T E S I S

"GESTION DE CONTINUIDAD DEL NEGOCIO

EN CASO DE DESASTRE"

(DRP - Disaster Recovery Plan)

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A :

ARTURO MAGNANI ARRIETA

México, D.F., Febrero del 2011

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

*A la **Universidad Nacional Autónoma de México** y en especial a la **Facultad de Ingeniería** que me brindaron la oportunidad de formar parte de ellas.*

¡Gracias!

Página

Índice General…….……... 2
Índice de Figuras……...…….. 4
Índice de Tablas……..……. 5
Prefacio…….…… 6
Introducción……..…… 9

Capítulo I. Fundamento Metodológico 11
1.1 Objetivo y alcance…….….. 12
1.2 Justificación de la implementación..……..…… 12
1.3 Antecedentes de la empresa.……..…..……. 13

Capítulo II. Fundamento Teórico 14
2.1 Fundamento teórico…….……..….... 15
2.2 Análisis del negocio (BIA)……. 15
2.3 Tecnología de seguridad……...….. 16
2.4 Modelo de seguridad de McCumber……... 17
2.5 Estados de la información…….…… 17
2.6 Medidas de seguridad……..…… 18
2.7 La arquitectura de seguridad…… 19
2.8 La política de seguridad……. 19
2.9 Procedimientos y soportes…… 20
2.10 Enfoque del proyecto de seguridad…… 21
2.11 Estrategias y políticas de seguridad……... 22
2.12 Seguridad física y lógica…… 23
2.13 Seguridad en las comunicaciones…….. 24
2.14 Prevención y recuperación……..…… 24

Capítulo III. Plan de Recuperación de Desastres 26
3.1 La importancia de un plan de recuperación de desastres…….… 27
3.2 Razones para recurrir a un DRP……...….. 27
3.3 Actividades previas al desastre…….…….. 30
3.4 Actividades durante el desastre……... 33
3.5 Actividades después del desastre…….. 36

Capítulo IV. Acciones frente al tipo de Riesgos 39
4.1 Clase de riesgo: Incendio o Fuego…….…… 40
4.2 Procedimiento para: Antes, Durante y Después del Incendio…….. 41
4.3 Clase de riesgo: Robo común de equipos y archivos..... 42
4.4 Clase de riesgo: Vandalismo…… 43
4.5 Clase de riesgo: Equivocaciones…… 43
4.6 Clase de riesgo: Fallas en los equipos…….…….. 44
4.7 Clase de riesgo: Acción de virus informático…….…… 46
4.8 Clase de riesgo: Accesos no autorizados…….……. 47
4.9 Clase de riesgo: Fenómenos naturales…….. 47
4.10 Clase de riesgo: Robo de datos…….. 48
4.11 Clase de riesgo: Manipulación y sabotaje…….. 49
4.12 Simulacros…….. 50

Página

Capítulo V. Gestión de la Continuidad del Negocio (GCN / BCP) 52
5.1 Perspectiva general de la GCN…….. 53
5.2 ¿Qué es la BCP / GCN?..... 54
5.3 La GCN y la estrategia organizativa…….. 54
5.4 La GCN y su relación con la gestión de riesgo……. 55
5.5 Ventajas al incorporar GCN en una organización……. 55
5.6 Los beneficios de un programa GCN……. 57
5.7 Elementos del ciclo de vida del GCN……. 58
5.8 Las políticas de la GCN…… 59
5.9 Alcances del programa GCN…… 61
5.10 Gestión del programa GCN…….. 61
5.11 Gestión continua…… 62
5.12 Documentación…….. 65
5.13 Análisis del Impacto del Negocio (AIN)……. 67
5.14 Determinación de necesidades de continuidad…… 68
5.15 Determinación de alternativas……. 70
5.16 Fijar la GCN en la cultura organizacional…….. 72

Capítulo VI. Propuesta de Mejora 75
b) La industria Bancaria y Plan de Recuperación de Desastres……... 76
6.2 Bancos – Están expuestos al tiempo en el desastre..... 78
6.3 Herramientas que ayudan al correcto BCP…….. 79
6.4 Recuperación de desastres y recuperación de datos…. 81
6.5 Objetivos del proyecto…….. 82
6.6 Escenario par el desarrollo del proyecto DRP…….. 86
6.7 Análisis de riesgo……... 87
6.8 Identificación de amenazas…….. 90
6.9 Clase de riesgo: Incendio o Fuego……. 90
6.10 Clase de riesgo: Robo común de equipos y archivo….. 92
6.11 Clase de riesgo: Vandalismo…… 92
6.12 Clase de riesgo: Fallas en los equipos…….. 93
6.13 Clase de riesgo: Equivocaciones…… 96
6.14 Clase de riesgo: Acción de virus informático……. 97
6.15 Clase de riesgo: Fenómenos naturales……. 98
6.16 Clase de riesgo: Accesos no autorizados…….. 98
6.17 Clase de riesgo: Robo de datos…….. 99
6.18 Clase de riesgo: Manipulación y sabotaje……. 100
6.19 Análisis en fallas de seguridad…… 101
6.20 Seguridad de información…… 102

Conclusiones…… 108
Recomendaciones…….. 110
Anexos……... 111
Medidas de precaución y recomendación 111
Glosario de términos…….. 115
Glosario de abreviaturas…… 118
Referencias……..…… 120

Índice de Figuras

No. Figura	Descripción	Página
1	Activos de información	9
2.1	Modelo de seguridad de McCumber	17
2.2	Niveles de la arquitectura de seguridad	19
2.3	Escenario de los servicios de seguridad	22
2.4	Principales áreas de actuación	22
3.1	Clase de riesgos	28
3.2	Desastre del 11 de Septiembre del 2001	28
3.3	Almacenamiento de dispositivos	31
3.4	Red de Área de Almacenamiento	35
4.1	Diagrama de respuesta de emergencia de “Incendio”	40
4.2	Diagrama de respuesta de emergencia de “Fallas en Hardware o Software”	44
4.3	Diagrama de respuesta de “Fenómenos Naturales”	48
4.4	Diagrama de respuesta ante “Manipulación y Sabotaje”	51
5.1	Plan de Continuidad de Negocios (BCP)	53
5.2	Flujo de para el desarrollo del GCN	56
5.3	Esquema de prioridad de recuperación en GCN	56
5.4	El ciclo de vida de la gestión de continuidad del negocio	58
5.5	Revisión y evaluación de procesos	61
5.6	Espiral de mejora continua	65
5.7	Procesos críticos de negocio, se incluyen aspectos externos como proveedores y clientes	66
5.8	Análisis de Impacto del Negocio (AIN)	67
5.9	Arquitectura “Golden Gate”	80
5.10	Recuperación de datos	82
6.1	Tipos de extintores	91

Índice de Tablas

No. Tabla	Descripción	Página
3.1	Impactos de Pérdidas	29
6.1	Escala de valores para criterios de posibles problemas	89
6.2	Escala factor de probabilidad por clase de riesgo	90

No. Tabla	Descripción	Página
6.3	Clase de riesgo: Incendio o fuego	90
6.4	Clase de riesgo: Robo común de equipos y archivos	92
6.5	Clase de riesgo: Vandalismo	92
6.6	Clase de riesgo: Falla de equipos	93
6.7	Clase de riesgo: Equivocaciones	96
6.8	Clase de riesgo: Acción de virus informático	97
6.9	Clase de riesgo: Fenómenos naturales	98
6.10	Clase de riesgo: Accesos no autorizados	98
6.11	Clase de riesgo: Robo de datos	99
6.12	Clase de riesgo: Manipulación y sabotaje	100
6.13	Niveles de acceso de información	105

Prefacio

Durante las operaciones normales de negocio existe la probabilidad de pérdidas potenciales o interrupciones no programadas asociadas con un desastre o contingencia mayor, por lo que es importante el desarrollo de un plan viable y factible de recuperación que asegure la continuidad de las operaciones de la Compañía.

El planeamiento adecuado, la preparación, y la comunicación son los ingredientes necesarios para un exitoso plan de continuidad de negocio (BCP) en caso de contingencia o desastre.

En el caso de una situación de contingencia o desastre, es importante disponer de una estrategia de recuperación que pueda proveer el reinicio del negocio en un tiempo razonable y predeterminado. Por lo tanto, la importancia de un Plan de contingencias y recuperación en caso de desastres es vital.

Asimismo, la seguridad informática es una disciplina cuya importancia crece día a día.

Aunque la seguridad es un concepto difícil de medir, su influencia afecta directamente a todas las actividades de cualquier entorno informatizado en los que interviene el Ingeniero en Informática, por lo que es considerada de vital importancia.

La seguridad se define como una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible, para el caso de sistemas informáticos, es muy difícil de conseguir (según la mayoría de los expertos, imposible) por lo que se pasa a hablar de “confiabilidad”.

La seguridad de la información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al negocio y maximizar el retorno sobre las inversiones y las oportunidades.

En cualquier entorno informatizado es necesario estar protegido de las múltiples (y hasta desconocidas) amenazas, garantizando, fundamentalmente, la preservación de tres características:

- **Integridad:** que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento.
- **Confidencialidad:** que la información sea accesible sólo a las personas autorizadas.
- **Disponibilidad:** que los usuarios autorizados tengan acceso a la información y a los recursos cuando los necesiten.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca: políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software. Básicamente, los problemas de

Seguridad Informática son sucesos que no deseamos que ocurran. La mayoría son inesperados, aunque en muchos casos se pueden prevenir.

Cuando hablamos de incidentes de seguridad, o problemas de seguridad informática nos referimos a:

- Acceso no autorizado a la información.
- Descubrimiento de información.
- Modificación no autorizada de datos.
- Invasión a la privacidad.
- Denegación de servicios.
- Etc.

Cada entorno informatizado es diferente, y maneja distintos tipos de información, y por ende, es distinta la forma en que se tratan los datos.

Los componentes de los entornos informatizados son distintos, por lo que las especificaciones de seguridad asociadas a cada uno varía notablemente dependiendo de la tecnología utilizada a nivel de plataforma, software base y dispositivos físicos.

La funcionalidad y características técnicas de los componentes de los entornos varían notablemente según la marca, en particular en los aspectos concernientes a la seguridad.

Hoy en día la amenaza más común en los ambientes informatizados se centra en la eliminación o disminución de la disponibilidad de los recursos y servicios que utiliza el usuario.

El crecimiento de las telecomunicaciones y la estricta dependencia que existe entre el negocio de las empresas y la tecnología informática hace crítica la inversión en seguridad. Cada vez más los procesos comerciales se ven estrechamente ligados a procesos informáticos.

Prácticamente toda la información vital para el negocio de una compañía comercial se encuentra informatizada, no sólo almacenada en dispositivos electrónicos, sino que, en la mayor parte de los casos, se encuentra distribuida físicamente y viaja constantemente a través de medios públicos como redes de telefonía e Internet.

Es por eso que se pone énfasis en el crecimiento de soluciones para el problema de la seguridad informática, por lo que el conocimiento en esta área ha crecido enormemente en los últimos años, al punto en que somos capaces de afirmar que es posible lograr una completa enumeración de las fallas de seguridad de los sistemas y los entornos en los que viven.

Estas fallas de seguridad son las que se convierten en amenazas susceptibles de ser aprovechadas por usuarios malintencionados para causar daño o algún tipo de invasión a la confidencialidad.

Protegerse contra accesos no autorizados es el problema más sencillo a resolver, ya que durante años se han desarrollado y perfeccionado algoritmos matemáticos para la encriptación de datos, para el intercambio seguro de información, para garantizar el correcto funcionamiento del software, que se ha traducido en herramientas capaces de proporcionar soluciones rápidas y sencillas a problemas técnicos de seguridad.

Desafortunadamente, no es suficiente simplemente arreglar los errores o eliminar las fallas técnicas de seguridad. El problema va mucho más allá, la Seguridad Informática es un problema cultural, en el que el usuario juega un rol protagónico.

La responsabilidad sobre la seguridad de los datos y equipos ya no recae solamente en el personal técnico especializado encargado de resguardar los bienes y servicios brindados por el entorno, si no que es el usuario el que debe velar por la seguridad de los bienes físicos y lógicos que maneja.

Para ello debe existir una conciencia de trabajo seguro, de resguardo de la confidencialidad y de protección de los activos utilizados a diario en el trabajo de cada individuo.

Por esta razón la seguridad Informática debe estar incorporada desde el principio de todo proceso, desde el diseño para garantizar la evaluación de todos los factores funcionales, (y no solamente los técnicos) a tener en cuenta para el uso seguro del entorno. Si esto sucede, el objetivo inicial de la seguridad habrá sido logrado.

Introducción

Todas las instituciones deberían contar con un plan de recuperación de desastres actualizado, ya que es una herramienta muy valiosa que basada por lo general en un análisis de riesgo, nos permitirá ejecutar un conjunto de normas, procedimientos y acciones básicas de respuesta que se debería tomar para afrontar de manera oportuna, adecuada y efectiva , la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir tanto en las instalaciones como fuera de ella, por ejemplo un temblor, tornado, incendio, etc.

Una estrategia de gestión de la información digital es esencial para sobrevivir en el mercado actual. En la Figura 1, se puede apreciar como los activos de información de una organización están rodeados de un complejo ambiente de objetos y amenazas que van desde simples virus de computadora hasta robos de la propiedad intelectual del negocio.

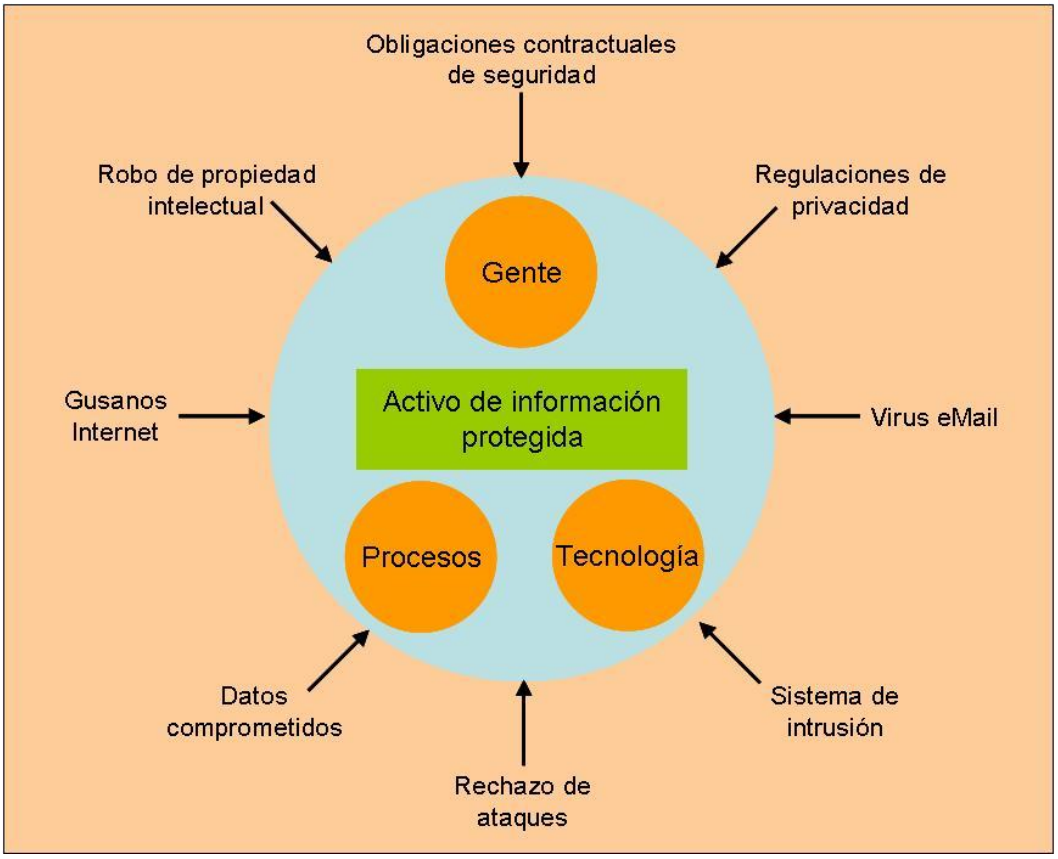


Figura 1. Activos de información

Los riesgos los puedes eliminar, transferir, mitigar o aceptar, ello dependerá de varios factores como probabilidad de ocurrencia o impacto del riesgo, los objetivos del plan de contingencia son el de planificar y describir la capacidad para respuestas rápidas, requerida para el control de emergencias, paralelo al plan se debe identificar los distintos tipos de riesgos que potencialmente

podrían ocurrir e incorporar una estrategia de respuesta para cada uno, algunos objetivos específicos:

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

Los planes de contingencia son necesarios en todo sistema de información y no podría dejarse de lado en el tema de seguridad, entendiéndose por plan de contingencia al conjunto de procedimientos alternativos a la operatividad normal de cada institución y su finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.

Haciendo una síntesis para su elaboración la podríamos dividir en cinco etapas.

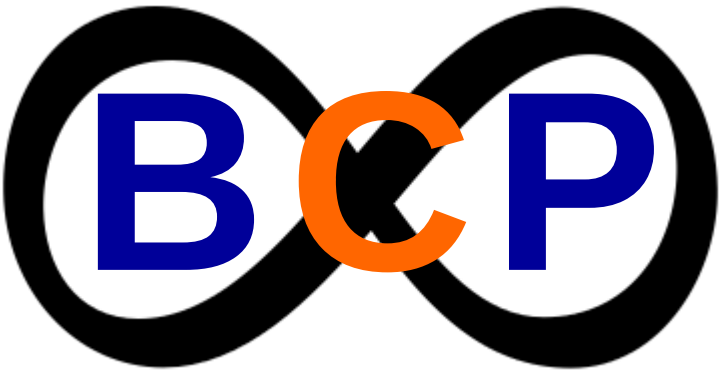
1. Evaluación.
2. Planificación.
3. Pruebas de viabilidad.
4. Ejecución.
5. Recuperación.

Las tres primeras etapas hacen referencia al componente preventivo y las ultimas a la ejecución del plan una vez ocurrido el siniestro.

Queda claro que lo único que permite que una institución, empresa o persona pueda reaccionar de manera adecuada ante una crisis de seguridad, es mediante la elaboración, prueba y mantenimiento de un plan de contingencia. Finalmente las instituciones financieras en general están en la obligación de elaborar y presentar un plan de contingencia.

Para resolver la problemática se realizará lo siguiente:

Capítulo I, se desarrollará el fundamento metodológico, mencionando el objetivo y alcance del presente proyecto, así como la justificación de la implementación y los antecedentes de la empresa.
Capítulo II, se describirá el fundamento teórico del plan de continuidad del negocio y el análisis de impacto del negocio.
Capítulo III, se mencionará la importancia del plan de recuperación de desastres y las actividades que se desarrollan previa, durante y posterior a un desastre.
Capítulo IV, se desarrollarán las actividades especificas a realizar en función del tipo de riesgo que se presente.
Capítulo V, se describirá como realizar la gestión de la continuidad del negocio (GCN / BCP), incluyendo la estrategia, los elementos que la integran, políticas, alcances, documentación y cultura organizacional, entre otros.
Capítulo VI, se detallará la propuesta de mejora aplicada a un banco, aplicando los elementos que integran la gestión de continuidad del negocio.



Business
Continuity Plan

Capítulo I

Fundamento Metodológico

1.1 Objetivo y alcance

El objetivo de la presente tesis es establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado Plan de Continuidad del Negocio en Caso de Desastre (DRP) en una institución financiera en México, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización.

En los años de experiencia en servicios y tecnología para instituciones financieras, el autor de la presente tesis pudo constatar que a través de la adopción de las medidas adecuadas, un DRP puede ayudar a una institución financiera a cumplir sus objetivos, protegiendo sus recursos financieros, sistemas, reputación, situación legal y otros bienes tanto tangibles como intangibles.

De igual forma el autor de la presente tesis pudo observar que desafortunadamente, en ocasiones, se ve a un DRP como una entidad complicada que dificulta la consecución de dichos objetivos, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo, debe vérselo no como un objetivo en sí mismo,sino como un medio de apoyo a la consecución de los objetivos.

Para este proyecto el objetivo primordial de la institución financiera, es llevar el proceso de implementación de DRP con las mejoras y las actualizaciones al actual sistema de Replicación para asegurar la continuidad de las operaciones y de la actividad económica, la seguridad de los clientes y sus transacciones. Con la certeza de la confiabilidad de las operaciones en tiempo real.

Deberá de considerarse que las necesidades de las políticas de Replicación deben de estar en mejora continua para cumplir con las exigencias del crecimiento de la institución financiera, con la responsabilidad de contar siempre con el mejor servicio y seguridad de sus transacciones.

1.2 Justificación de la implementación

La institución financiera parte de su política de mejora continua de TI, la cual se encuentra en proceso de actualización tecnológica, de cambios de infraestructura y continuidad ininterrumpida de la operación critica del negocio. Este último requerimiento de continuidad del negocio es el que se va a tratar en este documento.

Se requiere de las soluciones que se ofertan en el mercado de acuerdo a nuestros requerimientos y políticas de DRP para garantizar la seguridad y la integridad de la institución financiera, que se traduce en miles de millones de transacciones y acciones económicas.

Todo esto va encaminado a asegurar la operación de forma ininterrumpida para asegurar las transacciones de las operaciones que se realizan en esta institución financiera.

1.3 Antecedentes de la empresa

Para la realización del presente trabajo de tesis se respetará la confidencialidad e integridad de la información de la empresa propuesta para el caso de estudio, por esta razón, durante todo el desarrollo de la tesis se hará referencia a dicha empresa como la “institución financiera”.

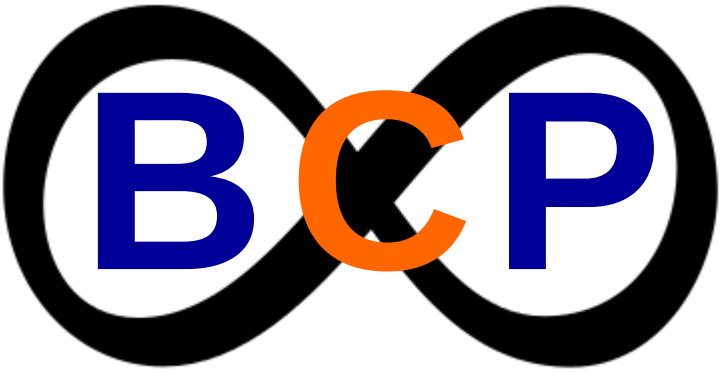
Esta institución financiera nació hace **16 años en México** con la premisa fundamental de ofrecer productos y servicios financieros de alta calidad con una atención personalizada. En toda su trayectoria se ha destacado por su **calidad en el servicio** y su crecimiento prudente.

Su primera sucursal inició operaciones en junio de **1994** y a la fecha cuentan con **31 oficinas** ubicadas dentro del Distrito Federal, Estado de México, Municipio de Metepec, Estado de Morelos y la ciudad de Monterrey.

Forman parte de un grupo financiero **sólido y en vertiginoso desarrollo**, mismo que se ha distinguido por su calidad y calidez en el servicio. Dentro de su portafolio albergan más de **50 productos y servicios bancarios y financieros** para satisfacer a sus clientes meta.

En esta institución financiera conocen lo importante que es el cliente, por ello trabajan con absoluta dedicación para **satisfacer sus necesidades** con productos y servicios innovadores, atención personalizada y recursos humanos altamente **competitivos**.

Dentro de la gama de productos que ofrecen, se incluyen: **instrumentos de inversión, ahorro, crédito y derivados**, así como una variedad de servicios para apoyar proyectos financieros y de **vida**.



