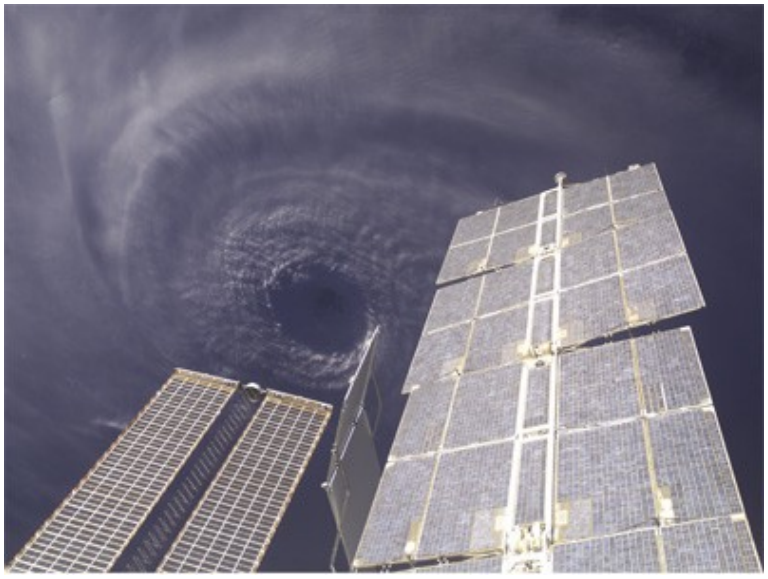
UNIVERSIDAD DE LA REPÚBLICA

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMNISTRACIÓN

"PLANES DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO"



TRABAJO DE INVESTIGACIÓN MONOGRÁFICO

CONTADOR PÚBLICO – PLAN 90

CÁTEDRA: Introducción a la Computación

Marzo de 2010

María José Vigo Jaccottet – C.I.: 1.888.962-6
Carlos Alberto Cardoso Flores – C.I.: 3.845.646-3
Wilson Adrián de Mello Cabrera – C.I.: 3.981.734-5

Tutor: Ing. Simón Mario Tenzer

AGRADECIMIENTOS

A nuestras familias, parejas y amigos, por la paciencia que nos han tenido a lo largo de ésta etapa, por entender las horas que les robamos para dedicarle a la carrera, y el esfuerzo que realizamos a lo largo de ella.

Particularmente a Simón Tenzer por el apoyo y la orientación brindada para poder llevar adelante éste proyecto.

Finalmente un agradecimiento a todos aquellos que accedieron a brindarnos información que nos fue de utilidad para la elaboración de éste trabajo.

ABSTRACT

La información es un activo muy importante, que con el pasar de los años ha adquirido más relevancia en el ciclo de vida de las organizaciones. Las empresas a diario están expuestas a una serie de amenazas que pueden afectar su normal operativa, y por ende interrumpir su continuidad. Dichas amenazas, pueden ser de naturaleza muy variada, desde negligencia hasta desastres naturales.

Las consecuencias pueden acarrear a las organizaciones altos costos, e incluso pueden llevarla a la quiebra. El impacto dependerá del tipo de organización, el ramo de actividad, el grado de dependencia de las TI, y de las previsiones que haya tomado al respecto.

Nuestro trabajo brinda un marco teórico para aquellas empresas interesadas en desarrollar estos planes, así como ejemplifica las consecuencias de no poseerlo Pretendemos exponer la realidad de nuestro mercado, a través de entrevistas tanto a empresas del medio local como a consultoras especialistas en el tema.

