

Elaboración del Plan de Recuperación ante Desastres (PRD)

Ing. María Victoria Bisogno
mbisogno@cidi.com.ar



Contenido

Contenido.....	2
Introducción	3
Objetivo	4
Componentes.....	5
Desarrollo del Plan de Recuperación ante Desastres	6
1. Determinación del escenario considerado.....	6
2. Definición de los tipos de operación en una contingencia	6
3. Establecimiento de criticidades.....	8
4. Determinación de las prestaciones mínimas	10
5. Análisis de riesgos	10
5.1 Probabilidad de ocurrencia de desastres	14
5.2 Determinación de los niveles de desastre	14
6 Estrategia de Recuperación.....	15
6.1 Presentación de las distintas estrategias posibles de recuperación	15
6.2 Selección de la estrategia de recuperación	15
6.3 Desarrollo de la estrategia de recuperación	15
6.4 Mitigación de riesgos – Medidas preventivas	15
6.5 Descripción de la estrategia.....	16
7 Requerimientos para llevar a cabo el Plan.....	16
7.1 Esquemas técnicos	17
7.2 Formación del Equipo de Recuperación del Entorno ante Desastres (ERED).....	17
7.2.1 Roles y responsabilidades	17
7.2.2 Asignación de roles	19
7.3 Desarrollo de procedimientos.....	20
8 Pruebas del PRD.....	20
9 Revisión del PRD	21
10 Cierre del proyecto.....	21
Anexo I – Bibliografía.....	22
Anexo II – Referencia a MAEI.....	23
Anexo III – Acerca de Cidicom S.A.....	24
Anexo IV - Definiciones	27

Introducción

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, para todo negocio, por lo que es considerada de vital importancia en todo el mundo.

[Huerta2000] define la seguridad 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*”.

[IRAM/ISO/IEC17799] sostiene que “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;

[IRAM/ISO/IEC17799] también agrega “La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software”.

Este trabajo es parte de la tesis de grado “*Metodología para el Aseguramiento de Entornos Informatizados – MAEI*” aprobada en Marzo del 2005 por las autoridades de la Universidad de Buenos Aires, Facultad de Ingeniería, en el que se desarrolló un marco de trabajo para asegurar cualquier tipo de entorno informatizado, con especial enfoque en el negocio y estrategia de la organización objetivo.

El Plan de Recuperación ante Desastres es un elemento más que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operatividad mínima luego de una contingencia, en la que se vean afectados los procesos y recursos informáticos que sostienen el negocio.

Este documento describe la metodología de análisis y desarrollo del Plan de Recuperación ante Desastres, basada en el estudio de estándares internacionales y mejores prácticas, citadas en el trabajo completo.

Objetivo

El Plan de Recuperación ante Desastres, en adelante PRD, tiene como objetivo detectar los riesgos presentes en el entorno, analizar su probabilidad de ocurrencia, establecer su criticidad según cómo afectan la continuidad del negocio, y finalmente proponer un plan que logre mitigar en cierta medida estos riesgos, y que permita la recuperación de la disponibilidad de los recursos lógicos, físicos y humanos ante situaciones de contingencia.

Muchas veces desastres naturales o accidentes, como incendios, inundaciones, hasta cortes en el suministro de energía eléctrica provocan pérdidas enormes no sólo en el ámbito de los bienes, sino pérdidas provocadas por la interrupción del negocio.

Hoy en día el negocio es más y más dependiente de la informática, ya que la mayoría de las empresas tiene sus sistemas productivos y financieros automatizados y computarizados. De esta forma es crucial contar con un plan para sostener el flujo de los negocios ante emergencias que imposibiliten el uso de los recursos de computación o del entorno completo.

En este trabajo se utilizarán indistintamente los términos "emergencia", "contingencia" y "desastre". Por lo tanto, el hecho de utilizar la palabra "contingencia" no indica menor gravedad que las situaciones en las que se referencia al hecho acontecido como un "desastre".

Componentes

El PRD contiene las siguientes 10 (diez) partes:

1. Establecimiento del escenario considerado;
2. Definición de los tipos de operación en una contingencia;
3. Establecimiento de criticidades:
 - Criticidades por equipo;
 - Criticidades por servicios;
 - Criticidades por aplicaciones;
4. Determinación de las prestaciones mínimas;
5. Análisis de riesgos:
 - Probabilidad de ocurrencia de desastres;
 - Determinación de los niveles de desastre;
6. Presentación de las distintas estrategias posibles de recuperación;
7. Selección de la estrategia de recuperación;
8. Elaboración de la estrategia de recuperación:
 - Mitigación de riesgos – Medidas preventivas;
 - Descripción de la estrategia;
 - Requerimientos para llevar a cabo el Plan;
 - Esquemas técnicos con pasos a seguir;
9. Formación del Equipo de Recuperación del Entorno ante Desastres (ERED):
 - Roles y responsabilidades;
 - Asignación de roles;
10. Establecimiento de los procedimientos:
 - Declaración de la emergencia;
 - Recuperación de las prestaciones;
 - Reestablecimiento de las condiciones normales.

A continuación se detallará cada una de estas partes que componen el PRD.