Business
Continuity Plan

Capítulo II

Fundamento Teórico

2.1 Fundamento Teórico

Plan de Continuidad de Negocio (BCP).- Dado el acaecimiento de tangibles y recientes desastres producidos a nivel mundial, como los efectos del 11 de septiembre del 2001 así como la evolución de la tecnología, este punto de vista ha cambiado, pero no afecta a todos los países y sectores por igual. Del mismo modo, dependiendo del tamaño de la compañía, las acciones varían considerablemente.

British Standards Institution (BSI) En 2007, el BSI publicó la segunda parte, BS 25999 2 "Especificación para la Gestión de Continuidad del Negocio", que especifica los requisitos para la aplicación, funcionamiento y mejora de un documentado Sistema de Gestión de la Continuidad del Negocio (BCMS).

Un reciente estudio del Business Continuity Institute del Reino Unido deja claro que los conceptos plan de continuidad de negocio (BCP, Business Continuity Plan) y plan de recuperación de desastres (DRP, Disaster Recovery Plan), no han sido asimilados adecuadamente por la dirección de las compañías provocando la ineficiencia de sus propios planes.

Un plan de continuidad de negocio (BCP) debe garantizar las operaciones necesarias para cumplir con el funcionamiento establecido en el desarrollo habitual del negocio ante cualquier tipo de desastre, interrupción o contingencia.

Un plan de recuperación de desastres (DRP), por su parte, es el plan que ejecuta Tecnologías de la Información para recuperar los sistemas que gestiona.

Los objetivos de un BCP son minimizar la pérdida financiera de la compañía, continuar con el servicio a los clientes y mitigar los efectos que pueden producirse en los planes estratégicos, la reputación, las operaciones y el mercado donde está situada la compañía.

Según ITIL 2007: (Diseño del Servicio) Plan que define los pasos que se requieren para el Restablecimiento de los Procesos de Negocio después de una interrupción. El Plan también identifica los disparadores para la Invocación, las personas involucradas, las comunicaciones, etc. El Plan de la Continuidad del Servicio TI es una parte importante de los Planes de Continuidad del Negocio.

2.2 Análisis de Impacto del negocio (BIA).- El propósito del BIA es poner en correlación los componentes específicos del sistema con los servicios críticos que ellos proporcionan, y basado en esa información, para analizar las consecuencias de una ruptura de los componentes del sistema.

El objetivo fundamental es identificar las áreas que sufrirían las pérdidas financieras y operacionales más grandes en el caso de un desastre.

Además identifica los sistemas críticos y estima el tiempo que la compañía

puede tolerar en caso de un desastre. Un análisis de impacto de negocio permite abordar un plan de acción con sólidos elementos de criterio basados no sólo en necesidades de capacidad, sino también de seguridad. Para poder definir las contingencias deseadas es necesario conocer los servicios de TI que el departamento de informática ofrece a la compañía, sus vulnerabilidades, así como las amenazas y posibles impactos; además de identificar que servicios de TI soportan los procesos de negocio de la compañía.

2.3 Tecnología de seguridad

Las nuevas Tecnologías de la Información han potenciado la comunicación y el acceso a la información. Por ello, la Sociedad de la Información, en la que estamos inmersos, debe de garantizar la seguridad de los sistemas.

Los sistemas de información deben estar preparados para prevenir, detectar y reaccionar ante las posibles amenazas.

Se entiende por "amenaza" una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Para hacer frente a las amenazas contra la seguridad, se definen una serie de servicios que hacen uso de uno o varios mecanismos de seguridad. Unos de ellos están enfocados a garantizar la seguridad de los datos (confidencialidad, integridad y disponibilidad).

Mecanismos de seguridad

- **Confidencialidad:** garantiza que la información sea accesible únicamente por las entidades autorizadas, protegiendo la identidad de las partes implicadas. Se utilizan métodos de "cifrado".
- **Integridad:** garantiza que la información sólo pueda ser modificada por las entidades autorizadas. Requiere el uso de tecnologías como el hash criptográfico con firma digital, y los time-stamps (marcas de tiempo).
- **Disponibilidad:** garantiza que los recursos del sistema informático estén accesibles para las entidades autorizadas cuando los necesiten.

Mientras que otros se orientan a protegerlos del entorno (autenticación, no repudio y control de acceso).

- **Autenticación:** garantiza la identidad de las partes implicadas en la comunicación. La tecnología más aplicada es: "firma digital", biometría, tarjetas de banda magnética y contraseñas.
- **No repudio:** ofrece protección a un usuario frente a que otro usuario niegue posteriormente que realizó cierta comunicación. La tecnología más aplicada es la "firma digital".
- **Control de acceso:** apoya a que el acceso a los recursos sea controlado y limitado por el sistema de destino, mediante el uso de contraseñas o llaves hardware.

La tecnología de seguridad puede considerarse en continua evolución, ya que su dinámica se basa en la lucha entre aquellos que deben garantizar la seguridad de los datos y aquellos otros que tratan de violarla. Por todo ello, nunca podría considerarse una tecnología totalmente madura, pues cualquier sistema de seguridad es quebrantable con tiempo e información suficiente. Sin embargo, el objetivo de las técnicas de seguridad no está en la absoluta inviolabilidad de los sistemas sino en garantizar un nivel de dificultad suficientemente alto que obstaculice el asalto a la seguridad de una cierta información. Puede decirse que ese nivel ya se ha alcanzado.

2.4 Modelo de seguridad de McCumber

John R. McCumber expuso en la decimocuarta edición de la National Computer Security Conference un modelo fácil y completo de seguridad, independiente del entorno, arquitectura o tecnología que gestiona nuestra información. Su aplicación es universal y no está restringido por diferencias organizacionales.

En la Figura 2.1, se muestra el modelo de tres dimensiones se convierte en un cubo con 27 celdillas como marco de actuación.

A partir de este modelo se puede definir la seguridad de la información como: “Todas aquellas medidas tecnológicas, de normas y procedimientos y de formación que aseguran la confidencialidad, integridad y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión”.

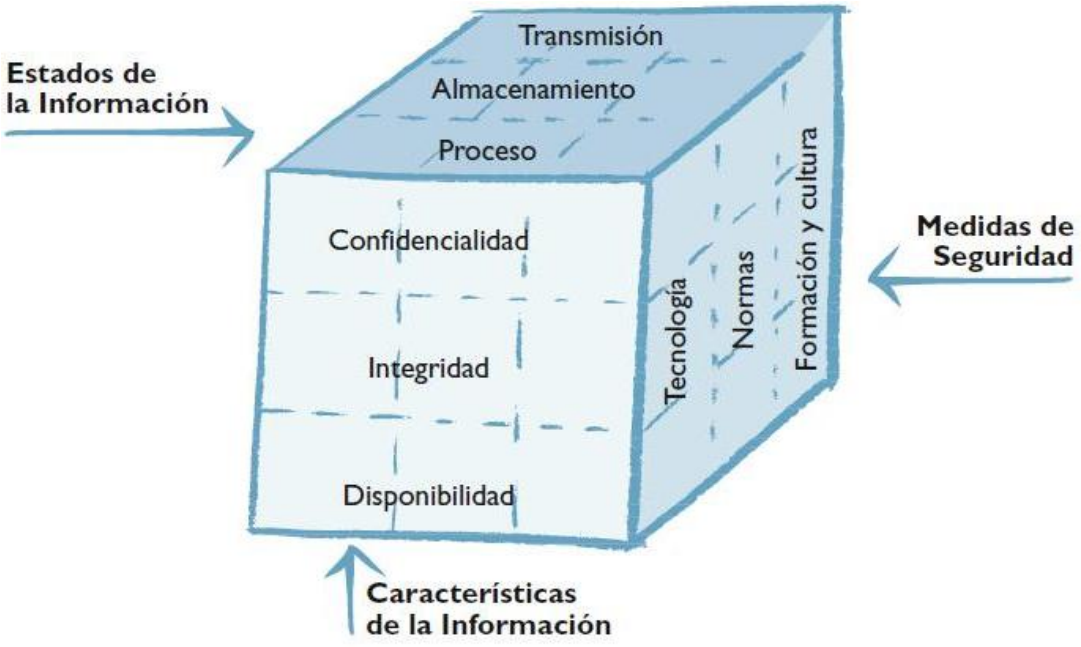


Figura 2.1 Modelo de seguridad de McCumber

2.5 Estados de la información

La información puede estar en tres estados: proceso, almacenamiento y transmisión.

- **Proceso**. La información se procesa cuando está siendo elaborada. El procesamiento es una combinación del almacenamiento y la transmisión, pero para este modelo es fundamental tener esta distinción entre los tres estados y aplicar el modelo de forma adecuada.

- **Almacenamiento**. La información está almacenada cuando reside en algún soporte informático accesible para su uso.

- **Transmisión**. La información está en estado de transmisión cuando viaja desde un sistema a otro con alguna finalidad.

Características de la información

Las características de la información con relación a la seguridad son: confidencialidad, integridad y disponibilidad.

- **Confidencialidad de la información**. La confidencialidad de la información pretende que una persona acceda sólo a la información que debe conocer y hacer con ella sólo lo que le esté permitido. Es decir, disponer de una política de seguridad que defina sujetos e información y determine a qué información pueden acceder dichos sujetos. La confidencialidad es tener la seguridad de que se ha realizado una completa implantación del control de accesos, de acuerdo con la clasificación de la información realizada en la organización.

- **Integridad de la información**. Integridad es el grado de fiabilidad del contenido. Integridad es calidad de información identificada como “fiel reflejo” del dato que representa en realidad. La definición de integridad debe comprender los términos de: exacta, autorizada y completa.

- **Disponibilidad de la información**. Esta característica provee a los usuarios autorizados de la información cuando es requerida o necesitada. Es decir, la información debe de estar siempre disponible y poder ser siempre recuperable en caso de pérdida o imposibilidad de uso de los sistemas de información de la organización

2.6 Medidas de seguridad

Es necesario definir el tipo de medidas que hay que implantar para asegurar las distintas características de la información a través de sus distintos estados.

- **Medidas tecnológicas**. Para este modelo se pueden definir las medidas tecnológicas como dispositivos físicos o lógicos, que son usados específicamente para asegurar las características de la información a través de los distintos estados.

- **Normas y procedimientos**. La adopción de normas y procedimientos de seguridad debe solucionar inmediatamente las carencias en la seguridad de la información y debe ser la orientación y guía para la seguridad de las soluciones tecnológicas.

- **Formación y cultura**. Este tipo de medida puede convertirse en la más importante y desde luego es absolutamente imprescindible. Comenzando por la comprensión de la seguridad, por parte de todos los componentes de la organización, para seguir por el análisis de las amenazas y vulnerabilidades, y la implantación posterior de todas las normas y procedimientos de seguridad. Todo ello hace que la seguridad de la información se convierta en cultura de la organización. Objetivo final que se debe perseguir cuando se decide implantar un Plan de Seguridad de la Información.

2.7 La arquitectura de seguridad

Partiendo del modelo de seguridad, anteriormente presentado, se ha definido una Arquitectura de Seguridad para los Sistemas de Información, articulada en tres niveles y que se muestra en la Figura 2.2:

- **Política de seguridad.**
- **Normas y estructuras.**
- **Procedimientos y soportes.**

Figura 2.2 Niveles de la arquitectura de seguridad

2.8 La política de seguridad

La política de seguridad debe establecer los criterios de protección de la información en el ámbito de la organización y servir de guía para la creación de las normas y procedimientos de seguridad. Recoge los objetivos estratégicos y directrices de actuación en este ámbito.

Debe sentar las bases para definir las normas básicas de protección de la información y establecer una primera aproximación a la estructura de recursos humanos, responsable de dicha protección, incluyendo los criterios para las funciones, tareas y responsabilidades en gestión, administración, control y auditoria de la seguridad de la información.

La política de seguridad debe partir de la base de que la información constituye un “activo de la organización”, resaltar este aspecto e implementar las medidas para su tratamiento.

Normas y Estructuras

En el nivel de normas y estructuras identificamos dos áreas de trabajo:

- Normativa y metodología.
- Organización.

Normativa y metodología. La normativa supone la definición de todo lo que debe existir y ser cumplido para garantizar la seguridad. Tiene que estar formalizada de forma suficiente, de manera que pueda ser transmitida y comunicada a todos los componentes de la organización y agentes relacionados, que deban conocerla.

Constituye el conjunto de reglas y procedimientos para la implementación de la seguridad. La normativa debe ser clara y abarcar los diferentes aspectos de actuación.

Entre otros, se pueden citar:

- Definición de perfiles.
- Autorizaciones de acceso.
- Administración del sistema.
- Almacenamiento de la información.
- Encriptación (transmisión y almacenamiento).
- Impresión de documentos.
- Clasificación de la información.
- Metodología en el desarrollo de aplicaciones.
- Auditoria y control.
- Respaldo y copias de seguridad.

Organización. Supone la definición de una estructura soporte de los sistemas de seguridad de acceso a la información. Son personas con funciones específicas y con actuaciones concretas (procedimientos), definidas metodológicamente y enmarcadas dentro de la política de seguridad.

Precisa la ubicación de las funciones relacionadas con la gestión, administración, control y auditoria, y el soporte técnico. Define las responsabilidades y funciones de la propia estructura de seguridad, del departamento de Informática y los usuarios.

2.9 Procedimientos y soportes

En el nivel de procedimientos y soportes se han identificado tres áreas de trabajo:

- Tecnología de seguridad.

- Control.
- Cultura.

Tecnología de seguridad. La tecnología de seguridad debe incorporar el hardware y software necesarios para proporcionar el soporte adecuado a la arquitectura definida. Se deben identificar los productos y sistemas informáticos existentes en el mercado para proceder a la valoración de sus características en función de los requerimientos y de los criterios de la política de seguridad.

Existen en el mercado multitud de productos dirigidos a garantizar la seguridad informática. Se debe realizar un proceso de evaluación y selección en función de los requerimientos y necesidades existentes.

Control. Las tareas de auditoria y control representan un elemento básico para el funcionamiento adecuado de los sistemas de seguridad. Cualquier sistema que se implante, que no incluya funciones de seguimiento y control, está condenado al fracaso en el medio plazo. Por consiguiente, se deben definir las funciones de control que hay que implementar dentro de la estructura de seguridad.

Para el desarrollo de las funciones se apoyarán en procedimientos de control, en los que se establecerá la periodicidad de aplicación, que dispondrá de herramientas de apoyo que optimicen las tareas asignadas.

Cultura de la organización. Uno de los eslabones fundamentales para la implantación de un sistema de seguridad con éxito es la cultura de la organización. La organización debe conocer en sus diferentes niveles cuáles son sus funciones y responsabilidades.

Para ello se deben articular los medios y soportes necesarios para transmitir, informar, comunicar y enseñar todo lo que cada miembro debe conocer del sistema de seguridad.

Esto supone el diseño de un plan de formación y un plan de comunicación adecuados a los objetivos de la política de seguridad definida.

2.10 Enfoque del proyecto de seguridad

La definición y diseño de la seguridad de la información requiere un proyecto completo y ordenado, que partiendo de la definición de la política de seguridad se concrete en la implantación de las normas, procedimientos, herramientas y sistemas informáticos que mediante un proceso de formación y comunicación adecuado a los usuarios, garanticen el cumplimiento de los objetivos de la organización en el ámbito de la seguridad de los sistemas de información, los cuales son mostrados en la Figura 2.3.

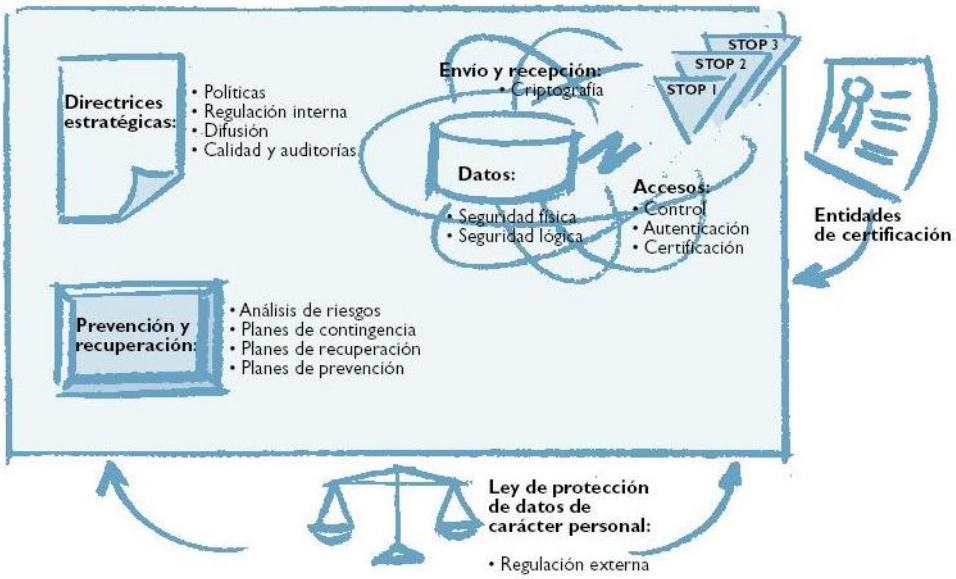


Figura 2.3 Escenario de los servicios de seguridad

La materialización de un proyecto completo que abarque todas las facetas de la seguridad se recoge en cuatro principales áreas de actuación y que se muestran en la Figura 2.4.

Se definen a continuación los objetivos de cada una de estas áreas, que serán el punto de partida para futuras actuaciones.

Figura 2.4. Principales áreas de actuación

2.11 Estrategias y políticas de seguridad

La implementación de los sistemas de información sobre sistemas informáticos posibilita de forma muy importante el acceso de los usuarios. Las Tecnologías de Información y Comunicaciones favorecen la distribución y uso de los datos de las organizaciones.

Ahora bien, esta ventaja aportada por las tecnologías informáticas puede llegar a ser un inconveniente o incluso una gran amenaza para el desarrollo de la

organización, si no existe un control y discriminación adecuados en el uso de los sistemas y la información que contienen.

Considerar la información como un activo de la organización requiere el establecimiento de:

Políticas y planes de seguridad, definición de objetivos y alcance de la seguridad en la organización. Planificación de acciones, tareas y medios encaminados a su realización.

Regulación de la seguridad, que permita cumplir los requisitos internos de seguridad marcados por la organización y los requerimientos externos dictados por la Ley de Protección de Datos entre otros, que garantizan la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Difusión en la organización de la política de seguridad. Se trata de impartir la formación en las normas, procedimientos y sistemas, minimizando las barreras ante el cambio y asegurando el éxito en la implantación del proyecto.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en la ley y normas de la organización.

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Objetivos de calidad y auditoria de la seguridad implantada. Establecimiento y seguimiento de indicadores, controles y alarmas que garanticen la bondad de la seguridad implantada, junto con acciones de control y estudio de la situación de la seguridad en diferentes áreas o niveles según el interés de la organización.

Además, deberá garantizar que cada usuario sólo acceda a la información a la que está autorizado, para realizar las operaciones a las que está autorizado, en el momento y lugar en que está autorizado, dejando los rastros necesarios para poder realizar tareas posteriores de revisión y control del acceso y uso de la información.

2.12 Seguridad física y lógica

Seguridad física: abarca una serie de acciones encaminadas a la protección de los medios físicos, en los que se sustenta la seguridad de la información, y de los medios de recuperación física (centros de respaldo), dispuestos para casos de emergencia.

Garantizar la seguridad física de los medios requiere establecer:

- Protección física del edificio y los equipos (CPD).
- Centros de recuperación (respaldo) de máquinas, equipos y comunicaciones.

Seguridad lógica: acciones encaminadas a garantizar la seguridad de la información ante ataques, manipulaciones o pérdidas de información.

Garantizar la seguridad lógica incluye:

- Protección de los sistemas de información.
- Gestión de los accesos.
- Seguridad de los contenidos.

2.13 Seguridad en las comunicaciones

Integración de productos, soluciones y servicios que garantizan la seguridad en el acceso y distribución de la información a través de las redes de comunicación.

Estudio y valoración de las soluciones disponibles en el mercado para seleccionar la más adecuada en relación con los objetivos y requerimientos planteados en la política de seguridad, así como en coherencia con la arquitectura tecnológica existente.

La seguridad en las comunicaciones engloba el diseño, proceso y herramientas destinadas a:

Control, autenticación y certificación de los usuarios, con tres niveles de profundización:

- **Nivel 1.** Contraseñas, servidores en red, etc.
- **Nivel 2.** Servidores de autenticación, soportes: token tarjeta inteligente, etc.
- **Nivel 3.** Firma electrónica, entidades de certificación, etc.

Criptografía. Encriptado y desencriptado de:

- Datos.
- Redes privadas virtuales.

2.14 Prevención y recuperación

Este último aspecto recoge los planes y medidas adoptadas con el fin de conocer y prevenir o reparar posibles pérdidas de la información o los medios, de acuerdo con las líneas de seguridad marcadas por la organización.

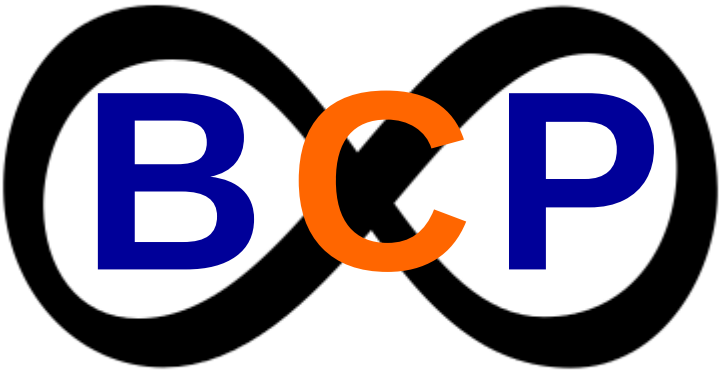
Incluye:

Análisis de riesgos: conocimiento, estudio, evaluación y gestión de los posibles riesgos que le afectan a la seguridad.

Planes de contingencia: medidas y acciones de emergencia y evacuación ante desastres naturales o humanos.

Planes de recuperación: medidas destinadas a preparar acciones y niveles de recuperación de medios y sistemas ante posibles caídas, así como el estudio y definición de alternativas ante no recuperaciones.

Planes de prevención: establecimiento de alarmas y controles que detecten situaciones anómalas y prevean sus medidas correctoras.



Business
Continuity Plan

Capítulo III

Plan de Recuperación de Desastres

3.1 La importancia de un Plan de Recuperación de Desastres

La mayoría de las veces la información controlada a través de un servidor, ya sea de aplicaciones, de base de datos o Web, es vital para la continuidad de un servicio dentro de la empresa o hacia los clientes.

Ante una catástrofe de cualquier índole, seguramente se afectará de manera negativa el desarrollo de las actividades normales de la empresa o institución, un Plan de Recuperación ante Desastres va a permitir una rápida recuperación del flujo de la información y por lo tanto un menor tiempo en la interrupción de los servicios que son provistos por el equipo que ha sufrido el daño.

La diferencia entre estar protegido con un Plan de Recuperación ante Desastres y no estarlo puede ir desde recuperar el servicio en 20 minutos (o menos) en caso de estar protegido o llegar hasta varios días en caso de no haberse preparado adecuadamente.

Un Plan de Recuperación ante Desastres deberá contemplar siempre la peor de las situaciones, ya que de este modo, la contingencia podrá ser solventada en el menor tiempo posible.