ÍNDICE

Página

CAPÍTULO I – INTRODUCCIÓN…….. 6

CAPÍTULO II - PLANIFICACIÓN DE CONTINGENCIA…….. 8

1. Planificación de Contingencia y Gestión de Riesgos…… 8

2. Tipos de Planes…… . 10

3. Plan de Contingencia y Desarrollo del Ciclo de Vida del Sistema…….. 12

CAPÍTULO III - PROCESO DE PLANIFICACIÓN DE CONTINGENCIA DE TI... 15

1. Declaración de Política de Planificación de Contingencia……. 15

2. Ejecución del Business Impact Analysis (BIA)……. 16

3. Identificar Controles Preventivos…… 19

4. Desarrollar Estrategias de Recuperación……. 20

5. Pruebas, Capacitación y Ejercicios del Plan…… 26

6. Plan de Mantenimiento……..... 28

CAPÍTULO IV - DESARROLLO DEL PLAN DE CONTINGENCIA……. 31

1. Información de Apoyo…… 31

2. Fase de Activación…… 32

3. Fase de Recuperación…….. 35

4. Fase de Reconstitución…… 37

5. Apéndices…… 38

CAPÍTULO V - CONSIDERACIONES TÉCNICAS DE CONTINGENCIA..... 39

1. Computadoras de Escritorio y sistemas Portátiles..... 39

2. Servidores..... 42

3. Sitios Web..... 49

4. Redes de Área Local (LAN)..... 51

5. Redes de Área Extensa (WAN)..... 53

6. Sistemas Distribuidos..... 56

7. Sistemas Mainframe..... 58

CAPÍTULO VI – LA CONTINUIDAD DEL NEGOCIO..... 60

CAPÍTULO VII – TRABAJO DE CAMPO..... 64

ENFOQUE DE CONSULTORA W..... 65

ENFOQUE DE CONSULTORA X..... 81

ENFOQUE DE CONSULTORA Y..... 90

ENFOQUE DE CONSULTORA Z..... 99

ENTREVISTAS CON EMPRESAS DEL MEDIO LOCAL..... 106

CAPÍTULO VIII – CONCLUSIONES..... 119

CONCLUSIONES ACERCA DEL TRABAJO DE CAMPO..... 119

RECOMENDACIONES..... 122

CAPÍTULO IX – EL ROL DEL EGRESADO..... 123

CAPÍTULO X – ANEXOS..... 124

1) EJEMPLOS DE PLANES DE CONTINGENCIA..... 124

A) Ejemplo de Plan de Contingencia de Empresa de la Industria Farmacéutica.... 124

B) Administración Nacional de Puertos – Análisis de Servidores y Servicios…… 135

2) EJEMPLOS DE CONTINGENCIAS OCURRIDAS…… 138

A) Pequeña Empresa Mejicana…… 138

B) Inundación en Banco Español…… 139

C) Ejemplo de Institución Médica Uruguaya…… 139

D) Ejemplo de Empresa Exportadora - Importadora Uruguaya…… 140

E) Atentado en el World Trade Center (Nueva York)…….. 140

F) Inundación en el CPD de Empresa Española…….. 141

G) Robo en Empresa Española…… 141

H) Daño en Fibra Óptica de Antel…… 141

I) Atentado de Bishopsgate…… 142

J) Centro de Cómputos del Banco de Previsión Social…… 142

BIBLIOGRAFÍA…… 143

CAPÍTULO I – INTRODUCCIÓN

Es vital para las empresas contar con información fiable, íntegra y oportuna, para llevar adelante sus negocios. Es por ello que con el correr de los años se han desarrollado sistemas informáticos abocados a la gestión de dicha información.

En la actualidad es casi impensable que una organización no cuente con un sistema informático, por pequeño que éste sea, y por lo tanto deben existir técnicas que lo protejan (física y lógicamente).

Con el crecimiento de la tecnología de la información y la confianza sobre datos cruciales, el panorama ha cambiado en años recientes, a favor de la protección de datos irremplazables.

Gracias a la informática y su apoyo diario al trabajo realizado en las empresas, pueden realizarse operaciones complejas de manera sencilla y transparente. Pero, ¿cómo actuar si un día dejara de funcionar todo nuestro sistema? ¿qué pasaría si perdiéramos los datos que hemos venido elaborando durante años, y que son de crucial importancia para el presente y futuro de nuestra organización? La respuesta se encuentra en el "desconocido" para muchos: Plan de Contingencia; documento en el que se recogen un conjunto de protocolos a seguir, ante situaciones de desastre para garantizar la continuidad del negocio y operaciones de la organización. Se trata de un tema sensible, que afecta la imagen de la organización (nadie querría hacer negocios con una empresa que demostró ser vulnerable), por lo cual el libre acceso a la información pertinente es dificultosa, e incluso muchas veces es ocultada o "filtrada" (por ejemplo el Incendio en Ute del año 1993).

