanceo de cargas

El balanceo de carga es una configuración de un arreglo de servidores que se caracteriza por distribuir, de manera simétrica, el trabajo entre los servidores configurados. Es decir con un *cluster* de balanceo de carga se logra procesar trabajos grandes y pesados que requieren de altos recursos por parte del sistema sin necesidad de afectar el rendimiento de todo el sistema.

El balanceador de carga distribuye trabajos entre los servidores configurados a medida que se van desocupando el procesamiento.

Figura 9. ***Cluster* de balanceo de carga**



Fuente: elaboración propia.

Balanceo de carga: las peticiones del usuario son direccionadas aleatoriamente hacia los servidores A, B o C para que respondan.

2.2.1.3. Redundancia en servidores

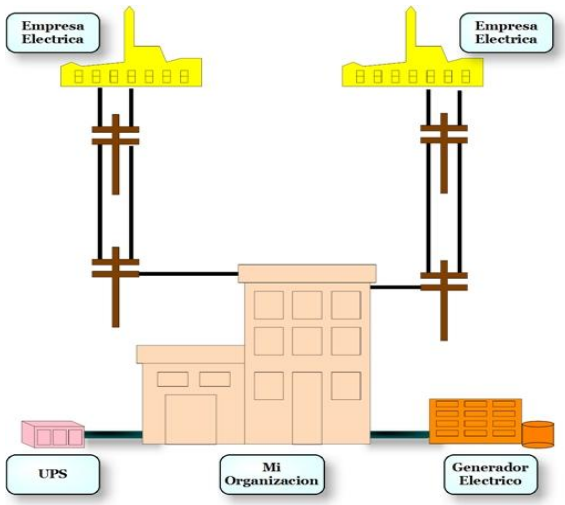
La redundancia es tener más de un servidor con los mismos datos y respondiendo de la misma manera. Con servidores redundantes se logra obtener un respaldo inmediato al servicio, en caso el servidor principal deja de responder a las peticiones.

Su contribución al plan de continuidad es evidente, debido a que en situaciones en las cuales el servidor principal tenga problemas para responder, la organización tiene una manera alternativa de seguir proveyendo información.

2.2.2. Redundancia en energía eléctrica

Una de las principales causas de discontinuidad en las operaciones de una empresa es por falta de energía eléctrica, ciertamente se depende de un proveedor el cual no garantiza el 100% de disponibilidad del servicio, por ello las empresas pueden tener cortes de energía de corto y largo plazo, para lo cual es necesario contar con medidas para atenuar este tipo de discontinuidades, entre las políticas para contrarrestar los efectos se tienen:

Figura 10. **Uso de sistemas ininterrumpidos**



Fuente: elaboración propia.

2.2.2.1. Sistema de protección eléctrica UPS

Los sistemas ininterrumpidos son arreglos de baterías que guardan carga para situaciones en que haya un corte del servicio. Esta es una medida para suplir el servicio en un corto tiempo. La duración de carga de un UPS es suficiente para poner en funcionamiento el generador alterno o conectar de una

empresa o institución a través de una fuente de energía eléctrica alterna como lo puede ser un segundo proveedor.

Los UPS tienen diferentes capacidades de carga, en promedio se tiene un margen de 20 minutos para restablecer la corriente eléctrica.

Los UPS funcionan a base de baterías, las cuales permanecen cargadas y a la hora de paro en el servicio eléctrico, estos utilizan la carga de las baterías dando energía a los ordenadores y servidores, no obstante se puede realizar arreglos para ampliar el tamaño de las baterías y tener más tiempo de energía por parte de estos.

Una buena propuesta para ampliar la carga de los UPS es conectar en paralelo una batería extra de 12 voltios, esta puede ser de automóvil. El tiempo de carga dependerá de la cantidad de amperios que sea el UPS de 20 minutos que es el promedio que garantizan los UPS a 24 horas con un batería de automóvil.

2.2.2.2. Plantas de poder

Los generadores eléctricos son pequeñas plantas capaces de entregar la cantidad de flujo eléctrico mínimo para que la institución continúe funcionando, estos son métodos para obtener energía eléctrica alternativa y no principal.

Las plantas de poder son generadores de energía que funcionan a base de un motor de combustión, por lo tanto las condiciones de su instalación deben ser seguras y en un sitio aledaño al edificio debido a que el funcionamiento de esta produce ruido excesivo, calor y gases tóxicos de desecho de la combustión.

2.2.2.3. Fuentes de poder redundantes

Una de las características de los servidores es que tienen que estar activos cerca del 100% del tiempo, en consecuencia las fuentes de poder son las encargadas de dar corriente eléctrica al servidor, estas tienden a fallar o a quemarse por tanto para garantizar continuidad de los servidores debe utilizarse fuentes de poder redundantes.

Las fuentes de poder redundantes son arreglos de dos o más fuentes de poder, las cuales están comunicadas entre si, al momento en que se detecte que una fuente de poder ha fallado, automáticamente la fuente alterna entra en funcionamiento.

Otra de las ventajas de estas fuentes, es que alternan entre la fuente de poder primaria y la fuente de poder alternativa con el fin de dar descanso a la fuente principal, alargar la vida útil de la fuente principal y de prevenir que se queme.

Figura 11. **Fuente de poder redundante**

Fuente: http://www.arcanosupply.net/Server/HPFuentedepoderredundante.jpg.

Es importante destacar que las fuentes de poder son específicas para cada marca de servidor, por lo tanto al momento de instalar una fuente de poder y que sea redundante se debe considerar el modelo del servidor y la marca porque no todos los servidores tienen la capacidad de adaptarse a una fuente de poder redundante ni los voltajes / amperajes de las fuentes son iguales en todos los casos.

2.2.2.4. Redundancia en proveedor de energía

Es recomendable tener a dos proveedores de energía eléctrica que sean diferentes y que además cuenten con cableado y estructura separadas, de esta manera si uno falla en la entrega del flujo eléctrico, la empresa o institución puede continuar operando con el segundo proveedor.

2.2.3. Respaldo a usuarios

Se considera usuario a las personas que utilizan los servicios de la empresa o institución TI, ya sea dentro o fuera de las instalaciones físicas (edificio).

Los usuarios son importantes para el funcionamiento de las empresas e instituciones debido a que sin ellos no tiene razón de ser la empresa ni el sistema de información.

Para garantizar que los usuarios puedan realizar sus tareas, cada uno con un rol especifico perteneciente a su puesto laboral se proponen las siguientes medidas:

2.2.3.1. *Hardware*

Para atenuar las fallas en un *hardware* debe existir un plan de mantenimiento, el cual permita alargar la vida útil del equipo de cómputo, no obstante el departamento de tecnología debe estar preparado con equipo extra en caso de tener que sustituir el *hardware*. Como mínimo este departamento debe tener unidades extra de mouse, teclado, tarjeta de red (NIC), tarjeta de video, monitor y disco duro con el sistema operativo configurado y las aplicaciones institucionales instaladas.

2.2.3.2. *Software*

Es importante tener en cuenta aspectos de *software* de usuario, este se divide en 3 tipos.

- Sistema operativo
- Aplicaciones institucionales
- Herramientas alternativas

Los sistemas operativos deben ser actualizados constantemente para garantizar seguridad, no obstante se deben estudiar las actualizaciones ya que las mismas pueden interferir en el funcionamiento de las aplicaciones institucionales.

Es recomendable, por políticas de continuidad, implementar una aplicación institucional basada en web para no hacer dependiente el sistema operativo ni el *hardware* de la aplicación institucional. Si la aplicación institucional no está basada en web para garantizar la continuidad en caso de incidentes, se debe mantener un espejo, clon o copia completa del disco duro en donde la aplicación institucional en conjunto con el sistema operativo funcionen y respondan de forma correcta en caso de que fallen las terminales de los clientes, el departamento TI puede hacer la restauración del sistema.

2.2.3.3. Datos

Los usuarios generan documentos que son propios de su función laboral, estos son almacenados en el disco duro local de su computadora personal. Esta es una práctica que va en contra de las políticas de continuidad debido a que en caso la computadora del usuario falle, no se puede sustituir esta fácilmente porque sus datos están dentro del equipo, por lo tanto, el usuario y el negocio deberán esperar a que la computadora sea reparada.

Para cambiar esta práctica se instala un servidor de datos institucional en el cual todos los usuarios guardan sus datos y documentos de carácter obligatorio, de esta forma los usuarios no son dependientes de la computadora asignada.

El funcionamiento de estos servidores es a través de FTP, con un usuario y una contraseña, los interesados pueden ingresar al servidor de datos y también crear nuevos documentos, leer los existentes o eliminar los que ya no son útiles.

2.2.4. Respaldo a redes

Las redes de comunicación son las encargadas de transmitir físicamente los datos entre servidores y usuarios. No obstante son vulnerables a sufrir fallos a nivel físico como a nivel lógico. Para ello las siguientes medidas de prevención.

2.2.4.1. Redundancia

Una red redundante involucra múltiples trazas de la red para poder realizar una misma conexión, no obstante no solo la redundancia en cableado es la solución, sino se debe pensar en redundancia de tarjetas de red para los servidores y los usuarios (NIC) así como, conmutadores extra los cuales puedan servir en caso emergente.

Con redundancia de red se logra mitigar el tiempo de recuperación ante fallos obtenidos por aspectos técnicos de la red, entre estos el cableado o condiciones meteorológicas.

En síntesis, para contar una red redundante se debe colocar conmutadores del doble de capacidad requerido, para en caso falle un conmutador fácilmente todo el cableado puede ser trasladado al conmutador más cercano, el cual posee el 50% de su capacidad disponible.

Otra política que se puede adoptar es el uso de una red cableada y una red inalámbrica, la cual normalmente debe estar deshabilitada por seguridad, no obstante, todas las computadoras deben tener una tarjeta de red inalámbrica así como estar configurados los puntos de acceso en caso ocurra un fallo con la red cableada emergentemente se puede tener conectividad.

2.2.4.2. Enrutamiento alternativo

Este consiste en crear una ruta alternativa principal de conectarse a un servidor, que a través de ella se pueda llegar al destino, el cual puede ser un servidor, una puerta de enlace, una computadora cliente, una impresora, etc.

Para que el enrutamiento alternativo en las redes se diseñe de forma correcta existen múltiples formas, una de ellas es colocar enrutadores el cual, según el protocolo de enrutamiento, direcciona el flujo de red hacia su punto destino tomando en cuenta diferentes criterios como la distancia, el tiempo de respuesta. Los protocolos más utilizados para enrutar son: RIP, RIPV2 o OSPF.

La otra forma de direccionar el tráfico de la red es a través de la creación de redes virtuales VLAN utilizando *switch* capa 3 los cuales son configurables y se puede especificar por dónde debe encaminarse el tráfico.

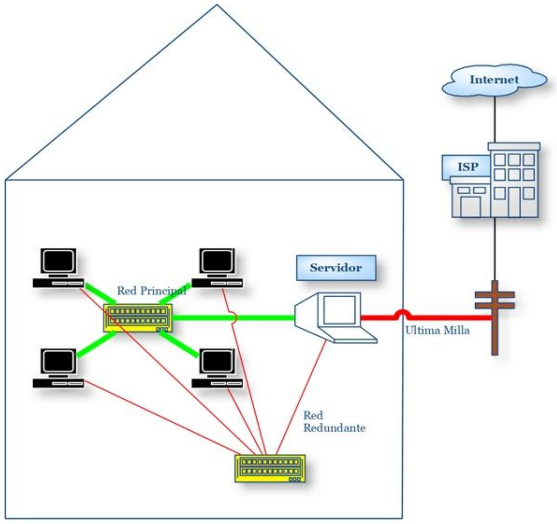
2.2.4.3. Protección última milla

Al paso final que lleva a cabo un servicio de Internet o de red en una casa u oficina del usuario final se le denomina última milla. En las aproximaciones existentes para la solución de última milla las compañías transportan la señal en las líneas eléctricas junto con la electricidad, mientras que otras ponen dispositivos *wireless* para enviar datos de forma inalámbrica.

Es importante manejar la última milla de manera conveniente para la organización porque, estadísticamente, se conoce que es en este espacio que las redes grandes tienen los fallos.

Para el plan de continuidad es recomendable considerar la protección última milla, debido a las inconsistencias de red, de esta forma la organización puede tener control sobre este servicio.

Figura 12. **Protección del circuito de última milla**



Fuente: elaboración propia.

2.2.5. Respaldo a datos

La información constituye uno de los activos más valiosos de las empresas e instituciones, esta está clasificada en crítica y transitoria.

La información transitoria son documentos que pueden ser sustituidos fácilmente y que el negocio no depende de esta información, como por ejemplo, las solicitudes de empleo.

La información crítica es difícil y costosa de sustituir, por ejemplo, la lista de clientes y los estados de cuenta de los créditos. Es por esa razón que las empresas e instituciones deben invertir en copias de seguridad. La cantidad monetaria destinada a los sistemas de copiado de información dependerá de los datos a resguardar y el nivel de criticidad de estos.

A continuación se proponen diferentes políticas para resguardar los datos:

2.2.5.1. Sistema de *backup*

Los sistemas de *backup* son respaldos de la información basados en hacer una copia exacta de los datos y almacenarlos en una ubicación diferente a donde los datos residen normalmente.

Estas copias externas pueden ubicarse en cintas magnéticas, discos duros externos, discos compactos, DVD, e inclusive en memorias USB, el objetivo principal es mantener una copia exacta de los datos en un lugar diferente para en caso de emergencia se pueda utilizar el respaldo.

Los *backup* tienden a ser extensos en información, por ello existen diferentes tipos de estos para facilitar el manejo de datos, los cuales son:

- Completo
- Diferencia
- Incremental

El *backup* completo consta de una copia entera de toda la información, este puede ser tardado e inclusive se puede saturar la red dependiendo del volumen de datos. Este tipo de resguardo de la información es fácil de restaurar debido a que todos los datos están integrados en una misma copia.

El *backup* incremental consiste en realizar un único *backup* completo al inicio y, posteriormente, efectuar otro solo de los datos que han tenido cambio a partir del último *backup* ejecutado. La ventaja de este procedimiento es que es rápido, no satura la red y no tarda mucho tiempo en completarse, sin

embargo, la desventaja radica en la restauración, es decir, primero se lleva a cabo el *backup* completo y posterior a ello, cada uno de los *backup* incrementales.

Este tipo de *backup* toma mucho tiempo en restaurarse debido a que no está integrado en absoluto.

El *backup* diferencial consiste en elaborar un *backup* completo inicial y, posteriormente, se realizan solo las modificaciones en la información a partir del *backup* completo. Quiere decir que para su restauración es necesario contar con el *backup* completo y el último diferencial.

Existen sistemas de *backup* y servidores de *backup* que tienen la tarea de respaldo de información mucho más fácil y organizada, para ello es recomendable que los *backup* se realicen mientras la red tiene poco tráfico y los usuarios no estén utilizando el máximo del sistema, además el servidor que resguarda la información, de preferencia, debe estar ubicado físicamente fuera de la empresa para resguardar mejor los datos.

Cuando el servidor de copia de seguridad se encuentra en una ubicación remota, también funciona como solución de recuperación de desastres.

2.2.5.2. Replicación

La replicación de datos es semejante a los sistemas de *backup* con la diferencia que la replicación se realiza en tiempo real mientras que el *backup* se realiza únicamente en la fecha y hora predeterminada. Dicho en otras palabras la replicación funciona bajo demanda del usuario y el *backup* cuando el administrador lo haya programado.

La replicación puede ubicarse en el mismo espacio físico que la información original, porque su función primordialmente es brindar un espejo de los datos para la mejor disponibilidad de los mismos.

Existen sistemas de replicación de datos los cuales, a partir de una carpeta o repositorio original, copian a una carpeta o repositorio destino cualquier archivo creado o modificado de forma instantánea y automática.

Estos sistemas son útiles cuando hay que compartir los documentos o múltiples usuarios deben acceder a ellos simultáneamente.

La replicación de datos también es utilizada en los sistemas de balanceo de cargas y de alta disponibilidad.

2.2.6. Capacitación al personal

La capacitación al personal es muy importante al momento de desarrollar un plan de continuidad debido a que los colaboradores juegan un papel importante y son quienes van a dar acción al plan.

Las ventajas que una empresa o institución obtienen al mantener un programa de capacitación constante son:

- Conduce a rentabilidad más alta y a actitudes más positivas
- Mejora el conocimiento del puesto a todos los niveles
- Crea mejor imagen
- Se promueve la comunicación a toda la organización
- Reduce la tensión y permite el manejo de áreas de conflictos
- Se agiliza la toma de decisiones y la solución de problemas
- Promueve el desarrollo con vistas a la promoción
- Contribuye a la formación de líderes y dirigentes

También es importante destacar que si los colaboradores están mejor preparados sabrán resolver las situaciones que se les presenta bajo presión de mejor manera, obteniendo mejores resultados.