Desarrollo del Plan de Recuperación ante Desastres

1. Determinación del escenario considerado

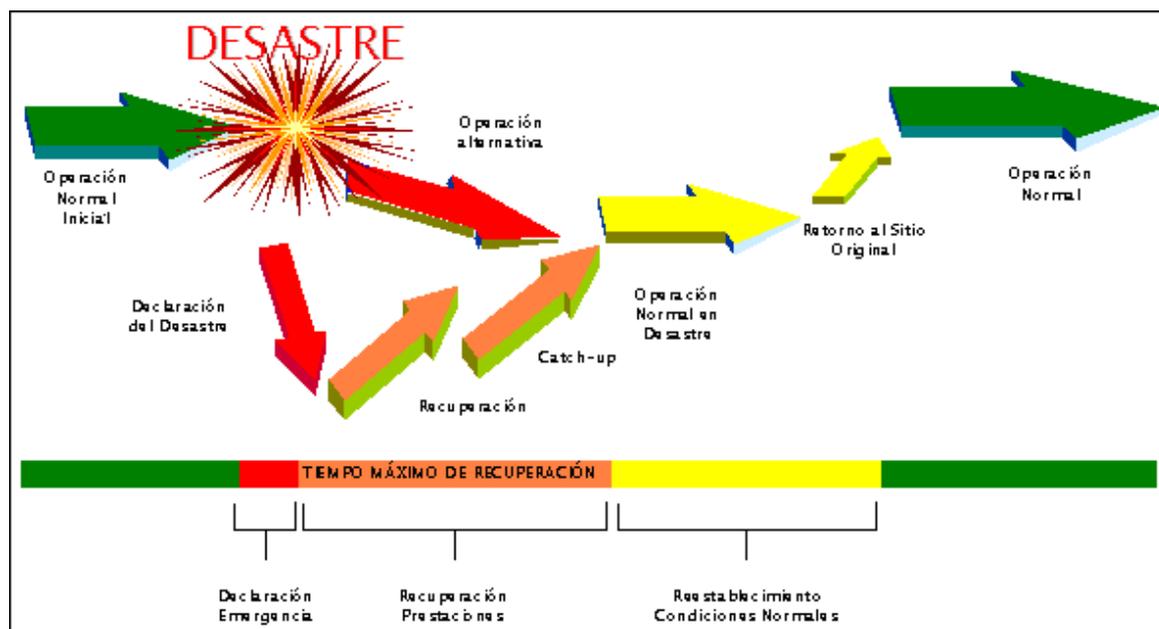
En esta primer instancia del PRD, se pone como objetivo identificar y delimitar el escenario que será objetivo de estudio para la realización del Plan.

La idea de este acercamiento inicial es conocer:

- Las condiciones físicas del entorno;
- Los servicios y aplicaciones existentes;
- Los equipos presentes;
 - Los servidores;
 - Los elementos de backup;
 - Los elementos de almacenamiento de datos;
 - Los elementos de comunicaciones.

2. Definición de los tipos de operación en una contingencia

Para elaborar el PRD, se consideran distintos estados de situación, que se definen a continuación, para establecer un marco claro que identifique y enumere las distintas instancias por las que puede atravesar el centro de cómputos en estudio antes, durante y luego de una contingencia.



Los principales tipos de operaciones considerados ante una emergencia son:

Operación Normal Inicial:

Es la operatoria que se registraba antes de ocurrir el desastre. Asimismo, define las condiciones que se deben alcanzar como objetivo final mediante la ejecución del Plan de Recuperación ante Desastres;

Operación Alternativa:

Mientras se trabaja en la recuperación de las prestaciones afectadas por la contingencia, los usuarios deberán utilizar una operatoria alternativa, constituida fundamentalmente por procesos manuales, durante la cual se genera información. A partir del momento en que los servicios y aplicaciones estén disponibles, existe un tiempo de "catch up" o actualización de la información del sistema, en el cual se ingresan las novedades ocurridas desde la ocurrencia de la emergencia;

Operación Normal en Desastre:

Mediante la ejecución de los procedimientos que reciben el nombre de "Recuperación de las prestaciones", se llega a esta instancia en la cual todos los servicios y aplicaciones han sido recuperados, pero no se encuentran ejecutando en su lugar original o bajo las mismas condiciones en que se encontraban originalmente.

Al finalizar el proceso de actualización de la información o "catch up", se considera que se ha llegado a la operación normal en desastre.

El tiempo desde la declaración de la emergencia hasta que se alcanza la operación normal en desastre no debe ser superior a los tiempos máximos tolerables de suspensión definido para cada una de las prestaciones.

Operación Normal Reestablecida:

Mediante la ejecución de los procedimientos que reciben el nombre de "Reestablecimiento de las condiciones normales" se alcanza esta última instancia, en la cual todos los servicios y aplicaciones se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaba antes de la contingencia.

Para alcanzar este tipo de operación, es posible que haya que considerar una suspensión programada de alcance total o parcial de las prestaciones, para lo cual es necesario acotar el tiempo de interrupción al mínimo indispensable, y que preferentemente sea imperceptible por los usuarios.

Ejemplo:

Bajo este esquema y considerando a modo de ejemplo muy sencillo para incorporar los conceptos y definiciones de más arriba, consideramos una contingencia producida por una falla técnica en el disco local de un servidor de archivos, los eventos que definen cada una de las operaciones son:

Operación Normal:

Es la operación del servidor utilizando su disco local;

Operación Alternativa:

Los usuarios almacenan los nuevos archivos en el disco local hasta tanto se habilite un lugar de almacenamiento central. En el momento en que se recupere las prestaciones del servidor de archivos, como parte del proceso de actualización de la información o "catch up", los archivos distribuidos se copian en el sitio habilitado;

Operación Normal en Desastre:

Se considera desde el momento en que la información del disco local del servidor se encuentra copiada en un disco de la cabina, la unidad ha sido montada en el servidor y todos los archivos generados durante la operatoria alternativa ha sido copiado en el sitio central.

Adicionalmente, a partir de la declaración de la emergencia, se debe realizar el reclamo al servicio técnico del proveedor del servidor, para que repare o reemplace el disco que ha fallado;

Operación Normal Reestablecida:

Se alcanza esta operatoria en el momento en que el servidor nuevamente utiliza su disco local;

3. Establecimiento de criticidades

El siguiente paso en la construcción del Plan de Recuperación ante Desastres es la determinación de la criticidad de los activos.

La idea es que en esta etapa se establezca la criticidad de las aplicaciones, de los equipos y los servicios que sostienen al negocio.

En función del impacto producido por la suspensión de las prestaciones del entorno informatizado, se determina la criticidad y el tiempo máximo de tolerancia de corte de las mismas.

A continuación se presenta el análisis realizado desde la perspectiva de los equipos y desde el punto de vista de servicios y aplicaciones.