El Uruguay carece de una normativa respecto a éste tema; además las empresas son reacias a los cambios, y a reconocer "fracasos" empresariales por carencia de planes de contingencia. Esto hace que los desarrollos bibliográficos en nuestro medio sean carentes, escasos o de difícil acceso.

De las empresas que tienen una pérdida importante de registros automatizados, el 43% nunca vuelve a abrir, el 52% cierra en menos de 2 años, y solo el 6 % sobrevivirá a largo plazo (Jim Hoffer, "Backing up Business-Industry Trend or Event" Health Management Technology).

Los sistemas son vulnerables a una variedad de trastornos, que van desde los leves (interrupción de la energía a corto plazo, falta de unidad de disco, etc.) a la destrucción severa que pueden provenir de una variedad de fuentes tales como los desastres naturales o las acciones terroristas. Si bien muchas vulnerabilidades pueden minimizarse o eliminarse a través de técnicas de gestión o soluciones operativas, es prácticamente imposible eliminar por completo todos los riesgos. En muchos casos, los recursos críticos pueden residir fuera del control de la organización (como la energía eléctrica o las telecomunicaciones), y la organización debería ser capaz de asegurar su disponibilidad. Por lo tanto, para una planificación exitosa acerca de las contingencias, la organización debe asegurar lo siguiente:

1. Entender el proceso de planificación de contingencia de TI y su lugar dentro de la continuidad global del Plan de Operaciones.

2. Desarrollar o reexaminar sus políticas de emergencia y el proceso de planificación. Aplicar los elementos del ciclo, incluyendo la planificación preliminar, análisis de impacto en el negocio, la selección de sitios alternativos, y las estrategias de recuperación.

3. Desarrollar o reexaminar sus políticas en materia de planificación de contingencia con énfasis en el mantenimiento, la formación y el ejercicio del plan.

Para desarrollar en forma ordenada el proceso de planificación de contingencia, las empresas pueden guiarse utilizando estos siete pasos:

1. **Definir una política de planificación de contingencia.** El desarrollo de una política formal proporciona a la organización la autoridad y la orientación necesarias para elaborar un plan de contingencia efectivo.

2. **Realizar el análisis de impacto en el negocio (Business Impact Analisys – BIA)**. El BIA ayuda a identificar y dar prioridad a sistemas críticos de TI y sus componentes.

3. **Identificar los controles preventivos.** Las medidas adoptadas para reducir las interrupciones del sistema pueden aumentar la disponibilidad del mismo y reducir costos de contingencia.

4. **Desarrollar estrategias de recuperación.** Buscando que el sistema pueda recuperarse con rapidez y eficacia tras una interrupción.

5. **Desarrollar un plan de contingencia de TI.** El plan de contingencia debe contener una guía detallada y los procedimientos para la restauración de un sistema dañado.

6. **Testeo del plan, capacitación y ejercicios.** Probar el plan permite identificar las deficiencias de planificación; la formación del personal se enfoca en la activación del plan de recuperación, tanto para mejorar la eficacia de las actividades de planificación como para la preparación general del organismo.

7. **Plan de mantenimiento.** El plan debe ser un documento vivo que se actualiza periódicamente para mantenerse al día con las mejoras en el sistema.

Se presenta un formato modelo para el desarrollo de un plan de contingencia de TI. El formato define tres fases que rigen las acciones que deben adoptarse después de una interrupción del sistema:

- **La notificación** o la fase de activación, que describe el proceso de recuperación y realización de una evaluación de daños.

- **La fase de recuperación** que describe una propuesta de medidas para la recuperación de equipos y personal para restablecer las operaciones de TI en un sitio alternativo o el uso de las capacidades de contingencia.

- **La fase final**, la reconstitución, se esbozan las medidas que pueden adoptarse para devolver el sistema a las condiciones normales de funcionamiento.