La rotación de personal es una buena dinámica para que todos los colaboradores puedan realizar las diferentes actividades, además de apoyar en diferentes áreas, en caso de emergencia.

Además es buena práctica que los administradores, gerentes, jefes y directivos hayan participado, aunque sea por corto tiempo, en puestos de operarios para que de esa forma conozcan cómo se lleva a cabo la función, qué dificultades se experimentan y qué tiempos se transcurren, lo anterior con el objetivo de que los dirigentes de las empresas e instituciones sientan empatía por el trabajo de sus subordinados.

2.3. Fase III. Desarrollo del plan

En los capítulos anteriores se explicaron los siguientes temas:

- Conocimiento de los procesos de la compañía, valorando cuáles son críticos para el funcionamiento del negocio;

- Valoración de los riesgos que pueden afectar al negocio y que pueden disparar el plan de continuidad de negocio;

- Estrategia de continuidad más adecuada para el negocio.

El análisis de los temas mencionados anteriormente será muy útil para desarrollar “El plan de continuidad”. Para ello, se iniciará con la identificación de:

- Los equipos necesarios para el desarrollo del plan
- Las responsabilidades y funciones de cada uno de los equipos
- Las dependencias orgánicas entre los diferentes equipos
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el plan
- Los procedimientos de actuación ante incidentes
- La estrategia de vuelta a la normalidad

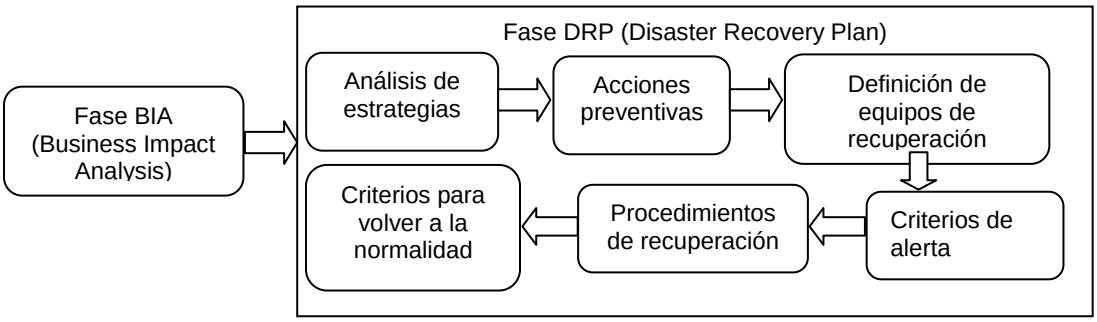
2.3.1. Estrategias de recuperación

Una estrategia de recuperación es una combinación de medidas preventivas, de detección y correctivas encaminadas a eliminar o reducir, en lo posible, el tiempo de inactividad de las amenazas.

Para garantizar una recuperación eficiente y eficaz, en primera instancia hay que identificar las estrategias de recuperación, la criticidad de los procesos de las operaciones y las aplicaciones que soportan los procesos.

También es importante identificar los costes que conllevan la recuperación, el tiempo requerido y la seguridad de la información, estos aspectos son los que determinan una recuperación buena o deficiente.

Figura 13. **Plan de contingencia**



Fuente: elaboración propia.

2.3.1.1. Aspectos tecnológicos para la recuperación

Cuando se habla de desastre, es pensar en una recuperación pronta de la información y comunicación de información en tecnología físicamente, el *hardware* son los componentes físicos que facilitan la comunicación de la información y por tal razón es indispensable tener en cuenta la tecnología de este y su configuración.

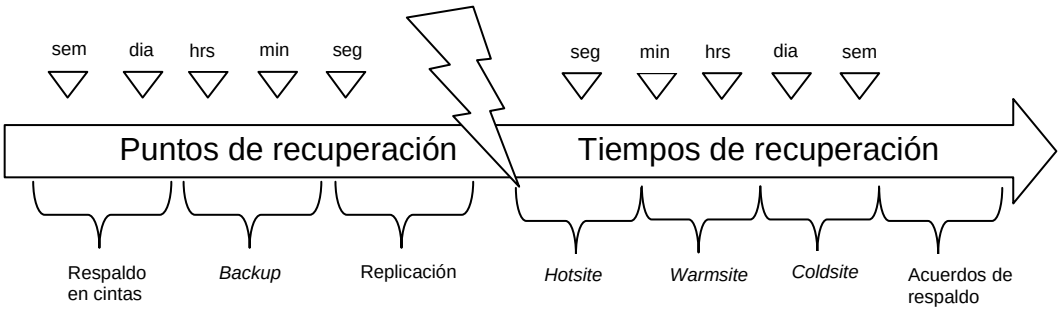
Un plan de continuidad incorpora mejores prácticas para el respaldo y la restauración de las actividades, mismas que involucran estrategias tecnológicas descritas a continuación:

- *Hot sites*: es el tipo de servidor que está listo para operar en pocas horas, tiene el equipo, la red y los sistemas necesarios para que las funciones se sigan dando, a este únicamente le hace falta el personal, los datos y la documentación.

- *Warm sites*: puede operar en menos de un día. Esta parcialmente configurado, cuenta con las conexiones de red y equipo periférico. la característica primordial de este equipo es que el CPU es de menor capacidad que el servidor principal.

- *Cold sites*: cuenta únicamente con la infraestructura básica. Esta listo para recibir equipo de cómputo (equipo periférico) y comunicaciones (conexión a red). La recuperación puede tardar varios días en concretarse.

Figura 14, **Punto de recuperación**

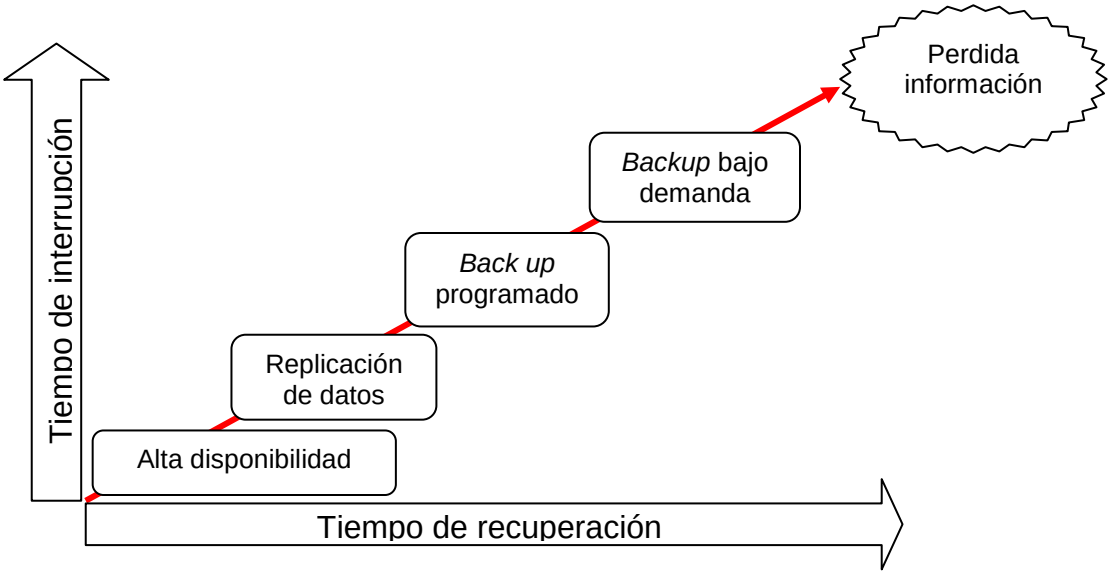


Fuente: http://www.ogosense.com/images/stories/dr-timeline.png.

Los componentes de este plan en cuanto al aspecto tecnológico incluyen:

- Personal clave para toma de decisiones informáticas
  - Información y gestión de tecnologías de la información
- Respaldo de los suministros requeridos
  - Configuración de las instalaciones
  - Mobiliario y equipo
- Métodos de recuperación de desastres para redes de telecomunicaciones

Figura 15. **Protección de información**



Fuente: http://www.gbm.net/bt/bt37/images/articulos/tendencias1c.jpg.

2.3.2. Metodología de implementación

La implementación del plan de continuidad de operaciones debe realizarse en forma integral, incorporando todos los niveles de la organización desde la alta gerencia hasta los últimos nodos del árbol jerárquico de la organización.

Además, es importante que todo personal que esté involucrado tenga claro en qué consiste el plan, sobre todo que esté completamente convencido y dispuesto a colaborar para la implementación; solo de esta manera se logrará colaboración activa de parte de ellos, en el proceso.

La implementación del plan de continuidad no es una actividad con un inicio y un fin bien establecido, sino por el contrario, tiene un inicio definido pero no un final.

El final no se establece debido a que el plan está diseñado para que constantemente se esté actualizando y mejorando. Solo con mejora continua se logrará madurez en la implementación del plan, así como de los tiempos de respuesta y recuperación de percances.

La resistencia al cambio es un factor que se va a presentar en la implementación del plan, situación que no se puede evitar, no obstante, se debe realizar gestiones para reducir, al mínimo, el rechazo. Esta se da cuando un usuario o grupo de usuarios no quiere adoptar las nuevas modalidades de funcionamiento porque esto implica adquirir nuevos conocimientos y actividades. Esta situación se da precisamente porque el ser humano está acostumbrado a acomodarse a un sistema y en consecuencia desestabiliza las labores que vienen desarrollándose diariamente.

Como se explicó en el párrafo anterior, la resistencia al cambio es un factor socio/cultural, no técnico o que involucre a la tecnología, es decir, está basada en las actitudes humanas (que las estudia la psicología) y la única manera de disminuir la resistencia al cambio, es logar una actitud positiva para realizar las nuevas actividades, que en un futuro ayudarán a mejorar el trabajo.

La resistencia al cambio se reduce cuando se concientiza a los trabajadores sobre la importancia de implementar nuevas políticas y procedimientos, para que en un futuro, el trabajo se realice más fácil.

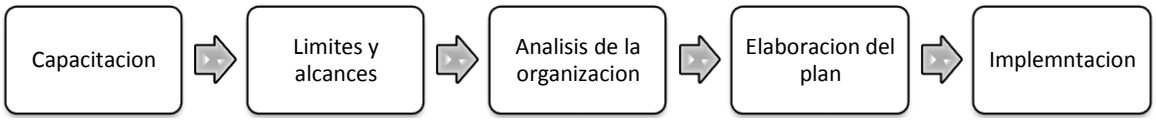
Otra de las maneras para disminuir la resistencia al cambio es involucrar al personal en el análisis y diseño de la solución, porque con la participación activa se logra que el usuario comprenda los beneficios y colabore para concretar la implementación.

La idea es que el trabajador sea parte del equipo de análisis y diseño del plan para que sus ideas sean tomadas en cuenta y él se sienta motivado con su participación, con ello se está reduciendo la resistencia al cambio.

Para la implementación se recomiendan 8 pasos, que son:

- Concientización o entrenamiento
- Fusión del manejo de la continuidad
- Entendimiento de la organización
- Plan de gestión de comunicación en crisis
- Plan de continuidad de negocios
- Plan de recuperación ante desastres
- Plan de respuesta de emergencias
- Simulacros

Figura 16. **Pasos de implementación**



Fuente: http://crisiscontrol.com.mx/wp-content/uploads/2011/06/BCM.jpg.

Estas etapas tienen sus características fundamentales y sobre todo sus entregables, que servirán de materia prima para el siguiente nivel del procedimiento de implementación según *International Standards for Business ISO*, http://www.iso.org/iso/home.htm, 2009.

I. Entrenamiento del personal para elaborar el plan

- Taller práctico

Entregable: material de dictado del curso

II. Límites y alcances del plan

- Diagnóstico / planeamiento estratégico en BCM

Entregable: informe del resultado del diagnóstico y el cronograma de acción

Entregable: modelo de desarrollo incluyendo medición de madurez

III. Entendimiento de la organización

- Análisis de Impacto al negocio (BIA)

Entregable: cuestionario de BIA

Entregable: informe final del BIA mostrando priorización

IV. Elaboración del plan

- Documentación de planes

Entregable: plan de continuidad del negocio / plan de recuperación ante desastres / plan de gestión y comunicación en crisis, conteniendo las actividades de recuperación a ser efectuadas por cada miembro del equipo de recuperación

Entregable: informe con las estrategias seleccionadas según nivel de criticidad

V. Implementación del plan

- Ejercicio de escritorio

Entregable: informe de resultado del ejercicio de escritorio.

Entregable: plan de pruebas

2.3.2.1. Delegación de funciones al personal (*empowerment*)

Es un proceso estratégico que busca una relación de socios entre la organización y su personal, aumentar la confianza responsabilidad autoridad y compromiso para servir mejor al cliente.

Los colaboradores son responsables de un producto, del servicio que comparten el liderazgo, colaboran en el mejoramiento del proceso del trabajo y planean y toman decisiones relacionadas con el método de trabajo.

Para el plan de continuidad es necesario que los colaboradores posean libertad en la toma de decisiones sobre el trabajo que realizan, para gestionar de manera eficiente y eficaz las actividades y procesos, lo anterior con el objetivo de obtener mejores resultados.

La gerencia y los administradores deben delegar la toma de decisiones y compartir la responsabilidad de las tareas designadas a los colaboradores, sin embargo, al momento de delegar la autoridad para tomar las medidas necesarias se está logrando agilizar los procesos de recuperación, tal actitud se logra confiando plenamente en las capacidades de los colaboradores de la organización.

El plan de continuidad involucra a todos los colaboradores de la organización, desde el nodo más alto en el organigrama hasta los empleados de línea, por este motivo la capacitación e información al personal juega un papel fundamental porque todos estarán informados y conocerán la forma de proceder ante una eventualidad, de esta forma se mitiga la resistencia al cambio por parte de los colaboradores y se involucran directamente en el plan.

Existen diferentes actividades que ayudan a la integración y capacitación del personal, entre ellas están:

- Talleres
- Charlas informativas
- Simulacros

2.3.2.2. Seleccionar estrategias

Existen diferentes estrategias para mitigar el impacto de una interrupción. Cada una de estas tiene unos parámetros de tiempo, disponibilidad y costes asociados que serán más o menos apropiados dependiendo de las funciones de negocio.

A continuación se describen diferentes estrategias para reubicación:

- No hacer nada: este tipo de actuación podría utilizarse en aquellas funciones o actividades que se han clasificado como “no urgentes” en el análisis de impacto. En este tipo de estrategia se asume el riesgo.

- Utilización de espacios propios: espacios existentes en la compañía, tales como: salas de formación, cafeterías, etc. Este tipo de estrategia requiere una planificación minuciosa.

- Recursos humano: es recomendable que se pueda reemplazar fácilmente un colaborador por otro, es decir, dentro de una empresa o institución no solo debe haber una persona capacitada para desempeñar una función sino todos los colaboradores y administradores deben estar capacitados para desempeñar cualquier puesto en la organización.

- Trabajo remoto o teletrabajo: posibilidad de trabajar en espacios exteriores a la compañía a través de conexión remota.

- Acuerdos recíprocos: acuerdos entre dos organizaciones (o entre dos unidades de la compañía) con características de equipamiento/espacio similares, con el objetivo de permitir a cada una de las partes recuperar funciones en otra ubicación. En este caso es importante definir las condiciones de uso y la realización de pruebas periódicas para asegurar las condiciones pactadas.

- Sitio alternativo subcontratado a terceros: contratación con compañías especializadas de espacios alternativos para la recuperación de la actividad. En este caso hay que asegurar que estas empresas proporcionen unos tiempos de recuperación acordes con las necesidades de la organización. Este tipo de instituciones pueden proporcionar diferentes soluciones:

    - Espacio dedicado: se garantiza la disponibilidad inmediata del espacio; es más caro que otras alternativas.

    - Espacio compartido: se comparte el espacio con otras compañías; es más económico que un centro dedicado a ello.

    - Espacios móviles: se pueden utilizar rápidamente, pero tienen un espacio limitado.

    - Módulos prefabricados: pueden tardar unos días en estar disponibles para su uso.

- Localizaciones diversas: se traslada la operación pero no el personal.

- Centro replicado: solución que permite trasladar, de forma inmediata, la operación, así como, continuar la actividad sin interrupción. También puede denominarse “centro espejo”. Esta solución es normalmente la más cara, pero la mejor solución para recuperar la operación.

A continuación se muestra una tabla que recoge la relación entre el tiempo objetivo de recuperación y la solución de continuidad más adecuada a este:

Tabla V. **Tiempo objetivo de recuperación**

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
MESES	Reconstrucción / Realojamiento	----
SEMANAS	Edificios prefabricados On-Site	Contratación de unidades móviles o prefabricados
DIAS	Recuperación “in situ” Trabajo en casa	Subcontratación de procesos en oficinas móviles
HORAS	Localizaciones diversas con empleados formados	Re-localización de un grupo de personas
INMEDIATO	Localizaciones diversas para la misma función	Cambio de funcionamiento a un centro de respaldo subcontratado

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.23.