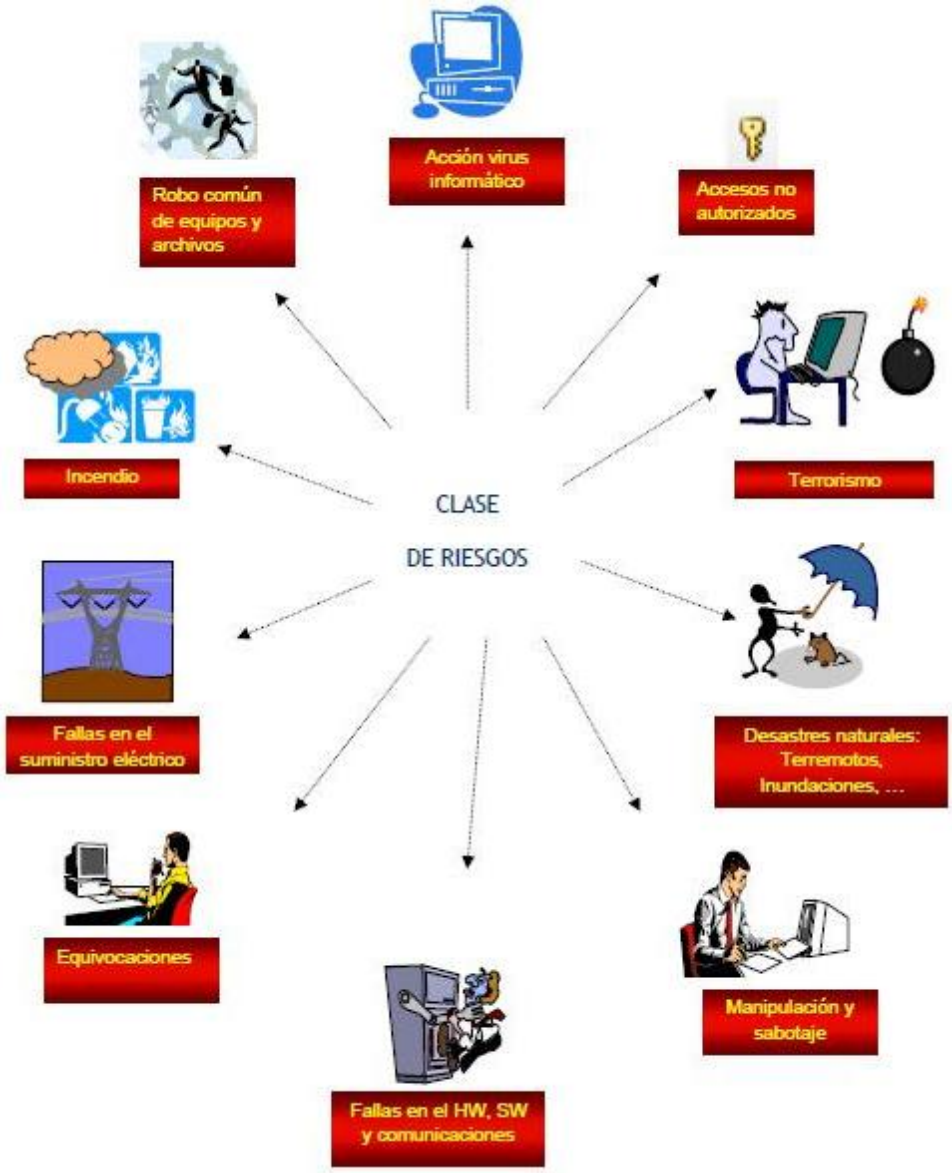
3.2 Razones para recurrir a un DRP

Existen diferentes riesgos que pueden impactar negativamente las operaciones normales de una organización.

Una evaluación de riesgo debería ser realizada para ver que constituye el desastre y a que riesgos es susceptible una empresa específica, incluyendo:

- Catástrofes.
- Fuego.
- Fallas de energía.
- Ataques terroristas.
- Interrupciones organizadas o deliberadas.
- Sistema y/o fallas de equipo.
- Error humano.
- Virus informáticos.
- Cuestiones legales.
- Huelgas de empleados.

A continuación en la Figura 3.1, se muestran en forma esquemática las clases de riesgos que pueden ocurrir en un desastre, en la Figura 3.2, fotografías del desastre del 11 de Septiembre del 2001 y en la Tabla 3.1, ejemplos del impacto de las perdidas.



Figuras 3.1. Clase de riesgos

Figura 3.2 Desastre del 11 de Septiembre del 2001

Tabla 3.1 Impactos de Pérdidas

Incidente	Fecha	Localización	Perdidas
Ataques terroristas	Sep / 2001	NY, PA y Wash DC.	$27 Billones
Huracán Andrew	Ago / 1992	Fla., Costa del Golfo	$24 Billones
Terremotos	Ene / 1994	Los Ángeles, CA	$11 Billones
Inundaciones	Abr / 1992	Medio Este	$10 Billones
Disturbios	May / 1992	Los Ángeles	$2 Billones
Ventisca	Mar / 1993	24 Estados	$1.8 Billones
Incendios forestales	Oct / 1991	Oakland, CA	$1.7 Billones
Bombardeo	Feb / 1993	NY WTC	$540 Millones
Fuertes lluvias	Ene / 1993	Arizona	$56 Millones
Tornados	Abr / 1991	Andover, KS	$50 Millones
Cortes del servicio eléctrico	Ago / 2003	US y Canada	$ N/A

Nota: Los datos reflejan costos de infraestructura y limpieza – no las pérdidas de ingresos de negocio.

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 07 o un incendio de controlable, estará dado por el valor no asegurado de equipos informáticos e información mas el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones.

Típicamente las personas pueden ser: personal del centro de cómputo, personal de Seguridad.

Las actividades a realizar en un Plan de Recuperación de Desastres se clasifican en tres etapas:

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

3.3 Actividades previas al desastre (durante la operación normal)

Se considera las actividades de planteamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguraran un proceso de recuperación con el menor costo posible para la institución financiera.

Establecimientos del Plan de Acción

En esta fase de planeamiento se establece los procedimientos relativos a:

1. Sistemas e información.
2. Equipos de Cómputo.
3. Obtención y almacenamiento de los respaldos de Información.
4. Políticas, normas y procedimientos para la realización de Respaldos.

1. Sistemas de Información

La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas.

2. Equipos de Cómputo

Se debe tener en cuenta el catastro de Hardware, impresoras, lectoras, scanner, ploters, modems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.

- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a las computadoras personales con información importante o estratégica, y color verde a las demás estaciones.

- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

Prevención en el hardware

De acuerdo a la cantidad e importancia de los datos y equipos puedes considerar algunas de las siguientes recomendaciones:

- Contar con una unidad de energía de respaldo para que en caso de sufrir un corte de energía no se dañen los componentes del equipo, el disco duro o el sistema de archivos del servidor.
- Mantener el equipo en un lugar adecuado considerando las especificaciones técnicas del ambiente óptimo de operación en cuanto a temperatura, humedad, etc.
- Tener redundancia en los componentes. En este punto habrá que evaluar la importancia de los datos y la necesidad de la continuidad en el servicio debido al costo que puede implicar en la adquisición o almacenamiento de dispositivos, ver Figura 3.3. Se pueden tener discos duros, memoria, procesadores, ventiladores o hasta otro equipo de reserva en caso de que falle el principal. No es necesario tener un servidor idéntico al que está en operación, puede ser uno de menor capacidad que funcionará de forma interina mientras se lleva a cabo la recuperación del original. Se podría considerar utilizar otro servidor con otras funciones que también se encuentre en operación.

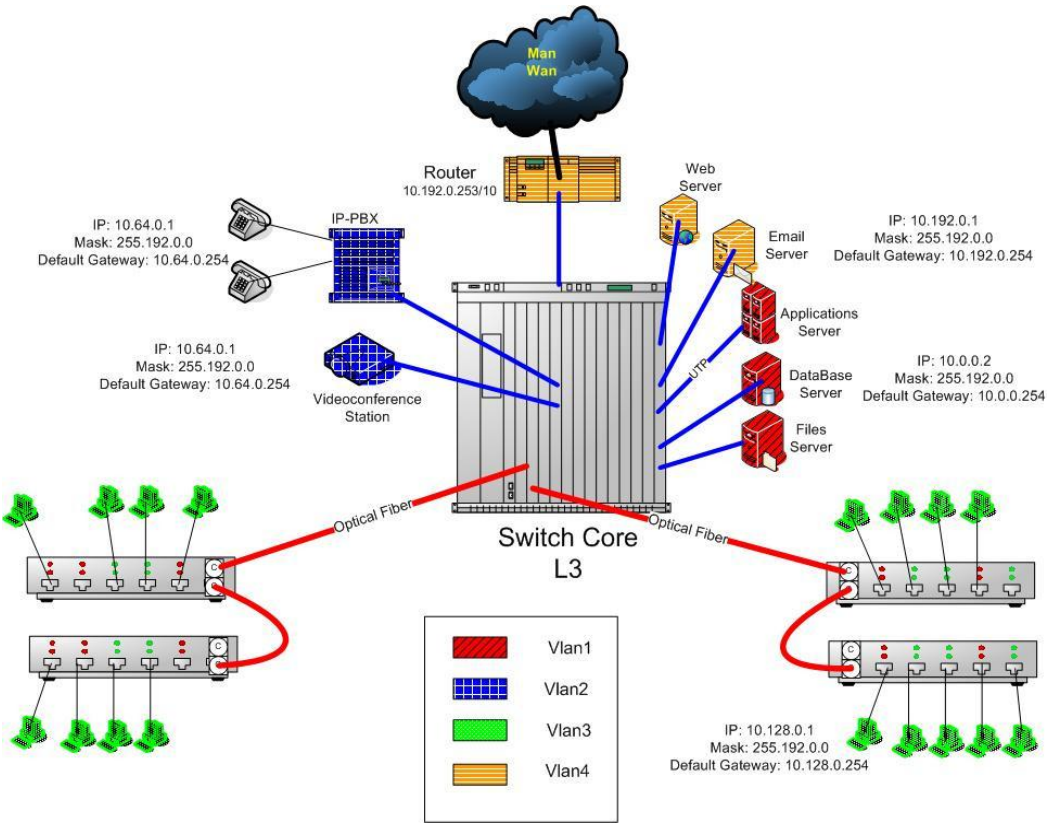


Figura 3.3 Almacenamiento de dispositivos

3. Obtención y almacenamiento de Copias de Seguridad (Respaldos)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:

- **Respaldo del sistema operativo:** o de todas las versiones de sistema operativo instalados en la Red.
- **Respaldo del software base:** Lenguajes de Programación utilizados en el desarrollo de los aplicativos institucionales.
- **Respaldo del software aplicativo:** respaldo de los programas fuente y los programas ejecutables.
- **Respaldo de los datos**: Base de datos, contraseña y todo archivo necesario para la correcta ejecución del software aplicativos de la institución.
- **Respaldo del hardware,** se puede implementar bajo dos modalidades:

Modalidad Externa: mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puestos a nuestra disposición al ocurrir una continencia mientras se busca una solución definitiva al siniestro producido.

En este Caso se debe definir claramente las condiciones del convenio a efectos de determinar la cantidad de equipos, periodos de tiempo, ambientes, entre otros, que se puede realizar con la entidad que cuente con equipo u mantenga un Plan de Seguridad de Hardware.

Modalidad Interna: si se dispone de mas de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas son susceptibles de ser usados como equipos de emergencia.

Es importante mencionar que en ambos casos se debe probar y asegurar que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas.

4. Políticas (Normas y Procedimientos)

Se debe establecer procedimientos, normas y determinación de responsabilidades en la obtención de los Respaldos o Copias de Seguridad. Se debe considerar:

- Periodicidad de cada tipo de respaldo: los respaldos de los sistemas informáticos se realizan de manera diferente.

- Respaldo de información de movimiento entre los periodos que no se sacan respaldos: días no laborales, feriados, etc. en estos días es posible programar un respaldo automático.

- Uso obligatorio de un formulario de control de ejecución del programa de respaldos diarios, semanales y mensuales: es un control a implementar, de tal manera de llevar un registro diario de los resultados de las operaciones de los respaldos realizados y su respectivo almacenamiento.

- Almacenamiento de los respaldos en condiciones ambientales optimas, dependiendo del medio magnético empleando.

- Reemplazo de los respaldos, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar. No se realiza reemplazos pero se realiza copias de las mismas, considerando que no se puede determinar exactamente el periodo de vida útil del dispositivo donde se ha realizado el respaldo.

- Almacenamiento de los respaldos en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local).

- Pruebas periódicas de los respaldos (Restauración), verificando su funcionalidad, a través de los sistemas comparando contra resultados anteriormente confiables. Esta actividad se realizara haciendo una comparación entre el contenido de la primera y segunda copia realizada o con el contenido de la información que se encuentra el Servidor de información histórica.

3.4 Actividades durante el Desastre

Presentada la contingencia o desastre de debe ejecutar las siguientes actividades planificadas previamente:

- Plan de Emergencias.
- Formación de Equipos.
- Entrenamiento.

Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro. Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas.

Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del siniestro causen mas daños o destrucciones. Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda. Todo el personal debe conocer lo siguiente:

- Localización de de vías de Escape o Salida: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina.

- Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local. Esa actividad se realizara utilizando las vías de escape mencionadas en el punto anterior.

- Ubicación y señalización de los elementos contra el siniestro: tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales.

- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

Formación de Equipos

Se deben establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

Entrenamiento

Se debe establecer un programa de practicas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc.

Es importante lograr que el personal tome conciencia en que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos y Ejecutivos, dando

el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

Prevención ante los desastres

- Incluir el software así como toda la información de datos, para facilitar la recuperación.
- Si es posible, usar una instalación remota de reserva para reducir al mínimo la pérdida de datos.
- Redes de Área de Almacenamiento (SANs) en múltiples sitios, que hace que los datos estén disponibles inmediatamente sin la necesidad de recuperarlos o sincronizarlos. Figura 3.4.
- Protectores de línea para reducir al mínimo el efecto de oleadas sobre un delicado equipo electrónico.
- El suministro de energía ininterrumpido (SAI).
- El software del antivirus.

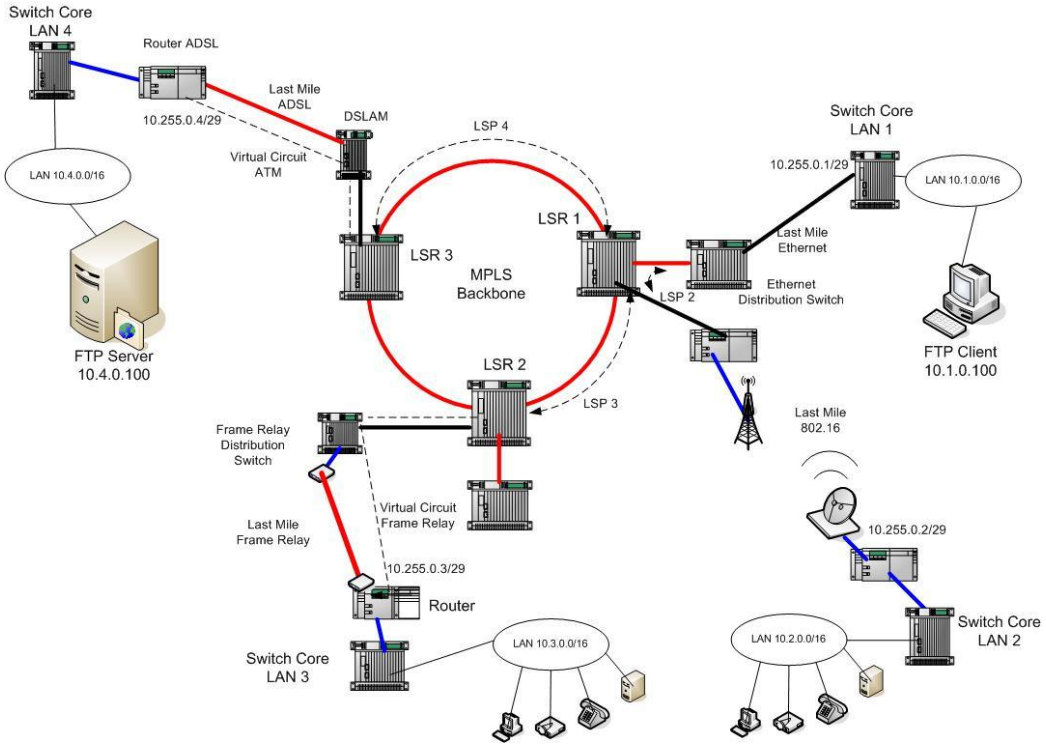


Figura 3.4 Red de Área de Almacenamiento

Prevención en el software

Para tener el software protegido y listo para la recuperación habrá que tener copias de respaldo que pueden ser de las siguientes formas:

- Discos duros en espejo, el cual tendrá una copia idéntica del software actual en operación para que en caso que se dañe un disco duro se pueda utilizar el otro de forma inmediata.

- Respaldos de archivos lo cuales tiene la opción de realizarse sobre el sistema completo de archivos o únicamente de los datos sensibles. Estos mismos podrán ser completos (full) si almacenan toda la información o incrementales si almacenan sólo los datos modificados en un periodo determinado de tiempo.

- Respaldos de archivos en dispositivos externos, siguen los parámetros anteriores y podrán ser en cintas magnéticas, dvd, cd's, discos duros externos, etc. Se puede considerar tenerlos almacenados en diferentes ubicaciones.

La recuperación es más controlada si se llevó a cabo un buen plan de respaldos. Los respaldos se pueden hacer:

- Al sistema operativo.
- A los programa y/o aplicaciones.
- A los datos.

La recomendación tener un programa de respaldos de manera automática. Cada cierto tiempo hacer respaldos completos y con más frecuencia hacer respaldos incrementales.

En el Plan de Recuperación ante Desastres deberá también describir el lugar donde se guardan estos respaldos y la forma en que se utilizarán para su recuperación.

En este punto se pueden utilizar herramientas de respaldo como el "Instant File Recovery" o alguna otra que le permita respaldar y posteriormente recuperar el respaldo lo más rápido posible.

3.5 Actividades después del desastre

Lo primero que habrá que hacer es un análisis del resultado del daño lo cual nos llevará a considerar los pasos de recuperación. Es posible que se dañe únicamente el software, el hardware o en el peor de los casos, ambos. Además, en cualquiera de los casos anterior habrá que analizar la posibilidad de recuperar los sistemas dañados, tanto físicos como lógicos.

Con base en los análisis anteriores es como se planteará el procedimiento a seguir.

Las actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

- Evaluación de Daños.
- Priorizar Actividades del Plan de Acción.

- Ejecución de Actividades.
- Evaluación de Resultados.
- Retroalimentación del Plan de Acción.

Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo.

Priorizar Actividades del Plan de Acción

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

Ejecución de actividades

La ejecución de actividades implica la creación de equipos de trabajo para realizar actividades previamente planificadas en el Plan de Acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación y, en caso de producirse un problema, reportarlo de inmediato a la Jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas:

- La primera la restauración del servicio usando los recursos de la institución o local de respaldo.

- La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta ultima etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución.

Evaluación de Resultados

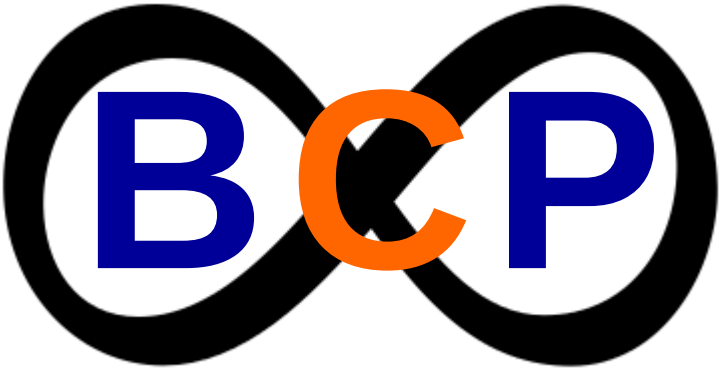
Una vez concluidas las labores de Recuperación de los sistemas que fueron afectado por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del Plan de Acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos de optimizar el Plan de Acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionan adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no contar con el Plan de Contingencias en la institución.



Business
Continuity Plan

Capítulo IV

Acciones frente al tipo de Riesgos

Acciones frente a los tipos de riesgo

4.1 Clase de Riesgo: Incendio o Fuego

Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. El procedimiento de respuesta a esta emergencia se observa en la Figura 4.1.

Cuando el daño ha sido menor:

1. Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
2. Se recogen los respaldos de datos, programas, manuales y claves.
3. Instalar el sistema operativo.
4. Restaurar la información de las bases de datos y programas.
5. Revisar y probar la integridad de los datos.

Figura 4.1 Diagrama de respuesta de emergencia de “Incendio”

4.2 Procedimiento para: Antes, Durante y Después de un Incendio

Antes:

- Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
- Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
- Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.
- No almacenar sustancias y productos inflamables.
- No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
- Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Seguridad.
- Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
- Tener a la mano los números telefónicos de emergencia.
- Portar siempre la foto check de identificación.

Durante:

- Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente del centro de cómputo.
- Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios,

solicitar ayuda.

- Si el fuego esta fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.

- No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.

- Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de el, intenta el traslado a pisos superiores.

- Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.

- Si es posible mojar la ropa.

- Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

Después:

- Retirarse inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.

- No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.

- El personal calificado realizara una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.

- Colaborar con las autoridades.

4.3 Clase de Riesgo: Robo común de equipos y archivos

Analizar las siguientes situaciones:

- En qué tipo de vecindario se encuentra la Institución.

- Las computadoras se ven desde la calle.

- Hay personal de seguridad en la Institución y están ubicados en zonas estratégicas.

- Cuánto valor tienen actualmente las Bases de Datos.

- Cuánta pérdida podría causar en caso de que se hicieran públicas.

- Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.

- Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

4.4 Clase de Riesgo: Vandalismo

Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

A continuación se menciona una serie de medidas preventivas:

- Establecer vigilancia mediante cámaras de seguridad en el Site, el cual registre todos los movimientos de entrada del personal.

- Instalar identificadores mediante tarjetas de acceso.

- Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).

Los principales conflictos que pudieran presentarse son:

- En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.

- Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la ubicación de la institución, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc.; en un sitio alterno, ya que no contarían con copia de la información.

4.5 Clase de Riesgo: Equivocaciones

- Cuánto saben los empleados de computadoras o redes.

- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

- Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

4.6 Clase de Riesgo: Fallas en los equipos

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración. El procedimiento de respuesta a esta emergencia se ve en la Figura 4.2.