CAPÍTULO II – PLANIFICACIÓN DE CONTINGENCIA

1. PLANIFICACION DE CONTINGENCIA Y GESTIÓN DE RIESGOS

Las empresas actúan en ámbitos donde factores tales como la globalización, la tecnología, las normas, las reestructuras, los mercados cambiantes y la competencia crean incertidumbre. La misma proviene de la dificultad de determinar con precisión la probabilidad de ocurrencia de acontecimientos eventuales y sus consecuencias asociadas.

El riesgo es una medida de la incertidumbre, y en ese sentido se lo puede definir como el nivel de exposición a las incertidumbres que una organización debe entender y efectivamente administrar para lograr alcanzar sus objetivos y crear valor para sus interesados.

Toda entidad existe para proveer valor a sus grupos de interés. Para cumplir con su misión debe enfrentar la incertidumbre, tanto riesgos como oportunidades. El desafío para la gerencia es determinar cuanta incertidumbre la entidad está dispuesta a aceptar en su esfuerzo para aumentar el valor a sus grupos de interés.

La gerencia debe considerar riegos interrelacionados desde una perspectiva conjunta a nivel de la entidad. Es necesario identificar los riesgos interrelacionados y actuar sobre ellos a efectos de considerar el riesgo en su totalidad dentro del nivel de riesgo aceptado. El riesgo correspondiente a las unidades operativas de la organización puede estar dentro de las tolerancias de riesgo de la unidad, pero tomado en su conjunto puede exceder el nivel de riesgo aceptado. El nivel global de riesgo aceptado se refleja en una organización a través de las tolerancias al riesgo, establecidas para objetivos específicos.

El nivel de riesgo aceptado, es la cantidad de riesgo que una entidad está dispuesta a aceptar en su búsqueda de valor. Las organizaciones a menudo consideran el nivel de riesgo aceptado en forma cualitativa, con categorías tales como alta, moderada o baja, o pueden aplicar un enfoque cuantitativo reflejando y buscando un equilibrio entre las metas de crecimiento, rendimiento y riesgo.

El nivel de riesgo aceptado por una entidad, orienta la asignación de recursos. La gerencia debe asignar recursos entre las unidades de negocio, tomando en cuenta el nivel de riesgo aceptado y la estrategia de las unidades de negocio individuales, para generar el rendimiento deseado de los recursos asignados. Además debe considerar su nivel de riesgo aceptado, según el mismo sea compatible con su organización, su gente y sus procesos, destinando la infraestructura necesaria para responder y monitorear eficazmente los riesgos.

La gestión del riesgo abarca una amplia gama de actividades para identificar, controlar y mitigar los riesgos de un sistema de TI. Las actividades de gestión de riesgos desde el

punto de vista informático de planificación de contingencia tienen dos funciones principales.

En primer lugar, la gestión del riesgo debe identificar las amenazas y las vulnerabilidades a fin de que los controles adecuados se puedan poner en cualquier lugar, para evitar incidentes que ocurran o para limitar sus efectos. Estos controles de seguridad protegen al sistema de TI frente a tres categorías de amenazas:

- Naturales - por ejemplo, huracanes, tornados, inundaciones, y el fuego.

- Humanas - por ejemplo, errores del operador, sabotaje, implante de códigos maliciosos y ataques terroristas.

- Ambientales - por ejemplo, fallos de equipos, errores de software, corte de la red de telecomunicaciones, falta de energía eléctrica.

Véanse ejemplos en el Capítulo X - Anexos, en el apartado “2”.

En segundo lugar, la gestión de riesgos debe identificar los riesgos residuales. El plan de contingencia, está íntimamente vinculado a los resultados de la evaluación del riesgo y su proceso de mitigación.

La siguiente figura ilustra la relación entre la identificación y aplicación de controles de seguridad, desarrollo y mantenimiento del plan de contingencia, y la aplicación del mismo, una vez haya ocurrido el evento.

Figura 1.- Fuente: Contingency Planning Guide for Information Technology Systems.