De todas las alternativas existentes hay que elegir la más adecuada en cada caso. Dependerá de las necesidades de cada compañía, en cuanto a tiempos de recuperación, costes económicos y recursos.

Además deberá considerarse otros factores como:

- Ubicación y superficie requerida
  - Espacio suficiente
  - Zonas acondicionadas para ubicar al personal de la institución

- Recursos técnicos necesarios
  - *Hardware*
  - *Software*
  - Comunicaciones
  - Datos de respaldo

- Recursos humanos requeridos
  - Recursos materiales y de infraestructura
  - Servicios auxiliares necesarios
  - Tiempos de activación
  - Coste

Suele ocurrir que cuanto menor sea el tiempo de recuperación objetivo, mayor será el coste de la solución. Por ello es conveniente realizar un análisis con tiempos de recuperación adecuados y adaptados a la realidad de la compañía.

Una vez tomada la decisión sobre el tipo de estrategia que se utilizará como respaldo en caso de interrupción del negocio, se continuará con el desarrollo de todos los procedimientos, funciones y actividades que permitirán restablecer los procesos de negocio en unos plazos razonables.

2.3.2.3. Errores frecuentes

Es común encontrar algunos de estos errores cuando se piensa en un plan de continuidad entre los cuales se pueden mencionar:

- La gerencia piense que es un asunto técnico y no se tome en cuenta que involucra recursos económicos, financieros y humanos.

- La gerencia no apoya abiertamente las políticas del plan de continuidad ni tampoco facilita recursos económicos ni de recurso humano.

- Planificar una fecha de finalización para el plan, porque este tiene una fecha de inicio establecida pero por las constantes actualizaciones no se puede pensar en una fecha de finalización.

- No publicar las actualizaciones ni ajustes del plan a todos los trabajadores para que cuenten con la última versión del documento.

- Delegar toda la responsabilidad del plan de continuidad a un grupo específico, esta debe ser tarea de todos los trabajadores.

- Crear el plan visionando únicamente los siniestros totales, de gran escala y no incluir procedimientos para siniestros parciales o de pequeña escala.

- Hacer redundantes y duplicar los procesos en vez de establecer procedimientos de prevención y recuperación los cuales aporten confiabilidad.

- Considerar que el plan de continuidad es un tema de moda y no una forma de garantizar servicio y producción de la empresa pese a los siniestros.

- No enfocar el plan de continuidad a atender a los clientes en todo momento quienes son uno de los objetivos principales de este plan.

- Pensar que para implementar este plan es trascendente el tamaño de la empresa, el número de colaboradores o en número de operaciones que esta tenga.

2.3.3. Desarrollo de procedimientos

Una vez que se ha definido los equipos y se han establecido las funciones que deben desempeñar cada uno de ellos, se tienen que desarrollar los procedimientos a seguir y su actuación en cada una de las fases de activación del Plan de Continuidad.

- Fase de alerta
  - Procedimiento de notificación del desastre
  - Procedimiento de lanzamiento del plan
  - Procedimiento de notificación de la puesta en marcha del plan a los equipos implicados

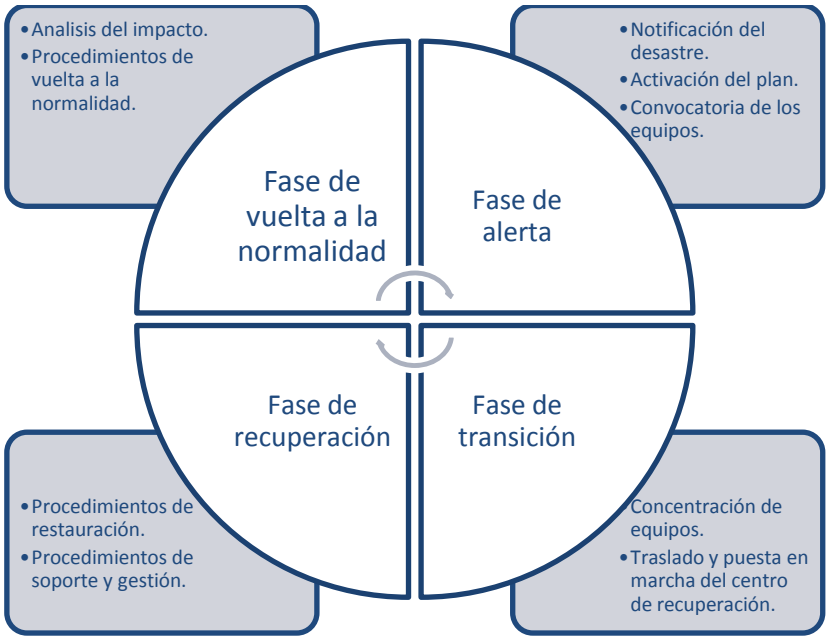
- Fase de transición
  - Procedimiento de concentración de equipos
  - Procedimiento de traslado y puesta en marcha de la recuperación

- Fase de recuperación
  - Procedimientos de restauración
  - Procedimientos de soporte y gestión

- Fase de vuelta a la normalidad
  - Análisis del impacto
  - Procedimientos de vuelta a la normalidad

En el siguiente esquema se observa las fases que componen el plan de continuidad de negocio:

Figura 17. **Desarrollo de procedimientos**



Fuente: elaboración propia.

2.3.3.1. Fase de alerta

Esta fase define los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos. Esta fase se divide en tres partes:

- Notificación: define cómo y quién debe ser informado, en primera instancia, de lo ocurrido;

- Evaluación: análisis de la situación y valoración inicial de los daños. Definición de estrategias;

- Ejecución del plan: decisión del equipo director de impulsar el plan debido al alcance de los daños.

    - Notificación

Como parte del plan de continuidad se debe elaborar un programa de información, en el que se comunique debidamente al personal de cómo actuar ante los diferentes incidentes y a quién comunicar lo ocurrido.

Tabla VI. **Notificación**

	EVENTO	ACCIÓN
1	Situación de contingencia/incidente detectado por algún empleado de la compañía. (Fuego, inundación, virus, etc.).	Aviso inmediato con el **máximo detalle posible** al Responsable de Personal de turno o a Seguridad.
2	El responsable de turno o de seguridad conoce que ha sucedido una contingencia.	Aviso a la persona de contacto del Comité de Crisis. Aviso a los equipos de emergencia (si procede).

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.30.

- Evaluación

Una vez que un miembro del comité de crisis es contactado e informado del incidente, este procederá, con la información recopilada, a evaluar la situación, posterior a ello, informará a los responsables de los distintos equipos de lo ocurrido y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de implementar el Plan, o bien iniciar otro tipo de estrategia.

Tabla VII. **Evaluación**

	EVENTO	ACCIÓN
3	Conocimiento por algún miembro del Comité de incidente ocurrido.	El equipo del Comité se reunirá en un **lugar acordado previamente** y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad. Será necesario informar de la situación a los siguientes responsables: • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación. • Responsable de los Equipos.

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.30.

- Ejecución del plan

Una vez que el comité de crisis ha decide poner en marcha el plan de recuperación, se inicia el árbol de llamadas para comunicar a los responsables de cada equipo la situación de inicio de las actividades e iniciar con los procedimientos de actuación de cada uno de ellos. Además, se deberá informar al comité de dirección de lo dispuesto.

Tabla VIII. **Ejecución del plan**

	EVENTO	ACCIÓN
4	Consideración por parte del Comité de Crisis y ejecución del Plan.	Iniciar el árbol de llamadas. Informar al Comité de Dirección.
5	Paso a la Fase de Transición.	

Fuente: Laura del Pino Jiménez, Guía de Desarrollo de un Plan de Continuidad, p.31.

2.3.3.2. Fase de transición

Fase previa a la de recuperación de los sistemas. Es importante que en esta fase exista una coordinación entre los diferentes equipos, así como de logística, ya que son éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible.

Esta fase se divide, principalmente, en dos partes:

- Procedimientos de concentración y traslado de personas y equipos
- Procedimientos de puesta en marcha del centro de recuperación

Ambos procedimientos son la base del proceso de recuperación de los sistemas. Si esta parte falla, no será posible iniciar la recuperación, y por tanto, el plan de continuidad fallará.

A continuación se describe, cada uno de los procedimientos y equipos que deben interactuar en esta fase de transición.

- Procedimientos de concentración y traslado de material y personas

Dependiendo de la solución final que se decida como estrategia de respaldo, (este procedimiento puede variar), se realiza una descripción general de los procedimientos, esta podrá completarse una vez que se tome una solución definitiva.

Una vez avisados los equipos y puesto en marcha el plan, estos deberán acudir al centro de reunión designado en el plan de emergencia, en el caso de que la emergencia se declare en horas de trabajo. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el centro de respaldo, o cualquier otro designado por el comité de dirección de crisis.

Además del traslado de personas al centro de recuperación (si es necesario), los materiales necesarios para poner en marcha el centro de recuperación (cintas de *backup*, material de oficina, documentación,...).

- Procedimientos de puesta en marcha del centro de recuperación

Con los distintos equipos que van a intervenir en la recuperación y todos los materiales indispensables se pone en marcha el centro de recuperación, estableciendo la infraestructura necesaria, tanto de *software* como de comunicaciones.

2.3.3.3. Fase de recuperación

En esta fase se procede a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

Esta fase se divide en dos procedimientos:

- De restauración
- De gestión y soporte

    - Procedimientos de restauración

Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.

    - Procedimientos de soporte y gestión

Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos de manera que se reanuden las operaciones con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

2.3.3.4. Fase de vuelta a la normalidad / fin de emergencia

Una vez los procesos críticos están en marcha y solventada la contingencia, se deben plantear las diferentes estrategias y acciones para recuperar las operaciones cotidianas y volver a los procesos como inicialmente se trabajaba en la empresa antes del siniestro. Esta etapa se divide los siguientes procedimientos:

- Análisis del impacto
- Procedimientos de vuelta a la normalidad

- Análisis del impacto

En esta etapa se realiza una evaluación completa de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.

- Procedimientos de vuelta a la normalidad

Es la etapa en donde la empresa o institución ya se ha recuperado del siniestro, sin embargo, el personal debe incorporarse a sus funciones especificas, reubicar el equipo y mobiliario que se utilizó durante la emergencia y actualizar los datos para que estén en sincronía con los de la empresa.

Es frecuente que esta etapa involucre la compra de nuevo equipo y mobiliario, e inclusive, la reconstrucción de espacios físicos por algún daño ocasionado por el siniestro.

2.3.3.5. Gestión de informes y evaluación

Una vez solventado el incidente y vuelto a la normalidad, cada equipo deberá elaborar un informe de las acciones llevadas a cabo, del cumplimiento de los objetivos del plan de continuidad, los tiempos empleados, dificultades con las que se encontraron, etc.

Toda esta información servirá para valorar si el plan ha funcionado según lo planeado, así como, conocer las posibles fallas, para el ajuste del mismo.

2.3.4. Organización de equipos

Los equipos de emergencia se integran con personal clave. A cada equipo se le asignan funciones, actividades y procedimientos que tendrán que desarrollar en las distintas fases del plan.

Aunque el número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se detallan los diferentes equipos que se debe crear:

- Comité de crisis: es el encargado de dirigir las acciones durante la contingencia y recuperación.

- Equipo de recuperación: su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.).

- Equipo logístico: responsable de toda la logística necesaria en el esfuerzo de recuperación.

- Equipo de las unidades de negocio: encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos.

- Equipo de relaciones públicas: encargado de las comunicaciones a los medios de comunicación y clientes.

Los siguientes equipos aunque no es frecuente su nombramiento, pueden contribuir a lograr la recuperación normal del funcionamiento de todo el sistema informático de la institución:

- Equipo de respuesta a incidentes
- Equipo de atención de emergencias
- Equipo de determinación de los daños
- Equipo de administración de la emergencia
- Equipo de almacenamiento externo
- Equipo de *software*
- Equipo de aplicaciones
- Equipo de seguridad
- Equipo de operaciones de emergencia
- Equipo de recuperación de red
- Equipo de comunicaciones
- Equipo de transporte
- Equipo de *hardware* de usuario
- Equipo de preparación de datos y registros
- Equipo de soporte administrativo
- Equipo de suministros
- Equipo de salvamento
- Equipo de reubicación
- Equipo de coordinación
- Equipo de asuntos legales
- Equipo de prueba de recuperación
- Equipo de entrenamiento

El personal asignado a cada uno de los equipos puede variar dependiendo del tamaño de la organización y de la estrategia de recuperación seleccionada. Una persona puede pertenecer a más de un equipo, siempre y cuando no existan incompatibilidades en las tareas a realizar.

2.3.4.1. Equipo director

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. La función de este comité es tomar las decisiones “clave” durante los incidentes, además de servir de enlace con la dirección de la compañía y tener informados regularmente, de la situación.

Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación
- Decisión de activar o no el plan de continuidad
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación

2.3.4.2. Equipo recuperación

Este equipo es el responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye todos los servidores, PC’s, comunicaciones de voz, datos y cualquier otro elemento necesario para la restauración de un servicio.

2.3.4.3. Equipo logística

Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

- Transporte de material y personas (si es necesario) al lugar de recuperación
- Suministros de oficina
- Comida
- Reservas de hotel, si fuere necesario
- Contacto con los proveedores

Este equipo debe trabajar conjuntamente con los demás, con el objetivo de asegurar que todas las necesidades logísticas sean cubiertas.

2.3.4.4. Equipo de relaciones públicas y atención a clientes

Uno de los valores más importantes de una compañía son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.

Es decir, se trata de canalizar la información que se lleva a cabo al exterior de la institución, en un solo punto; para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

- Elaboración de comunicados para la prensa
- Comunicación con los clientes

2.3.4.5. Equipo de unidades de negocio

Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas e iniciar con el funcionamiento de las operaciones.

Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.

2.4. Fase IV. Pruebas y mantenimiento

2.4.1. Plan de pruebas

El plan de continuidad de operaciones juega un papel fundamental en una empresa u organización, este brinda un valor agregado significativo para los clientes al permitir darles un servicio sin interrupciones o con interrupciones muy cortas.

Es por eso que no se puede esperar a que ocurra una situación de riesgo o un percance para aplicar el plan de continuidad, sino que se debe efectuar pruebas con anticipación.

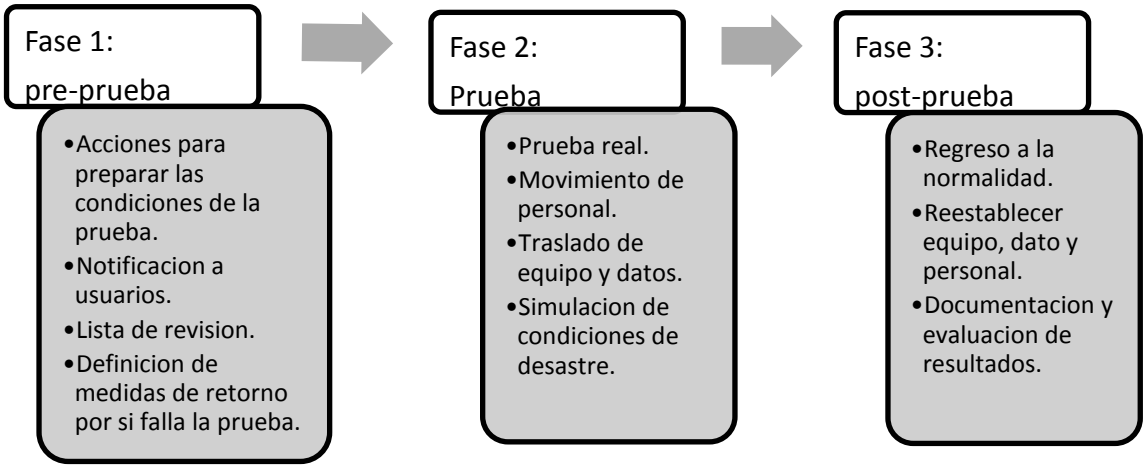
Es importante analizar y diseñar el plan de pruebas con la finalidad de contar con información verídica y óptima para que los objetivos del plan se cumplan.

Las especificaciones del plan de prueba son las siguientes:

- Medir la habilidad y capacidad del lugar de respaldo
- Evaluar la capacidad de recuperación de registros vitales
- Evaluar estado y cantidad de equipos y suministros en el lugar de recuperación
- Medir el desempeño general de actividades operativas y de sistemas relacionados con el negocio
- Verificar si el plan es completo y preciso
- Evaluar el desempeño del personal involucrado

- Evaluar el entrenamiento y conocimiento del personal que no pertenece al negocio
- Evaluar la coordinación entre equipo continuidad y proveedores externos

Figura 18. **Pruebas del plan**



Fuente: http://www.seguridadinformacion.cl/imagenes/bcp.png.