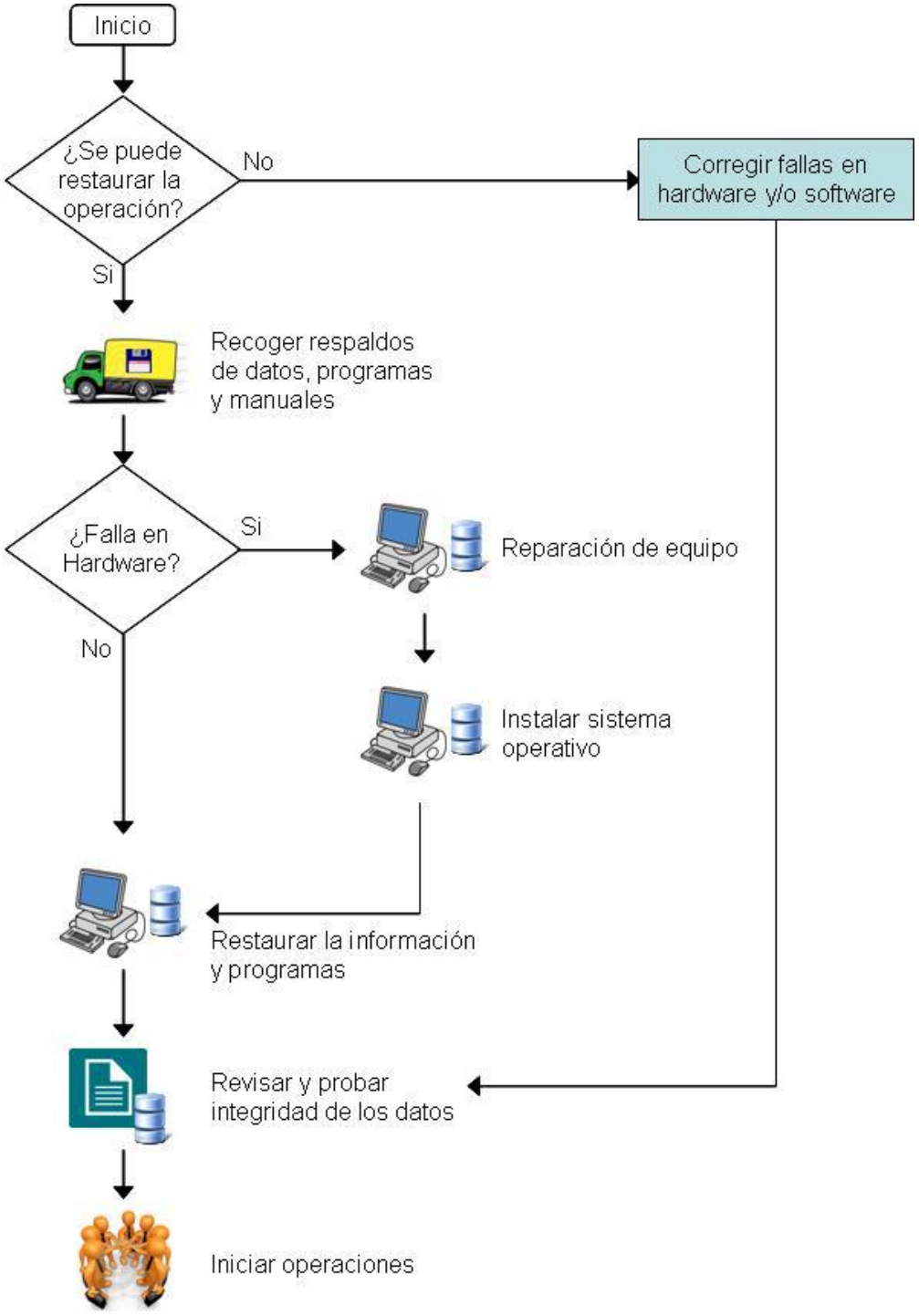


Figura 4.2 Diagrama de respuesta de emergencia de "Fallas en Hardware o Software"

Casos

Error Físico de Disco de un Servidor (Sin RAID)

Dado el caso crítico en que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- Ubicar el disco con falla.
- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
- Bajar el sistema y apagar el equipo.
- Retirar el disco dañado y reponerlo con otro del mismo tipo, formatearlo y darle partición.
- Restaurar el último respaldo, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- Verificación el buen estado de los sistemas.
- Habilitar las entradas al sistema para los usuarios.

Error de Memoria RAM y Tarjeta(s) Controladora(s) de Disco

En el caso de las memorias RAM, se dan los siguientes problemas:

- El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores.
- Es recomendable que el servidor cuente con ECC (“Error Correct Checking”), por lo tanto si hubiese un error de paridad, el servidor se auto corregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por

red y teléfono a jefes de área.

- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias dañadas.
- Retirar las memorias dañadas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el dispositivo activo, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable.
- Habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

4.7 Clase de Riesgo: Acción de Virus Informático

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:
Para servidor:

- Se contará con antivirus para el sistema; aislar el virus para su futura investigación.
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

- Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.
- Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado, reconstruir el “Master Boot” del disco duro.

4.8 Clase de Riesgo: Accesos No Autorizados

Enfatiza los temas de:

Contraseñas. Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos infructuosos. El centro de cómputo implementa la complejidad en sus contraseñas de tal forma que sean mas de siete caracteres y consistentes en números y letras.

Trampas o Jaula al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

Privilegio. En los sistemas informáticos, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red.

Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en “Grupos” con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

4.9 Clase de Riesgo: Fenómenos naturales

Terremoto e Inundación

- Para evitar problemas con inundaciones ubicar los servidores a un promedio de 50 cm. de altura.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- **Cuando el daño del edificio ha sido mayor**, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.
- **Cuando el daño ha sido menor se procede**: Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
- Recoger los respaldos de datos, programas, manuales y claves.
- Instalar el sistema operativo.
- Restaurar la información de las bases de datos y programas.
- Revisar y probar la integridad de los datos.

En la Figura 4.3, se muestra el diagrama de respuesta ante fenómenos naturales.

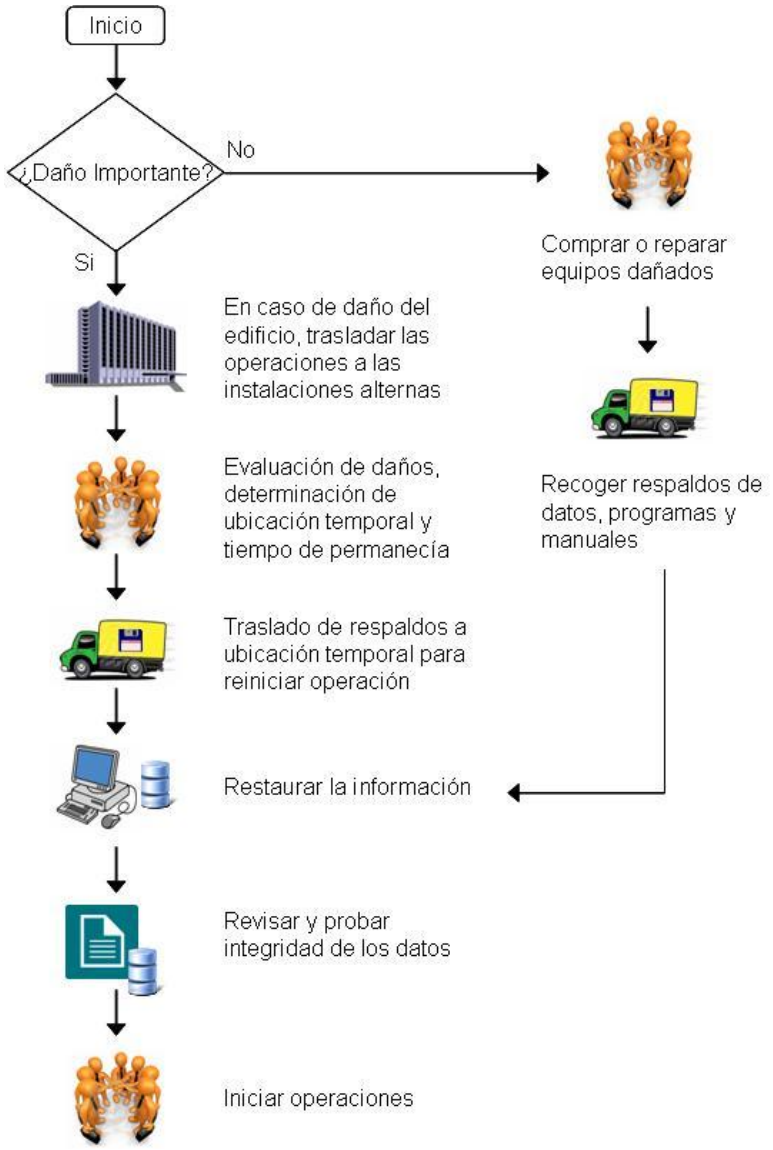


Figura 4.3 Diagrama de respuesta de “Fenómenos Naturales”

4.10 Clase de Riesgo: Robo de Datos

Se previene a través de las siguientes acciones:

Acceso no Autorizado: Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Área de Sistemas.
- Computadoras personales y/o terminales de la red.
- Información confidencial.

Control de acceso al Área de Sistemas: El acceso al área de Informática estará restringido:

- Sólo ingresan al área el personal que trabaja en el área.
- El ingreso de personas extrañas solo podrá ser bajo una autorización.

Acceso Limitado a los Terminales: Cualquier Terminal que puede ser utilizado como acceso a los datos de un Sistema, las siguientes restricciones pueden ser aplicadas:

- Determinación de los períodos de tiempo para los usuarios o las terminales.
- Designación del usuario por Terminal.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un Terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).

Niveles de Acceso: Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas.

- Nivel de consulta de la información.- privilegio de lectura.
- Nivel de mantenimiento de la información.- El concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.

4.11 Clase de Riesgo: Manipulación y Sabotaje

La protección contra el sabotaje requiere:

- Una selección rigurosa del personal.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Asignar a una persona la responsabilidad de la protección de los equipos en cada área.

A continuación, algunas medidas que se deben tener en cuenta para evitar

acciones hostiles:

- Mantener una buena relación de trabajo con el departamento de policía local.
- Mantener adecuadamente los archivos de respaldo.
- Planear para probar el funcionamiento de los respaldos de los servicios de procesamiento de datos.
- Identificar y establecer operaciones criticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Usar registros de auditorias o de bitácoras como medida de seguridad.

Cuando la información eliminada se pueda volver a capturar, se procede con lo siguiente:

- Capturar los datos faltantes en las bases de datos de los sistemas.
- Revisar y probar la integridad de los datos.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectados. El diagrama de respuesta cuando se presenta una manipulación y/o sabotaje puede observarse en la Figura 4.4.

4.12 Simulacros

Es conveniente realizar con alguna frecuencia diferentes tipos de simulacros de desastre, desde instalar el sistema operativo hasta la recuperación de los últimos datos. Este programa de simulacros también podrá estar contenido en el Plan de Recuperación ante Desastres.

Durante la realización de un simulacro de manera posterior podrá modificarse o adicionarse alguna característica al Plan de Recuperación ante Desastres, así mismo, se puede llevar una bitácora de simulacros y los sucesos ocurridos durante el mismo para tenerlos en cuenta a la hora de llevar a cabo una recuperación.

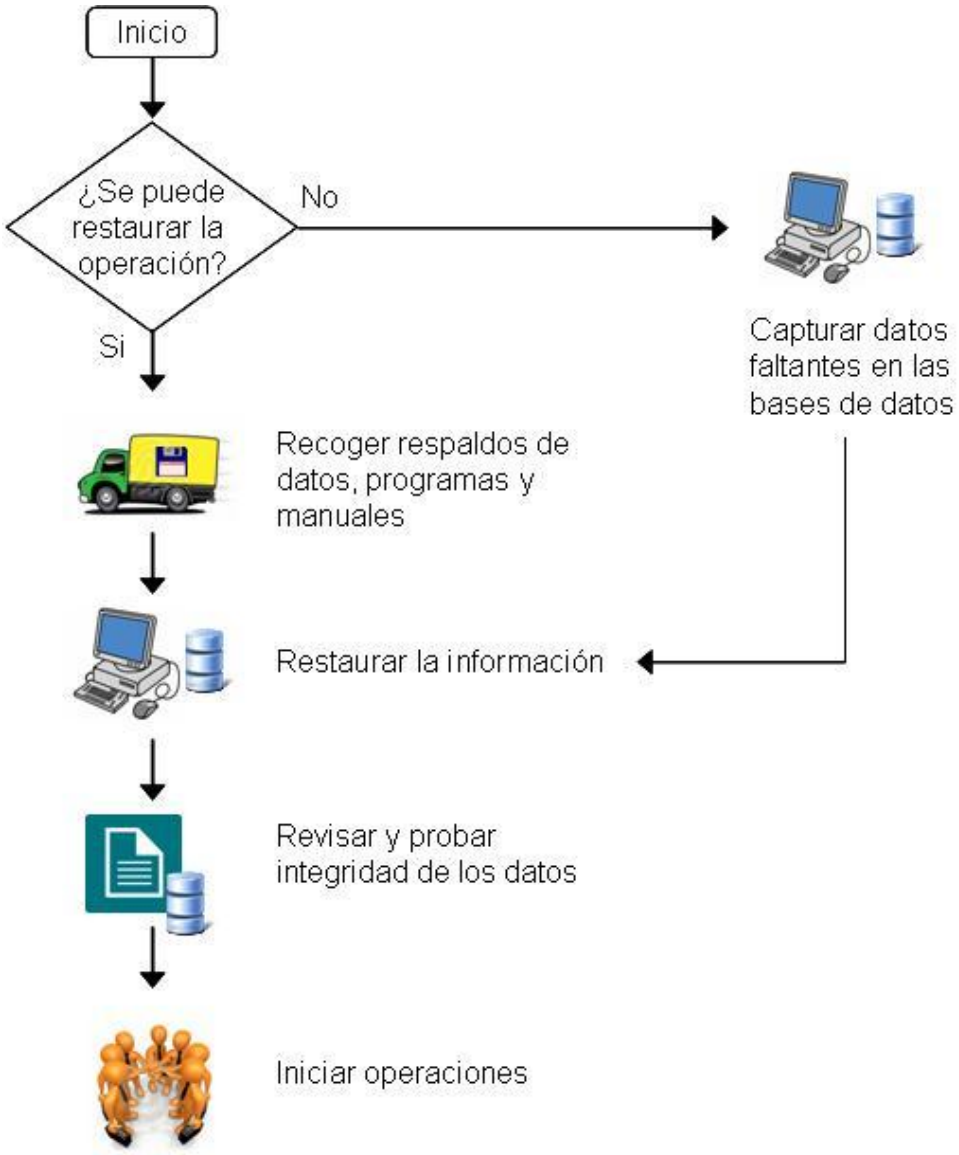
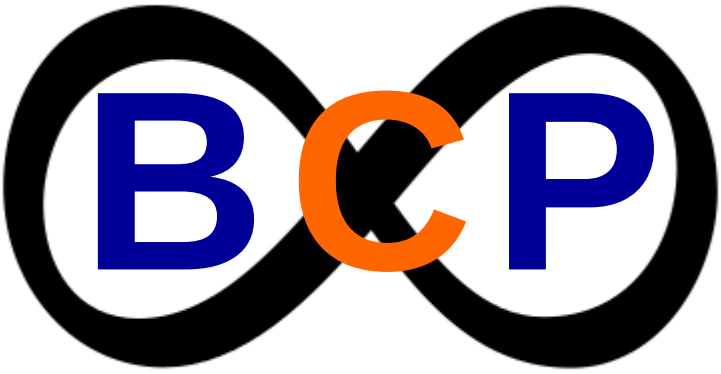


Figura 4.4 Diagrama de respuesta ante “Manipulación y Sabotaje”



Business
Continuity Plan

Capítulo V

Gestión de la Continuidad del Negocio (GCN / BCP)

5.1 Perspectiva general de la gestión de la continuidad del negocio (GCN / BCP)

Normalmente, durante la interrupción, imprevista, de la actividad de una organización, se generan pérdidas financieras, sin embargo, el impacto más significativo es normalmente la pérdida de imagen corporativa o la pérdida de confianza que resulta de un incidente mal gestionado. Por el contrario, un incidente bien gestionado puede realzar la imagen de una organización.

La Gestión de la Continuidad de Negocio (GCN), ver Figura 5.1, es un proceso holístico de gestión, que identifica los impactos de incidentes potenciales que amenazan una organización y proporciona un marco para desarrollar una respuesta eficaz y una capacidad de recuperación de la organización, que proteja los intereses de sus grupos de interés, su imagen, el valor de su marca y sus actividades.

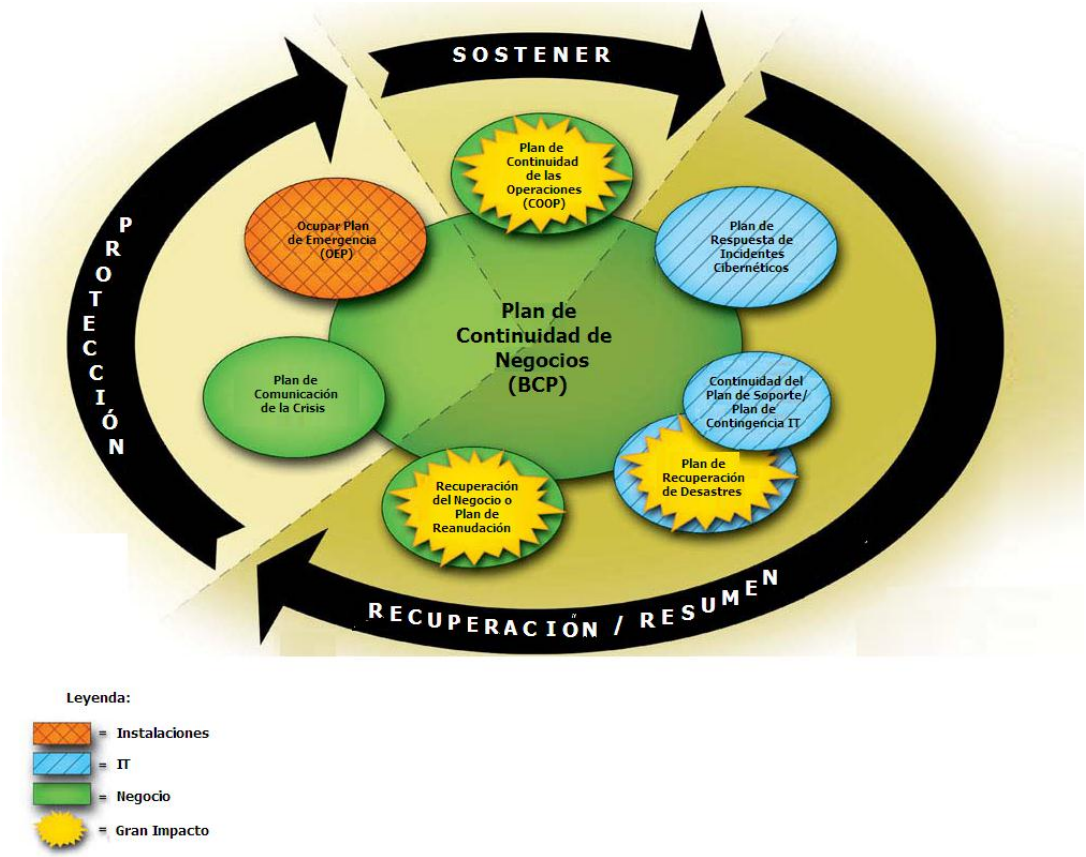


Figura 5.1 Plan de Continuidad de Negocios (BCP)

La GCN se desarrolla en la organización tanto verticalmente (niveles estratégico, táctico y operativo), como horizontalmente (en todas sus sedes y su cadena de valor, incluyendo la propia cadena de suministro).

La responsabilidad del desarrollo de la GCN recae en los componentes de al Alta Dirección, quienes deberán tener en cuenta los intereses a largo plazo del personal, los clientes y de todos los grupos de interés que dependen de una u otra manera de la organización.

Por tanto, la GCN debe estar completamente integrada en el proceso de gestión de la organización, formando parte de su cultura.

En la actualidad, existen diferentes iniciativas a nivel mundial para normalizar los Sistemas de Gestión de la Continuidad de Negocio, SGCN, siendo el estándar de facto la familia de normas británicas BS 25000, la BS 25999-1:2006 desarrollada como guía de referencia del SGCN y la BS 25999-2:2007 como especificación del SGCN y otras en desarrollo como la BS 25777 sobre continuidad de servicios TI.

5.2 ¿Qué es la BCP/GCN?

La gestión de la continuidad del negocio (GCN) es un proceso perteneciente a, e impulsado por, el negocio, que establece un marco estratégico y operativo a la medida de las necesidades, el cual:

- Mejora de manera proactiva la fortaleza de una organización para hacer frente a la interrupción de su capacidad para alcanzar sus objetivos clave.

- Proporciona un método probado para restablecer la capacidad de una organización para proveer sus productos y servicios clave a un nivel acordado, dentro de un período de tiempo acordado luego de la interrupción; y

- Ofrece una capacidad comprobada para gestionar la interrupción de un negocio y para proteger la reputación y marca de la organización

Aunque los procesos individuales de continuidad del negocio pueden cambiar de acuerdo con el tamaño, estructura y responsabilidades de una organización, los principios básicos son exactamente los mismos para organizaciones benéficas, públicas o privadas, más allá de su tamaño, alcances o complejidad.

5.3 La GCN y la estrategia organizativa

Todas las organizaciones, sean grandes o pequeñas, tienen metas y objetivos, tales como crecer, proveer servicios y adquirir otros negocios. Estas metas y objetivos por lo general se cumplen mediante planes estratégicos diseñados para lograr los fines de corto, mediano y largo plazo de una organización. Comprender la GCN en los niveles más elevados de una organización garantizará que estas metas y objetivos no se vean comprometidos por interrupciones inesperadas.

Las consecuencias de un incidente varían y pueden tener un gran impacto. Estas consecuencias pueden implicar pérdida de vidas, pérdida de activos o ingresos, o la incapacidad para proveer productos y servicios de los que dependen la estrategia, la reputación e incluso la supervivencia de la organización.

La GCN debe reconocer la importancia estratégica de las partes interesadas

identificadas. Además, a medida que se exponen las consecuencias de una interrupción, surgen nuevas partes interesadas que tienen un impacto directo sobre el alcance eventual de los daños. Por ejemplo, grupos y movimientos pueden tratar de presionar a una organización cuando ocurre una interrupción del negocio.

Todos estos temas son motivo de preocupación estratégica para la organización.

5.4 La GCN – su relación con la gestión de riesgo

La GCN es el complemento de un marco de gestión de riesgo cuya misión es comprender los riesgos de operaciones o negocios, y las consecuencias de dichos riesgos.

La gestión de riesgo busca administrar el riesgo existente en torno de los productos y servicios clave que provee una organización. La provisión de productos y servicios puede ser interrumpida por una amplia variedad de incidentes, muchos de los cuales son difíciles de predecir o de analizar según sus causas. Al centrarse en el impacto de la interrupción, la GCN identifica aquellos productos y servicios de los que depende la organización para su supervivencia, y es capaz de identificar aquello que se requiere para que la organización continúe cumpliendo con sus obligaciones. Por medio de la GCN, una organización puede descubrir qué debe hacer antes de que ocurra un incidente para proteger a su personal, su local, su tecnología, su información, su cadena de suministros, a sus partes interesadas y su reputación.

Luego de adquirir este conocimiento, la organización podrá tener una visión realista de las respuestas que es más probable que requiera mientras, y cuando, ocurre una interrupción, de manera que tendrá la seguridad de poder gestionar cualquiera de sus consecuencias sin ningún retraso inaceptable en la provisión de sus productos o servicios.

Una organización que cuente con medidas adecuadas de GCN podría ser capaz de sacar provecho de oportunidades que tengan un riesgo elevado.

5.5 Ventajas al incorporar GCN en una organización

La GCN es un elemento importante para una buena gestión del negocio, una buena provisión de servicios y una buena prudencia empresarial.

Los gerentes y propietarios tienen la responsabilidad de mantener la capacidad de la empresa para operar sin interrupciones. Las organizaciones constantemente asumen compromisos o tienen la obligación de proveer productos y servicios, es decir, celebran contratos o despiertan expectativas. Todas las organizaciones tienen responsabilidades morales y sociales, en particular cuando proveen una respuesta de emergencia o un servicio público o de beneficencia.

En algunos casos, las organizaciones deben asumir la GCN debido a

obligaciones estatutarias o de reglamentación.

Toda actividad de negocios está sujeta a interrupciones, tales como fallas en la tecnología, inundaciones, interrupción de servicios y terrorismo. La GCN provee la capacidad para reaccionar de manera adecuada a interrupciones operativas, a la par que se protege el bienestar y la seguridad, ver Figuras 5.2 y 5.3.

En la actualidad, la GCN debería ser considerada no como un costoso proceso de planificación, sino como uno que añade valor a la organización.