Para determinar efectivamente los riesgos específicos de un sistema de TI durante la interrupción del servicio, una evaluación del riesgo del entorno de TI del sistema es necesaria. Una evaluación exhaustiva de los riesgos debe identificar las vulnerabilidades del sistema, la amenaza, y los controles actuales y tratar de determinar el riesgo sobre la

base de la probabilidad y el impacto de las amenazas. Estos riesgos, deben ser evaluados y un nivel de riesgo asignado (por ejemplo, alto, medio o bajo).

Debido a que los riesgos pueden variar con el tiempo y los nuevos riesgos pueden reemplazar a los viejos como un sistema que evoluciona, el proceso de gestión del riesgo debe ser continuo y dinámico. La persona responsable debe ser consciente de los riesgos para el sistema y reconocer si el plan de contingencia actual es capaz de abordar los riesgos residuales por completo y eficazmente.

2. TIPOS DE PLANES

La planificación de contingencia de TI representa una amplia gama de actividades destinadas a mantener y recuperar los servicios críticos después de una emergencia; ésta se ajusta en un entorno mucho más amplio de preparación para emergencias que incluye la organización, la continuidad de procesos de negocio y la planificación de la recuperación.

En última instancia, una organización debería utilizar un conjunto de planes para preparar adecuadamente la respuesta, recuperación y continuidad de los incidentes que afectan a las TI, procesos de negocio, y a las instalaciones.

Debido a que existe una relación intrínseca entre un sistema de TI y los procesos de negocio que apoya, debería haber una coordinación entre todos los planes durante el desarrollo y las actualizaciones, para garantizar que las estrategias de recuperación y apoyo a los recursos no se contradicen entre sí ni duplican esfuerzos.

En general, las definiciones universalmente aceptadas para la planificación de contingencia y la planificación de estas áreas correspondientes no han estado disponibles. En ocasiones, esta falta de disponibilidad ha dado lugar a confusión sobre el verdadero alcance y el propósito de los distintos tipos de planes. Para proporcionar una base común de entendimiento en relación con la planificación de contingencia de TI, se identifican otros tipos de planes y se describe su finalidad y ámbito de aplicación en relación con la planificación de contingencia.

Business Continuity Plan (BCP). El BCP se centra en el mantenimiento de las funciones comerciales de una empresa durante y después de una interrupción. Un ejemplo de una función de negocio puede ser el proceso de pagos de una organización o el proceso de atención al cliente. El BCP puede estar escrito para un proceso de negocio específico o puede resolver todos los procesos clave de negocio. Los sistemas de TI se consideran en el BCP en términos de su apoyo a los procesos de negocio. En algunos casos, el BCP no puede tratar la recuperación a largo plazo de los procesos y restablecer el funcionamiento normal, sólo cubre los requisitos de continuidad del negocio de corto plazo. El BCP puede incluir además un plan de recuperación de desastres, plan de reanudación de negocios, y el plan de emergencia de los ocupantes. El BCP debe coordinarse con el Plan de Continuidad de Operaciones (COOP) para eliminar los posibles conflictos, siempre siguiendo los lineamientos establecidos en la política de continuidad.

Business Recovery Plan (BRP). El BRP se refiere a la restauración de los procesos de negocio después de una emergencia, pero a diferencia del BCP, carece de procedimientos para garantizar la continuidad de los procesos críticos a lo largo de una emergencia o interrupción. El BRP también puede incluir el BCP.

Continuity of Operations Plan (COOP). El COOP se centra en la restauración de las funciones esenciales en un sitio alternativo (de hasta 30 días antes de regresar a sus operaciones normales). Debido a que el COOP hace hincapié en la recuperación de la capacidad operativa de una organización en un sitio alternativo, el plan no incluye necesariamente las operaciones de TI, ni las interrupciones de menor importancia, pues no requieren traslado a un sitio alternativo. Sin embargo, COOP podrá incluir el BCP, BRP, y el plan de recuperación de desastres como apéndices.