Es importante que se conozcan las etapas de las pruebas y los tipos de pruebas existentes debido a que estas deben ser aplicadas de manera integral. Los pasos para la realización de pruebas, son los siguientes:

- Pre-prueba
- Prueba
- Post-prueba

Tipos de prueba

- Prueba sobre papel
- Prueba del estado de preparación
- Prueba operativa completa

Los documentos son una parte fundamental del plan de continuidad y es un aspecto que culturalmente no se está acostumbrado a realizar. Las pruebas deben ser documentadas detalladamente para guardar los registros de lo que está sucediendo y lo que ha sucedido a manera de bitácora. También son importantes para documentar los pasos y las actividades que debe realizar cualquier persona que vaya a implementar el plan.

Una buena práctica es llevar una bitácora en la cual se escribe, informalmente, lo que sucedió y las pruebas que se realizaron, también, es importante anotar la percepción de la persona que lideró las pruebas y de los hechos.

Los documentos que contienen los resultados deben estructurarse de la siguiente manera:

Análisis de resultados

- Tiempo
- Cantidad
- Conteo
- Exactitud.

Las pruebas de un plan de continuidad deben tener dos características principales:

- Realismo: la utilidad de las pruebas se reduce con la selección de escenarios irreales. Por ello es importante reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.

- Exposición mínima: las pruebas deben diseñarse de forma que impacten lo menos posible en el negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible para el negocio.

En algunos casos puede resultar complicado realizar una prueba completa del plan de continuidad de negocio. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal hayan sido ensayados durante un período de tiempo.

2.4.1.1. Ejercicios técnicos

Este tipo de ejercicio requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de *hardware*, *software* y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos verificados durante un ejercicio de simulación son:

- Procedimientos de emergencia
- Métodos alternativos
- Líneas de telecomunicaciones de *backup*
- Procedimientos de notificación vendedores / clientes
- Capacidad y rendimiento del *hardware*
- Portabilidad del *software*
- Accesibilidad al centro de respaldo
- Movilización de los equipos de trabajo
- Recuperación de ficheros y documentación almacenados en lugar externo
- Recuperación de datos

2.4.1.2. Caja negra

Se denomina caja negra a aquel elemento que es estudiado desde el punto de vista de las entradas que recibe y las salidas o respuestas que produce, sin tener en cuenta su funcionamiento interno. En otras palabras, de una caja negra lo que interesa es su forma de interactuar con el medio que lo rodea, pero sin dar importancia a como lo hace internamente.

Por tanto, en una caja negra deben estar muy bien definidas sus entradas y salidas, sin embargo, no precisa definir ni conocer los detalles internos de su funcionamiento.

Por lo anterior, un sistema formado por módulos que cumplan las características de caja negra será más fácil de entender, ya que permitirá dar una visión más clara y general del conjunto y su interacción.

2.4.1.3. Caja blanca

Se denomina caja blanca a un tipo de pruebas de sistemas que se realiza sobre las funciones internas de un módulo. Así como las pruebas de caja negra ejercitan los requisitos funcionales desde el exterior del módulo, las pruebas de caja blanca están dirigidas a las funciones internas.

Entre las técnicas usadas se encuentran, la cobertura de caminos (pruebas que se realizan para recorrer todos los posibles caminos de ejecución) pruebas sobre camino de datos.

Las pruebas de caja blanca se llevan a cabo en primer lugar, sobre un módulo concreto, para luego realizar las de caja negra sobre varios subsistemas evaluando la integración.

2.4.1.4. Test completo

Estos son ejercicios planificados que implican la restauración real de la capacidad de proceso en un centro alternativo. Generalmente, los procesos en producción no son interrumpidos, pero puede planificarse su restauración y validación en el centro alternativo. Este tipo de prueba requiere la participación de toda la organización de continuidad del negocio, incluyendo usuarios, personal técnico y de operaciones.

2.4.2. Mantenimiento del plan de continuidad

Debido a que la tecnología cambia constantemente, es imprescindible mantener actualizado el plan de continuidad de operaciones. Es por eso que surge el concepto del plan de mantenimiento, en donde se analiza los cambios que ha tenido el sistema y con base en estos se determina la frecuencia de ellos, así como, los mantenimientos periódicamente para que no se quede olvidado el tema de la continuidad.

Entre las responsabilidades que debe afrontar el equipo encargado de mantener el plan de continuidad de operaciones se encuentran:

- Desarrollar un plan para revisión y mantenimiento periódico
- Exigir revisiones no programadas ante cambios significativos
- Examinar las revisiones y actualizarlas después de las revisiones
- Coordinar pruebas programadas y no programadas para evaluar suficiencia
- Participar en las pruebas anuales
- Desarrollar un programa de entrenamiento

- Mantener registro de las actividades de
    - Mantenimiento
    - Pruebas
    - Entrenamiento
    - Revisiones
- Actualizar trimestralmente las listas de contactos

2.4.2.1. Importancia

Es de vital importancia contar con un plan de mantenimiento para el plan de continuidad cuando ya se ha implementado en la organización y está en funcionamiento.

El plan de continuidad no es un grupo de documentos que se crean y se colocan en una gaveta, es todo lo contrario, debe ser un documento utilizado todos los días, este es una herramienta que va a servir en caso de emergencia (ante desastres).

Cuando la organización adquiere un plan de continuidad y lo implementa en sus actividades diarias debe existir una manera organizada y estructurada de velar porque se mantenga actualizado día a día, además de seguir en la línea de la realidad del funcionamiento tal y como cuando fue implementado.

La naturaleza del ser humano y de sus actividades es eminentemente cambiante, por tal motivo es de esperarse que los procesos dentro de una organización sufran cambios drásticos en un periodo corto de tiempo o que sufran cambios mínimos a lo largo del tiempo dando como resultado cambios evidentemente drásticos.

Partiendo de esta premisa de que los procesos cambian con el tiempo, se debe contar con un plan para actualizar los cambios en el plan de continuidad, incluir los nuevos procedimientos adoptados por la organización y eliminar los procesos desactualizados o que ya se encuentran en desuso.

El plan de continuidad debe ser siempre funcional para que los resultados sean óptimos e inmediatos ante cualquier desastre.

3. OPERACIONES EN BIBLIOTECA CENTRAL DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

3.1. Antecedentes

La Biblioteca Central es la dependencia técnica y de servicio de la Universidad de San Carlos de Guatemala, encargada de seleccionar, adquirir, clasificar, catalogar, actualizar y mantener la conformación de un fondo bibliográfico acorde a las necesidades de los planes, programas y proyectos académicos de la universidad.

La biblioteca se inició en el año 1967 con 2,368 volúmenes aproximadamente, los cuales correspondían a las colecciones de la biblioteca de estudios generales y de la Biblioteca Central.

Posteriormente, en agosto de 1974, se amplió el material bibliográfico con las colecciones de las unidades académicas de Ciencias Económicas, Humanidades, Ciencias Jurídicas y Sociales, Medicina, Odontología, Arquitectura y Agronomía.

En 1974, se inaugura el Edificio de Recursos Educativos, diseñado y construido para la Biblioteca Central, así como para centralizar las colecciones de todas las bibliotecas especializadas de las unidades académicas de la Universidad de San Carlos de Guatemala.

El Consejo Superior Universitario en acta No. 43-79, de noviembre de 1979, ordenó descentralizar las colecciones y que volvieran las bibliotecas especializadas a cada unidad académica y que no hubiese centralización alguna.

En 1984, se dieron los primeros pasos para la automatización de las colecciones bibliográficas de la biblioteca, con equipo y *software* donados por la embajada de Estados Unidos de América para las bibliotecas universitarias del país, siendo pioneras en la automatización en Guatemala.

En 1993, se inició el proyecto de modernización de la biblioteca, con la automatización, implementación y creación de nuevos servicios y secciones, con el fin de prestar un servicio bibliotecario más ágil y eficiente; ofreciendo a la comunidad universitaria y público en general: bases de datos de texto completo, bases de datos de la biblioteca, intranet, préstamo y devolución automatizado de materiales bibliográficos, multimedia, catálogos-manuales y electrónicos.

En este mismo año se inicia el servicio de audiovisuales con material actualizado y dos salas, actualmente, cuenta con cuatro, cada una con capacidad para cien personas; equipadas todas con mobiliario y equipo audiovisual para apoyar el proceso enseñanza aprendizaje.

Asimismo, se reestructuró la hemeroteca, se creó el archivo vertical, el cual está conformado con recortes de artículos de publicaciones periódicas o con temas de economía, problemas sociales, política, arte, literatura, entre otros, nacionales e internacionales.

En 2001, se recibió una donación de equipo de computación del cantautor guatemalteco Ricardo Arjona. Este equipo fue instalado en una sala destinada para impartir cursos de computación. Así también se arrenda a otras unidades académicas de la universidad y a otros sectores para la impartición de cursos, conferencias, charlas, pláticas y video-conferencias.

En 2004, se inauguró la Biblioteca de la Paz “Periodista Irma Flaquer”, su fondo lo constituyen revistas, libros, videos, recortes y folletos con información sobre el proceso de paz en Guatemala, donados por la Misión de Verificación de Naciones Unidas en Guatemala -MINUGUA-.

En 2007, se rediseño la página web institucional con un diseño orientado a la web 2.0 en donde el estudiante podía hacer sugerencias sobre bibliografía siempre y cuando esta atendiera los temas de los primeros dos años de cada carrera universitaria.

En 2009, se implementó el sistema de búsqueda de bibliografía por anaquel abierto, el estudiante busca el material a consultar a través de un sistema de información que específica claramente en qué anaquel se encuentra el material y un número correlativo para poder localizarlo más fácil[10].

Con el sistema de anaquel abierto se implementó un sistema de inventario 3M el cual consiste en un escáner que detecta, de forma automática, los libros que están prestados con el fin de actualizar la base de datos y reducir la incertidumbre del estado de existencias del anaquel.

[10] Biblioteca Central, Universidad de San Carlos de Guatemala. Manual institucional.

En 2010, se instaló el primer salón de video conferencias de alta definición, este sistema consiste en una cámara panorámica la cual permite visualizar remotamente la audiencia en el salón, además de una pantalla de 50 pulgadas con el propósito de proyectar al expositor en tiempo real.

El sistema de video conferencias es un plan piloto que tiene la Universidad de San Carlos para integrar a los Centros Regionales Universitarios y Centros Universitarios de la Universidad con el propósito de transmitir en línea, las cátedras a los estudiantes.

3.2. Justificación

La Biblioteca Central de la Universidad de San Carlos de Guatemala es la dependencia que brinda servicio a todas las facultades, escuelas y carreras técnicas que se imparten la Universidad de San Carlos, así como, a colegios, escuelas e institutos públicos que deseen realizar consultas bibliográficas en la misma.

Esta dependencia cuenta con material adecuado para los primeros dos años de cada una de las carreras que se imparte en la universidad.

También, cuentan con salas individuales para los alumnos que se preparan para sustentar sus exámenes privados, salones audiovisuales los cuales están equipados con computadora, cañonera, pizarrón, video casetera, televisión, DVD, aire acondicionado, sistema de audio.

Esta unidad posee un laboratorio de computación “Ricardo Arjona”, este tiene dos extensiones dentro de la biblioteca y está orientado a impartir cursos básicos sobre computación y ofimática. Estos laboratorios son alquilados para talleres a particulares que lo deseen.

Por los motivos expuestos, la población a la cual sirve la Biblioteca Central es extensa, por ello necesitan contar con un plan de continuidad que garantice el servicio a todos los usuarios inclusive en situaciones de alto impacto a las que esta vulnerable la Universidad de San Carlos de Guatemala.

3.3. Operaciones en Biblioteca Central

3.3.1. Estructura de la red informática

Segundo nivel

En este nivel del edificio de Recursos Educativos se encuentra ubicada la jefatura de Biblioteca Central quien tiene a su cargo la gestión administrativa de las diferentes secciones en la cual está estructurada la misma.

También se encuentra un área de cómputo que está destinada a la búsqueda electrónica de bibliografía, estas computadoras son terminales con poca capacidad de procesamiento y su finalidad es acceder a la base de datos de bibliografías disponibles y mostrar el número de catalogación.

Tercer nivel

En este nivel se encuentra el área de préstamos de bibliografías. Los préstamos en esta sala son internos para el público en general y externo para estudiantes con carné vigente de la Universidad de San Carlos de Guatemala.

También se encuentra la sección de devoluciones. En esta área el usuario de Biblioteca Central devuelve los libros prestados, el encargado de recibir los libros verifica que no haya excedido el tiempo establecido, en caso de ser así, el usuario deberá cancelar la multa correspondiente.

Los pagos de los cursos de computación y de los suvenires se realizan en el área de devoluciones.

Cuarto nivel

En este nivel se encuentra el depósito de tesis, área destinada a recibir nuevas tesis, verificar su contenido y prestar a sus usuarios las tesis almacenadas.

Para realizar la búsqueda de tesis se utiliza el mismo sistema (aplicación de cómputo) que para la búsqueda de libros, el resultado de la búsqueda es el código con el cual el bibliotecario clasificó el material.

También se encuentra la mapoteca que es un repositorio de mapas detallados de Guatemala y del mundo y los dos laboratorios de computación destinados a cursos de computación y talleres de informática.

Esta área de la Biblioteca Central se caracteriza por tener cuatro salas audiovisuales acondicionadas con todas las características tecnológicas: cañonera, televisión, sistema de sonido, video grabadora, banderas, aire acondicionado e internet de alta velocidad, para llevar a cabo exposiciones, conferencias y capacitaciones.

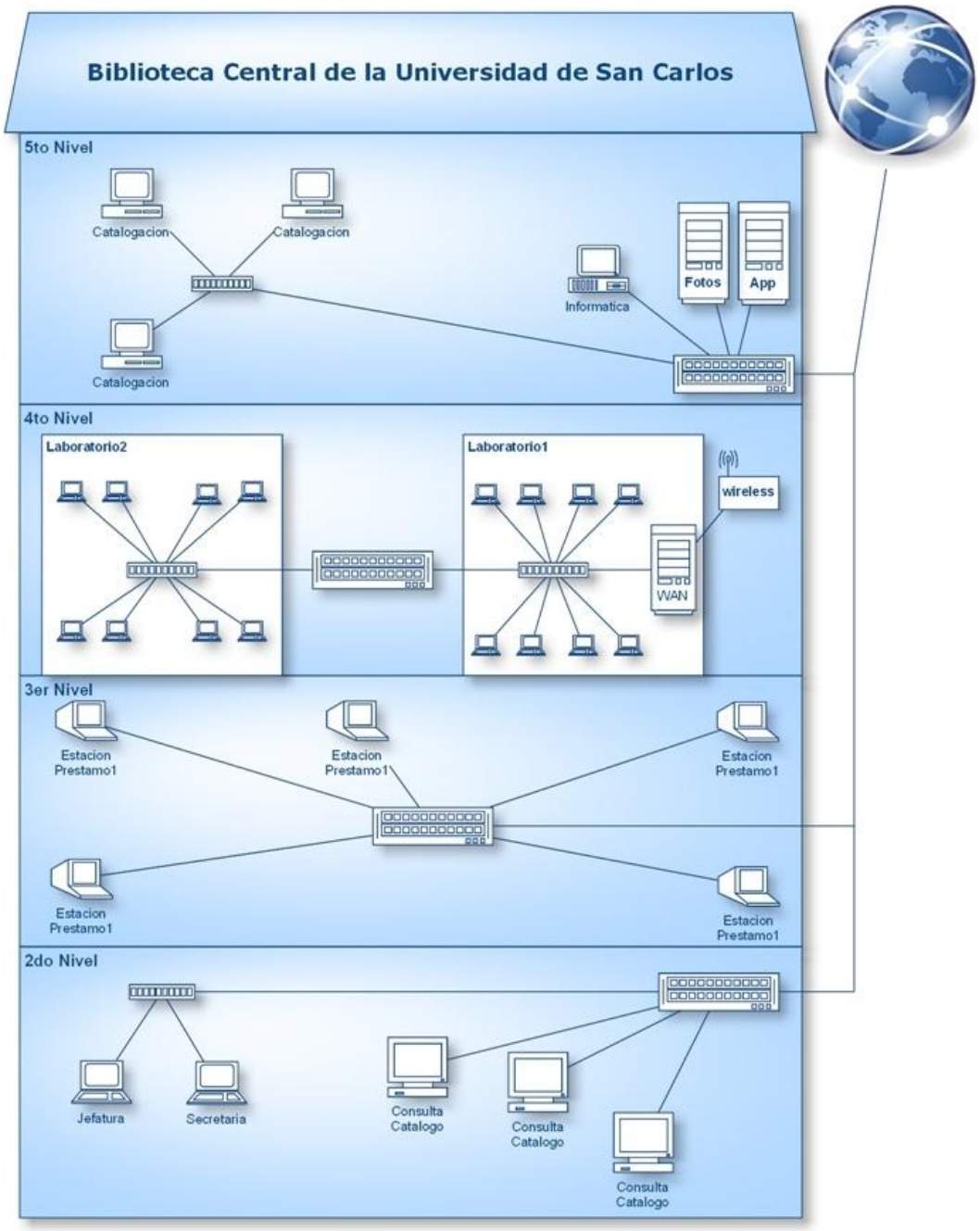
Los salones audiovisuales se prestan a catedráticos universitarios y a las diferentes unidades administrativas y académicas y se alquilan al público en general previa solicitud del interesado y autorización del administrador.