Los documentos que registran las criticidades los organizamos en tablas llamadas: Tabla de Criticidades por Equipo, Tabla de Criticidades por Servicios y Tabla de Criticidades por Aplicaciones. A modo de ejemplo se exhiben las dos primeras.

Ejemplo - Tabla de Criticidades por Equipo.

El siguiente ejemplo muestra la Tabla de Criticidades por Equipo para 3 servidores de bases de datos con distinta tolerancia máxima de pérdida según su utilización, y su impacto en el negocio.

#	Equipo	Función	Sistema Operativo	Criticidad	Tolerancia Máxima	Impacto
1	DB1	Bases de datos	Solares 9	Alta	1 día	Perdida de imagen pública Reprocesamiento de formularios cargados manualmente
2	DB2	Bases de datos	Solares 9	Media	1 semana	Pérdida / inconsistencia de información
3	DB3	Bases de datos	Solares 9	Baja	2 semanas	Pérdida / inconsistencia de información

Se ve que el equipo DB1 tiene una criticidad alta y menor tiempo de tolerancia, por lo que deberá tener mayor foco al momento de definir la estrategia de recuperación.

Ejemplo - Tabla de Criticidades por Servicios.

El siguiente ejemplo muestra la Tabla de Criticidades por Servicios para el repositorio de archivos y el correo electrónico.

#	Servicio	Criticidad	Período crítico	Procedim. Alternat.	Parada Máxima	Plataf.	Usuarios
1	Servidor de Archivos	Media	Cierre a fin de mes	Guardar los archivos en las PC locales	1 semana	Novell Netware 5.0	Todos
2	Correo electrónico Lotus Domino Server	Alta	Todos los días	Toma de pedidos telefónicos	1-2 días	Windows 2000	Compras, ventas, despacho.

En este ejemplo se muestra que el servidor de correo electrónico es el más crítico dentro de los servicios prestados por la compañía, y requiere de 1 a 2 días como máximo para su recuperación. Esto deberá ser considerado al momento de establecer el tiempo mínimo de recuperación de las prestaciones en la estrategia seleccionada.

4. Determinación de las prestaciones mínimas

En esta etapa, mediante distintas formas de relevamiento que pueden ser entrevistas personales, llamadas telefónicas, observación y verificación de las principales unidades de negocio de la empresa objetivo, se pretende entender y determinar cuáles son las aplicaciones, los servicios o prestaciones mínimas que son críticos para el funcionar del negocio, y que deberán ser recuperadas de forma prioritaria ante el suceso de una emergencia, para preservar la continuidad del negocio.

Asimismo se debe estimar el tiempo máximo para recuperar estas prestaciones.

5. Análisis de riesgos

En esta etapa se analizan los riesgos presentes en el entorno, para determinar qué riesgos se pueden mitigar, cuáles se pueden transferir y cuáles se deben asumir.

No es posible eliminar todos los riesgos sino que se pueden mitigar (empleando medidas para reducirlos), transferir (ceder su responsabilidad a otra persona) o asumir (cuando se decide correr el riesgo con sus posibles consecuencias).

Sin embargo, siempre existen riesgos remanentes y desconocidos.

Es más, constantemente surgen nuevos riesgos a medida que la tecnología avanza y los sistemas cambian. Los entornos informatizados suelen acompañar estos cambios adaptándose a los requerimientos tecnológicos del momento. Es por eso que surgen nuevos riesgos día a día.

Los riesgos pueden ser:

- **Tecnológicos:** si tienen origen o afectan aspectos técnicos del entorno (como deterioro de equipamientos, falta de disponibilidad de recursos, etc);
- **Funcionales:** si tienen origen o afectan aspectos funcionales del entorno (como posible descubrimiento de información por la existencia de usuarios con contraseña por default, o el acceso no autorizado a los recursos por una pobre autenticación de usuarios).

Todos los entornos están expuestos a amenazas. Todos los entornos tienen vulnerabilidades, algunas conocidas, otras no, pero están presentes, esperando ser usadas por un atacante para penetrar las barreras de seguridad y apoderarse de información, denegar servicios, o provocar toda clase de daño.

No importa la plataforma tecnológica, no importa la marca de software que se usa. Tampoco importa la infraestructura edilicia, los equipos, el cableado. Siempre existen riesgos.

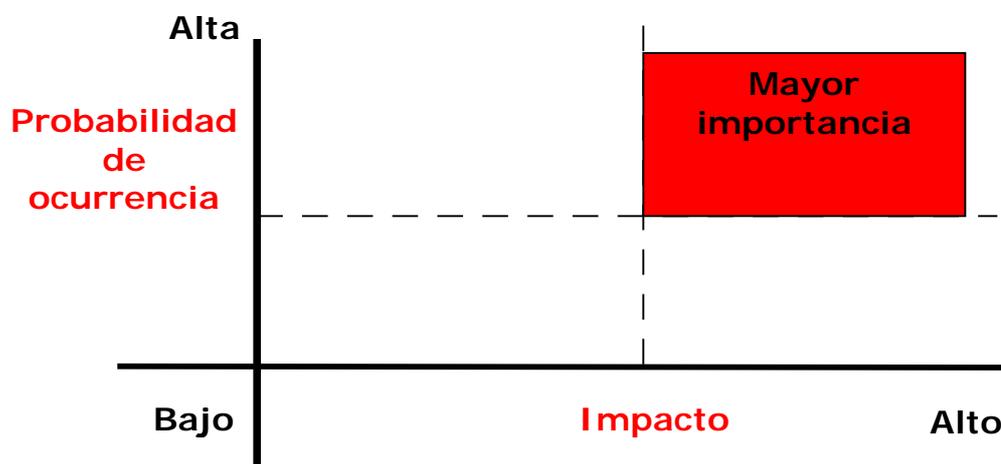
Existe una relación entre tipo de desastre y sus efectos, y, por supuesto, su probabilidad de ocurrencia. Los riesgos reales y potenciales son variables en el tiempo y en el lugar.