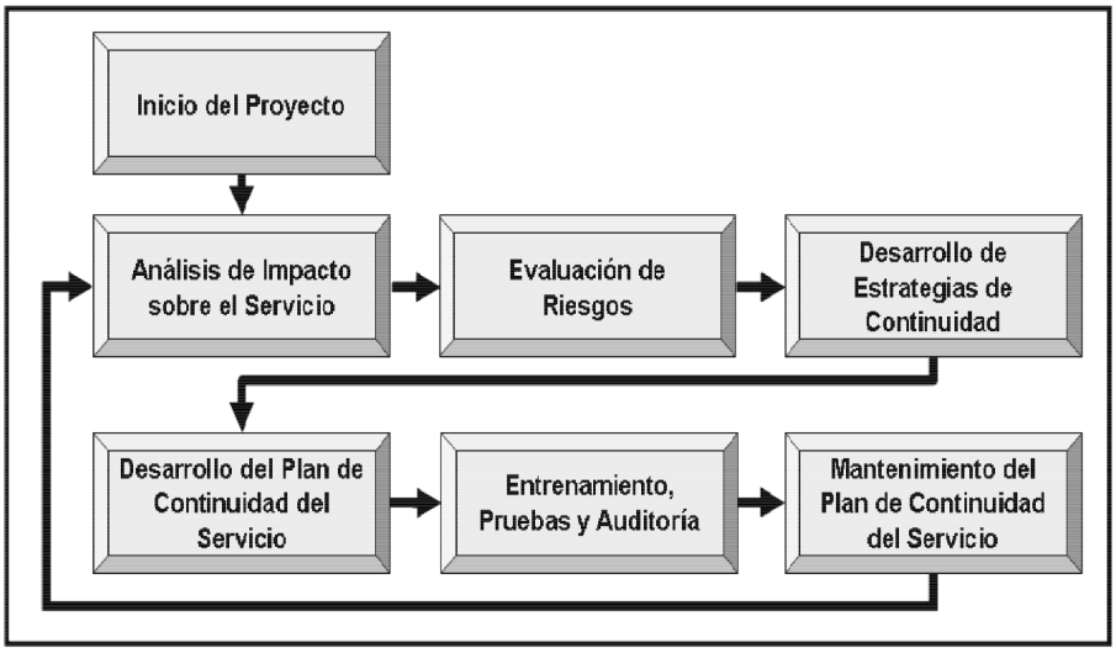


Figura 5.2 Flujo de para el desarrollo del GCN

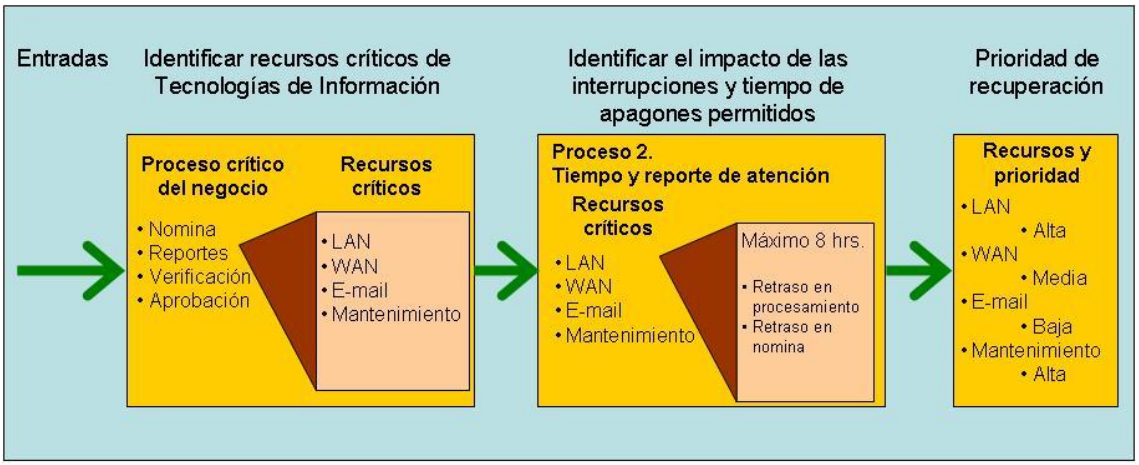


Figura 5.3 Esquema de prioridad de recuperación en GCN

5.6 Los beneficios de un programa eficaz de GCN

Los beneficios de un programa eficaz de GCN son que la organización:

- Es capaz de identificar de manera proactiva los impactos de una interrupción operativa;
- Tiene en marcha un proceso de respuesta eficaz a interrupciones, que minimiza el impacto de las mismas sobre la organización;
- Mantiene su capacidad para gestionar riesgos no asegurables;
- Alienta el trabajo de equipo entre sus diversas unidades;
- Es capaz de demostrar una respuesta verosímil por medio de un proceso de práctica;
- Podría mejorar su reputación; y
- Podría obtener una ventaja competitiva, gracias a su capacidad demostrada de mantener la provisión de productos y servicios.

Los resultados de un programa eficaz de GCN

Considerando que todos los sistemas de procesamiento de información, infraestructura, desarrollos, aplicaciones, archivos, procesos de desarrollo y mantenimiento de sistemas de información de una empresa, deben ser controlados, además de tener una adecuada seguridad. Con base a lo anterior, los resultados de un programa eficaz de GCN son los siguientes:

- Se protege los productos y servicios clave, asegurando su continuidad;
- Se activa una capacidad de gestión de incidentes para proveer una respuesta eficaz;
- Se desarrolla, documenta y comprende de manera adecuada el conocimiento que la organización tiene de sí misma y de sus relaciones con otras importantes organizaciones, entes reguladores o entidades gubernamentales, autoridades locales y los servicios de emergencia;
- El personal es capacitado para responder de manera eficaz a un incidente o interrupción, mediante la práctica adecuada;
- Se comprende cuáles son las necesidades de las partes interesadas y se está en capacidad de proveerlas;
- El personal recibe el respaldo y la información adecuada en caso de una interrupción;

- Se protege la cadena de suministros de la organización;
- Se protege la reputación de la organización; y
- la organización mantiene el cumplimiento de sus obligaciones legales y de reglamentación.

5.7 Elementos del ciclo de vida de la gestión de la continuidad del negocio

El ciclo de vida de la GCN comprende seis elementos, como se aprecia en la Figura 5.4.

Estos pueden ser implementados por organizaciones de todos los tamaños, en todos los sectores: público, privado, sin fines de lucro, educativo, de manufactura, etcétera. Los alcances y estructura de un programa de GCN pueden variar, y el esfuerzo que se le destine deberá adaptarse a las necesidades de cada organización en particular, pero, aun así, será necesario incluir los siguientes elementos fundamentales.

a) **Gestión del programa de GCN**. La gestión del programa permite establecer (en caso sea necesario) y mantener la capacidad de continuidad del negocio de una forma adecuada al tamaño y complejidad de la organización.

b) **Comprender la organización**. Las actividades asociadas con "Comprender la organización" proporcionan información que permite priorizar los productos y servicios de una organización, y el grado de urgencia de las actividades requeridas para su provisión. Esto establece las necesidades que determinarán la selección de estrategias adecuadas de GCN.

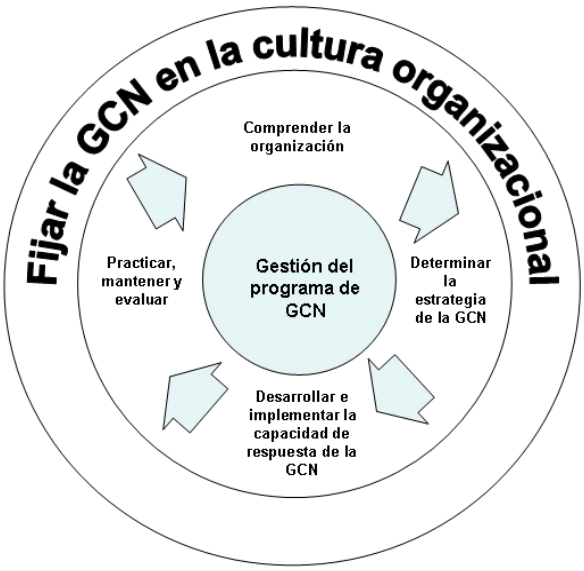


Figura 5.4 El ciclo de vida de la gestión de continuidad del negocio

b) **Determinar la estrategia de continuidad del negocio.** Determinar la estrategia de continuidad del negocio permite evaluar una amplia variedad de estrategias. Ello permite escoger una respuesta adecuada para cada producto o servicio, de manera tal que la organización pueda continuar proveyendo dichos productos y servicios:

- A un nivel aceptable de operación; y
- Dentro de un período de tiempo aceptable durante y después de una interrupción. La elección que se haga deberá tomar en cuenta la fortaleza y las opciones de contramedida que ya se encuentren presentes dentro de la organización.

d) **Desarrollar e implementar la capacidad de respuesta de la GCN.** Desarrollar e implementar una respuesta de GCN tiene como resultado la creación de un marco de gestión y una estructura de gestión de incidentes, continuidad del negocio y planes de recuperación del negocio que detallan los pasos que deberán tomarse durante y después de un incidente para mantener o restablecer las operaciones.

e) **Práctica, mantenimiento y evaluación de acuerdos de GCN.** La práctica, mantenimiento, evaluación y auditoria de la GCN conduce a que una organización sea capaz de:

- Demostrar hasta qué punto están completos, son vigentes y precisos sus planes y estrategias; e
- identificar oportunidades de mejora.

f) **Fijar la GCN en la cultura organizacional.** Fijar la GCN en la cultura organizacional permite que la GCN se convierta en parte de los valores fundamentales de la organización y que infunda seguridad en todas las partes interesadas sobre la capacidad de la empresa para hacerse cargo de las interrupciones.

5.8 Las políticas de la gestión de la continuidad del negocio

Perspectiva general

Las políticas de GCN definen los siguientes procesos:

- Las actividades de montaje para determinar una capacidad de continuidad del negocio; y
- La gestión y el mantenimiento continuos de la capacidad de continuidad del negocio.

Las actividades de montaje incluyen la especificación, diseño completo, construcción, implementación y práctica inicial de la capacidad de continuidad

del negocio.

Las actividades continúas de mantenimiento y gestión incluyen fijar la continuidad del negocio dentro de la organización, realizar prácticas de manera regular con los planes y actualizarlos y difundirlos, específicamente cuando se produce algún cambio importante en las instalaciones, el personal, el proceso, el mercado, la tecnología o la estructura organizativa.

Contexto

La organización debería asegurarse de que sus políticas de GCN sean adecuadas a la naturaleza, escala, complejidad, geografía e importancia de sus actividades de negocio, y que reflejen su cultura, dependencias y entorno operativo. Las políticas de GCN definen las necesidades del proceso para garantizar que los acuerdos de continuidad del negocio sigan cumpliendo con las necesidades de la organización en caso de algún incidente. Estas políticas deberían asegurar que la capacidad de continuidad de un negocio se difunda dentro de la cultura de la organización. La capacidad de GCN debería estar integrada a la actividad de gestión de cambios de la organización, de manera tal que sea incluida en el crecimiento y desarrollo de los productos y servicios de la organización.

Desarrollo de las políticas de continuidad del negocio

La organización debería desarrollar políticas de continuidad del negocio que establezcan los objetivos de la GCN dentro de la organización. Inicialmente, esto podría hacerse por medio de una declaración de intenciones de alto nivel que sea refinada y mejorada a medida que se desarrolla la capacidad.
Las políticas de continuidad del negocio deberían proporcionar a la organización con principios documentados a los cuales aspirar y en comparación con los cuales debe medirse la capacidad de continuidad del negocio. Las políticas de GCN deberían ser reconocidas en el más alto nivel, por ejemplo: el presidente de la junta directiva o su representante electo.

La organización podría tomar en consideración lo siguiente al desarrollar sus políticas de GCN:

- Definir los alcances de la GCN dentro de la organización;
- Obtener recursos para la GCN;
- Definir los principios, directrices y estándares mínimos de GCN para la organización;
- Mencionar cualquier estándar, reglamentación o políticas pertinentes que deban ser incluidos o puedan emplearse como punto de referencia.

La organización debería mantener y revisar con regularidad sus políticas, estrategias, planes y soluciones de GCN, conforme a las necesidades de la organización, ver Figura 5.5.

Los alcances de las políticas de GCN deberían definir claramente cualquier limitación o exclusión que sea aplicable, por ejemplo: exclusiones geográficas o de productos.

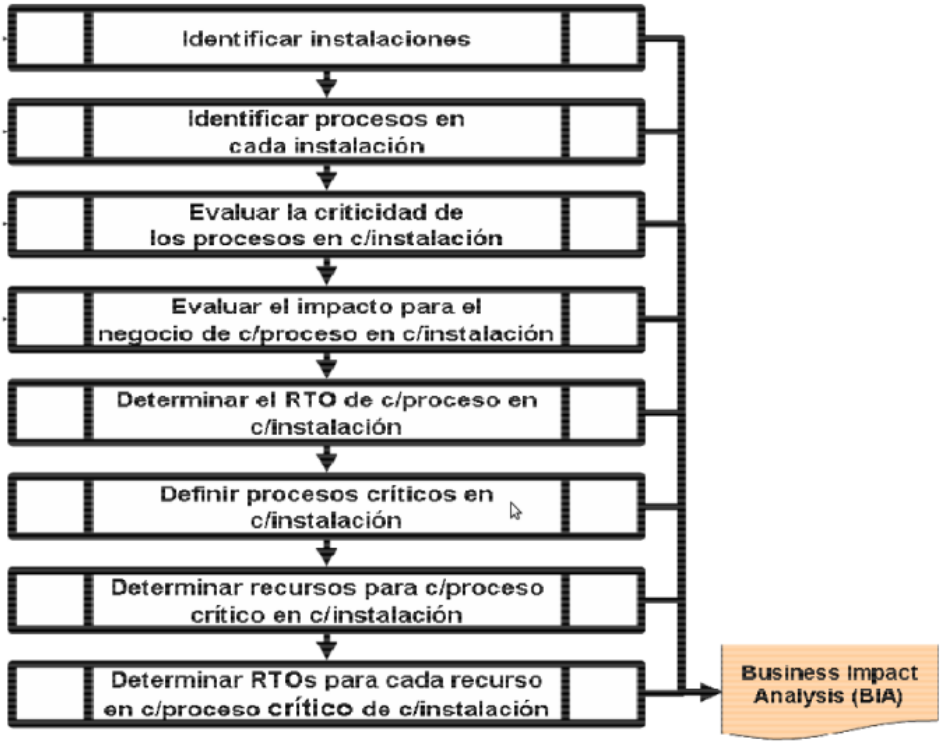


Figura 5.5 Revisión y evaluación de procesos

5.9 Alcances del programa de GCN

La alta gerencia podría determinar los alcances del programa de GCN mediante la identificación de productos y servicios clave que respalden los objetivos, las obligaciones y deberes estatutarios de la organización. La determinación de lo que es clave debería ser consecuente con el análisis de impacto del negocio con un alto nivel de atención.

Actividades tercerizadas

Si un producto, servicio o actividad ha sido tercerizado, la responsabilidad de riesgo por tal producto servicio o actividad sigue siendo de la organización. En consecuencia, toda organización debería asegurarse de que sus proveedores clave o socios de tercerización tienen acuerdos de GCN eficaces en marcha. Un método para lograr esto es obtener evidencia de auditoria de la viabilidad de los planes de continuidad y programas de práctica y mantenimiento de los proveedores clave.

5.10 Gestión del programa de GCN

La gestión del programa es parte fundamental del proceso de GCN. Una gestión eficaz del programa determina el enfoque de la organización respecto

de la continuidad del negocio.

La participación de la alta gerencia es clave para asegurar que el proceso de GCN es correctamente introducido, adecuadamente respaldado y establecido como parte de la cultura organizacional.

Perspectiva general

Debería ponerse en marcha un programa de GCN para alcanzar los objetivos definidos en las políticas de continuidad del negocio. La gestión del programa de GCN incluye tres pasos:

- Asignar responsabilidades;
- Implementar la continuidad del negocio en la organización; y
- La gestión continúa de la continuidad del negocio.

Asignar responsabilidades (Gobierno)

La gerencia de la organización debería:

- Designar o nombrar a una persona que tenga la antigüedad y autoridad adecuadas para hacerse responsable de las políticas y la implementación de la GCN; y
- Designar o nombrar a una o más personas para que se encarguen de la implementación y el mantenimiento del programa de GCN.

Si la estructura de la organización así lo establece, la alta gerencia podría nombrar representantes en diversas áreas del negocio, según su función o ubicación, para que apoyen en la implementación del programa de GCN.

Las funciones, responsabilidades, obligaciones y autoridad respectivas deberían formar parte de la descripción de los diversos cargos y de las habilidades que se requieren para ocuparlos.

El proceso de auditoria de la organización debería evaluar dichas responsabilidades.

Es posible reforzar estas responsabilidades incluyéndolas en las políticas de evaluación, compensaciones y reconocimientos de la organización.

Implementar la continuidad del negocio en la organización

Las actividades para implementar un programa de continuidad del negocio deberían incluir el diseño, elaboración e implementación del programa.

La organización debería:

- difundir el programa entre sus partes interesadas;
- organizar o proveer una capacitación adecuada para el personal; y
- hacer prácticas para probar la capacidad de continuidad del negocio.

La organización podría adoptar un método reconocido de gestión de proyectos para asegurarse de que la implementación se realice de manera eficaz.

5.11 Gestión continúa

Perspectiva general

Las actividades de gestión continua deberían garantizar que la continuidad del negocio se fije dentro de la organización. Cada componente de la capacidad de continuidad del negocio de una organización debería ser evaluado, practicado y actualizado de manera regular. Además, los acuerdos y planes de continuidad del negocio también deberían ser evaluados y actualizados cuando se produce un cambio importante en el entorno operativo, el personal, los procesos o la tecnología de la organización, y cuando una práctica o incidente saca a relucir alguna deficiencia.

Mantenimiento continúo

No importa cómo se provea de recursos a la GCN, hay actividades que deberían llevarse a cabo tanto en un inicio como de manera continua.

Estas podrían incluir:

- Definir los alcances, funciones y responsabilidades de la GCN;
- Designar a una persona o equipo adecuado para gestionar la capacidad continua de GCN;
- Mantener la vigencia del programa de continuidad del negocio mediante la práctica adecuada;
- Promover la continuidad del negocio en todos los ámbitos de la organización y más allá, cuando sea oportuno;
- Aplicar el programa de prácticas;
- Coordinar la evaluación y la actualización regular de la capacidad de continuidad del negocio, incluyendo la revisión y corrección de evaluaciones de riesgo y análisis de impacto del negocio (AIN);
- Mantener una documentación que se adecue al tamaño y complejidad de la organización;
- Monitorear el desempeño de la capacidad de continuidad del negocio;

- Administrar los costos asociados con la capacidad de continuidad del negocio; y

- Establecer y monitorear los regímenes de gestión de cambio y gestión de la sucesión.

Ciclo del PDCA

El ciclo PDCA, también conocido como "Círculo de Deming" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua, como se muestra en la Figura 5.6. Es muy utilizado en los Sistemas de Gestión de Sistemas de Información.

Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planear, Hacer, Verificar, Mejorar).

PLAN (Planear)

Planificar todo lo que se desea realizar.

DO (Hacer)

Poner en practicado todo lo anteriormente planeado.

CHECK (Verificar)

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada.

- Documentar las conclusiones.

ACT (Mejorar)

- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario.

- Aplicar nuevas mejoras, si se han detectado errores en el paso anterior.

- Documentar el proceso.

Figura 5.6 Espiral de mejora continua

5.12 Documentación de la GCN

Las personas asignadas al mantenimiento de la continuidad del negocio deberían crear y mantener la documentación de la continuidad del negocio. Esto podría incluir lo siguiente:

a) políticas de GCN:
   - declaración de alcances de la GCN,
   - términos de referencia de la GCN;
b) análisis de impacto del negocio (AIN);
c) evaluación de riesgo y amenazas;
d) estrategia/estrategias de GCN;
e) programa de toma de conciencia;
f) programa de capacitación;
g) planes de gestión de incidentes;
h) planes de continuidad del negocio;
i) planes de recuperación del negocio;
j) cronogramas e informes de las prácticas;
k) acuerdos y contratos de niveles de servicio.

Comprender la organización

El objetivo de este elemento del ciclo de vida de la GCN es ayudar a comprender la organización mediante la identificación de sus productos y servicios clave, y de las actividades críticas y los recursos que los respaldan. Este elemento garantiza que el programa de GCN está alineado con los objetivos, las obligaciones y los deberes estatutarios de la organización.

Es importante tener bien definidos los roles en el GCN.

Introducción

En un contexto de continuidad del negocio, la comprensión de la organización es resultado de:

- Identificar los objetivos, partes interesadas, obligaciones y deberes estatutarios de la organización, y el entorno en el que opera la organización;
- Identificar las actividades, activos y recursos, incluyendo a aquellos externos a la organización, que respaldan la provisión de estos productos y servicios;
- Evaluar el impacto y las consecuencias en el tiempo de posibles fallas en estas actividades, activos y recursos;
- Identificar y evaluar las amenazas encontradas que podrían interrumpir la provisión de los productos y servicios clave de la organización, y las actividades, activos y recursos críticos que los respaldan.

Es importante que la organización tenga una buena comprensión de:

- Las interdependencias de sus actividades, y
- Cualquier dependencia que ella tenga de organizaciones externas, y cualquier dependencia que otros tengan de ella, ver Figura 5.7.

Figura 5.7 Procesos críticos de negocio, se incluyen aspectos externos como proveedores y clientes

5.13 Análisis de Impacto del Negocio (AIN)

La organización debería determinar y documentar el impacto que puede tener una interrupción sobre las actividades que respaldan sus productos y servicios clave. A este proceso se le conoce como análisis de impacto del negocio (AIN), en sus siglas en idioma Inglés BIA ("Business Impact Analysis"), ver Figura 5.8.

Para cada actividad que respalda la provisión de productos y servicios clave dentro del alcance de su programa de GCN, la organización debería:

a) Evaluar en el tiempo los impactos que ocurrirían si hubiera una interrupción de la actividad;

b) Establecer un período máximo tolerable de interrupción de cada actividad mediante la identificación de:

- El período máximo de tiempo luego del inicio de una interrupción dentro del cual es necesario reanudar la actividad,
- El nivel mínimo en el que la actividad debe ser realizada tras su reanudación,
- El período de tiempo dentro del cual se requiere volver a los niveles normales de operación;

c) Identificar cualquier actividad, activo, infraestructura de respaldo o recurso interdependiente que también requiera de un mantenimiento continuo o de su restablecimiento en un período de tiempo determinado.

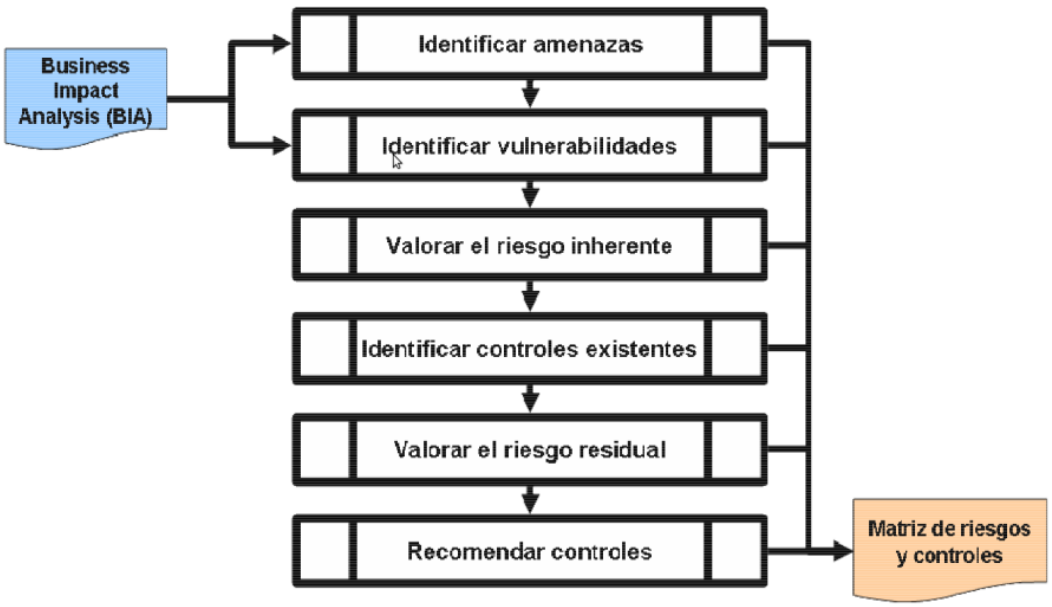


Figura 5.8 Análisis de Impacto del Negocio (AIN)

Al evaluar impactos, la organización debería tomar en consideración aquellos que tengan relación con sus metas y objetivos de negocio y con sus partes interesadas. Estos podrían incluir:

- El impacto sobre el personal o sobre el bienestar público;
- El impacto del daño a, o pérdida de, instalaciones, tecnología o información;
- El impacto de incumplimiento de deberes estatutarios o requisitos de reglamentación;
- Daño a la reputación;
- Daño a la viabilidad financiera;
- Deterioro del producto o la calidad del servicio.
- Daño ambiental.