Quinto nivel

En este nivel se encuentra el café internet en el cual alquilan computadoras para el uso de los estudiantes, impresión de documentos y navegación en internet, este servicio es particular no pertenece a los servicios de la Biblioteca.

También se encuentra el departamento de procesos técnicos, el cual se encarga de cotizar, adquirir y catalogar las nuevas bibliografías y tesis. Es en esta sección en donde se encuentran los servidores de internet y base de datos los cuales sirven para proveer sistema a Biblioteca Central. Asimismo, la hemeroteca que conserva las colecciones de diferentes periódicos que se publican en Guatemala y de la Universidad de San Carlos. Y varios cubículos, los cuales son alquilados, únicamente, a estudiantes universitarios quienes tiene que acreditar fecha de privado, es decir, estos son exclusivamente para que el estudiante se prepara para sus exámenes técnicos profesionales (privados).

Figura 19. **Red informática en Biblioteca Central**



Fuente: elaboración propia.

Bajo los lineamientos descriptivos de Biblioteca Central, Universidad de San Carlos de Guatemala, Manual institucional.

3.3.2. Catalogación electrónica

La catalogación electrónica es un proceso que se lleva a cabo en el quinto nivel de Biblioteca Central. Profesionales de la bibliotecología basados en criterios pre establecidos y guiándose de un tesauro clasifican la nueva bibliografía asignándole un código, un correlativo, clasificación y temas acerca de los cuales trata el libro.

El sistema Glifos, es el *software* que utiliza Biblioteca Central, este provee una interface amigable para que los catalogadores ingresen información de cada libro y, posteriormente, almacenarla en la base de datos.

Los valores que se almacenan por cada libro son básicos, entre ellos están: nombre del libro, autor, edición, fecha de publicación, editorial, número de páginas, notas asociadas, medidas en centímetros y temas con los cuales se puede asociar la bibliografía.

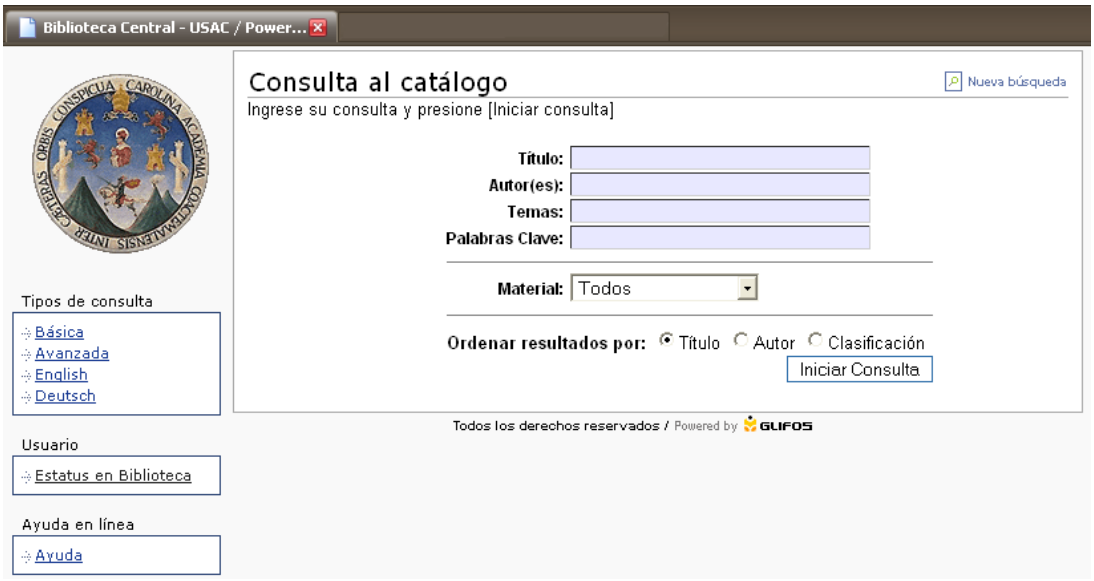
Este procedimiento es efectuado por una cantidad considerable de trabajadores, quienes cuentan con una terminal de ingreso de información (computadora cliente).

3.3.3. Consulta al catálogo electrónico

La consulta electrónica es el proceso que llevan a cabo los usuarios para identificar la catalogación del material que están buscando, esta consulta puede ejecutarse desde Biblioteca Central o a través de internet.

Los criterios de búsqueda pueden ser por: titulo, autor o autores, tema o palabras clave. O bien por diferentes soportes como audio, casete, cuaderno, CD-ROM, disquete, folleto, libro, libro electrónico, microficha, música, página web, revista, tesis, video digital, VHS, DVD.

Figura 20. **Pantalla de consulta al catalogo**



Fuente: http://biblos.usac.edu.gt/infolib/userStatus.html.

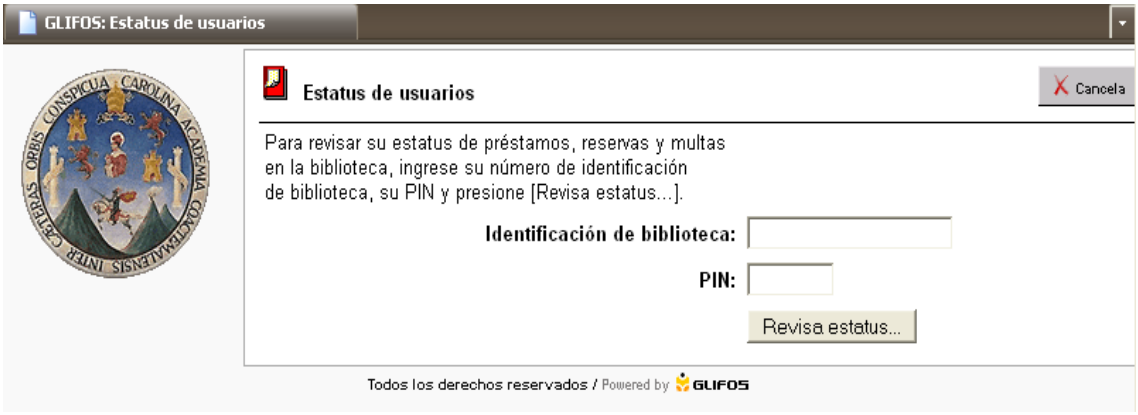
3.3.4. Consulta de estatus del estudiante

Cada estudiante universitario cuenta con un número de carné, el cual lo identifica de manera única en la Universidad de San Carlos. Él puede hacer uso de los recursos de la biblioteca siempre que su carné universitario esté vigente.

Por tal motivo, el número de usuario en Biblioteca Central es el número de carné del estudiante y el pin es generado en el 3er nivel de la biblioteca.

Cuando el estudiante ha solicitado la activación de su usuario y la contraseña de acceso, él tiene opción a través, de la página web de Biblioteca Central (http://biblos.usac.edu.gt/infolib/userStatus.html), a consultar los préstamos realizados, la fecha de vencimiento, así como, tiene opción a renovar libros y a reservar material bibliográfico. Es importante que el estudiante pueda consultar su estado dentro de Biblioteca Central, ya que para graduarse de la universidad es requerido un certificado en el cual Biblioteca Central hace constar que el estudiante es solvente.

Figura 21. **Pantalla de consulta de status al usuario**



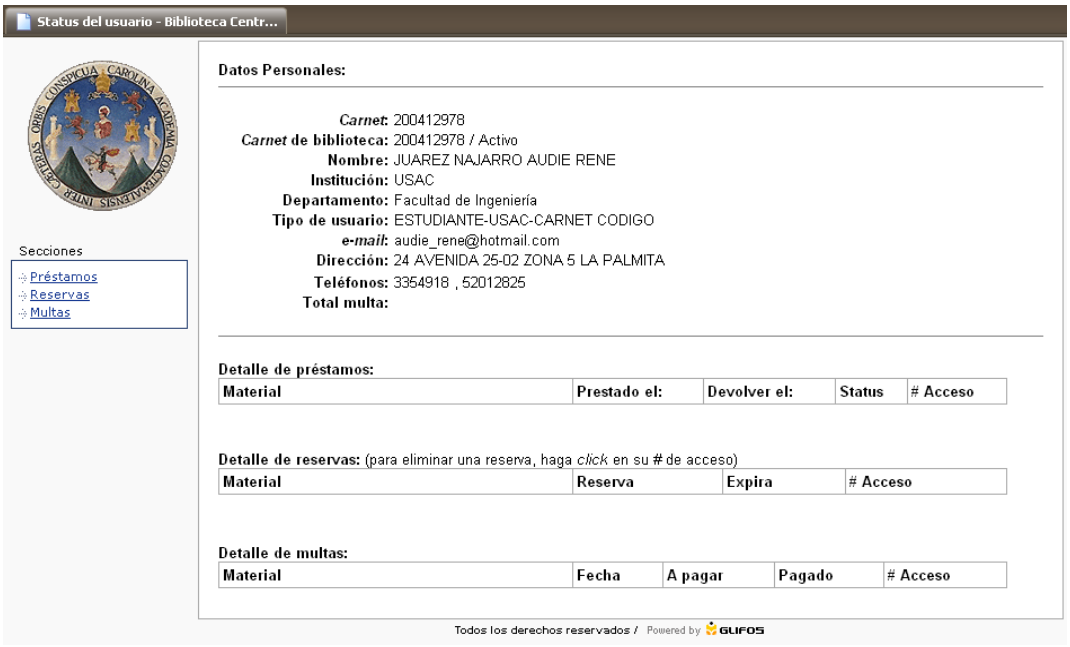
Fuente: http://biblos.usac.edu.gt/.

3.3.5. Préstamos y renovaciones en línea

Los estudiantes universitarios que tengan vigente su carné universitario pueden realizar préstamos de bibliografía a través de internet o renovar los mismos para no incurrir en multa por no devolver el material en el tiempo establecido.

El sitio desde el cual se puede consultar el estatus actual de préstamos y reservaciones además de realizar renovaciones de bibliografía es: http://biblos.usac.edu.gt/infolib/userStatus.html.

Figura 22. **Pantalla de préstamos y devoluciones**

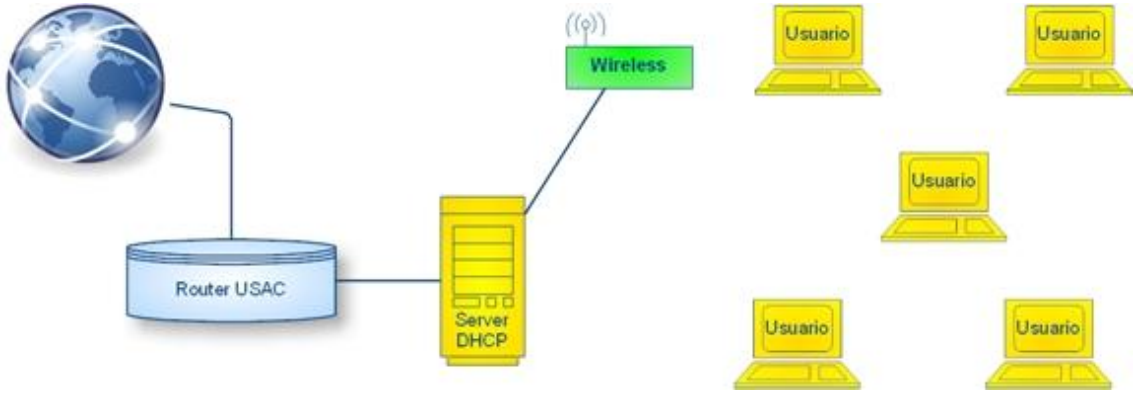


Fuente: http://biblos.usac.edu.gt/.

3.3.6. Internet público

El internet público que ofrece Biblioteca Central es un servicio que se le brinda al estudiante universitario en forma gratuita, es transmitido a través de una antena *wireless* omnidireccional conectada directamente a un servidor DHCP el cual asigna direcciones IP de forma automática en un rango de (192.168.1.1 a la 192.168.1.253) además de establecer políticas de acceso como por ejemplo filtrado de sitios web y filtrado de contenido para optimizar el ancho de banda y mantener la velocidad de conexión estable.

Figura 23. **Diagrama de Internet público Biblioteca Central**



Fuente: elaboración propia.

3.4. Límites y alcances del plan de continuidad

Límites:

El trabajo se limita a la identificación y análisis de los procesos vulnerables en Biblioteca Central, al diseño de las políticas y procedimientos que garanticen la continuidad de las operaciones analizadas previamente y a la elaboración del plan de pruebas y mantenimiento. Por la magnitud que involucra la implementación y las pruebas de rendimiento de un plan de continuidad de operaciones TI, en este trabajo no se va a desarrollar el tema.

Alcance:

- El caso de estudio involucra análisis y diseño del plan de continuidad además de elaborar un plan de pruebas y mantenimiento.
- El análisis está compuesto por la evaluación del impacto (*bussines impact análisis* – BIA) y la identificación de riesgos (*risk análisis* - RA).

- Qué estrategias de respaldo son útiles en Biblioteca Central partiendo del equipo con que cuenta esta institución.

- El diseño de los equipos de recuperación así como las responsabilidades que estos tienen en la etapa de alerta, transición, recuperación y vuelta a la normalidad.

- Destacar los errores que podrían ocurrir en la implementación del plan y, finalmente, elaborar un plan detallado de pruebas y mantenimiento para garantizar la continuidad en todo momento.

3.5. Importancia de un plan de continuidad en Biblioteca Central

Para Biblioteca Central es de suma importancia contar con un plan de continuidad, porque facilita recursos a todo público incluyendo a estudiantes e investigadores para su aprendizaje a través de material bibliográfico, equipo tecnológico y espacio físico para su consulta. Por esa razón, es necesario prestar servicios de calidad garantizados en todo momento, para lograrlo es esencial poseer un plan de continuidad.

En ese sentido, las tecnologías de la información que se utilizan en la biblioteca son competitivas y vanguardistas, por lo que esta institución controla la calidad y continuidad de servicio a sus usuarios.

4. ANÁLISIS PARA LA IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD TI EN BIBLIOTECA CENTRAL

4.1. Análisis de riesgo (RA)

Una parte importante dentro del desarrollo del plan de continuidad es el análisis de riesgos el cual va a ayudar a identificar los activos y procesos de la biblioteca, así como, priorizar cuáles de estos activos y procesos son determinantes para seguir prestando el servicio y gestionarlos en forma adecuada.

4.1.1. Identificación de activos en Biblioteca Central

Los activos son todos aquellos bienes tangibles e intangibles con los que cuenta la biblioteca y que hacen posible el continuar prestando un servicio de calidad.

Los activos pueden ser de tipo *hardware*, *software* y comunicaciones. También existen activos subjetivos difíciles de cuantificar, como lo son; el prestigio de la institución, la motivación del personal, entre otros.

Tabla IX. **Listado de activos en Biblioteca Central**

Activo/ Descripción	Tipo	Propietario	Localización	Valor
Servidor de aplicaciones bibliográficas	Hardware	Biblioteca Central	Quinto nivel, procesos técnicos	Alto
Firewall de seguridad en la red, Servidor DHCP y Servidor DNS	Hardware	Biblioteca Central	Quinto nivel, procesos técnicos	Alto
Aplicación para bibliotecas (Glifos)	Software	Biblioteca Central	Quinto nivel, procesos técnicos	Alto
Scanner	Hardware	Biblioteca Central	Quinto nivel, procesos técnicos	Bajo
Impresoras	Hardware	Biblioteca Central	En cada computadora.	Medio
Redes de Comunicación	Comunicaciones	Biblioteca Central	Quinto nivel, procesos técnicos	Alto
Aplicación de cobros	Software	Tesorería USAC	Tercer nivel, devoluciones	Medio
Aplicación de inventario de material bibliográfico	Software	Biblioteca Central	Tercer nivel, prestamos	Medio
Pistola RFID para inventario	Hardware	Biblioteca Central	Tercer nivel, prestamos	Medio
Computadoras de Consulta	Hardware	Biblioteca Central	Segudno, tercer y cuarto nivel	Alto
Computadoras de Prestamos	Hardware	Biblioteca Central	Tercer, cuarto y quinto nivel	Alto
Cámaras de vigilancia	Hardware	Biblioteca Central	Segundo nivel	Medio
Marcos de seguridad magnética	Hardware	Biblioteca Central	Segundo y tercer nivel	Alto
Magnetizador / Des magnetizador de libros	Hardware	Biblioteca Central	Tercer nivel	Alto
Internet	Comunicación	Procesamiento de datos	Quinto nivel, procesos técnicos	Alto
Servidor Web	Hardware	Procesamiento de datos	Procesamiento de datos	Bajo
Portal Web	Software	Procesamiento de datos	Procesamiento de datos	Bajo
Servidor de Cursos	Hardware	Biblioteca Central	Cuarto nivel, laboratorio	Bajo
Plataforma de cursos	Software	Biblioteca Central	Cuarto nivel, laboratorio	Bajo
Antena internet	Hardware	Biblioteca Central	Cuarto nivel, laboratorio	Bajo

Fuente: elaboración propia.