En esta parte de la elaboración del PRD de debe evaluar su riesgo asociado a cada uno de los activos (aplicaciones, servidores, etc), determinar su probabilidad de ocurrencia y medir su impacto en el entorno.

Los riesgos observados que presentan una probabilidad de ocurrencia no despreciable en función de las características del entorno varían desde los factores climáticos y meteorológicos que afectan a la región hasta el factor humano de los recursos de la empresa.

Para la evaluación de riesgos es posible utilizar métodos muy variados en composición y complejidad, pero para todos ellos es necesario realizar un diagnóstico de la situación.

Un método comúnmente utilizado es el diagrama:



Este análisis de riesgos permite ofrecer un informe de los riesgos entorno, los peligros que corre e identificar los requerimientos de seguridad del sistema objetivo y su prioridad.

El análisis de riesgos se realiza en cada área de la empresa, mediante métodos de adquisición de información como entrevistas con los usuarios.

Informe de Riesgos

A continuación se presenta un documento que ayuda a la formalización de estos conceptos para su estudio: el Informe de Riesgos.

Esta es una adaptación de la Tabla de Riesgos utilizada en el análisis de sistemas en la que se ha agregado la criticidad que implica la vulnerabilidad en estudio.

Se recomienda agrupar las vulnerabilidades con algún criterio, como por ejemplo por nivel de criticidad, que puede clasificarse en:

- Alta;
- Media;
- Baja.

U ordenarlas en forma decreciente según su impacto o probabilidad de ocurrencia.

Formato del Informe de Riesgos

#	Activo	Riesgo	Criticidad	P(ocurrencia)	Impacto

Descripción de los campos

- #: Número correlativo de vulnerabilidad.
- AMENAZA: Vulnerabilidad o situación que afecta a una aplicación, servicio o servidor que se está evaluando.
- RIESGO: Breve descripción del riesgo detectado en el análisis. Es todo evento, falla o bien que ponga en peligro la integridad, la confidencialidad o la disponibilidad de la información o los recursos y activos;
- CRITICIDAD: Una medida de la criticidad del riesgo, según el siguiente criterio:
 - § Baja: Representa una amenaza casi despreciable o no representa amenaza alguna;
 - § Media: Amenaza leve;
 - § Alta: Gran amenaza al sistema.
- P (ocurrencia): Es la probabilidad de ocurrencia de dicho evento tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.
- IMPACTO: Es el efecto potencial de una falla de seguridad, teniendo en cuenta sus consecuencias en el negocio.

Ejemplo – Informe de Riesgos.

La siguiente tabla muestra un ejemplo de Informe de Riesgos elaborado para una empresa, en el que se evaluó el centro de cómputos, el edificio y las distintas sedes regionales.

#	AMENAZA	RIESGO	CRITICIDAD	P(ocurrencia)	IMPACTO
1	Existencia de material inflamable en el CPD (Centro de Procesamiento de Datos)	Fuego en el Data Center	Alta	0.5	Dstrucción de equipos y espacio físico
2	Existencia de material inflamable en el CPD y en las oficinas aledañas	Fuego en lugares cercanos	Alta	0.45	Dstrucción de documentación impresa y posibilidad de afección del centro de cómputos
3	Ubicación física en zona inundable	Inundación	Media	0.1	Posibles cortocircuitos, equipos quemados, incendios

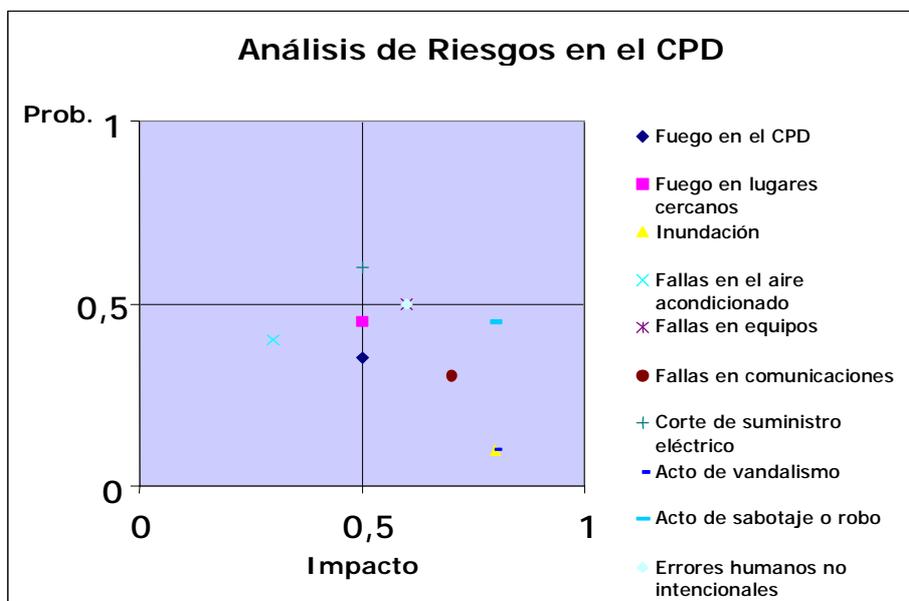
#	AMENAZA	RIESGO	CRITICIDAD	P(ocurrencia)	IMPACTO
4	Falta de equipo de aire acondicionado de backup	Fallas en el aire acondicionado	Alta	0.4	Mal funcionamiento por recalentamiento de equipos
5	Falta de mantenimiento de los equipos de procesamiento de datos.	Fallas en equipos	Media	0.5	Indisponibilidad de los servicios
6	Existencia de cables de red al descubierto atravesando los pasillos	Fallas en comunicaciones	Media	0.3	Indisponibilidad de los servicios
7	Descuido del cableado eléctrico, falta de acondicionamiento de la central eléctrica y pobre aislamiento.	Corte de suministro eléctrico	Media	0.6	Indisponibilidad de los servicios, pérdida de datos.
8	Exposición de los equipos a personal no autorizado.	Acto de vandalismo	Alta	0.1	Pérdida de equipos, negación de servicios, pérdida de información, mala imagen en clientes, pérdida de confiabilidad.
9	Exposición de los equipos a terceros.	Acto de sabotaje o robo	Alta	0.45	Pérdida de confiabilidad, pérdida de información.
10	Administración de los equipos por personal no especializado.	Errores humanos no intencionales	Baja	0.5	Indisponibilidad de los servicios, pérdida de datos.