La organización debería documentar su forma de evaluar el impacto de la interrupción y sus hallazgos y conclusiones.

Identificación de actividades críticas

La organización podría clasificar sus actividades de acuerdo con cuán prioritaria es su recuperación. Aquellas actividades cuya pérdida, identificada durante el AIN, tendría el mayor impacto en el menor período de tiempo, y que requiere ser recuperada o repuesta más rápidamente que las demás, puede ser calificada como “actividad crítica”. Cada actividad crítica respalda uno o más productos o servicios clave.

La organización podría querer concentrar sus actividades de planificación en actividades críticas, pero debería darse cuenta de que otras actividades también necesitarán ser recuperadas o repuestas dentro de su período máximo tolerable de interrupción y que también podrían requerir de preparativos anticipados en marcha.

5.14 Determinación de las necesidades de continuidad

La organización debería calcular los recursos que requerirá cada actividad en el momento de su reanudación. Estos podrían incluir:

a) recursos de personal, incluyendo número, desempeño y conocimiento (personas);

b) el lugar e instalaciones de trabajo requeridos (local);

c) tecnología, maquinaria y equipo (tecnología);

d) provisión de información (sea esta digital o en papel) sobre trabajos previos o el trabajo actual en curso, que tenga la suficiente actualidad y precisión como para permitir que la actividad continúe desarrollándose de manera eficaz en el nivel acordado (información); y

e) servicios y proveedores externos (suministros).

Al determinar los niveles de recursos, la organización debería tomar en consideración las necesidades de las partes interesadas.

Evaluación de amenazas a las actividades críticas (emprender una evaluación de riesgo)

En un contexto de GCN, el nivel de riesgo debe ser comprendido de manera específica con respecto a las actividades críticas de la organización y el riesgo de una interrupción de las mismas. Las actividades críticas son apuntaladas por recursos tales como personas, local, tecnología, información, suministros y partes interesadas. La organización debería comprender las amenazas a estos recursos, las vulnerabilidades de cada recurso, y el impacto que ocurriría si una amenaza se convierte en incidente y ocasiona una interrupción del negocio.

Compete totalmente a la organización decidir qué enfoque de evaluación de riesgo emplear, pero es importante que dicho enfoque sea conveniente y adecuado para abordar todas las necesidades de la organización.

El BS ISO/IEC 27001 establece el marco para elegir el enfoque de evaluación de riesgo al describir los elementos obligatorios que debería contener el proceso de evaluación de riesgo. Los elementos más comunes son los siguientes:

- Determinación de los criterios para la aceptación de riesgos. Estos describen las circunstancias en las cuales la organización está dispuesta a aceptar riesgos.

- Identificación de niveles aceptables de riesgo. No importa qué enfoque de evaluación de riesgo se elija, la organización necesita identificar los niveles de riesgo que considera aceptables.

- Análisis de los riesgos. Es necesario que el enfoque de evaluación de riesgo de la organización.

Las amenazas específicas pueden ser descritas como eventos o acciones que podrían, en algún momento, causar un impacto sobre los recursos, por ejemplo: amenazas como incendios, inundaciones, pérdida de personal, ausentismo del personal, virus informáticos y fallas de hardware.

Podría darse el caso de vulnerabilidades como debilidades en los recursos, las cuales pueden, en algún momento, ser aprovechadas por las amenazas, por ejemplo: fallas específicas, defectos en la protección contra incendios, capacidad de la red eléctrica, niveles de asignación de personal, seguridad de

TI y fortaleza de la TI.

Los impactos (ver Figura 21) podrían ser resultado de un aprovechamiento de vulnerabilidades por parte de las amenazas.

5.15 Determinación de alternativas

Perspectiva general

Como consecuencia del AIN y la evaluación de riesgo, la organización debería identificar medidas que:

- Reduzcan la probabilidad de una interrupción;
- Reduzcan el período de tiempo de la interrupción; y
- Limiten el impacto de una interrupción sobre los productos y servicios clave de la organización.

Estas medidas son conocidas como reducción de pérdidas y tratamiento de riesgo. Las estrategias de reducción de pérdidas pueden ser empleadas junto con otras opciones, puesto que no todos los riesgos pueden ser prevenidos o reducidos a un nivel aceptable. La organización podría incluir una o más o todas las estrategias.

Continuidad del negocio

Si la continuidad del negocio es la estrategia elegida para un producto o servicio clave, se debería establecer un Objetivo de Tiempo de Recuperación (OTR) y las estrategias de continuidad deberían ser evaluadas sobre la base de este objetivo.

Las estrategias de continuidad buscan mejorar la fortaleza de la organización frente a una interrupción al asegurar que las actividades críticas continúen funcionando o sean reanudadas a un nivel mínimo aceptable y en los plazos estipulados por el AIN.

Aceptación

Un riesgo podría ser aceptable sin que se deba tomar ninguna acción adicional. Aun si no es aceptable, la capacidad de hacer algo sobre ciertos riesgos podría ser limitada, o el costo de tomar medidas podría ser desproporcionado en comparación con el beneficio potencial que se obtendría. En estos casos, la respuesta podría ser tolerar el nivel existente de riesgo, siempre y cuando la alta gerencia determine que el riesgo es aceptable y que se encuentra dentro del apetito de riesgo de la organización. En algunas circunstancias, el impacto de un riesgo puede encontrarse fuera del apetito de riesgo normal de la organización, pero, debido a la baja posibilidad de que el riesgo se manifieste y/o el costo desproporcionado de controlarlo, la alta gerencia podría aceptar dicho riesgo.

La aceptación debe estar complementada por un plan para controlar los impactos que surgirán en caso de que el riesgo se manifieste.

Transferencia

En el caso de algunos riesgos, la mejor respuesta podría ser transferirlos. Esto se puede hacer por medio de seguros convencionales o arreglos contractuales, o pagándole a un tercero para que se ocupe del riesgo de una manera distinta. Esta opción es particularmente buena para reducir los riesgos financieros o riesgos a los activos. Los riesgos pueden transferirse para reducir la exposición de la organización al riesgo o porque otra organización es más capaz de lidiar de manera eficaz con dicho riesgo. Es importante notar que algunos riesgos no son (totalmente) transferibles; específicamente, por lo general no es posible transferir el riesgo a la reputación, aun si se contrata la provisión de un servicio.

La adquisición de un seguro podría formar parte de una estrategia de tratamiento de riesgos y proveerá una compensación financiera por algunas pérdidas. Sin embargo, no todas las pérdidas son completamente asegurables (por ejemplo: incidentes no asegurables, daño a una marca o reputación, pérdida de valor para las partes interesadas, reducción de la participación de mercado y consecuencias de carácter humano). Es poco probable que una simple compensación financiera proteja completamente a la organización de una manera tal que satisfaga las expectativas de todas las partes interesadas. Es más probable que se deba emplear una cobertura de seguros junto con una o más estrategias adicionales.

Cambio, suspensión o terminación

En algunas circunstancias, podría ser adecuado cambiar, suspender o terminar el servicio, producto, actividad, función o proceso. Esta opción solo debería ser considerada cuando no hay conflictos con los objetivos, obligaciones estatutarias o expectativas de las partes interesadas de la organización. Lo más probable es que este enfoque sea tomado en cuenta cuando el servicio, producto, actividad, función o proceso tiene un tiempo de vida limitado.

Nota: En ocasiones se hace referencia a los cuatro elementos antes mencionados con el nombre de modelo **“4T”:**

- “**Tratar** (continuidad del negocio),
- “**Tolerar**” (aceptar los riesgos),
- “**Transferir**” y
- “**Terminar**”.

Aprobación

La alta gerencia debería aprobar la lista documentada de productos y servicios clave, el análisis de impacto del negocio y la evaluación de riesgo, para así garantizar que el trabajo efectuado ha sido el adecuado y refleja correctamente los objetivos y naturaleza de la organización.

5.16 Fijar la GCN en la cultura organizacional

Para tener éxito, la continuidad del negocio debe estas integrada a la manera en que una organización es gestionada, al margen de su tamaño o del sector al que pertenezca. En cada etapa del proceso de GCN, existen oportunidades para introducir y mejorar la cultura de GCN de la organización.

Generalidades

Crear, promover y fijar una cultura de GCN dentro de una organización garantiza que esta se vuelva parte de los valores fundamentales y de la gestión eficaz de la misma.

Una organización con una cultura positiva de GCN:

- Desarrollará de manera más eficaz un programa de GCN;
- Infundirá entre sus partes interesadas (en especial entre su personal y clientes) seguridad en su capacidad para lidiar con interrupciones del negocio;
- Aumentará su fortaleza con el tiempo, para garantizar que las implicancias de la GCN sean tomadas en cuenta en las decisiones en todos los niveles; y
- Minimizará la probabilidad y el impacto de las interrupciones.

El desarrollo de una cultura de GCN debe apoyarse en:

- El liderazgo del personal con más años de experiencia en la organización;
- La asignación de responsabilidades;
- La toma de conciencia;
- La capacitación; y
- Los planes de prácticas

Toma de conciencia

La organización debería contar con un proceso para identificar y satisfacer las necesidades de toma de conciencia sobre GCN en la organización, y evaluar la eficacia de dicho proceso.

El personal de GCN debería tomar conciencia de la información externa sobre GCN. Esto puede hacerse junto con la búsqueda de orientación de los servicios de emergencia, las autoridades locales y los entes reguladores.

La organización debería iniciar, mejorar y mantener una toma de conciencia mediante un programa de información y educación continua sobre GCN para todo el personal.

Tal programa podría incluir:

- Un proceso de consulta con personal de todos los ámbitos de la organización, sobre la implementación del programa de GCN;
- Debatir sobre la GCN en los boletines, comunicados, programas de reclutamiento o revistas de la organización;
- Inclusión de la GCN en páginas Web o intranets pertinentes;
- Extraer lecciones de incidentes internos y externos;
- Integrar la GCN como un tema de las reuniones de equipo;
- Practicar planes de continuidad en lugares alternativos (por ejemplo, un centro de recuperación); y
- Visitas a cualquier lugar alternativo designado (por ejemplo, un centro de recuperación).

La organización podría hacer extensivo su programa de toma de conciencia sobre GCN a sus proveedores y otras partes interesadas.

Capacitación

La organización debería contar con un proceso para identificar y satisfacer las necesidades de capacitación en GCN de los participantes pertinentes, y para evaluar la eficacia de este proceso.

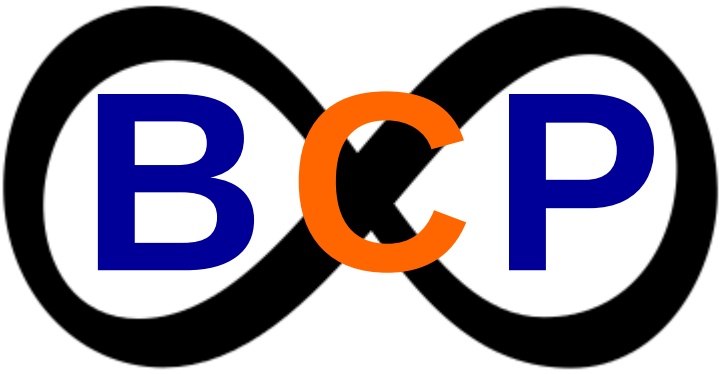
La organización debería emprender la capacitación de:

a) personal de GCN para tareas como:

   - Gestión de programas de GCN,
   - Realizar un análisis de impacto del negocio,
   - Desarrollar e implementar PCN,
   - Llevar a cabo un programa de prácticas en GCN,
   - Evaluación de riesgos y amenazas, y
   - Comunicación con los medios;

b) personal que no se encarga de GCN pero que requiere de habilidades para asumir sus funciones asignadas en procesos de repuesta a incidentes o recuperación del negocio.

Se debería desarrollar las habilidades y capacidad de respuesta de todos los ámbitos de la organización mediante la capacitación práctica, incluyendo una participación activa en las prácticas.



Business
Continuity Plan

Capítulo VI

Propuesta de Mejora

6.1 La Industria Bancaria y el Plan de Recuperación de Desastres

Los bancos se encuentran entre los primeros en adoptar las tecnologías de la información en el mundo de los negocios. Se adaptaron a los beneficios de las computadoras, casi desde el nacimiento de la industria de alta tecnología. Al mismo tiempo generaron una mayor dependencia de la industria en tecnología, esto a sido el nacimiento y la evolución de otra industria - la industria de la recuperación de desastres.

La Cámara de compensación automatizada fue fundada con la Asociación de siete bancos con sede en Filadelfia a mediados de la década de 1970 con el único fin de hacer frente a la cuestión de cómo los bancos deberían gestionar la recuperación de datos si sus sistemas informáticos caían. Desde la formación de este grupo llegó el comienzo de la industria de recuperación de desastres en 1978 por el Servicio de Recuperación de SunGard.

En 1983, el gobierno federal intervino para obligar a los bancos a desarrollar y mantener planes de recuperación ante desastres. Estos eventos muestran por qué no es exagerado decir que el sector bancario a generado al día de hoy miles de millones de dólares recuperados. Y las necesidades sofisticadas de la comunidad bancaria continuarán impulsando la evolución de la recuperación de desastres.

El sector bancario tiene necesidades específicas de recuperación de desastre y explicar algún estado de soluciones de recuperación de última generación que han surgido como una consecuencia directa de esas necesidades. La planificación es fundamental. Un enfoque proactivo es crítico para los bancos. La planificación es vital para la recuperación de desastres debido a que el objetivo principal es evitar los problemas antes de que ocurran.

Planear es Crítico

La importancia de tener una planificación se hizo dolorosamente evidente durante el atentado contra el “World Trade Center” en 1993. Dos tercios de las empresas ubicadas en el centro se quedaron sin un plan de recuperación sólida. Este hecho demuestra que a pesar de tener una creciente conciencia sobre la necesidad de tener una planificación de desastres, aun se tiene mucho espacio de mejora.

"En la Encuesta Global de Seguridad de la Información 2004, aplicada por Mancera Ernst & Young a mil doscientas treinta organizaciones de cincuenta y un países, resalta que a pesar de que el setenta y dos por ciento de los encuestados consideran importante el tema, las acciones de prevención y protección no son suficientes".

En las organizaciones públicas y privadas de nuestro país existe una visión muy limitada y distorsionada sobre la seguridad del entorno informático y de la seguridad de la información misma.

En México 61 empresas fueron encuestadas, la mayoría coincidió en señalar que prevalece una falta de conciencia sobre el tema de la seguridad.

Asimismo, constantemente aparecen en los titulares de los diarios de nuestro país noticias como las siguientes:

- "Avanza explotación sexual de niños" (en Internet).
- "Sabotean sitio de internet de la Presidencia".
- "Contrabando y piratería ganan batalla a industriales".
- "Inerme la Red Cibernética; alerta máxima de empresarios".
- "Casi el 60% del software que se usa en México es pirata".
- "'Hackean a Microsoft".
- "Millonarias pérdidas por ataques a redes".
- "Epidemia en el ciberespacio".
- "Internet rompe la frontera de la privacidad".
- "Desastres ponen a prueba corporativos".
- "Alerta PGJDF sobre fraudes por internet".
- "Temen usuarios operaciones bancarias en línea".
- "Visión miope" sobre seguridad de información en México".
- "Aviso importante sobre violación de patentes".
- "Aumentan fraudes en el ciberespacio".
- "México requiere nueva ley para proteger a internautas".
- "Denuncian ciberespionaje para detectar hábitos de internautas".
- "Aumentan pérdidas de empresas por ataques de hackers".
- "Pronostican aumento de virus informáticos".
- "Ataques informáticos por fallas en software de MS".

Existen, desde mi punto de vista, varias situaciones significativas para que esto suceda:

- El desconocimiento de la realidad informática y de la alarmante propagación e incremento de la gravedad y las repercusiones de los delitos informáticos.

- La incredulidad de que un riesgo pueda convertirse en un percance o siniestro para una organización.

- Los costos que implica la inversión en seguridad, así como las restricciones presupuestales que enfrentan actualmente la mayoría de las organizaciones.

- La negligencia hacia la prevención en materia informática.

- Nuestro país tiene un atraso considerable con respecto a países desarrollados en lo que a legislación informática se refiere. México no cuenta aún con la aplicación de un marco legal idóneo para tipificar, perseguir y castigar las acciones en las que las tecnologías y los sistemas de información son instrumento para cometer un delito o son blancos de él. Este escenario se torna crítico ya que un ataque, así como cualquier daño o perjuicio sufrido por alguna organización,

difícilmente podrá ser demostrado, cuantificado y reclamado ante las autoridades competentes.

6.2 Bancos – Están expuestos al tiempo en el desastre

La recuperación de desastres es de particular importancia para los bancos en una localidad golpeada por la crisis - más que otros negocios - porque sus servicios son de gran demanda en tiempos de desastres de la comunidad. Ya que se cuenta con múltiples ubicaciones y variadas operaciones y aplicaciones informáticas.

Las fusiones y adquisiciones, junto con la tecnología cada vez más sofisticadas, han complicado la situación de los bancos. Las fusiones y adquisiciones han causado a los bancos a heredar las aplicaciones más variadas. Normalmente, los bancos ejecutan entre 20 y 30 aplicaciones críticas a la vez, cuando las organizaciones se fusionan o se adquieren este número podría duplicarse. Además, las operaciones bancarias de muchos se están convirtiendo en las instituciones financieras descentralizadas como ampliar su alcance más allá de la oficina de apoyo en las ubicaciones satélite. Sin embargo, los bancos también continuarán dependiendo en gran medida del papel, sobre todo a nivel de rama.

¿Qué sucede con estas operaciones descentralizadas y múltiples aplicaciones si un banco sufre un desastre?

¿Qué sucede con las transacciones en papel en muchas ramas que no han entrado en el sistema central?

Ya sea el atentado contra el “World Trade Center”, las inundaciones del medio oeste o simplemente una crisis local, la realidad sigue siendo la misma - los desastres pueden interrumpir las operaciones críticas de negocio de manera significativa durante semanas ya veces meses. La preparación concienzuda puede reducir drásticamente el tiempo de recuperación y mantener las operaciones bancarias en curso.

Capacitación del personal

Como la mayoría de los oficiales de seguridad del banco sabe, los bancos deben pensar primero en sus empleados en el desarrollo de planes de recuperación ante desastres. A raíz de un desastre, los empleados de un banco primero y principal preocupación serán la seguridad de las familias y la propiedad personal. Una vez que las necesidades que rodean estas dos áreas son alojados, los trabajadores se harán cargo del empresario y sus clientes. Para el empleador, esto puede significar proporcionar esenciales tales como alimento, refugio y asistencia médica, así como el asesoramiento e información sobre los esfuerzos de recuperación.

Más allá del centro de datos

Las operaciones comerciales de recuperación ya no son el único propósito de

lo que hay dentro del centro de datos. La recuperación es una empresa a nivel corporativo. Como las operaciones bancarias se han descentralizado, centros de operaciones regionales y oficinas satélites más expuestos. Grupos de trabajo del Banco, como los empleados de servicio al cliente que atiende a clientes por teléfono desde ubicaciones remotas deben ser parte del plan de recuperación de desastres en general. La recuperación de negocios ha ido más allá de la recuperación de sistemas informáticos para restaurar y volver a crear procesos de negocio. La interrupción de los servicios de su conjunto tiene que ser considerado, y cómo el trabajo y la información fluirán de un lugar a otro o de un departamento a otro debe ser estudiado. Estas cuestiones inmediatas que se incluye en todos los planes de recuperación de desastres.

6.3 Herramientas tecnológicas que nos pueden ayudar a llevar un correcto plan de continuidad del negocio

Oracle Golden Gate (OGG)

Es la solución empresarial para las necesidades de datos en línea, tanto para alta disponibilidad (acceso en línea) así como para integración de datos (información en línea). Ofrece operaciones continuas para aplicaciones de misión crítica eliminando los cortes no planeados y reduciendo los costos de las interrupciones planificadas. Además, OGG puede reducir los costos de infraestructura al hacer replicaciones hacía sistemas de menor costo.

OGG permite alta flexibilidad en las posibles configuraciones y alternativas en la implementación de un sistema de “High Availability / Disaster Recovery (HA / DR)”. Ya que no sólo permite una solución uní-direccional, sino también permite soluciones bi-direccionales tanto en modo Activo-Pasivo, como Activo-Activo o Multimaster.

Por otra parte OGG también permite trabajar en ambientes heterogéneos (por ejemplo: misma base de datos, diferente sistema operativo y/o hardware), lo cual permite mayor flexibilidad en la configuración de los sitios alternos del DRP.

Arquitectura

La arquitectura de “Oracle Golden Gate” se compone de tres principales componentes: Capture, “Trail Files” y “Delivery”, ver Figura 5.9. Este enfoque modular permite que cada componente realice su tarea independientemente de los otros, permitiendo acelerar la replicación y asegurando la integridad de los datos.

Capture

Este módulo reside en el sistema fuente y está a la expectativa de capturar todas las transacciones que están ocurriendo en el sistema. Este módulo lee las operaciones de “inserts”, “deletes” y “updates” directamente de los “Logs” transaccionales (redo) e inmediatamente prepara los datos para su distribución,

además de que sólo distribuye aquellas operaciones a las que se les haya hecho “commit”. Esto implica que no necesariamente replica el redo log completo, permitiendo minimizar ancho de banda al enviar la información. De igual manera al estar capturando de los redo “logs”, hace que no sea intrusivo en la base de datos fuente.

Trial Files

Estos archivos contienen las transacciones capturadas por el proceso Capture en formato universal, esto para que diferentes manejadores de bases de datos puedan leerlos. El objetivo de estos archivos es asegurar la heterogeneidad, mejorar la confiabilidad y minimizar la pérdida de los datos. Suelen colocarse en el sistema fuente y destino. En caso de fallo en alguno de los sistemas, los “Trial Files” contienen la última transacción que fue capturada y será ese el punto donde se empezará a replicar la información una vez que el sistema se recupere para mantener la sincronización de los datos.

Delivery

Este módulo toma los datos modificados desde el último “Trail File” y lo aplica a la base de datos destino a través de secuencias SQL. La entrega puede hacerse a cualquier base de datos abierta y que sea compatible. El módulo aplica cada transacción en el mismo orden en que se hizo “commit” en el fuente, permitiendo la coherencia y la integridad de los datos. Para aumentar la flexibilidad de TI, los datos capturados también pueden aplicarse a “Java Message Service” (JMS) o archivo de texto plano (esto a través de algunos adaptadores de Golden Gate).