4.1.2. Identificación de procesos en Biblioteca Central

A continuación se detallan los procesos que dan lugar al funcionamiento de la biblioteca, además se tomará en cuenta el *hardware*, *software*, comunicaciones y logística necesaria para que se desarrollen las actividades en Biblioteca Central.

- Adquisición de nuevas bibliografías
  - Recolección de sugerencias
  - Aprobación y priorización de la bibliografía a comprar
  - Proceso de compra

- Catalogación
  - Consulta de bases de catalogación
  - Ingreso al sistema
  - Escaneo de portada para el catalogo
  - Etiquetado y colocación de seguridad

- Recepción de tesis
  - Verificación del archivo digital contra el impreso
  - Extender certificado de recepción de tesis

- Prestamos de bibliografía
  - Búsqueda de material en la base de datos
  - Préstamos externos de material

- Cobro de cursos y multas
  - Cobros de multas y cursos

- Alquiler de salas
    - Control prestamos y tecnología

- Certificar solvencia de biblioteca
    - Verificación del estado del usuario
    - Pago de multas pendientes

- Cursos de computación
    - Inscripción a cursos
    - Impartir cursos
    - Extender diplomas
    - Hacer exámenes de suficiencia

4.1.2.1. Proceso de selección y adquisición de nuevas bibliografías

En este proceso se recopila y analiza una lista de propuestas de nuevas bibliografías efectuada por el usuario a través de la página web:

http://biblioteca.usac.edu.gt/sugerencia.php

Posteriormente, se cotiza el material en diferentes editoras y distribuidoras de libros en Guatemala con el objetivo de realizar la compra de múltiples ejemplares con base en las cotizaciones que mejor convenga a la biblioteca, tomando en cuenta aspectos de calidad, tiempo de entrega, precio y ofertas o beneficios por múltiples compras.

Tabla X. **Proceso adquisición nuevas bibliografías**

Nombre del sistema	Descripción	Critico	Tipo de sistema (PC/servidor/ mainframe)	No de equipos con la aplicación	Responsable	Contacto técnico
Recolección de sugerencias	Obtener una lista de bibliografías requeridas por los usuarios	2	Servidor del sitio web y PC del encargado	2	Jefe de informatica	Rectoría, división de informática
Compra	Hacer un desembolso económico a cambio de material	1	PC del encargado	1	Jefe de procesos tecnicos	Procesos técnicos.

Fuente: elaboración propia.

Tabla XI. ***Hardware* en la adquisición de nuevas bibliografías**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
Servidor Web	Ubuntu server	Dell	1	Rectoría
PC	Windows xp	Dell	3	Biblioteca Central

Fuente: elaboración propia.

Tabla XII. **Otros activos en la adquisición de nuevas bibliografías**

Descripción	Tipo	Criticidad	Localización
Teléfono	Comunicaciones	1	Planta, Biblioteca Central

Fuente: elaboración propia.

4.1.2.2. Proceso de catalogación

La catalogación es un proceso fundamental para biblioteca central, es a través de esta actividad que se clasifican los libros, tesis, revistas, folletos, videos y material audio visual nuevo. Con base en criterios bibliotecológicos y con herramientas, tales como: diccionarios de apellidos, de temas y tesauros los bibliotecólogos de biblioteca organizan y catalogan las nuevas adquisiciones.

Tabla XIII. **Procesos para la catalogación**

Nombre del sistema	Descripción	Critico	Tipo de sistema (PC/servidor/ mainframe)	No de equipos con la aplicacion	Responsable	Contacto técnico
Consulta	Consulta a diccionario bibliotecológico	1	PC	6	Procesos técnicos	Jefe de informatica
Distribución	Distribución del material bibliográfico a su respectiva sección	3	PC	6	Procesos técnicos	Jefe de procesos tecnicos
Etiquetado	Colocar código de barras y etiquetas conteniendo la clasificación	1	PC	6	Procesos técnicos	Jefe de procesos tecnicos

Fuente: elaboración propia.

Tabla XIV. ***Hardware* para la catalogación**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
PC	Acceso a internet	Dell	2	Quinto nivel, procesos técnicos
impresora	Laser	Hp	2	Quinto nivel, procesos técnicos
Lector código barras	Lector de código de barras para las etiquetas		2	Quinto nivel, procesos técnicos

Fuente: elaboración propia.

Tabla XV. **Proceso de consulta en catalogación**

Nombre del sistema	Descripción	Critico	Tipo de sistema (PC/ servidor/ mainframe)	No de equipos con la aplicación	Responsable	Contacto técnico
Consulta	Consulta a diccionario bibliotecológico.	1	PC	6	Procesos técnicos	Jefe de informatica
Distribución	Distribución del material bibliográfico a su respectiva sección.	3	PC	6	Procesos técnicos	Jefe de procesos tecnicos
Etiquetado	Colocar código de barras y etiquetas conteniendo la clasificación	1	PC	6	Procesos técnicos	Jefe de procesos tecnicos

Fuente: elaboración propia.

Tabla XVI. ***Hardware* para consulta en catalogación**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
PC	Acceso a internet	Dell	2	Quinto nivel, procesos técnicos
Impresora	laser	Hp	2	Quinto nivel, procesos técnicos
Lector código barras	Lector de código de barras para las etiquetas		2	Quinto nivel, procesos técnicos

Fuente: elaboración propia.

Tabla XVII**.** **Material para catalogación**

Descripción	Tipo	Criticidad	Localización
Etiquetas	Adheribles imprimibles	2	Quinto nivel, procesos técnicos

Fuente: elaboración propia.

4.1.2.3. Proceso de recepción de tesis

Es el proceso que se encarga de recibir las tesis nuevas que los estudiantes entregan a Biblioteca Central como requisito de graduación, con la finalidad de enriquecer el contenido de dicha institución.

Se verifica que la tesis cumpla con los estándares aceptados por la universidad, así como, que el material físico coincida con el material digital. Finalmente, se extiende una constancia al interesado de haber entregado los ejemplares requeridos y que estos fueron verificados y aceptados.

Tabla XVIII. **Procesos en recepción de tesis**

Nombre del sistema	Descripción	Crítico	Tipo de sistema (PC/ servidor/ mainframe)	No de equipos con la aplicación	Responsable	Contacto técnico
Verificación de digital	Verificación que el contenido digital coincida con el contenido físico	2	PC	2	Tesario interno	Cuarto nivel, tesis

Fuente: elaboración propia.

Tabla XIX. ***Hardware* en la recepción de tesis**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
Lector de CD	Cd /DVD	Hp, Compaq 3M, Dell	2	Cuarto nivel, tesis

Fuente: elaboración propia.

4.1.2.4. Proceso para préstamos de bibliografía

El préstamo de bibliografía es el proceso más importante de Biblioteca Central, pues una de sus funciones es prestar a sus usuarios, el material de consulta que este está buscando.

Para llevar a cabo este proceso, el usuario busca en el catálogo el material que necesita, para la búsqueda puede utilizar internet en la página de biblioteca:

www.biblioteca.usac.edu.gt

o a través de las computadoras instaladas en el segundo nivel del edificio.

Con base en la catalogación del material, el usuario pueda adquirirlo en: si es tesis debe dirigirse al quinto nivel; si es audiovisual, al cuarto nivel; y, finalmente, si es libro, revista o folleto, al tercer nivel (esta información es desplegada en pantalla a la hora de la búsqueda).

Finalmente, cuando el usuario encuentra la información que necesita, este puede consultar el material dentro de Biblioteca Central, para el préstamo interno o externo el estudiante debe identificarse previamente como alumno activo de la Universidad de San Carlos.

Tabla XX. **Proceso de préstamos de bibliografía**

Nombre del sistema	Descripción	Crítico	Tipo de sistema (PC/ servidor/ mainframe)	No de Equipos con la aplicación	Responsable	Contacto técnico
Glifos	Sistema para manejo de material bibliográfico	1	Servidores	2	Procesos técnicos	Jefe de informatica
	Terminal de trabajo	2	Computadoras	6	Procesos técnicos	Jefe de informatica
Maxell RFID	Sistema para inventario de materiales bibliográficos a través de RFID	2	Computadoras	2	Procesos técnicos	Jefe de informatica

Fuente: elaboración propia.

Tabla XXI. ***Hardware* para préstamos de bibliografía**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
Lector de barras	Ninguno	Ninguno	2	Tercer nivel, prestamos
Lector RFID	Lectora conectada con el software Maxell y con la memoria conteniendo la base de datos	Maxell	2	Tercer nivel, prestamos

Fuente: elaboración propia.

4.1.2.5. Proceso de cobro de cursos y multas

Es el proceso que verifica cuándo un estudiante ha excedido el tiempo establecido para préstamos de material externo y aplica una penalización por cada día fuera de lo establecido. El cobro de cursos, exámenes por suficiencia y multas se lleva a cabo en el cuarto nivel.

Los ingresos en efectivo son registrados en un recibo extendido por la Universidad de San Carlos de Guatemala.

Tabla XXII. **Proceso de cobro de cursos y multas**

Nombre del sistema	Descripción	Crítico	Tipo de sistema (PC/ servidor/ mainframe)	No de equipos con la aplicación	Responsable	Contacto técnico
Cobros	Sistema de caja para llevar control de los ingresos	1	Computadora	2	Devoluciones	Jefe de informatica
Cupo/ asistencia	Programa de control académico	3	Computadora	1	Instructóres	Cuarto nivel, laboratorio de computo

Fuente: elaboración propia.

Tabla XXIII. ***Hardware* para el cobro de multas**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
Computadóra	Programa proporcionado por rectoría	Dell	2	Tercer nivel, devoluciones
Computadóra	Control académico	Dell	3	Cuarto nivel, laboratorio de cómputo

Fuente: elaboración propia.

Tabla XXIV. **Otros materiales para el cobro de cursos y multas**

Descripción	Tipo	Criticidad	Localización
Impresora	Matriz	2	Tercer nivel, devoluciones
Impresora	Inyección	3	Cuarto nivel, laboratorio de cómputo

Fuente: elaboración propia.

4.1.2.6. Proceso de alquiler de salas

El alquiler de salas se realiza a través de un oficio de solicitud dirigido a la jefatura de biblioteca, indicando el día, hora, número de personas que van hacer uso de la misma y el equipo que necesitaran en la sala.

Con base en esta solicitud se verifica el estado de reservaciones y si está disponible se otorga en alquiler de la sala, en caso contrario, el encargado del préstamo de salas en Biblioteca Central propone una fecha en la cual haya disponibilidad.

Finalmente, el encargado envía los requerimientos al encargado de laboratorio para que este se asegure que estén instalados el día y la hora en que los ha solicitado el usuario.

Tabla XXV. **Proceso de alquiler de salas**

Nombre del sistema	Descripción	Crítico	Tipo de sistema (PC/ servidor/ mainframe)	No de equipos con la aplicación	Encargado	Contacto Técnico
Control prestamos y tecnología	Programa que lleva el control de las salas prestadas y que tecnologías se requieren	2	computador	1	Jefa de servicios especiales	Cuarto nivel, Encargado de laboratorio

Fuente: elaboración propia.

Tabla XXVI. **Proceso de alquiler de salas**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
Computador	Windows xp y Excel 2007	Dell	3	Tercer nivel, oficina de servicios especiales

Fuente: elaboración propia.

4.1.2.7. Proceso para certificar solvencia de Biblioteca Central

La certificación de solvencias es un proceso que se lleva a cabo en Biblioteca Central y en ella se hace constar que el estudiante universitario esta solvente en cuanto a préstamo de material externo.

Las constancias son utilizadas por los estudiantes para renovar su carné estudiantil, para gestionar trámites de graduación y para inscribirse en la universidad.

Tabla XXVII. ***Software* para gestionar usuarios y solvencias**

Nombre del sistema	Descripción	Crítico	Tipo de sistema (PC/ servidor/ mainframe)	No de equipos con la aplicación	Responsable	Contacto técnico
Glifos	Status del usuario	2	Computador	1	Devoluciones	Jefe de informatica

Fuente: elaboración propia.

Tabla XXVIII. ***Hardware* para solvencias**

Tipo de hardware	Detalles del modelo/ configuración	Distribuidor	Criticidad	Localización
Computadora	Conectada a la red	Dell	2	Tercer nivel, devoluciones

Fuente: elaboración propia.

Tabla XXIX. **Otro equipo utilizado para extender solvencias**

Descripción	Tipo	Criticidad	Localización
Impresora	Matriz	2	Tercer nivel, devoluciones
Carne	Personal	1	Portación por el estudiante

Fuente: elaboración propia.

4.1.2.8. Proceso de impartir cursos de computación

Los cursos de computación se imparten en horarios de 8:00 AM a 1:00 PM, y de 2:00 PM a 7:00 PM, de lunes a viernes y días sábado, de 8:00 AM a 12:00 PM y de 2:00 PM a 5:00 PM.

Los cursos se planifican en forma mensual y la información de los mismos, horarios y contenido está disponible en carteleras ubicadas en el laboratorio de computación o en la página web oficial de Biblioteca Central:

http://www.biblioteca.usac.edu.gt/detalle_curso.php

El procedimiento para participar en los cursos es: consultar los horarios publicados, realizar el pago correspondiente en el 3er nivel de Biblioteca Central sección de devoluciones, con el recibo de pago asignarse el curso en el laboratorio de computación.

Tabla XXX. **Proceso de cursos**

Nombre del sistema	Descripción	Critico	Tipo de sistema (PC/ servidor/ mainframe)	No de equipos con la aplicación	Responsable	Contacto técnico
Windows xp y Office 2007	Sistema operativo xp y Office 2007	2	Computadóra	20	Instructor	Jefe de servicios especiales
Windows xp y Office 2003	Sistema operativo xp y Office 2003	2	Computadóra	15	Instructor	Jefe de servicios especiales

Fuente: elaboración propia.

Tabla XXXI. ***Hardware* para cursos**

Tipo de hardware	Detalles del Modelo/ configuración	Distribuidor	Criticidad	Localización
Computadóra	Windows xp y Office 2007	Dell	2	Cuarto nivel, laboratorio de computación 1
Computadóra	Windows xp y Office 2003	Dell	2	Cuarto nivel, laboratorio de computación 2

Fuente: elaboración propia.

Tabla XXXII. **Otros para cursos**

Descripción	Tipo	Criticidad	Localización
Antena inalámbrica	dlink	3	Cuarto nivel, laboratorio de computación 2

Fuente: elaboración propia.

4.1.3. Identificación de amenazas en Biblioteca Central

De la lista de amenazas se marcaron las que pueden afectar a Biblioteca Central en su situación actual.

Tabla XXXIII. **Listado de amenazas a los que Biblioteca Central está expuesta**

AMENAZAS	POSIBILIDAD
DESASTRES NATURALES	
Huracanes	No
Inundaciones	No
Incendios	Si

AMENAZAS	POSIBILIDAD
DAÑOS ACCIDENTALES	
Fuego fortuito	Si
Inundaciones	NO
Fallo del aire acondicionado	Si
Exceso de humedad	Si
Humo, gases tóxicos	No
Subida de tensión	Si
Fallo de suministro eléctrico	Si
Fallo de la UPS	Si
Accidentes del personal	Si
Capacidad inadecuada de las comunicaciones	Si
Fallo/degradación del hardware	Si
Fallo/degradación de las comunicaciones	Si
Errores de operación	Si
Fallos en las copias de seguridad	Si
Fallos de los sistemas de autenticación/autorización	No
Pérdida de confidencialidad	No
Incumplimientos legales	No

Continuación tabla XXXIII

AMENAZAS	POSIBILIDAD
ATAQUES INTENCIONADOS	
Explosivos	No
Fuego intencionado	No
Accesos no autorizados al edificio	No
Actos de vandalismo	No
Radiaciones electromagnéticas	No
Robos intencionados	Si
Manipulación de datos/software	Si
Manipulación de hardware	No
Uso de software por personal no autorizado	No
Acceso no autorizados a datos de la biblioteca	No
Software malicioso	Si
Robo de equipos	Si
Robo de documentos	Si
Robo de software	No
Descarga de software no controlada	Si
Interceptación de las líneas de comunicación	No
Manipulación de las líneas de comunicación	No
Abuso de privilegios de acceso	No
Introducción de virus en los sistemas	No
Troyanos	Si
Ataques por ingeniería social	No
Bombas lógicas	No
Ataques de denegación de servicio	Si
Errores intencionados	No
Copias incontroladas de documentos/software/datos	Si
Errores en el mantenimiento	No
Corrupción de datos	No
Incumplimientos legales intencionados	No

Fuente: elaboración propia.