Diagrama de riesgos:

El diagrama de riesgos esquematiza el impacto de los riesgos en función de su probabilidad de ocurrencia.

Cuanto mayor sea el impacto y la probabilidad de ocurrencia, más fuertes deberán ser los controles a aplicar para mitigar el riesgo asociado.

Los riesgos más altos, por ende, se ubicarán en el cuadrante derecho superior del siguiente diagrama:



5.1 Probabilidad de ocurrencia de desastres

Los riesgos considerados para el plan de recuperación ante desastres, son aquellos que presentan una probabilidad de ocurrencia no despreciable en función de las características del entorno:

- Características meteorológicas de la región;
- Características generales del edificio;
- Condiciones ambientales;
- Equipamiento alojado;
- Condiciones de acceso;
- Condiciones de las oficinas contiguas.

5.2 Determinación de los niveles de desastre

En función del impacto producido por una contingencia, se definen 3 grandes tipos de desastres:

Total o Mayor:

En el caso en que el lugar físico no pueda disponerse por un período máximo tolerado para la interrupción de las prestaciones mínimas o el tiempo que demoran las tareas de reestablecimiento de todas o algunas de las prestaciones sea mayor al período máximo aceptable.

Parcial:

En el caso en que los equipos han sufrido daños menores que permiten su funcionamiento parcial o sus prestaciones pueden ser realizadas por otros equipos, y es necesaria la acción de alguien externo (proveedores, mantenimiento, etc.)

Menor:

En el caso en que los desperfectos se solucionan mediante la reinstalación y/o reconfiguración de los equipos, y por lo tanto no es necesaria la acción de alguien externo para superar la situación de emergencia.

6 Estrategia de Recuperación

6.1 Presentación de las distintas estrategias posibles de recuperación

En esta etapa el consultor analiza las distintas alternativas que aporten solución al problema, teniendo en cuenta todo el análisis anterior.

Las distintas estrategias de recuperación van a estar inclinadas a:

- Recuperación total del centro de cómputos
- Recuperación parcial de los equipos
- Recuperación individual de equipos, aplicaciones o servicios.

Dentro de cada clase, deben presentarse distintas alternativas para darle al oportunidad al cliente de que elija la que más le conviene.

6.2 Selección de la estrategia de recuperación

El consultor, experto en Seguridad de la Información, presenta las distintas alternativas al cliente quién decide por cuál opta.

6.3 Desarrollo de la estrategia de recuperación

Una vez seleccionada la estrategia a seguir, se procede al desarrollo de la misma, que deberá ofrecer medidas preventivas y de mitigación de los riesgos existentes, además de la estrategia de recuperación de las prestaciones.

6.4 Mitigación de riesgos – Medidas preventivas

La estrategia de recuperación supone la realización de acciones de mitigación de los riesgos considerados en el análisis correspondiente, las cuales deben considerar las actuales condiciones de redundancia y tolerancia a fallas existentes, por ejemplo:

- Realizar pruebas periódicas de recuperación de las cintas de backup;
- Almacenamiento de cintas de backups adicionales en locaciones externas al edificio del entorno analizado;
- Generación periódica de backups en medios de recuperación universal (cintas DAT).

6.5 Descripción de la estrategia

En esta parte el consultor, experto en Seguridad de la Información, describe detalladamente la estrategia seleccionada por el cliente, y especifica las medidas a tomar para la eficaz recuperación del entorno, luego de un desastre.

Cada estrategia dependerá pura y exclusivamente del entorno informatizado en estudio, y del Alcance del Plan. Muchas empresas suelen implementar el PRD en varias etapas, comenzando por ejemplo por los servidores de datos, continuando por las aplicaciones, luego las comunicaciones y el Centro de Cómputos (CC) o Centro de Procesamiento de Datos (CPD), o Data Center (DC). Otras, en cambio, deciden hacer un solo plan completo en una fase, que abarque todos sus bienes y activos físicos y lógicos.

Lógicamente esta es una decisión empresarial, influenciada fuertemente por el presupuesto de la empresa y los límites de tiempo.

El PRD suele ser requerido por auditorías, por lo que a veces el cliente se ve presionado por las fechas y se decide dejar ciertos elementos fuera del Alcance.

En general, en la descripción de la estrategia se definirán las medidas a tomar para la recuperación del entorno, como por ejemplo:

- Creación de un Equipo de Recuperación del Entorno ante Desastres (ERED) con responsabilidades y conocimientos específicos que actuará ante las situaciones de contingencia;
- Recuperación de las prestaciones de los elementos afectados por una contingencia utilizando la redundancia existente;
- Utilización de un CPD alternativo con un servidor de contingencia para la recuperación de la aplicación más crítica en caso de un desastre mayor;
- Exigencia del cumplimiento de los tiempos de respuesta especificados en los contratos de soporte con proveedores de hardware.

7 Requerimientos para llevar a cabo el Plan

Los requerimientos conforman una guía de las principales características y condiciones que deben cumplir los elementos sobre los cuales versa el documento, a fin de ser utilizados en procedimientos de mantenimiento y auditoría.

Los documentos desarrollados establecen las condiciones de:

- Características físicas del Centro de Cómputos alternativo, si la estrategia requiriera la instalación de un CPD alternativo para la recuperación;
- Características físicas de los equipos de recuperación, si la estrategia implicara la compra de equipos de contingencia;
- Miembros del Equipo de Recuperación ante Desastres;

7.1 Esquemas técnicos

Los esquemas definen pasos generales a seguir de manera operativa para la ejecución de una determinada tarea.

La ejecución de dichos pasos supone el conocimiento técnico de la tarea que se está realizando y tiene por objetivo brindar un marco integral de rápida referencia.