Crisis Communications Plan (CCP). Las organizaciones deben preparar sus procedimientos de comunicaciones internas y externas antes de un desastre. Un plan de comunicación de crisis es a menudo desarrollado por la unidad responsable de la divulgación pública. Los procedimientos de comunicación del plan deberían coordinarse con todos los otros planes para garantizar que sólo las declaraciones aprobadas son liberadas al público.

Los procedimientos del plan deberían ser incluidos como un apéndice del BCP. Plantillas para los comunicados de prensa forman parte del documento.

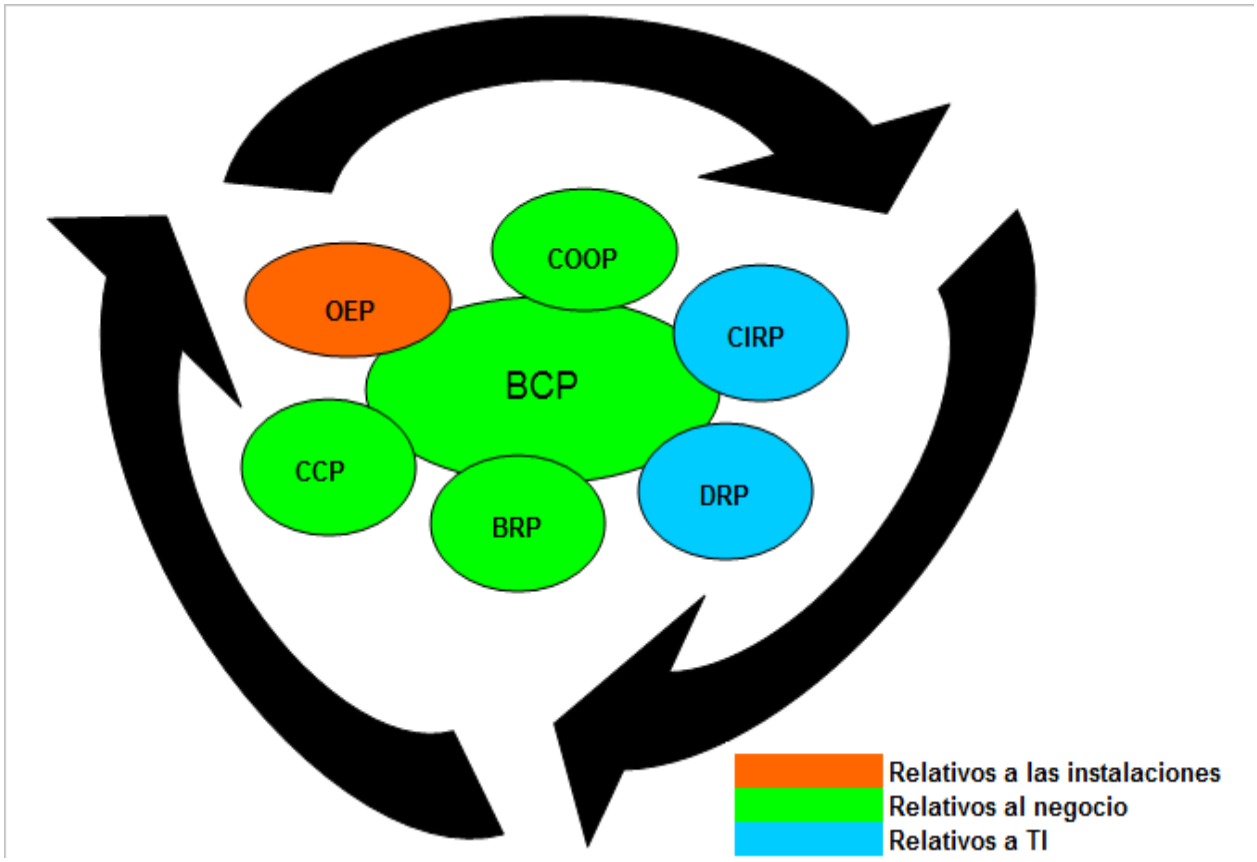
Cyber Incident Response Plan (CIRP). Establece los procedimientos para hacer frente a los ataques cibernéticos contra el sistema de TI de una organización. Estos procedimientos están diseñados para permitir que el personal de seguridad pueda identificar, mitigar y recuperarse de incidentes informáticos maliciosos, como el acceso no autorizado. Establece individuos específicos como única autoridad para responder a las preguntas del público en relación con los desastres de TI. También pueden incluir procedimientos para la autorización de acceso a un sistema o base de datos; la denegación de servicios, o de cambios no autorizados al sistema de hardware, software o datos (lógica maliciosa, como un virus, gusano o caballo de Troya). Este plan puede ser incluido entre los apéndices del BCP.