4.1.4. Evaluación de vulnerabilidades en Biblioteca Central

Con base en la tabla de vulnerabilidades ubicada en los anexos de esta tesis, se llevó a cabo un estudio de cada aspecto a través de visitas a Biblioteca Central y entrevistas al personal de la mencionada institución, se obtuvo como resultado, el siguiente cuadro de estado de vulnerabilidades.

Tabla XXXIV. **Listado a los que Biblioteca Central esta vulnerable**

Vulnerabilidad	Nivel de protección	Posibilidad
Existencia de materiales inflamables como papel o cajas	¿Existen sensores de incendios?	No
Cableado inapropiado	¿Existen estándares en el cableado?	Si
Ancho de banda inapropiado	¿Está estructurada la red informática de acuerdo a las demandas tecnológicas?	Si
Suministro eléctrico inapropiado	¿El edificio cuenta con planta generadora externa?	No
Mantenimiento inapropiado del servicio técnico	¿Se elabora un mantenimiento exhaustivo periódicamente?	Si
Educación inadecuada del personal en virus y malware	¿Existe capacitación acerca de informática para el personal?	No
Políticas de firewall inadecuadas	¿Hay auditoria de redes?	No
Política de seguridad de la información inadecuada	¿Existe un plan conteniendo las políticas de seguridad en cuanto a la información?	No
Derechos de acceso incorrectos	¿El personal cuenta con un rol específico basado en su usuario y contraseña?	Si
Ausencia de un sistema de extinción automática de fuegos/humos	¿Hay extintores en el edificio y se verifican frecuentemente?	Si
Ausencia de backup	¿Hay un plan de backup?	Si
Ausencia de control de cambios de configuración eficiente y efectiva	¿Existe documentación sobre los sistemas y sus cambios?	No
Ausencia de mecanismos de identificación y autenticación	¿Existe sistema de identificación por carne o biométrica?	No
Ubicación física en un área susceptible de desastres naturales	¿Se encuentra ubicada la biblioteca en un lugar susceptible de desastres naturales?	no
Carencia de software antivirus	¿Existe antivirus en todas las maquinas y servidores además de contarse con un plan de actualización?	Si
Descarga incontrolada y uso de software de Internet	¿En la red privada como la red pública se encuentran controladas por proxy?	No
Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales	¿Se utilizan algoritmos de encripción dentro de la comunicación en la red interna?	No
Protección física de equipos inadecuada	¿Existe protección física extra a los servidores de datos?	No
Definición de privilegios de acceso inadecuada	¿Se manejan roles de usuarios y contraseñas?	Si
Ausencia de un Plan de recuperación de incidentes	¿Existen medidas de continuidad?	No
Fallo del suministro Eléctrico	¿Existen unidades de suministro Eléctrico Alternativo?	Si
Perdida de información clave para la biblioteca	¿Se realizan copias de seguridad periódicamente?	No
Perdida de servicios por infección de virus	¿Están los equipos protegidos con un antivirus?	Si

Fuente: elaboración propia.

4.1.5. Evaluación del impacto en Biblioteca Central

Tabla XXXV. **Evaluación de impacto en Biblioteca Central**

Descripción	Probabilidad	Impacto
DESASTRES NATURALES		
Lluvia de arena volcanica	Alta	Medio
Huracanes	Baja	Medio
Inundaciones	Baja	Bajo
Incendios Masivos	Baja	Alto

Descripción	Probabilidad	Impacto
DAÑOS ACCIDENTALES		
Fuego fortuito	Media	Alto
Inundaciones	Baja	Bajo
Fallo del aire acondicionado	Media	Bajo
Exceso de humedad	Media	Alto
Humo, gases tóxicos	Baja	Medio
Subida de tensión	Alta	Medio
Fallo de suministro eléctrico	Alta	Alto
Fallo de la UPS	Alta	Medio
Accidentes del personal	Media	Medio
Capacidad inadecuada de las comunicaciones	Media	Medio
Fallo/degradación del hardware	Media	Medio
Fallo/degradación de las comunicaciones	Media	Medio
Errores de operación	Alta	Medio
Fallos en las copias de seguridad	Media	Alto
Fallos de los sistemas de autenticación / autorización	Media	Medio
Pérdida de confidencialidad	Media	Medio

Continuación tabla XXXV

Descripción	Probabilidad	Impacto
ATAQUES INTENCIONADOS		
Explosivos	Bajo	Medio
Fuego intencionado	Medio	Alto
Accesos no autorizados al edificio	Medio	Bajo
Actos de vandalismo	Bajo	Medio
Radiaciones electromagnéticas	Bajo	Bajo
Robos intencionados	Alta	Medio
Manipulación de datos/software	Medio	Medio
Manipulación de hardware	Medio	Medio
Uso de software por personal no autorizado	Medio	Medio
Acceso no autorizados a datos de la biblioteca	Medio	Alto
Software malicioso	Alto	Medio
Robo de equipos	Alto	Alto
Robo de documentos	Alto	Medio
Robo de software	Bajo	Bajo
Descarga de software no controlada	Alta	Medio
Interceptación de las líneas de comunicación	Media	Bajo
Manipulación de las líneas de comunicación	Baja	Bajo
Abuso de privilegios de acceso	Media	Medio
Introducción de virus en los sistemas	Alta	Medio
Troyanos	Alta	Medio
Ataques por ingeniería social	Baja	Bajo
Bombas lógicas	Baja	Bajo
Ataques de denegación de servicio	Media	Alto
Errores intencionados	Baja	Medio
Copias incontroladas de documentos/software/datos	Baja	Bajo
Errores en el mantenimiento	Baja	Bajo
Corrupción de datos	Baja	Bajo

Fuente: elaboración propia.

4.1.6. Evaluación del riesgo en Biblioteca Central

La evaluación de riesgos es el resultado de medir la probabilidad de ocurrencia y el impacto que represente para la continuidad de las operaciones.

El siguiente análisis de riesgos para Biblioteca Central fue elaborado con base en la tabla propuesta en el anexo 3 de esta tesis.

Tabla XXXVI. **Evaluación de riesgos en Biblioteca Central**

Descripción	Probabilidad	Impacto	Riesgo
DESASTRES NATURALES			
Lluvia de arena volcanica	Alta	Media	Alto
Huracanes	Baja	Medio	Bajo
Inundaciones	Baja	Bajo	Bajo
Incendios	Bajo	Alto	Medio

Descripción	Probabilidad	Impacto	Riesgo
Daños Accidentales			
Fuego fortuito	Media	Alto	Ato
Inundaciones	Baja	Bajo	Bajo
Fallo del aire acondicionado	Media	Bajo	Bajo
Exceso de humedad	Media	Alto	Alto
Humo, gases tóxicos	Baja	Medio	Bajo
Subida de tensión	Alta	Medio	Alto
Fallo de suministro eléctrico	Alta	Alto	Alto
Fallo de la UPS	Alta	Medio	Alto
Accidentes del personal	Media	Medio	Medio
Capacidad inadecuada de las comunicaciones	Media	Medio	Medio
Fallo/degradación del hardware	Media	Medio	Medio
Fallo/degradación de las comunicaciones	Media	Medio	Medio
Errores de operación	Alta	Medio	Alto
Fallos en las copias de seguridad	Media	Alto	Alto
Fallos de los sistemas de autenticación/autorización	Media	Medio	Medio
Pérdida de confidencialidad	Media	Medio	Medio

Continuación tabla XXXVI

Descripción	Probabilidad	Impacto	Riesgo
Ataques Intencionados			
Explosivos	Bajo	Medio	Bajo
Fuego intencionado	Medio	Alto	Alto
Accesos no autorizados al edificio	Medio	Bajo	Bajo
Actos de vandalismo	Bajo	Medio	Bajo
Radiaciones electromagnéticas	Bajo	Bajo	Bajo
Robos intencionados	Alta	Medio	Alto
Manipulación de datos/software	Medio	Medio	Medio
Manipulación de hardware	Medio	Medio	Medio
Uso de software por personal no autorizado	Medio	Medio	Medio
Acceso no autorizados a datos de la biblioteca	Medio	Alto	Alto
Software malicioso	Alto	Medio	Alto
Robo de equipos	Alto	Alto	Alto
Robo de documentos	Alto	Medio	Alto
Robo de software	Bajo	Bajo	Bajo
Descarga de software no controlada	Alta	Medio	Alta
Interceptación de las líneas de comunicación	Media	Bajo	Bajo
Manipulación de las líneas de comunicación	Baja	Bajo	Bajo
Abuso de privilegios de acceso	Media	Medio	Medio
Introducción de virus en los sistemas	Alta	Medio	Alto
Troyanos	Alta	Medio	Alto
Ataques por ingeniería social	Baja	Bajo	Bajo
Bombas lógicas	Baja	Bajo	Bajo
Ataques de denegación de servicio	Media	Alto	Alto
Errores intencionados	Baja	Medio	Bajo
Copias incontroladas de documentos/software/datos	Baja	Bajo	Bajo
Errores en el mantenimiento	Baja	Bajo	Bajo
Corrupción de datos	Baja	Bajo	Bajo

Fuente: elaboración propia.

4.2. Análisis del impacto (BIA)

Para desarrollar el plan es necesario elaborar un inventario de los procesos críticos de Biblioteca Central, estableciendo los tiempos de recuperación de los mismos antes de incurrir en pérdidas graves. Para llevar a cabo esta actividad fue necesario realizar una entrevista con los responsables de los procesos, se obtuvo la siguiente información:

Tabla XXXVII. **Análisis de impacto en Biblioteca Central**

Proceso	Subproceso	Breve descripción	Frecuencia (Diario/ Semanal/ Mensual)	Responsable
Adquisición de nuevas bibliografías	Cotización y compra o donación	Basados en la página web la comisión toma las propuestas y la cotiza, cuando se ha aprobado la compra se ejecuta el desembolso.	Mensual	Jefe de procesos técnicos
Catalogación	--	En base a criterios bibliotecológicos, se clasifican los materiales bibliográficos según el contenido.	Diario	Jefe de procesos técnicos
Recepción Tesis	Revisión y verificación de contenido	Verificación que el material físico coincida con el material digital.	Diario	Jefe de servicios especiales
Préstamo de bibliografías	Validación de vigencia de carne o documento de identificación	Identificando al prestamista, se busca el material solicitado a través del número de catalogación y se anota en el sistema de préstamos.	Diario	Jefe de prestamos
Cursos de computación	Inscripción, desarrollo del curso y certificación.	Se publican los cursos de computación, los alumnos se inscriben y participan de la capacitación al finalizar se ejecuta una evaluación y se extienden diplomas.	Mensual	Instructor
Alquiler de salas	Toma de requerimientos	Se verifica la disponibilidad de la sala y se toman requerimientos tecnológicos a instalar en la sala.	Mensual	Jefe de servicios especiales
Certificar Solvencia en Biblioteca	--	Se consulta la base de información de préstamos y en caso de no tener libros prestados se extiende solvencia.	Diaria	Jefe de prestamos
Cobro de cursos y multas	Verificación de estado actual del curso o del alumno.	Se verifica el número de días excedente a los reglamentados y se cobra la multa. Se verifica el cupo de los cursos y en caso de no estar lleno se cobra el curso.	Mensual	Área de devoluciones

Fuente: elaboración propia.

Bajo los lineamientos descriptivos de Herrera, Salomon. Reporte anual estado informatico de Biblioteca Central. 2009.

4.2.1. Relación para cada proceso del negocio en Biblioteca Central

Tabla XXXVIII. **Relación procesos - funciones de Biblioteca Central**

Proceso	Adquisición de nuevas bibliografías
Relacion	Recolección de sugerencias
	Aprobación y priorización de la bibliografía a comprar
	Proceso de compra

Proceso	Catalogación
Relacion	Consulta de bases de catalogación
	Ingreso al sistema
	Escaneo de portada para el catalogo
	Etiquetado y colocación de seguridad

Proceso	Recepción de Tesis
Relacion	Verificación del archivo digital contra el impreso
	Extender certificado de recepción de tesis

Proceso	Prestamos de Bibliografía
Relacion	Búsqueda de material en la base de datos
	Préstamos externos de material

Proceso	Cobro de Cursos y multas
Relacion	Cobros de multas y cursos
	Verificación de cupo para cursos

Proceso	Alquiler de Salas
Relacion	Control prestamos y tecnología

Proceso	Certificar solvencia de biblioteca
Relacion	Verificación del estado del usuario
	Pago de multas pendientes

Proceso	Cursos de Computación
Relacion	Inscripción a cursos
	Impartir cursos
	Extender diplomas
	Hacer exámenes de suficiencia

Fuente: elaboración propia.

4.2.2. Relación para cada aplicación utilizada en Biblioteca Central

Tabla XXXIX. **Relación aplicaciones - funciones de Biblioteca Central**

Activo/Descripción	Localización	Relación
Aplicación para bibliotecas (Glifos)	Quinto nivel, procesos técnicos	El sistema Glifos es el encargado de almacenar todo el material bibliográfico que se encuentra disponible para consultas, por tato es el catalogo de la bibliteca.
Aplicación de cobros	Tercer nivel, devoluciones	Es el sistema encargado de llevar control del ingreso de dinero.
Aplicación de inventario de material bibliográfico	Tercer nivel, prestamos	Es el sistema encargado de monitoriar las bibliografias prestadas, las existentes y las que estan en mantenimiento.
Portal Web	Procesamiento de datos	Difusion de informacion institucional.
Plataforma de cursos	Cuarto nivel, Laboratorio	Sistema para llevar control de alumnos, notas por cada curso que se imparte.
Lectora inalámbrica RFID	Tercer nivel, prestamos	Sistema para comparar el estado fisico de los anaqueles con el estado de la base de datos en cuanto a libros prestados.

Fuente: elaboración propia.

4.2.3. Aporte de cada departamento y usuario en Biblioteca Central

Tabla XL. **Función de los departamentos en Biblioteca Central**

Nivel	Departamento	Función / Aporte
Segundo	Jefatura	Dirección y coordinación de todas las actividades administrativas, académicas y financieras de Biblioteca Central.
Segundo	Consultas	Los usuarios consultan el catalogo de material disponible para consultas.
Tercero	Deposito legal	Almacenamiento y protección de material bibliográfico que es edición limitada y que son ejemplares exclusivos.
Tercero	Anaquel abierto	Consulta en sala y préstamo externo de material bibliográfico.
Cuarto	Tesis interna	Préstamo interno de tesis y recepción de nuevas tesis.
Cuarto	Laboratorio de cómputo	Impartir cursos de computación y exámenes de suficiencia. El laboratorio también es rentado para capacitaciones.
Cuarto	Salas	Alquiler de salas totalmente equipadas con sistema de video conferencias, cañonera, puntos de red, aire acondicionado especialmente para conferencias
Quinto	Cubículos	Préstamo de espacio físico para estudio de examen general privado.
Quinto	Adquisiciones	Recolección de sugerencias para nuevo material bibliográfico, cotización y compra del mismo a las editoriales.
Quinto	Catalogación	Clasificación basado en estándares para que la búsqueda y selección de material sea rápida y fácil.
Quinto	Informática	Monitoreo a la red, administración de la base de datos, mantenimiento al portal web y a la aplicación, mantenimiento a servidores y a computadoras del personal y de consulta.
Quinto	Biblioteca la paz	Préstamo de material bibliográfico exclusivamente asociado al tema del conflicto armado interno en Guatemala.
Quinto	Préstamo tesis	Préstamo de tesis para consulta externa.

Fuente: elaboración propia.

4.2.4. Máximo tiempo de interrupción en los procesos

Tabla XLI. **Tiempo máximo de recuperación en adquisición de nuevas bibliografías**

Proceso	Necesidad de recuperación	Criticidad
Adquisición de nuevas bibliografías	De 15 – 30 días	2

Fuente: elaboración propia.

El proceso de adquisición de nuevas bibliografías no es tan crítico, es decir, es importante mantener actualizado el material pero no es urgente que se tengan que adquirir. Por tal razón, la recuperación preferiblemente debe ser antes del mes y no tiene un alto impacto a corto plazo.

Tabla XLII. **Tiempo máximo de recuperación en la catalogación**

Proceso	Necesidad de recuperación	Criticidad
Catalogación	Menos de 15 días	2

Fuente: elaboración propia.

El proceso de catalogación es medianamente crítico, debido a que las nuevas adquisiciones pueden esperar cuando mucho 15 días para ser publicadas, pasado este tiempo es pérdida para la biblioteca porque se des actualiza la información del material adquirido.

Tabla XLIII. **Tiempo máximo de recuperación en la recepción de tesis**

Proceso	Necesidad de recuperación	Criticidad
Recepción Tesis	De 1 – 5 días	1

Fuente: elaboración propia.