Todas estas tareas deben estar predefinidas y documentadas al momento de enfrentar una situación de emergencia.

Algunos de los esquemas a desarrollar son:

- Activación del CPD alternativo;
- Recuperación de equipos;
- Reestablecimiento de servidores;
- Reestablecimiento de bases de datos;
- Reestablecimiento de Aplicativos;
- Ejemplos de notificación de la emergencia.

7.2 Formación del Equipo de Recuperación del Entorno ante Desastres (ERED)

El Formación del Equipo de Recuperación del Entorno ante Desastres (ERED) tiene como fin determinar y asignar distintas responsabilidades para lograr una exitosa recuperación del entorno ante una emergencia, según el Plan (PRD) establecido.

Para ello se establecen ciertas pautas que las personas que lo componen deben cumplir:

7.2.1 Roles y responsabilidades

El Equipo de Recuperación del Entorno ante Desastres tiene las siguientes responsabilidades:

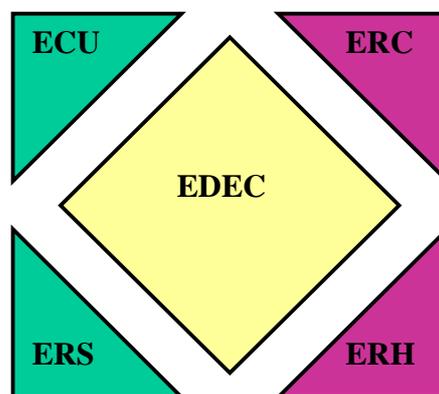
- Definir las medidas preventivas necesarias y factibles de aplicar, a fin de disminuir la probabilidad de ocurrencia de desastres;
- Definir, probar, ajustar y mantener actualizado el Plan de Recuperación del Entorno ante Desastres;
- Ante un desastre que afecte al Centro de Cómputos debe:
 - Recuperar las prestaciones en el menor tiempo posible y dentro de los plazos máximos establecidos;
 - Reestablecer las condiciones normales que se presentaban antes del desastre;
 - Analizar las causas del desastre y la forma en que se ha procedido a fin de emitir un informe y modificar las medidas preventivas y plan de recuperación en función de las conclusiones.

A su vez, el ERED está compuesto por sub-equipos con distintas obligaciones.

Estos equipos son:

- Equipo de dirección estratégica y coordinación [EDEC]
- Equipo de recuperación de hardware [ERH]
- Equipo de recuperación de software [ERS]
- Equipo de recuperación de comunicaciones [ERC]
- Equipo de comunicaciones a usuarios [ECU]

Gráficamente el Equipo de Recuperación del Entorno ante Desastres se esquematiza de la siguiente forma:



Equipo de dirección estratégica y coordinación

Las responsabilidades de este equipo son:

- Dirigir y coordinar las actividades del resto de los equipos que conforman el Equipo de Recuperación del Entorno ante Desastres;
- Realizar las declaraciones de los distintos estados: emergencia, contingencia y reestablecimiento de las condiciones normales;
- Determinar el nivel de desastre producido por una contingencia: total o mayor, parcial, menor;
- Elaborar los planes de recuperación de las prestaciones y reestablecimiento de las condiciones normales;
- Controlar la ejecución de los planes, detectar desvíos y realizar los ajustes de los planes en función de los inconvenientes, problemas y errores hallados durante la aplicación de los mismos;
- Interactuar con personal de mantenimiento para la resolución de contingencias físicas del Centro de Cómputos.

Equipo de recuperación de hardware

Las responsabilidades de este equipo son:

- Identificar los elementos de hardware que hayan sido dañados por una contingencia;

- Coordinar con los proveedores de hardware el cumplimiento de los contratos de mantenimiento, garantías y niveles de soporte;
- Participar en las instalaciones de sistemas operativos que realicen los proveedores;
- Verificar el correcto funcionamiento de los elementos de hardware que hayan sido restaurados o reemplazados por los proveedores.

Equipo de recuperación de software

Las responsabilidades de este equipo son:

- Identificar los servicios, procesos, bases de datos y aplicaciones que hayan sido afectados por una contingencia;
- Instalar, configurar y ajustar todo el software que haya sido afectado por una contingencia.

Equipo de recuperación de comunicaciones

Las responsabilidades de este equipo son:

- Identificar los elementos de comunicaciones que hayan sido dañados por la contingencia;
- Detectar los problemas de conectividad de los equipos del CPD y determinar las causas;
- Coordinar con el responsable los cambios que haya que realizar en las comunicaciones que no sean internas del Centro de Cómputos para que los usuarios puedan seguir utilizando las prestaciones ;
- Verificar el correcto funcionamiento de los elementos de comunicaciones y la conectividad general para que los usuarios puedan acceder a los recursos del CPD.

Equipo de comunicaciones a usuarios

Las responsabilidades de este equipo son:

- Participar en la generación de las comunicaciones oficiales a usuarios ante contingencias, recuperación de prestaciones, demoras incurridas que invaliden o modifiquen lo comunicado anteriormente y el reestablecimiento de las condiciones normales;
- Realizar las comunicaciones a los usuarios internos.

7.2.2 Asignación de roles

Luego de determinar las características de los equipos de recuperación, el cliente debe designar recursos humanos para cubrir todos los roles, teniendo en cuenta que una persona no puede formar parte de más de dos equipos.

7.3 Desarrollo de procedimientos

Más allá del alcance del PRD, se deben especificar procedimientos claros que ayuden a alcanzar el reestablecimiento de las condiciones normales del entorno informatizado.

Los principales procedimientos a definir son:

Declaración de la emergencia

Abarca desde la detección del desastre hasta que el mismo es comunicado a los afectados; Durante el mismo no se procede a recuperar nada, simplemente se evalúa los daños causados;

Se encuentra conformado por los siguientes sub-procedimientos:

- Respuesta inicial ante la detección de un siniestro o contingencia;
- Evaluación del nivel de desastre;
- Notificación de la emergencia.