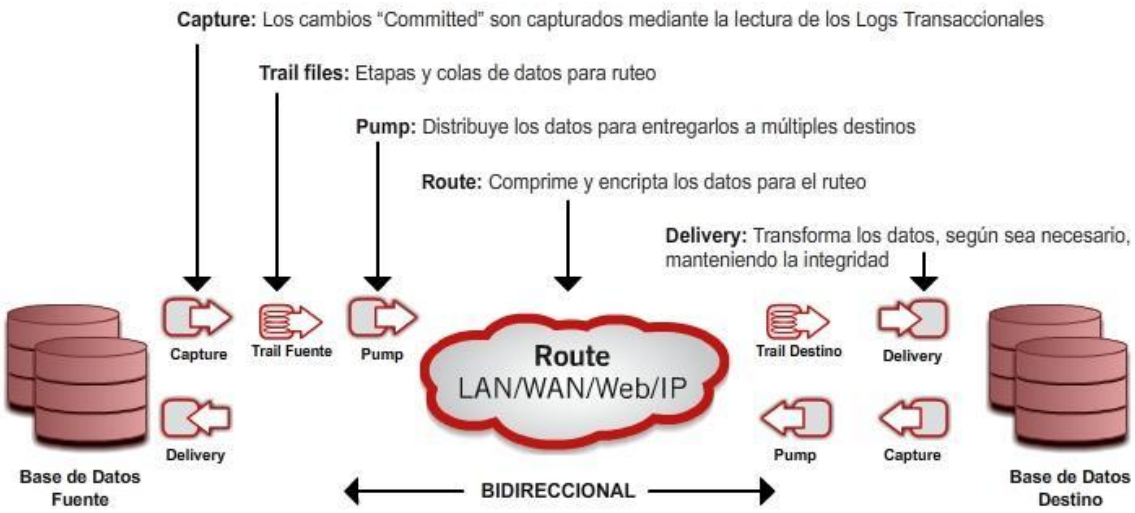


Figura 5.9 Arquitectura “Golden Gate”

Soluciones

OGG es una sola tecnología para diferentes necesidades: recuperación de desastres y protección de datos; cero tiempo de inactividad en migraciones, actualizaciones y mantenimiento; reporteo operacional y descarga de

consultas; inteligencia de negocios en línea; distribución y sincronización de datos.

6.4 Recuperación de desastres y protección de datos

Dentro del esquema de alta disponibilidad, “Golden Gate” cuenta con soluciones para recuperación de desastres. Al poder replicar entre sistemas heterogéneos, se puede tener el sistema DRP con diferentes bases de datos o sistemas operativos.

La recuperación de desastres de “Golden Gate” permite tener una arquitectura mucho más flexible que un DRP simple. Además, la base de datos secundaria siempre está abierta y puede ser utilizada para operaciones de reporteo y respaldo.

Funcionamiento

Mientras la base de datos en producción está siendo utilizada, ésta se está replicando en línea hacia una base de datos de recuperación (ver Figura 5.10). En caso de ocurrir alguna eventualidad en la base de datos productiva, basta con hacer un “FailBack” de las aplicaciones a la base de datos de recuperación para seguir trabajando sin interrupciones. Como la replicación se hace en línea, la base de datos de recuperación tendrá exactamente la misma información que la base de datos productiva.

Una vez que las aplicaciones están escribiendo en la base de datos de recuperación, las transacciones se estarán guardando en el “Trail File” que está en el sistema de recuperación. Cuando el sistema productivo se recupera, se enciende el “Delivery” en éste y se replican las transacciones que ocurrieron durante la caída del mismo. Cuando los datos están sincronizados (esto se asegura con “Golden Gate Veridata”) se puede hacer el “SwitchOver” de las aplicaciones al sistema productivo para continuar trabajando como en un principio.

Beneficios

- Recuperaciones rápidas.
- Sincronización entre los sistemas en caso de fallo.
- Reducción de pérdida y corrupción de datos.
- Sin límites geográficos.
- Sistema de recuperación puede ser utilización para reporteo y respaldos incrementales.

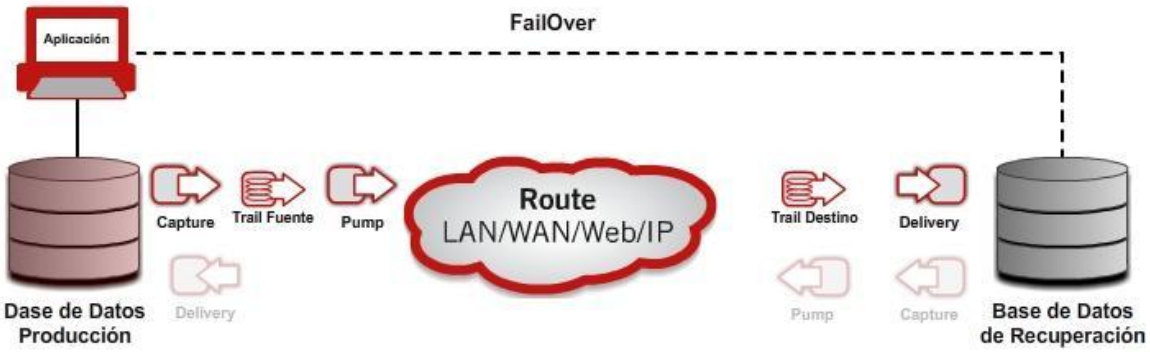


Figura 5.10 Recuperación de datos

6.5 Objetivos del proyecto

Es importante considerar que el objetivo primordial de la institución financiera, es llevar el proceso de implementación de DRP con las mejoras y las actualizaciones al actual sistema de Replicación para asegurar la continuidad de las operaciones y de la actividad económica, la seguridad de los clientes y sus transacciones. Con la certeza de la confiabilidad de las operaciones en tiempo real.

Deberá de considerarse que las necesidades de las políticas de Replicación deben de estar en mejora continua para cumplir con las exigencias del crecimiento de la institución financiera, con la responsabilidad de contar siempre con el mejor servicio y seguridad de sus transacciones.

La consideración de un servicio por parte de los proveedores de contar con la disponibilidad del soporte de 7 X 24 con Técnicos certificados, deberá de presentar el proveedor un nivel de servicio de acuerdo a las necesidades de la disponibilidad de las aplicaciones y las transacciones. De acuerdo a la certificación previa de las instalaciones y las características de las políticas actuales del SLA.

La posibilidad de medir el servicio y la presentación de planes por escrito de las actividades relacionadas con el análisis previo de factibilidad realizado a la actual infraestructura y la que se considera como SIDE principal para producción.

Deberán de ser consideradas las herramientas con las que se aplica la funcionalidad requerida de acuerdo a las necesidades de:

- Monitoreo de Replicaciones.
- Control de Versiones.
- Control de Replicaciones.
- Manejo de Incrementales de:

    - Espacio físico.
    - Compresión de replicación (“sizing”).
    - Objetos de la base de datos DML, DCL, DDL.

- Capacidad de manejo de diversas plataformas.
- Capacidad para coordinar arreglos externos de HW y SW.

Servicios Requeridos

- Es importante considerar que el producto o productos de software requeridos, deberán cumplir con los requerimientos de acuerdo a una clasificación previamente realizada y estudiada del trabajo e la generación de la replicación de las bases de datos desarrolladas para el SW Productivo de FInacle, E-Banking entre otros desarrollados para la operación de la institución financiera.

- Las características y requerimientos mínimos que deberán cubrir para cumplir con los estándares preestablecidos por el área de TI para el DRP y SLA.

- Según el esquema de las operaciones y de los servidores solicitados para la granja de servidores productivos, de Aseguramiento de Calidad y de Desarrollo.

- Con las características de sistema operativo, para que la o las herramientas cubran el requerimiento solicitado.

Antecedentes

La institución financiera requiere determinar de acuerdo al crecimiento definido las políticas del DRP y los SLA para las actividades de replicación respaldo y monitoreo de las aplicaciones del CORE críticas y son:

- FINACLE.
- E-BANKING.
- Desarrollos propios.
- DWH.
- Sistemas Satelitales.

Actualmente la institución financiera tiene su DRP implementado en el SITE de IBM y se requiere migrar toda la infraestructura de este SITE a la empresa de Hosteo KIO donde será necesario realizar el plan de logística del movimiento de infraestructura, aplicaciones y basados en la normas actuales ya implantadas en el SITE actual del DRP. Para el proyecto de migración se requiere puntos como:

1. Estrategia de implementación.
2. Ejecución de DRP.
3. Propuesta de migración.
4. Pruebas dirigidas.
5. Cuestionario para dimensionamiento de pruebas.
6. Inventario de aplicaciones.
7. Carga inicial.
8. Información de comparativos.

9. Aplicación de parches al sistema operativo.
10. Control de archivos fuentes.
11. Análisis y evaluación de la replicación.
12. Definición de nuevos procesos (en caso de ser necesario).
13. Ambiente productivo provisional.
14. Definición de usuarios claves para la operación.
15. Definición de fechas para pruebas del DRP anuales o semestrales.
16. Conectividad LAN y WAN con conexión remota para todos los usuarios.
17. Definición del SITE ACTIVO-PASIVO.
18. Definición de esquemas virtualizados para la replicación.
19. Utilizando base de datos ORACLE y SQL para la replicación.

Requerimientos técnicos para el SW

El software deberá cubrir los siguientes requerimientos:

1. Características básicas para replicación.
2. Características de sistema operativo.

    - Deberá dar soporte de los sistemas operativos HP-UX y Windows.

    - Deberá hacer la replicación de una base de datos Oracle: datos y catálogos (estructuras, usuarios, etc.).

    - Deberá hacer la replicación de una base de datos SQL Server: datos y catálogos (estructuras, Usuarios, etc.).

    - Deberá hacer la replicación de File System y/o volúmenes (dispositivos en crudo), sin importar el tipo de datos de las aplicaciones.

Capacidad del manejo de elementos de replicación

- Deberá incluir la capacidad de incrementar el tamaño del sistema de archivos y/o del volumen en línea.

- Deberá incluir la capacidad para agregar file system y/o volúmenes a la Configuración de la replicación en línea.

- Deberá incluir la capacidad de replicar en modo síncrono y asíncrono y tener la propiedad de cambiar de modalidad en línea.

- Deberá incluir la capacidad para replicar entre servidores físicos y virtuales; y en sentido inverso.

- Deberá incluir la capacidad de realizar la primera sincronización de datos Utilizando respaldos y una sincronización.

Características de validación y control de replicaciones realizadas

- Deberá incluir la capacidad verificación de consistencia entre la fuente y el Destino con la corrección automática en discrepancias.

- Deberá garantizar la consistencia lógica de los datos replicados.

- Deberá incluir la capacidad de replicación múltiple (a más de 1 sitio en forma concurrente).

- Deberá incluir la capacidad de Soporte para iniciar un gestor de base de datos en el SITE secundario en forma de consulta.

    - Proporcionar funcionalidad para efectuar el “FailBack”.
    - Administración mediante una consola centralizada.
    - Cifrado de datos en la transferencia.

Facilidad de elaboración, manejo y ejecución de reportes y estadísticas

- Deberá incluir la capacidad de envío de alertas en retardo de alguna replicación.

- Deberá incluir la capacidad de envío de alertas en caso de que se interrumpa alguna replicación.

- Deberá incluir la capacidad de envío de alertas en caso de saturación del espacio en disco.

- Deberá incluir la capacidad de envío de alertas en caso de saturación del ancho de banda en caso de que los administradores propios de a red fallen.

- Deberá incluir la capacidad de generación de estadísticas de tráfico de red como adicional para la administración de la red.

- Deberá incluir la capacidad de envío generación de estadísticas de replicación.

Seguridad en soporte y mantenimiento de la aplicación de parte del fabricante (Garantías)

- El proveedor de software de la solución deberá tener oficinas en México.

- El proveedor de Software debe contar con consultores certificados para proporcionar soporte e implantar soluciones.

- El proveedor de software debe proporcionar soporte de 7X24 los 365 días del año.

Opcionales

- Actualización en ambos SITE con sincronización en ambas direcciones.
- Envío de alertas vía SMS de acuerdo a las características de la empresa de telefonía contratada que permita el envió de e-Mails.
- Replicación en cascada.
- Capacidad de cambiar las IP's de replicación en línea.
- Replicación con protocolo UDP o TCP y tener la capacidad de hacer el cambio en línea. Solo en caso de que no se cuente con las herramientas propias para la administración del protocolo.
- Capacidad de integración con productos de alta disponibilidad local y remota.
- Contar con arquitectura, comandos y conceptos similares sin importar la plataforma en que se encuentre implantada la replicación, para los ambientes HP-UX y Windows.

6.6 Escenario para el desarrollo del proyecto DRP en una institución financiera

La institución financiera parte de su política de mejora continua de TI, la cual se encuentra actualmente en proceso de actualización tecnológica, de cambios de infraestructura y continuidad ininterrumpida de la operación critica del negocio. Este ultimo requerimiento de continuidad del negocio es el que se va a tratar en durante el desarrollo de este proyecto.

Se requiere de las soluciones que se ofertan en el mercado de acuerdo a nuestros requerimientos y políticas de DRP para garantizar la seguridad y la integridad de la institución financiera, que se traduce en miles de millones de transacciones y acciones económicas.

Todo esto va encaminado a asegurar la operación de forma ininterrumpida para asegurar las transacciones de las operaciones que se realizan en la institución financiera.

Es importante que la selección de las herramientas que se requieren para la replicación de las actividades críticas, productivas de aseguramiento de calidad y de desarrollo de la institución financiera, queden garantizadas y resguardadas.

Bajo la premisa de las políticas de DRP y la definición del SLA, para la

definición del cumplimento de las políticas internas predefinidas para llevar a cabo la replicación de “Site” local y el “Site” Remoto, consideran:

- Transacciones.
- Usuarios.
- Aplicaciones.
- Objetos.
- Bases de datos, etc.

Considerando los rubros principales descritos arriba y de acuerdo a los arreglos de los equipos designados para el productivo.

El presente estudio implica la realización de un análisis de todas las posibles causas a los cuales pueden estar expuestos los equipos de la institución financiera al estar conectados a la Red, así como la información contenida en cada medio de almacenamiento. También se realizara un análisis de riesgo y el plan de operaciones tanto para reducir la posibilidad de ocurrencia como para reconstruir el sistema de información y/o sistema de red de computadoras en caso de desastres.

El presente Plan incluye la formación de equipos de trabajo durante las actividades de establecimiento del Plan de Acción, tanto para la etapa preventiva, correctiva y de recuperación.

El Plan de Continuidad del Negocio se complementa con un Plan de Seguridad, en la que se considera todos los riesgos conocidos, para lo cual se hará un Análisis de riesgos.

6.7 Análisis de Riesgos

El presente realiza un análisis de todos los elementos de riesgos a los cuales esta expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos.

Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

1. Personal.
2. Hardware.
3. Software y utilitarios.
4. Datos e información.
5. Documentación.
6. Suministro de energía eléctrica.
7. Suministro de telecomunicaciones.

Daños

Los posibles daños pueden referirse a:

1. Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

2. Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico / lógico de información clave, proceso de información no deseado.

3. Divulgación de información a instancias fuera de la institución financiera y que afecte su patrimonio estratégico, sea mediante robo o falta de confianza.

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la compañía son:

- Acceso no autorizado.
- Ruptura de las claves de acceso a los sistemas computacionales.
- Desastres Naturales:
    a) Movimientos telúricos.
    b) Inundaciones.
    c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, falta del condicionamiento atmosférico necesario).

- Fallas de Personal Clave: por los siguientes inconvenientes:
    a) Enfermedad.
    b) Accidentes.
    c) Renuncias.
    d) Abandono de sus puestos de trabajo.
    e) Otros.

- Fallas de Hardware:
    Falla en los Servidores (HW).
    Falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall).

- Incendios.

Características

El Análisis de Riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el Costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

- Lo que intentamos proteger.
- El valor relativo para la organización.
- Los posibles eventos negativos que atentarían lo que intentamos proteger.
- La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un Plan adecuado. Los criterios que usaremos para tipificar los posibles problemas son:

Tabla 6.1 Escala de valores para criterios de posibles problemas

Criterios	Escala			
Grado de negatividad	Leve	Moderado	Grave	Muy severo
Posible frecuencia del evento negativo	Nunca	Aleatorio	Periódico	Continuo
Grado de impacto o consecuencias	Leve	Moderado	Grave	Muy severo
Grado de certidumbre	Nunca	Aleatorio	Probable	Seguro

Clases de Riesgo

La Tabla 6.2 proporciona el Factor de Probabilidad por Clase de Riesgo en función a la ubicación geográfica de la institución financiera y a su entorno; por ejemplo, si la institución:

- Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.

- Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.

- Se ubica en zona industrial las probabilidades de “Fallas en los equipos” será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.

- Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.

6.8 Identificación de Amenazas:

Tabla 6.2 Escala Factor de Probabilidad por Clase de Riesgo

Clase	Factor
Incendio o Fuego	0.40
Robo común de equipos y archivos	0.75
Sabotaje	0.60
Falla en los equipos	0.40
Equivocaciones	0.70
Acción virus informático	0.50
Fenómenos naturales	0.25
Accesos no autorizados	0.75
Robo de datos	0.80
Manipulación y sabotaje	0.80

Estos valores son estimados con base a la experiencia de trabajar con instituciones financieras en los últimos años. Corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo

En lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios de techos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

6.9 Clase de Riesgo: Incendio o Fuego

Tabla 6.3

Grado de negatividad	Muy severo
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
El área de servidores de la institución financiera cuenta con extintores	Ninguna
No se cuenta con un programa de capacitación formal sobre el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos	Implementar un programa de capitación formal para el manejo de extintores y primeros auxilios

Situación actual	Acción correctiva
Debido al incremento del número de computadores por oficina se hace necesario contar con extintores en las zonas estratégicas de las oficinas.	Incrementar el número de extintores por área con base en un análisis de distancia y accesibilidad
Se encontró un extintor con fecha de caducidad vencida	Asegurar que el proveedor mantenga los extintores con fechas vigentes para su uso en caso de emergencia

En caso de tener una contingencia de este tipo, podemos suponer que en el área de servidores se tendría un impacto mínimo, por las medidas de seguridad y el ambiente que lo protege. Esta información, permite resaltar el tema sobre el mejor lugar donde almacenar los respaldos. El incendio, a través de su acción calorífica, es más que suficiente para destruir los dispositivos de almacenamiento, tal como CD's, DVD's, cartuchos, discos duros, los cuales residen en una caja fuerte (medio de seguridad que nos protege frente a robo o terremoto, pero no del calor). Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se colocaran estratégicamente en lugares distantes, con una segunda copia de seguridad custodiada en un lugar externo de la institución financiera.

Las áreas funcionales distribuidas en la institución financiera, existe al menos una computadora, por lo que se debe incrementar los elementos y medidas de seguridad contra incendios.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca del las posibles áreas de riesgo que se debe proteger. A continuación en la Figura 6.1, se detallan las clases de extintores que debe conocer todo el personal en el uso del extinguidor.

Figura 6.1 Clases de extintores

6.10 Clase de Riesgo: Robo Común de Equipos y Archivos

Tabla 6.4

Grado de negatividad	Grave
Frecuencia de evento	Aleatorio
Grado de impacto	Moderado
Grado de certidumbre	Aleatorio

Situación actual	Acción correctiva
Vigilancia permanente	Existe vigilancia. La salida de un equipo informático es registrada por el personal de la oficina y por el personal de seguridad en turno
No se verifica si el personal de seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada	Al respecto personal de seguridad emite recomendaciones sobre medidas de alerta y seguridad
Remitir aviso a la oficina de seguridad patrimonial, para retirar equipo de informático	Se cumple

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre el responsable del área funcional y jefe de sistemas. Esto demuestra que los equipos se encuentran protegidos de personas no autorizadas y no identificables.

Según antecedentes de otras instituciones, se sabe de robos ocasionales de accesorios y equipos informáticos, en los cuales el personal de intendencia estaba en colusión con el personal de vigilancia. Es relativamente fácil remover un disco duro del CPU, una disquetera, tarjeta, etc. y no darse cuenta del faltante hasta días después. Estas situaciones no se han presentado en la institución financiera en estudio, sin embargo, se recomienda siempre estar alerta.

6.11 Clase de Riesgo: Vandalismo

Tabla 6.5

Grado de negatividad	Moderado
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
La institución financiera esta en una zona donde el índice de vandalismo es bajo	Existe vigilancia
Alguna probabilidad de turbas producto de manifestaciones que llegan a pasar frente a la institución financiera	Mantener buenos vínculos y coordinaciones permanentes con las autoridades pertinentes

La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.

6.12 Clase de Riesgo: Falla en los Equipos

Tabla 6.6

Grado de negatividad	Grave
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
La red de servidores en la institución financiera cuenta con una fuente de suministro eléctrico estable	Continuar con el programa de manteniendo preventivo
Cada área funcional se une a la red a través gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red: los Sistemas Informáticos, Teléfonos IP, mantenimiento remoto.	Proteger los gabinetes, y su adecuado apagado y encendido, dependen los servicios de red en el área
La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo	Existe un programa de mantenimiento de los equipos de cómputo. Sin embargo, es importante contar con proveedores calificados, en caso de requerir reemplazo de piezas y reparaciones urgentes

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas, pero si el corte se prolongara por tiempo indefinido podría provocar un trastorno en las operaciones.

El equipo de aire acondicionado es indispensable en el área de servidores para

favorecer su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, se requiere de una fuente se alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se han identificado los siguientes problemas de energía mas frecuentes:

- Fallas de energía.
- Transitorios y pulsos.
- Bajo voltaje.
- Ruido electromagnético.
- Distorsión.
- Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de picos.
- Estabilizadores.
- Sistemas de alimentación ininterrumpida (UPS).

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a tierra o puestas a tierra

Se denomina así a la comunicación entre el circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra húmeda, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobre tensiones de origen atmosférico o industrial.

La Toma a Tierra tiene las siguientes funciones principales:

1. Protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.

2. Protege a personas, equipos y materiales, asegurando la actuación de

los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.

3. Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Las inspecciones deben realizarse trimestralmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los meses de verano o en tiempo de sequía. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

Fusibles

Al cablear la computadora, la carcaza normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad fugara a través del aislante y llegase a la carcaza, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito.

Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (un fusible se debe sustituir tras fundirse, un diferencial se debe restaurar tras saltar).

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema se puede a conectar el equipo.

Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Asegurarse que el fusible de recambio es de la misma capacidad que el fundido. Por ejemplo si el fusible fundido viene marcando 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejara pasar 1 amperio mas de la intensidad de lo que fijo el diseñador del equipo.

No aprobar las reparaciones de los fusibles, usando hilos de cobre o similares.

Extensiones eléctricas y capacidades

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista, si no también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.

- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase mas corriente de la que los cables están diseñados para soportar. Se debe utilizar los enchufes de pared siempre que sea posible.

- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.

- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.

- Adquirir toma de corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.

- Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

6.13 Clase de Riesgo: Equivocaciones

Tabla 6.7

Grado de negatividad	Moderado
Frecuencia de evento	Periódico
Grado de impacto	Moderado
Grado de certidumbre	Probable

Situación actual	Acción correctiva
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario	Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con el Manual de Procedimientos
Cuando el usuario es practicante y tiene conocimientos de informática,	En lo posible se debe cortar estos accesos, limitando su accionar en

Situación actual	Acción correctiva
tiene el impulso de navegar por los sistemas	función a su labor de rutina
La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información	Reuniones y minutas de trabajo para fortalecer los procedimientos
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet	Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas. Convocar reuniones de capacitación antes nuevas opciones en los sistemas

6.14 Clase de Riesgo: Acción de Virus Informático

Tabla 6.8

Grado de negatividad	Muy severo
Frecuencia de evento	Continuo
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
Se cuenta con un Software Antivirus corporativo y hay un contrato anual para su actualización	Se cumple. Se debe evitar que las licencias no expiren, se requiere la renovación de contrato anualmente
Todo software instalado en las PCs cumplen con el estándar corporativo	Se cumple, sin embargo, hay que monitorear que los usuarios no instalen software no autorizado
Se tiene un programa permanente de bloqueo acciones como: cambiar configuraciones de red, acceso a los servidores, etc.	Se cumple a través de políticas de usuarios
Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de “logear” una maquina a la red (dominio) se comprueba al existencia de virus en la PC	Cumple

En estos últimos años la acción del virus informático ha sido contrarrestada con la diversidad de productos que ofrece el mercado de software. Las firmas y/o corporaciones que proporcionan software antivirus, invierten mucho tiempo en recopilar y registrar virus, indicando en la mayoría de los casos sus características y el tipo de daño que puede provocar, por este motivo se requiere de una actualización periódica del software antivirus.