Disaster Recovery Plan (DRP). Como sugiere su nombre, el DRP se aplica a los grandes desastres, por lo general hechos catastróficos que niegan el acceso a la instalación normal por un período prolongado. Con frecuencia, se refiere a un DRP de TI centrada en el plan destinado a restablecer la operatividad del sistema de destino, aplicación o instalación de equipo en un sitio alternativo después de una emergencia. El ámbito de aplicación de DRP puede superponerse a la del plan de contingencia de TI, sin embargo, el DRP es más limitado en su alcance y no responde a las interrupciones de menor importancia que no requieren de reubicación. Dependiendo de las necesidades de la organización, el DRP también puede incluir el BCP.

Occupant Emergency Plan (OEP). El OEP prevé los procedimientos de respuesta para los ocupantes de una instalación en caso de una situación que suponga una amenaza potencial para la salud y la seguridad del personal, el medio ambiente o propiedad. Dichos sucesos incluyen un incendio, un huracán, una inundación, un ataque criminal, o una emergencia médica. El OEP se desarrolla en el nivel de instalación, considerando las características de la ubicación geográfica y el diseño estructural del edificio

La siguiente figura pretende esquematizar la interrelación que hay entre todos los planes, con las actividades de protección, mantenimiento y recuperación.

Figura 2.- Fuente: Contingency Planning Guide for Information Technology Systems.



3. PLAN DE CONTINGENCIA Y DESARROLLO DEL CICLO DE VIDA DEL SISTEMA

El desarrollo del ciclo de vida del sistema se refiere a todo el ámbito de las actividades realizadas por los propietarios del mismo que están asociadas durante su vida útil.

Aunque la planificación de contingencia se asocia con actividades que ocurren en la operación o fase de mantenimiento, medidas de emergencia deben ser identificadas e integradas en todas las fases del ciclo de vida del sistema.

Este enfoque reduce los costos generales de planificación de contingencia, mejora las capacidades de contingencia, y reduce los impactos de las operaciones del sistema cuando se aplique el plan de contingencia.

Fase de iniciación. Los requisitos de planificación de contingencia deben ser considerados cuando un nuevo sistema se concibe. En la fase de iniciación, los requisitos

del sistema son identificados, así como los procesos relacionados con el funcionamiento y requisitos de contingencia inicial.

Requisitos del sistema de muy alta disponibilidad pueden indicar la necesidad de contar con un sistema espejado en tiempo real, en un sitio alternativo. Del mismo modo, si el sistema está concebido para funcionar en condiciones inusuales, como en una aplicación móvil o un lugar inaccesible, el diseño puede necesitar incluir características adicionales, tales como capacidades de cura de diagnóstico a distancia o por cuenta propia.

Durante esta fase, el nuevo sistema también debe ser evaluado respecto de todos los demás existentes y previstos, para determinar su prioridad. Esta prioridad se utilizará para el desarrollo de la secuencia para la recuperación de múltiples sistemas de TI.

Fase de desarrollo y adquisición. A medida que evolucionan los conceptos iniciales en diseños de sistemas, soluciones de contingencia específicas pueden ser incorporadas. Al igual que en la fase inicial, las medidas de contingencia se incluyen en esta etapa del ciclo de vida y deben reflejar las necesidades operacionales. El diseño debe considerar la arquitectura de sistema de modo de optimizar la fiabilidad, mantenimiento y disponibilidad, durante la fase operativa. De esta manera, se reducen los costos y los problemas asociados con la adaptación o la modificación del sistema durante la fase operativa o de mantenimiento. Si varias aplicaciones son alojadas dentro del nuevo sistema de apoyo general, las prioridades individuales de las aplicaciones deben ser establecidas para ayudar con la selección de las medidas de contingencia adecuadas y la secuencia de la ejecución de recuperación. Si un sitio alternativo es elegido como una medida de contingencia, los requisitos para el sitio alternativo deben ser abordados en esta fase.