Recuperación de las prestaciones

Consta básicamente del diseño y ejecución del plan de recuperación de las prestaciones, conforme a lo acontecido;

Contempla la aparición de imprevistos que puedan alterar o modificar el plan inicialmente armado;

Se encuentra conformado por los siguientes sub-procedimientos:

- Definición del plan de recuperación de las prestaciones;
- Ejecución del plan;
- Ajustes al plan.

Reestablecimiento de las condiciones normales

Consiste en el diseño y ejecución del plan de reestablecimiento de las condiciones normales de operación, finalizando con el análisis de la situación ocurrida a fin de ajustar el PRD en función de los errores, demoras e inconvenientes acontecidos, así como también la posible toma de nuevas medidas preventivas;

Se encuentra conformado por los siguientes sub-procedimientos:

- Definición del plan de reestablecimiento de las condiciones normales;
- Ejecución del plan;
- Evaluación y análisis de la contingencia.

8 Pruebas del PRD

Una de las últimas etapas en la elaboración del PRD es la de pruebas. El plan debe ser probado en su totalidad al menos una vez al año, según las mejores prácticas y regulaciones internacionales, y probado parcialmente en distintas oportunidades mediante un esquema continuo de mejoras y revisión, que contribuyan al mantenimiento vigente del plan a lo largo del tiempo y garanticen la recuperación de las prestaciones en un futuro.

9 Revisión del PRD

El Plan debe ser revisado con regularidad para garantizar su adecuación a los cambios que sufre el entorno, manteniendo vigente su aplicabilidad frente a desastres.

10 Cierre del proyecto

Para finalizar el proyecto, luego del consenso interno, se presenta la documentación final a los responsables.

Anexo I – Bibliografía

- [IRAM/ISO/IEC17799] IRAM/ISO/IEC 17799 Julio 2002. Proyecto 1 de norma argentina. Código de práctica para la gestión de la seguridad de la información. Basada en ISO/IEC Standard 17799: Information Technology – Code of Practice for Information Security Management.
- [BS7799] British Standard - Information technology. Code of practice for information security management.
- [Cobit] Cobit Standard- Objetivos de Control para la Información y Tecnologías - 2000, emitido por el Comité directivo del Cobit y la Information Systems audit. And Control Fundation.
- [Stallings1999] Stallings, W. 1999. Cryptography and Network Security: Principles and Practice, 2da edición, Prentice Hall, Inc.
- [Martorell] Martorell, M. Control de Accesos. Escola Universitaria Politecnica de Mataro.
- [hispasec] Hispasec Sistemas.
<http://www.hispasec.com>
- [isecom] ISECOM - Institute for security and Open Methodologies.
<http://www.isecom.org>
- [iss.net] ISS- Internet Security Systems.
<http://iss.net>
- [xforce.iss] Base de datos de vulnerabilidades y amenazas de ISS.
<http://xforce.iss.net/>
- [bsi] British Standards Online.
<http://www.bsi-global.com/index.xalter>
- [Benson] Microsoft Solutions Framework. Estrategias de Seguridad. Christopher Benson, Inobits Consulting (Pty) Ltd.
<http://microsoft.com/latam/technet/articulos/200011/art04>
- [Consid-MS] Microsoft Solutions Framework. Consideraciones de seguridad para la autoridad administrativa.
<http://msn.com>
- [10laws-MS] Microsoft Technet. The Ten Immutable Laws of Security. 2003
<http://microsoft.com/technet/columns/security/assays/10imlaws.asp>
- [Technet] Microsoft Technet.
<http://microsoft.com/technet>
- [ISACA] ISACA (Information Systems Audit and Control Association).
<http://www.isaca.org>

Anexo II – Referencia a MAEI

La metodología para el Aseguramiento de Entornos Informatizados (MAEI) se encuentra basada en un enfoque que va de lo general a lo particular, y sirve para generar planes integrales de aseguramiento para entornos informatizados de cualquier tipo, cualquiera sea su alcance. Incluye las mejores prácticas en el campo de la seguridad de la Información en el ámbito mundial.

La misma esta disponible en formato electrónico en el sitio www.fi.uba.ar.

Anexo III – Acerca de Cidicom S.A

Cidicom es una compañía regional que provee servicios profesionales de tecnología de la información para empresas, entidades financieras y el sector público. Ofrece soluciones de alto valor agregado, pensadas en función de las necesidades específicas de cada industria. Posee un plantel mayor a 100 ingenieros certificados y especializados en múltiples plataformas.

Cidicom basa su operación en un sistema de gestión de la calidad certificado bajo la norma ISO 9001:2000 y bajo pautas de vocación de servicio las 24 horas, todos los días del año.

Las principales áreas de especialización de Cidicom son:

Soluciones y servicios en seguridad

Asesoría en la implementación de estrategias en seguridad, ofreciendo análisis de riesgos, recuperación de datos y sitio de recuperación ante desastres, asesoramiento técnico especializado, auditoría en seguridad y planes de contingencia, entre otros. El concepto básico es brindar al cliente una solución integrada en los temas referidos a seguridad, con excelencia y alto profesionalismo.

Los servicios brindados por Cidicom permiten asegurar la confidencialidad, integridad y disponibilidad de la información, independientemente del dispositivo de almacenamiento en que se encuentre (físico o lógico) de acuerdo a los requerimientos de las normas internacionales como ISO 17799.

En la actualidad, la seguridad informática es de gran importancia para las empresas a nivel mundial. El espionaje electrónico, el robo de información y los desastres naturales, son algunos de los factores que pueden llevar a una compañía a sufrir pérdidas de información. Según un estudio realizado por Price Waterhouse & Coopers, el 70% del valor de una empresa está dado por su propiedad intelectual.

Al igual de lo ocurrido en otros países con la implementación de normas como ISO 17799 y la alineación con leyes como Sarbannes Oxley, Health Insurance Portability and Accountability Act, entre otras -con el fin de afrontar temas de seguridad y de resguardo de la información- Cidicom apuesta a la pronta aplicación de los mismos o similares estándares en nuestro país.