La recepción de tesis es un proceso altamente crítico, porque los estudiantes deben entregar a Biblioteca Central un ejemplar de su tesis para poder graduarse, por tanto, si el proceso de recepción de tesis se paraliza, los estudiantes tienen que atrasar la fecha de su graduación.

Tabla XLIV. **Tiempo máximo de recuperación para préstamos de bibliografía**

Proceso	Necesidad de recuperación	Criticidad
Prestamos de Bibliografía	De 1 – 2 días	1

Fuente: elaboración propia.

El préstamo de bibliografía es el proceso más crítico y de mayor importancia para Biblioteca Central debido a que la naturaleza de esta institución es el préstamo de material bibliográfico.

En caso de interrumpir este proceso, se pierde imagen ante el usuario lo cual es desprestigio para la biblioteca y para la Universidad de San Carlos en general, por lo cual el servicio debe restaurarse, como máximo, en 2 días.

Tabla XLV. **Tiempo máximo de recuperación en los cursos de computación**

Proceso	Necesidad de recuperación	Criticidad
Cursos de Computación	Menos de 1 mes	3

Fuente: elaboración propia.

Los cursos de computación no son críticos para Biblioteca Central, es decir, puede pasar hasta un mes sin impartir cursos.

Tabla XLVI**.** **Tiempo máximo de recuperación en los alquileres de salas**

Proceso	Necesidad de recuperación	Criticidad
Alquiler salas	Menos de 1 mes	3

Fuente: elaboración propia.

Las salas es un proceso poco crítico al igual que los cursos de computación, debido a que este no es el objetivo primordial de Biblioteca Central.

Tabla XLVII. **Tiempo máximo de recuperación de certificar solvencias de biblioteca**

Proceso	Necesidad de recuperación	Criticidad
Certificación solvencia de biblioteca	De 5 a 15 días	2

Fuente: elaboración propia.

Los certificados de solvencia de Biblioteca Central son utilizados como prerrequisito para graduación e inscripción de año estudiantil, estos se extienden en el 3er nivel de la biblioteca y su tiempo de recuperación debe ser menor a 15 días, de lo contrario se atrasan los trámites en la universidad.

Tabla XLVIII. **Tiempo máximo de recuperación en los cobros de multas y cursos**

Proceso	Necesidad de recuperación	Criticidad
Cobro de cursos y multas	De 15 a 20 días	3

Fuente: elaboración propia.

El cobro de cursos y multas tiene criticidad 3, esto quiere decir que no impacta fuertemente una interrupción en el proceso, no obstante esta debe restaurarse de 15 a 20 días máximo.

Tabla XLIX. **Tiempo máximo de recuperación del internet público**

Proceso	Necesidad de recuperación	Criticidad
Internet publico	Menos de 3 meses	3

Fuente: elaboración propia.

El internet público que presta Biblioteca Central es un servicio poco crítico, este es un servicio extra que se le brinda al estudiante, además de existir múltiples redes públicas para el uso de los estudiantes de la Universidad de San Carlos de Guatemala.[11]

[11] Herrera, Salomon. Reporte anual estado informatico de Biblioteca Central. 2009.

4.2.5. Determinar y priorizar los procesos críticos en Biblioteca Central

Tabla L. **Priorización de procesos en Biblioteca Central**

Proceso	Prioridad
Adquisición de nuevas bibliografías	Bajo
Recolección de sugerencias	Bajo
Aprobación y priorización de la bibliografía a comprar	Bajo
Proceso de compra	Bajo
Catalogación	Medio
Consulta de bases de catalogación	Medio
Ingreso al sistema	Medio
Escaneo de portada para el catalogo	Bajo
Etiquetado y colocación de seguridad	Alto
Recepción de Tesis	Alto
Verificación del archivo digital contra el impreso	Medio
Extender certificado de recepción de tesis	Alto
Prestamos de Bibliografía	Medio
Búsqueda de material en la base de datos	Bajo
Préstamos externos de material	Medio
Cobro de Cursos y multas	Bajo
Cobros de multas y cursos	Bajo
Verificación de cupo para cursos	Bajo
Alquiler de Salas	Bajo
Control prestamos y tecnología	Bajo
Certificar solvencia de biblioteca	Alto
Verificación del estado del usuario	Alto
Pago de multas pendientes	Medio
Cursos de Computación	Bajo
Inscripción a cursos	Bajo
Impartir cursos	Medio
Extender diplomas	Medio
Hacer exámenes de suficiencia	Bajo

Fuente: elaboración propia.

4.2.6. Propuesta de Contramedidas TI para cada proceso en Biblioteca Central

Las recomendaciones propuestas están basadas en los riesgos y vulnerabilidades que se analizó en secciones anteriores a esta tesis, catalogando de acuerdo a su categoría y el tipo de contramedida.

Tabla LI. **Contramedidas recomendables para Biblioteca Central**

Descripción	Contramedida	Tipo de contramedida
Incendios	Múltiples detectores de Humo en cada nivel.	Monitoreo
	Extintores de humo colocados estratégicamente y bien señalizados.	Preventivo
Exceso de humedad	Múltiples sensores de humedad	Monitoreo
Subida de tensión	Utilizar ups y reguladores	Correctiva
Fallo de suministro eléctrico	Tener a mano una planta eléctrica	Correctiva
Fallo de la UPS		Preventivo
Errores de operación	Crear auditoria de operaciones	Monitoreo
Fallos en las copias de seguridad	Replicación de datos	Preventivo
	Plan de Back Up general	Correctivo
Robos intencionados	Alarma electromagnética	Correctivo
Acceso no autorizados a datos de la biblioteca	Creación de sesiones de usuarios	Preventivo
Software malicioso	Políticas de instalación y uso de periféricos del ordenador en base a rol de usuarios	Correctivo
Robo de equipos	Alarma electromagnética	Preventivo
Robo de documentos	Alarma electromagnética	Correctivo
Descarga de software no controlada	Servidor proxy	Preventivo
Introducción de virus en los sistemas	Múltiples firewall y auditoria de redes	Preventivo
Troyanos	Software anti-troyano y actualización de antivirus	Preventivo
Ataques de denegación de servicio	Auditoria de redes	Preventivo

Fuente: elaboración propia.

CONCLUSIONES

1. En la elaboración de la guía análisis y diseño para la implementación y mantenimiento del plan de continuidad de operaciones, se tomaron en cuenta aspectos tecnológicos, capital intelectual y factores externos que representen vulnerabilidad sobre la continuidad, basados en el análisis de impacto y análisis de riesgo.

2. En la guía se da a conocer los antecedentes del plan de continuidad para comprender y concientizar de los beneficios que aporta la implementación de este plan, así como, se analizó cómo la continuidad aporta valor a los servicios dentro del mercado competitivo.

3. Detalle de los aspectos fundamentales a tomar en cuenta para la elaboración de un plan de continuidad de operaciones basado en las tecnologías de la información TI de la empresa u institución.

4. En el caso de estudio llevado a cabo en Biblioteca Central se efectuó el análisis de riesgos, análisis de impacto y la elaboración de contramedidas que ayuden a mitigar las pérdidas tanto materiales como inmateriales a la hora de un siniestro, enfocado fundamentalmente en los datos a salvaguardar y los procesos que involucren tecnologías de la información.

5. En el desarrollo del plan de continuidad del caso de estudio, fue abordada la creación de los grupos y comités que ayuden a gestionar los procedimientos de recuperación, además, se definió sus responsabilidades en las diferentes etapas del plan.

6. Creación de un plan de pruebas y mantenimiento el cual garantiza mantener el plan de continuidad actualizado y que los resultados sean funcionales.

RECOMENDACIONES

1. En la fase de análisis y diseño de un plan de continuidad de negocios se debe asegurar que la gerencia no piense que es un asunto puramente técnico, debido a que por su naturaleza este plan funciona integralmente en toda la empresa o institución, incluyendo aspectos humanos y técnicos.

2. No se debe proyectar el plan de continuidad con una fecha final específica y establecida, si bien es cierto este inicia con el análisis y diseño, no es correcto pensar en un final, debido a que un plan acompaña a la empresa o institución a lo largo de la vida de ésta, por ello debe estar siempre preparados al momento de desastres, por tal motivo no tiene un fin establecido.

3. Aunque exista personal dedicado a velar por la continuidad de las operaciones no se debe permitir que toda la responsabilidad caiga sobre este grupo, sino presentarlo como un plan a cargo de este conjunto de personas, pero que involucra a todo el personal de la institución.

4. Al momento del desarrollo del plan se recomienda implementar procedimientos de recuperación y continuidad no solo para ocasiones de emergencia o siniestros totales, sino también pensar en un plan de operaciones que incluya procedimientos para siniestros parciales y situaciones riesgosas, en los cuales se aborda con una prevención.

5. Recomendar a los analistas y diseñadores no pensar en dar continuidad a las operaciones a través de realizar actividades repetidas o duplicadas, con ello se estará implementando más redundancia en los procesos.

6. Revisar continuamente el plan de continuidad para verificar que este esté ajustado a la realidad de la empresa o institución y en caso haya habido una variación, se debe modificar, inmediatamente, el plan para que este sea, en todo momento útil.

7. Tener muy en cuenta que el cliente lo que más estima es su tiempo, por tal razón, si la empresa o institución disminuye el tiempo de espera del cliente por servicio, éste estará satisfecho con el trabajo. Sin embargo, en tiempos de crisis o siniestro, es difícil garantizar el servicio; por tal motivo, el plan de continuidad ayuda a mantener el liderato de la organización.

BIBLIOGRAFÍA

1. Biblioteca Central Universidad de San Carlos de Guatemala. Manual insitucional. [en linea]. Editorial Universitaria. Disponible en web: <http://biblioteca.usac.edu.gt/manual_ins.pdf >, [consulta: 10 de enero de 2009].

2. The Business Continuity Institute. *About the business continuity institute*. [En línea]. Disponible en web: < http://www.thebci.org >, [consulta: 5 de diciembre de 2009].

3. Disaster Recovery Guide. *Disaster recovery guide*. [En línea]. Disponible en web: <http://disaster-recovery-guide.com>, [consulta: 21 de diciembre de 2009] .

4. GASPAR MARTÍNEZ, Juan. *El plan de continuidad de negocio: guía práctica para su elaboracion.* Madrid: DIAZ DE SANTOS, 2006. 206p. ISBN: 9788479786472.

5. GASPAR MARTINEZ, Juan. *Planes de contingencia.* Madrid: DIAZ DE SANTOS, 2004. 125 p. ISBN:978-84-7978-647-2.

6. HERRERA, Salomón. *Informe anual de la situacion informática en Biblioteca Central.* Informe inedito. Biblioteca Central de la Universidad de San Carlos de Guatemala, 2009. 20 p.

7. International Standards for Business, Government and Society. *International Standards for Business, Government and Society ISO*. [En línea]. Disponible en web: < http://www.iso.org/iso/home.htm >, [consulta: 15 de noviembre de 2009].

8. JIMÉNEZ, Laura del Pino. *Guia de desarrollo de un plan de continuidad de negocio.* Madrid : Nuevo Mundo del Saber, 2007. 145 p. ISBN: 978843574852.

9. MARCOMBO, Alexander. *Diseño de un sistema de gestion de seguridad de información.* Santiago de Chile : FUGA, 2007. 350 p. ISBN: 8426709761.

10. VILCHIS, Xavier. *Business continuity plan ¿Ya lo tiene?.* 2ª ed. Madrid : KPMG, 2009. 95 p. ISBN: 9843275678356.

ANEXOS

1. Sitios de interés

- http://www.contingencyplanning.com/ - revista de continuidad de negocio.
- http://www.globalcontinuity.com/ - portal *de business continuity plan.*
- http://www.thebci.org/pas56.htm - *business continuity institute*.
- http://www.disaster-recovery-guide.com/ - información y guías sobre continuidad.
- http://www.nist.org/ - mejores prácticas en seguridad informática.
- http://www.iss.net/ - base de datos de vulnerabilidades X-Force.
- http://nvd.nist.gov/ - base de datos de vulnerabilidades del NIST.
- http://www.securityfocus.com/ - base de datos de vulnerabilidades.
- http://www-5.ibm.com/services/es/portfolios/recuperacion.html - proveedor de servicios de continuidad de negocio.
- http://h20219.www2.hp.com/services/cache/9270-0-0-197-470.html - proveedor de servicios de continuidad de negocio.

2. Listado de vulnerabilidades

VULNERABILIDADES
Existencia de materiales inflamables como papel o cajas
Cableado inapropiado
Ancho de banda inapropiado
Suministro eléctrico inapropiado
Mantenimiento inapropiado del servicio técnico
Ausencia de mantenimiento
Educación inadecuada del personal en virus y *malware*
Políticas de *firewall* inadecuadas
Política de seguridad de la información inadecuada
Ausencia de política de seguridad
Derechos de acceso incorrectos
Ausencia de un sistema de extinción automática de fuegos/humos
Ausencia de *backup*
Ausencia de control de cambios de configuración eficiente y efectiva
Ausencia de mecanismos de identificación y autenticación
Ausencia de política de restricción de personal para uso licencias de *software*
Ubicación física en un área susceptible de desastres naturales
Carencia de *software* antivirus
Descarga incontrolada y uso de *software* de Internet

Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales
Protección física de equipos inadecuada
Personal sin formación adecuada
Incumplimientos legales (LOPD, Ley Sarbanes Oxley, etc.)
Definición de privilegios de acceso inadecuada
Ausencia de un plan de recuperación de incidentes

3. Lista de amenazas y riesgos

AMENAZAS	POSIBLE
DESASTRES NATURALES	
Huracanes	Si/No
Inundaciones	Si/No
Incendios	Si/No
DAÑOS ACCIDENTALES	
Fuego fortuito	Si/No
Inundaciones	Si/No
Fallo del aire acondicionado	Si/No
Exceso de humedad	Si/No
Humo, gases tóxicos	Si/No
Subida de tensión	Si/No
Fallo de suministro eléctrico	Si/No
Fallo de la UPS	Si/No
Accidentes del personal	Si/No
Capacidad inadecuada de las comunicaciones	Si/No
Fallo/degradación del *hardware*	Si/No
Fallo/degradación de las comunicaciones	Si/No
Errores de operación	Si/No
Fallos en las copias de seguridad	Si/No

Fallos de los sistemas de autenticación/autorización	Si/No
Pérdida de confidencialidad	Si/No
Incumplimientos legales	Si/No
ATAQUES INTENCIONADOS	
Explosivos	Si/No
Fuego intencionado	Si/No
Accesos no autorizados al edificio	Si/No
Actos de vandalismo	Si/No
Radiaciones electromagnéticas	Si/No
Robos intencionados	Si/No
Manipulación de datos/*software*	Si/No
Manipulación de *hardware*	Si/No
Uso de *software* por personal no autorizado	Si/No
Acceso no autorizados a datos de la biblioteca	Si/No
Software malicioso	Si/No
Robo de equipos	Si/No
Robo de documentos	Si/No
Robo de *software*	Si/No
Descarga de *software* no controlada	Si/No
Interceptación de las líneas de comunicación	Si/No
Manipulación de las líneas de comunicación	Si/No

Abuso de privilegios de acceso	Si/No
Introducción de virus en los sistemas	Si/No
Troyanos	Si/No
Ataques por ingeniería social	Si/No
Bombas lógicas	Si/No
Ataques de denegación de servicio	Si/No
Errores intencionados	Si/No
Copias incontroladas de documentos/*software*/datos	Si/No
Errores en el mantenimiento	Si/No
Corrupción de datos	Si/No
Incumplimientos legales intencionados	Si/No

4. Cuadros de recogida de datos

CUADRO DE PROCESOS

En este cuadro se escriben los procesos y subprocesos que componen la organización donde se va a desarrollar el plan de continuidad.

Proceso	Subproceso	Breve descripción	Frecuencia (Diario/Semanal Mensual)	Persona responsable

SISTEMAS QUE SOPORTAN EL PROCESO

En este apartado se anotan los componentes *hardware* que soportan los procesos.

Nombre del Sistema	Descripción	Criticidad	Tipo de Sistema (PC/Servidor/ Mainframe)	Nº de Equipos con la aplicación	Responsable	Contacto Técnicos

SISTEMAS QUE SOPORTAN EL PROCESO

En este cuadro se consignan los sistemas que soportan el proceso analizado.

Tipo de hardware	Detalles del Modelo/Configuración	Distribuidor	Criticidad	Localización

OTROS ACTIVOS

En este apartado se recogen todos aquellos activos (comunicaciones, datos, infraestructura, etc.), que forman parte del proceso y que son necesarios para dar continuidad al mismo en caso de interrupción.

Descripción	Tipo	Criticidad	Localización

TIEMPO MÁXIMO DE INTERRUPCIÓN

Para cada uno de los procesos, se determinará el tiempo máximo de interrupción, especificando cuántos días puede permanecer el proceso sin incurrir en pérdidas económicas graves.

Proceso	Necesidades de Recuperación	Criticidad