6.15 Clase de Riesgo: Fenómenos Naturales

Tabla 6.9

Grado de negatividad	Grave
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
La ultima década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, aluviones, etc.	Mantener medidas de prevención
Potencialmente existe la probabilidad de sufrir inundaciones debido a lluvias que ocurren en épocas de verano y otoño	Mantener medidas de prevención
El ambiente donde se encuentras los servidores principales, es apropiado para evitar las filtraciones	Mantener trabajos de mantenimiento preventivo

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en el “site” de cómputo, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

6.16 Clase de Riesgo: Accesos No Autorizados

Tabla 6.10

Grado de negatividad	Grave
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
Se controla el acceso al sistema de red mediante la definición de la cuenta con su respectiva clave	Cumple

Situación actual	Acción correctiva
A cada usuario de Red se le asigna los “atributos de confianza” para el manejo de archivos y acceso a los sistemas	Cumple
Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera	Se cumple de modo extemporáneo, siendo lo indicado actualizar los accesos al momento de producirse el cese o cambio
Se forman grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos	Cumple
No se tiene un registro electrónico de Altas / Bajas de usuarios, con las respectivas claves	Se debe implementar

Todos los usuarios sin excepción tienen un “login” o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de cinco (5) dígitos. No se permiten claves en blanco. Además, están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas en la institución financiera, si lo tuviere.

6.17 Clase de Riesgo: Robo de Datos

Tabla 6.11

Grado de negatividad	Grave
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
Las oficinas tienen disponible disqueteras, quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador	Personal con contrato indefinido debe manejar información delicada de la oficina
El servicio de Internet es potencialmente una ventaja abierta para el robo de información	Existen políticas que regulan el uso y acceso del servicio de Internet

Situación actual	Acción correctiva
Los documentos impresos (informes, reportes, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser. Si no se toma conciencia que esta es una manera de atentar contra el Sistema Informático de la institución financiera, el problema podría persistir	Resguardar la información en archivos. Destruir los reportes malogrados, sobre todo de contenido relevante
El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas se seguridad se impide el ingreso a los servidores	Cumple

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar “copia no autorizada” a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.

- La segunda modalidad y tal vez la mas sensible, es la sustracción de reportes impresos y/o informes confidenciales.

- La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la gestión empresarial.

6.18 Clase de Riesgo: Manipulación y Sabotaje

Tabla 6.12

Grado de negatividad	Grave
Frecuencia de evento	Aleatorio
Grado de impacto	Grave
Grado de certidumbre	Probable

Situación actual	Acción correctiva
Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la	La protección contra el sabotaje requiere: ▪ Una selección rigurosa del personal ▪ Buena administración de los recursos humanos

Situación actual	Acción correctiva
institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje	▪ Buenos controles administrativos ▪ Buena seguridad física en los ambientes donde están los principales componentes del equipo ▪ Asignar a una persona la responsabilidad de la protección de los equipos en cada área
Existe el antecedente de origen sabotaje interno. Como es el caso de trabajadores que han sido despedidos y/o están enterados que van a ser rescindidos su contrato, han destruidos o modificado archivos para su beneficio inmediato o futuro	Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado

El peligro mas temido por los centros de procesamiento de datos, es el sabotaje. Instituciones que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes.

Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática u un problema “puntual”, sino que requiere un constante y continuo esfuerzo y dedicación.

6.19 Análisis en las fallas en la seguridad

En este se abarca el estudio del hardware, software, la ubicación física de la estación su utilización, con el objeto de identificar los posibles resquicios en la seguridad que pudieran suponer un peligro.

Las fallas en la seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona, de ahí que resulte obvio el interés creciente sobre este aspecto. La seguridad de la información tiene dos aspectos importantes como:

- Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.

- Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

Por ejemplo, en el uso del Servicio Virtual Público de Red (VPN), implica una vía de acceso a la red de la institución financiera, la seguridad en este servicio es la validación de la clave de acceso.

Protecciones actuales

Se realizan las siguientes acciones:

1. Se hace copias de los archivos que son vitales para la institución.
2. Al robo común se cierran las puertas de entrada y ventanas.
3. Al vandalismo, se cierra la puerta de entrada.
4. A la falla de los equipos, se realiza el mantenimiento de forma regular.
5. Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus.
6. A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados.
7. A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente plan de contingencias da pautas al respecto.
8. Al acceso no autorizado, se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del teclado.
9. Al robo de datos, se cierra la puerta principal y gavetas de escritorios. Varias computadoras disponen de llave de bloqueo del teclado.
10. Al fuego, en la actualidad se encuentran instalados extintores, en sitios estratégicos y se brindara entrenamiento en el manejo de los extintores al personal, en forma periódica.

6.20 Seguridad de información

La seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen institucional de las empresas, incluso la vida privada de personas. Es obvio el interés creciente que día a días se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.

La seguridad de información tiene tres directivas básicas que actúan sobre la protección de datos, las cuales ejercen control de:

1. La lectura: consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar

protección de la privacidad, si se trata de datos personales y mantenimiento de la seguridad en el caso de datos institucionales.

2. La escritura: es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad que se les ha confiado.

3. El empleo de esa información: es secreto de logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos.

   Por otro lado, es importante definir los dispositivos de seguridad durante el diseño del sistema y no después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a se criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

Acceso no autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados:

- Control de acceso al “site”: la libertad de acceso al “site” puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que trabaja en esta oficina. Cualquier otra persona puede tener acceso únicamente bajo control.

- Debemos mantener la seguridad física de la oficina como primera línea de defensa. Para ello se toma en consideración el valor de los datos, el costo de protección, el impacto institucional por la perdida o daño de la información. La forma propuesta de implantar el control de acceso al “site”, seria la siguiente:

  - Para personas visitantes, vigilancia otorgara el credencial de visitante.
  - Para personal de la institución financiera, con autorización del encargado de la oficina.

- Acceso limitado a computadoras personales y/o terminales de la red: las terminales que son dejadas sin protección pueden ser mal usados. Cualquier Terminal puede ser utilizado para tener acceso a los datos de un sistema controlado.

- Control de acceso a la información confidencial: sin el debido control, cualquier usuario encontrara la forma de lograr acceso al sistema de red, a una base de datos o descubrir información clasificada. Para revertir la posibilidad de ataque se debe considerar:

Programas de control a los usuarios de red

El sistema operativo residente en los servidores del “site” es Windows Server. A través del servicio de “Active Directory” permite administrar a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

Palabra de acceso (contraseña)

Es una palabra o código que se ingresa por teclado antes que se realice un proceso.
Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. La identificación del usuario debe ser muy difícil de imitar y copiar.

El Sistema de Información debe cerrarse después que el usuario no autorizado falle tres veces de intentar ingresar una clave de acceso. Las claves de acceso no deben ser largas puesto que son más difíciles de recordar. Una vez que se obtiene la clave de acceso al sistema, esta se utiliza para entrar al sistema de red de información vía sistema operativo.

La forma común de intentar descubrir una clave es de dos maneras:

- Observando el ingreso de la clave.
- Utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar.

En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice de forma periódica la contraseña de los usuarios.

Niveles de Acceso

Las políticas de acceso aplicadas, deberá identificar los usuarios autorizados a emplear determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas. Cada palabra clave deberá tener asignado uno de los niveles de acceso a la información o recursos de red disponibles en la institución financiera.

La forma fundamental de autoridad la tiene el administrador de redes con derechos totales. Entre otras funciones puede autorizar nuevos usuarios, otorgar derechos para modificar estructuras de las Bases de Datos, etc.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información Tabla 6.13.

Tabla 6.13

Nivel	Concepto
Consulta de la información	El privilegio de lectura esta disponible para cualquier usuario y solo se requiere presentaciones visuales o reportes. La autorización de lectura permite leer pero no modificar la Base de Datos
Mantenimiento de información	Permite el acceso para agregar nuevos datos, pero no modifica los ya existentes, permite modificar pero no eliminar los datos

Destrucción

Sin adecuadas medidas de seguridad la institución financiera puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas o sabotaje, etc.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos, bases de datos, documentos o trabajar sin ellos.

Esta comprobado que una gran parte del espacio en disco esta ocupado por archivos de naturaleza histórica, que es útil tener a mano pero no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia conservados como documentos de referencia o plantilla. Si se guarda una copia de seguridad de estos archivos las consecuencias de organización pueden ser mínimas.

Sin los datos al día, si el objetivo se vería seriamente afectado. Para evitar daños mayores se hacen copias de seguridad de la información vital para la institución financiera y se almacenan en lugares apropiados (de preferencia en lugar externo a las instalaciones).

Hay que protegerse también ante una posible destrucción del hardware o software por parte del personal no honrado. Por ejemplo, hay casos en la que, trabajadores que han sido recientemente despedidos o están enterados que ellos van a ser cesados, han destruido o modificado archivos para su beneficio inmediato o futuro. Depende de los jefes inmediatos de las áreas funcionales dar importancia a estos eventos, debiendo informar al jefe del “site” para el control respectivo.

Revelación o Deslealtad

La revelación o deslealtad es otra forma que utilizan los malos trabajadores

para su propio beneficio. La información de carácter confidencial es vendida a personas ajenas a la institución financiera. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

- Control de uso de información en paquetes / expedientes abiertos, cintas / disquetes y otros datos residuales. La información puede ser conocida por personal no autorizadas.

- Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de esa a aquellas personas que pueden usar mal los datos residuales de estas.

- Mantener información impresa o magnética fuera del trayecto de la basura. El material de papel en la plataforma de descarga de la basura puede ser la fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Para tener una mayor seguridad de protección de la información residual y segregada, esta deberá ser destruida, eliminada físicamente, manualmente o mecánicamente (picadores de papel).

- Preparar procedimientos de control para la distribución de información. Una manera de controlar la distribución y posible derivación de información, es mantener un rastro de copias múltiples indicando la confidencialidad o usando numeración como “pagina 1 de 9”.

Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de las oficinas y relativamente disponible a gran número de personas.

Modificaciones

Hay que estar prevenido frente a la tendencia a asumir que “si viene de la computadora, debe ser correcto”.

La importancia de los datos modificados de forma ilícita, esta condicionada al grado en que la institución financiera, depende de los datos para su funcionamiento y toma de dediciones. Esto podría disminuir su efecto su los datos procedente de las computadoras se verificaran antes de constituir fuente de información para la toma de decisiones.

Los elementos en la cual se han establecido procedimientos para controlar modificaciones ilícitas son:

1. Los programas de aplicación: adicionalmente a proteger sus programas de aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionales a los datos o a su uso no autorizado.

2. La información en Bases de Datos: como medidas de Seguridad, para

proteger los datos en el sistema, efectuar auditorias y pruebas de consistencia de datos en nuestros históricos. Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

3. Nuestra mejor protección contra la perdida / modificación de datos consiste en hacer copias de seguridad, almacenando en copias no autorizadas de todos los archivos valiosos en un lugar seguro.

4. Los usuarios: los usuarios deben estar concientes de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados, profundizarse con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema.

Para la realización de las copias de seguridad se tiene que tomar algunas decisiones previas como:

- ¿Que soporte de copias de seguridad se va utilizar?
- ¿Se van a usar dispositivos especializados para copia de seguridad?
- ¿Con que frecuencia se deben realizar las copias de seguridad?
- ¿Cuales son los archivos a los que se le sacara copia de seguridad y donde se almacenara?

El responsable del “site” establecerá directivas y/o reglamentos en estas materias, para que los usuarios tomen conocimiento de sus responsabilidades. Tales reglas y normativas deben incorporarse en una campaña de capacitación educativa.

La institución financiera debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

- Hacer de la copia de seguridad una política, no una opción.
- Hacer de la copia de seguridad resulte deseable.
- Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).
- Hacer de la copia de seguridad obligatoria.

Conclusiones

El desarrollo del presente trabajo de tesis me ha permitido aportar una solución para la gestión de la seguridad de la información en una institución financiera, basado en la experiencia profesional que he adquirido como resultado de haber creado mi propia empresa, la cual actualmente proporciona productos, servicios y soluciones de negocios en tecnologías de la información. Esta empresa la formé hace más de 20 años con el objetivo principal de crear valor en las empresas, a través de proporcionar soluciones de calidad en sistemas de tecnología de información. Adicionalmente, es una satisfacción personal el poder contribuir en el crecimiento del país generando trabajos directos e indirectos, manteniendo la visión de apoyar a las empresas a mejorar su rentabilidad y posición en el mercado nacional e internacional utilizando soluciones tecnológicas de vanguardia.

Cabe mencionar, que todo lo anterior no sería posible, si no contara con la formación que adquirí en la Facultad de Ingeniería de la UNAM, la cual me proporcionó las bases necesarias para consolidar el éxito profesional que he logrado y que me compromete cada día a buscar nuevos retos para continuar en constante crecimiento.

Por lo antes expuesto, para implantar una adecuada gestión de seguridad de información en dicha institución financiera, el primer paso fue obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de los procesos de negocio de su empresa.

Una vez que contamos con el apoyo continuo de ellos, se transmitió a los dueños de procesos de negocio más importantes de la institución financiera, que generalmente son jefes de áreas. Dándoles a conocer la importancia de la seguridad de información en los procesos que manejan, obteniendo el apoyo de todo el personal a su cargo. Es en este punto, es donde se detallaron todos los lineamientos del modelo de gestión expuesto, el cual se ve reflejado en las políticas, normas, estándares y procedimientos de seguridad, soportados por la tecnología de información de la institución.

En mi experiencia proporcionando servicios de consultaría estratégica, puedo mencionar que no necesariamente la tecnología de información por sí sola garantiza la seguridad de información. Se vuelve imperativo gestionarla de acuerdo siempre a los objetivos de negocio. De nada sirve contar con los últimos adelantos tecnológicos, si no se da la importancia debida a la protección de la información, la cual se verá reflejada en el cumplimiento de todas las políticas de seguridad de información, siempre actualizadas de acuerdo a los cambios constantes en los negocios propios de una institución financiera.

Es por lo anterior, que el presente Plan de Continuidad del Negocio desarrollado para la institución financiera, tiene como fundamental objetivo el salvaguardar la infraestructura de la red y sistemas de Información extremando las medidas de seguridad para protegerlos y estar preparados a una

contingencia de cualquier tipo.

Las principales actividades que fueron requeridas para la implementación del Plan de Continuidad del Negocio son: identificación de riesgos, evaluación de riesgos, asignación de prioridades a las aplicaciones, establecimiento de los requerimientos de recuperación, elaboración de la documentación, verificación e implementación del plan, distribución y mantenimiento del plan.

Por último, puedo mencionar en mi experiencia que no existe un Plan de Continuidad del Negocio único que pueda aplicarse para todas las organizaciones, esto depende de la infraestructura física y las funciones que se realizan en el centro de procesamiento de datos, mejor conocido como Centro de Cómputo.

Recomendaciones

Programar las actividades propuestas en el presente Plan de Continuidad del Negocio.

Hacer de conocimiento general el contenido del presente Plan de Continuidad del Negocio, con la finalidad de instruir adecuadamente al personal de la institución financiera.

Adicionalmente al Plan de Continuidad del Negocio se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo / beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa.

Anexos

Medidas de precaución y recomendación

Referencia “Guía Practica para el Desarrollo de Planes de contingencia de Sistemas de Información”. Instituto Nacional de Estadística Geográfica e Informática (INEGI).

1. En el Área de Servidores:

- Es recomendable que no esté ubicado en áreas de alto tráfico de personas o con un alto número de invitados.

- Evitar, en lo posible, los grandes ventanales por el riesgo de terrorismo y sabotaje; además de que permiten la entrada del sol y calor (inconvenientes para los equipos).

- En su construcción, no debe existir materiales altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.

- Su acceso debe estar restringido al personal autorizado. El personal de la Institución deberá tener su documento de identificación siempre en un lugar visible.

- Establecer un medio de control de entrada y salida al Área de Servidores.

- Se recomienda que al personal, de preferencia, se les realice exámenes psicológicos y médicos, y tener muy en cuenta sus antecedentes de trabajo, ya que el Área de Servidores depende en gran medida, de la integridad, estabilidad y lealtad del personal.

- El acceso a los Sistemas de Información, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

- Establecer controles para una efectiva disuasión y detección, de intentos de acceso no autorizados a los sistemas de información.

- Se recomienda establecer políticas para la creación de las contraseñas y establecer periodicidad de cambios.

- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.

- Establecer políticas de control de entrada y salida del personal, en el caso de visitas, verificar los paquetes u objetos que portan.

- La seguridad de las terminales de un sistema en red podrán ser controlados por medio de anulación del disk drive, anulación de

compartir discos duros, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.

- La ubicación de los controles de acceso (vigilancia) y el acceso en sí deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña.

- Las cámaras fotográficas no se permitirán en el área de servidores, sin permiso por escrito de la jefatura.

2. En la Administración de las Impresiones:

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.

- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.

- Establecer controles respecto a los procesos remotos de impresión.

3. En los Niveles de Control:

- Existen dos tipos de activos en un Centro de Cómputo (Área de Servidores): los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo, daño del equipo, revelación y/o destrucción no autorizada de la información, que interrumpen el soporte a los procesos del negocio.

- El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Para el nivel clasificado, deben observarse todas las medidas de seguridad de la información que estos equipos contengan.

4. Recomendaciones para los Medios de Almacenamientos:

Mantenimiento de Medios Magnéticos:

Deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada. Medidas a considerar:

- La temperatura y humedad relativa del ambiente de almacenamiento, debe ser adecuada.

- Las cintas deben colocarse en estantes o armarios adecuados.

- Deberá mantenerse alejados de los campos magnéticos.

- Dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas.

Recomendaciones para el Mantenimiento de los Discos Duros

- Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

- El ordenador debe colocarse en un lugar donde no pueda ser golpeado.

- Se debe evitar que la computadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros.

- No se debe mover el CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

Respecto a los Monitores

- La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la reflexión. Se recomienda no mirar directamente a la pantalla, si no mirar con una inclinación.

- Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones, sino que puede ayudar a reducir el esfuerzo visual.

- También manténgase por lo menos a 1 metro o 1.20 metros del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.

- Finalmente apague su monitor cuando no lo esté usando.

Recomendación para el cuidado del Equipo de Cómputo

- **Teclado:** mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

- **Cpu:** mantener la parte posterior del cpu liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.

- **Mouse:** poner debajo del “mouse” una superficie plana y limpia.

- **Protectores de pantalla:** para evitar la radiación de las pantallas que causan irritación a los ojos.

- **Mantener las Áreas Operativas Limpias.** Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas. Sin embargo, algunos de los problemas que podemos evitar son: el peligro de fuego generado por la excesiva acumulación de papeles, el daño potencial al equipo por derramar líquidos en los componentes del sistema, el peligro por fumar y las falsas alarmas creadas por detectores de humo.

Glosario de términos y abreviaturas

Glosario de términos

Acceso: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

Amenaza: Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

Asimismo, es la posible interrupción del negocio a continuar, ya que son agentes capaces de explotar los fallos de seguridad denominados vulnerabilidades causando pérdidas o daños a los activos.

Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque Activo: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

Ataque Pasivo: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red.

Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

Respaldo.- Son copias de seguridad, es el respaldo regular que se da a los sistemas de datos. Los datos podrían respaldarse en discos magnéticos, cintas, discos ópticos (CDs). El método específico escogido para respaldar debe ser basado en los sistemas, disponibilidad de los datos y requisitos de Integridad.

Base de Datos: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (“Data Base Management System – DBMS”).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos
- Provee lenguajes de consulta (interactivo)
- Provee una manera de introducir y editar datos en forma interactiva
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación

Contingencia.- Una contingencia se define como cualquier evento no planeado provocando que las actividades de negocio no sean operadas normalmente durante un determinado periodo de tiempo, para la cual existe una solución que permite la recuperación en un tiempo razonable.

Core business.- Es la parte principal de la operaciones del negocio. Es el producto principal del negocio, la razón de venta al cliente.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

Desastre.- Un desastre se define como cualquier evento no planeado que hace un lugar inoperable o inaccesible.

Diversos tipos de desastre pueden ocurrir y varían de comunes, naturales, extraordinarios, etc.

Golpe (Breach): Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

Incidente: Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

Información: es un activo, el cual, como cualquier otro activo de negocios, tiene valor para una organización y consecuentemente necesita ser protegido adecuadamente.

Integridad: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

Privacidad: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

Punto de Recuperación.- El punto de recuperación es en el momento que se puede restablecer todas las operaciones a continuar.

Riesgo.- Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático causando un impacto en la empresa.

Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

Seguridad de Información: Está caracterizada por la preservación de los siguientes aspectos:

- Confidencialidad: Asegurando que la información sea accesible solo por aquellos que están autorizados
- Integridad: Salvaguardando la exactitud de la información en su procesamiento, así como su modificación autorizada
- Disponibilidad: asegurando que los usuarios autorizados tenga acceso a la información y a los activos asociados cuando sea requerido

Sistema de Gestión: Es un sistema para *establecer políticas* y objetivos de tal manera que se puedan cumplir estos últimos. Son usados por las organizaciones para diseñar sus políticas y para poner estas en funcionamiento a través de objetivos. Para ello se basa en:

- Estructuras organizacionales
- Procesos sistemáticos y recursos asociados
- Metodologías de evaluación y medida
- Revisión de procesos para asegurar que los problemas sean corregidos y las oportunidades para mejorarlos sean reconocidas e implementadas cuando sea necesario

Tiempo de Recuperación.- Es el tiempo que toma recuperar las operaciones continuas del negocio.

Tipos de Información: la información puede ser clasificada de diversas maneras, según la forma de comunicarse:

- Impresa o escrita en papel
- Almacenada electrónicamente

- Transmitida por correo convencional o electrónicamente
- Exhibida en videos corporativos
- Hablada en reuniones

No importando la forma que tome la información, ésta deberá ser siempre protegida.

Vulnerabilidad.- Cualquier debilidad en los sistemas informáticos que puedan ser explotados por las amenazas y causar pérdidas.

Glosario de abreviaturas

Abreviatura	Descripción
AIN	Análisis de Impacto del Negocio
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BD	Base de Datos
BIA	Business Impact Analysis
BSI	British Standards Institution
CPD	Centro de Procesamiento de Datos
DBMS	Data Base Management System
DCL	Digital Command Language
DDL	Data Definition Language
DML	Data Manipulation Language
DR	Disaster Recovery
DRP	Disater Recovery Plan
DWH	Data Ware House
ECC	Error Correct Checking
GCN	Gestión de la Continuidad de Negocio
HA	High Availability
HW	Hardware
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization
IT	Information Tecnology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
OGG	Oracle Golden Gate
OTR	Objetivo de Tiempo de Recuperación
PDCA	Plan, Do, Check, Act
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory

Abreviatura	Descripción
SAI	Suministro de Energía Ininterrumpido
SAN	Atorage Area Network
SGCN	Sistemas de Gestión de la Continuidad de Negocio
SLA	Service Level Agreement
SMS	Short Message Service
SO	Sistema Operativo
SQL	Structured Query Language
SW	Software
TI	Tecnología de Información
UDP	User Datagram Protocol
WAN	Wide Area Network

Referencias

Valerie A. Zeithmanr, A. Parasuman, Leonrar L. Berry, Calidad total en la gestión de servicios, Díaz de Santos, 1era edición, 1992.

A. C. Rosander, Los catorces puntos de Deming aplicados a los servicios, Díaz de Santos, 1era. Edición, 1994.

E. del Peso Navarro, M. A. Ramos González, Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas, Díaz de Santos, 1era. Edición, 1994.

www.ibermatica.com, documentos de reflexión estratégica y tecnológica Nº 93, Noviembre 2010