Una sólida política de seguridad y manejo de información brinda innumerables beneficios. Entre ellos:

- Eficiencia operativa
- Continuidad del negocio
- Ventajas competitivas
- Aumento en el valor de mercado

Soluciones y servicios en infraestructura

Consultoría especializada en temas de infraestructura física y tecnológica, adecuada a las necesidades de cada empresa, optimizando los recursos aplicados al armado de la

infraestructura, incluyendo esquema de telefonía sobre IP y soluciones de almacenamiento de la información.

El concepto principal detrás del servicio de asesoría en infraestructura física es el de optimizar todos los componentes, desde el control de accesos, las cámaras de video vigilancia digital, el cableado estructurado, las medidas de detección y prevención, las soluciones de energía, entre otros. Estos componentes deben estar integrados para un óptimo resultado.

El montaje de una arquitectura que permite el crecimiento con mínima inversión es elemental para la infraestructura tecnológica. Para lograr esto, Cidicom pone a disposición sus recursos especializados en temas tecnológicos que permiten definir la mejor infraestructura tecnológica en base a los requerimientos actuales y proyección futura de la empresa.

La óptima estrategia de infraestructura tecnológica se traduce en algunos de estos beneficios:

- Soluciones para centros de contacto
- Implementación de redes
- Soluciones de conectividad y soluciones de almacenamiento

En la actualidad, muchas empresas se encuentran en un proceso de redefinición de su arquitectura debido al crecimiento o a normativas. Los hechos ocurridos -desastres naturales, actos de terrorismo, sabotaje, etc.- llevan a revisar la infraestructura. Así también a replantear la estrategia, acudiendo a sitios de contingencia, planes de recuperación de desastre, revisión de los accesos, conectividad, entre otros.

Algunos de los beneficios que la empresas pueden obtener a partir de una correcta infraestructura son:

- Reducción de los costos de mantenimiento y operación
- Continuidad del negocio
- Aumento en la productividad de los empleados
- Aprovechamiento de la base de conocimiento de la empresa

Actualmente, las empresas se suman a la tendencia mundial en comunicaciones e invierten en telefonía por Internet alentadas por la reducción del costo de las llamadas, permitiendo también integrar la telefonía a los procesos de negocios. Cidicom ofrece elevar la productividad, reducir costos operativos de la empresa mediante la afinidad de las comunicaciones; además de proveer soluciones de acuerdo a las necesidades de las empresas, las cuales pueden ser corporativas, medianas o pequeñas.

Soluciones de negocios

Cidicom no esta ajeno a la necesidad de las empresas de contar con soluciones de negocios de alto valor agregado, que permiten enfocar todos sus esfuerzos en ser más competitivos y no en la plataforma tecnológica. Cidicom cuenta con profesionales especializados en la definición, diseño, implementación y soporte de algunas de las soluciones de negocios mas conocidas como digitalización, CRM, centro de contactos, automatización de procesos industriales.

Particularmente, Cidicom demuestra un crecimiento sostenido en el área de automatización industrial ofreciendo soluciones de software e integración especialmente diseñadas:

mbisogno@cidi.com.ar - Tel.: (5411) 4334-9959 int. 106 - Cel.: +54 (9) 11 (15) 6024-2508

- Control y monitoreo de procesos
- Comunicaciones e ingeniería de planta
- Análisis de factibilidad
- Soporte técnico de sistemas de control
- Asistencia remota

Además, dentro del marco industrial, Cidicom brinda servicios profesionales para que las áreas encargadas de la toma de decisiones de las empresas cuenten con información detallada y confiable, tomada directamente de la fuente. Entre los servicios provistos, se encuentran:

- Manejo y administración de fórmulas
- Simulaciones de procesos
- Planificación de líneas de producción
- Coordinación de equipos
- Planificación de paradas de planta
- Optimización de los procesos productivos

Un Staff certificado y especializado

Cidicom cuenta con un plantel regional mayor a 100 ingenieros certificados y especializados en múltiples plataformas. Estos asisten a los clientes adecuando las mejores prácticas a las necesidades de seguridad de las empresas.

Cidicom invierte el 7% de su facturación anual en planes de capacitación continua. Como consecuencia directa de los planes de capacitación se desarrollan laboratorios de investigación y prueba de distintas tecnologías. El objetivo es entregar al cliente soluciones supervisadas por especialistas certificados.

Más información: www.cidi.com.ar

Anexo IV - Definiciones

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Autorización: Garantizar que todos los accesos a datos y/o transacciones que los utilicen, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Confiabilidad: Garantizar que los sistemas informáticos brinden información correcta para ser utilizada en la operatoria de cada uno de los procesos.

Confidencialidad: Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Disponibilidad: Garantizar que la información y la capacidad de su tratamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de las actividades.

Eficacia: Garantizar que toda información que sea utilizada es necesaria y entregada de forma oportuna, correcta, consistente y útil para el desarrollo de las actividades.

Eficiencia: Asegurar que el tratamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

ID: Nombre o identificación de usuario.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Incidencia o incidente: cualquier anomalía que afecte o pudiera afectar a la seguridad del entorno.

Integridad: Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de las actividades en cada uno de los sistemas informatizados y procesos transaccionales.

No Repudio: Garantizar los medios necesarios para que el receptor de una comunicación pueda corroborar fehacientemente la autenticidad del emisor.

Password: (palabra de paso, contraseña) Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

PC: Personal Computer. Computadora Personal.

Protección Física: Garantizar que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

Propiedad: (derecho a propiedad) Asegurar que todos los derechos de propiedad sobre la información utilizada en el desarrollo de las tareas, estén adecuadamente establecidos a favor de sus propietarios.

Recurso: cualquier parte componente de un entorno informatizado.

Seguridad de la Información: La preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistemas de información: conjunto de archivos automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.

Software malicioso: (malware) Es un término común que se utiliza al referirse a cualquier programa malicioso o inesperado o a códigos móviles como virus, troyanos, gusanos o programas de broma.

Soporte: objeto físico susceptible de ser tratado en un entorno informatizado y sobre el cual se pueden grabar o recuperar datos.