Fase de ejecución. Aunque el sistema está siendo sometido a pruebas iniciales, las estrategias de contingencia también deben ser probadas para asegurar que las características técnicas y los procedimientos de recuperación son precisos y eficaces. Para probar las estrategias de contingencia, será necesario desarrollar un plan de prueba. Cuando estas medidas de contingencia hayan sido verificadas, debe estar claramente documentado en el plan de contingencia.

Fase operativa o de mantenimiento. Cuando el sistema está operativo, los administradores y directivos deben mantener un programa de capacitación y sensibilización a los procedimientos de un plan de contingencia, dirigido a los usuarios. Los ejercicios y pruebas deben llevarse a cabo para garantizar que los procedimientos siguen siendo eficaces. Respaldos (backups) periódicos deben llevarse a cabo y almacenarse fuera del sitio. El plan debe ser actualizado para reflejar los cambios en los procedimientos basados en las lecciones aprendidas. Cuando el sistema de TI experimente actualizaciones o cualesquiera otras modificaciones, como cambios en las interfaces externas, estas modificaciones deben reflejarse en el plan de contingencia. Coordinación y documentación de los cambios en el plan deben realizarse en forma oportuna para mantener un plan eficaz.

Fase de eliminación. Consideraciones de contingencia no deben descuidarse, porque un sistema informático es jubilado y otro sistema lo reemplaza. Hasta que el nuevo sistema esté en funcionamiento y probado completamente (incluyendo sus capacidades de contingencia), el plan de contingencia del sistema original debe estar listo para su aplicación. Como se sustituirán los sistemas de legado, que pueden proporcionar una

capacidad de reserva de valor, si la pérdida o el fracaso del nuevo sistema ocurren. En algunos casos, las piezas del equipo (por ejemplo, discos duros, fuentes de alimentación, chips de memoria, o tarjetas de red) que ha sido sustituido por nuevos sistemas, pueden ser utilizadas como repuesto para equipos nuevos, en funcionamiento. Además, los sistemas heredados pueden ser utilizados como sistemas de pruebas para nuevas aplicaciones, permitiendo que los defectos del sistema potencialmente perjudiciales puedan ser identificados y corregidos en los sistemas fuera de operación.

CAPÍTULO III - PROCESO DE PLANIFICACIÓN DE CONTINGENCIA DE TI

El proceso que se presenta aquí es común a todos los sistemas de TI. Consta de siete pasos:

1. Desarrollar la declaración de política de planificación de contingencia.

2. Realizar el análisis de impacto en el negocio (BIA).

3. Identificar los controles preventivos.

4. Desarrollar estrategias de recuperación de TI.

5. Desarrollar un plan de contingencia de TI.

6. Testeo del plan, entrenamiento y ejercicios.

7. Plan de mantenimiento.

Estos pasos constituyen elementos clave para una amplia capacidad de planificación de contingencia.

La responsabilidad por el proceso de planificación general, cae bajo el auspicio del "Coordinador de Planificación de Contingencia " o "Planificador de Contingencia", que normalmente es un funcionario o administrador de recursos dentro de la organización. La coordinación de la estrategia se desarrolla en cooperación con otros empleados y administradores de recursos asociados con el sistema o los procesos de negocios apoyados por el mismo. El Coordinador de Planificación de Contingencia también administra el desarrollo y ejecución del plan de contingencia. Todas las principales aplicaciones y sistemas de apoyo en general deben tener un plan de contingencia.

1. DECLARACIÓN DE POLÍTICA DE PLANIFICACIÓN DE CONTINGENCIA

Para ser eficaz y para garantizar que el personal comprende plenamente las necesidades de planificación de la organización, el plan de contingencia debe basarse en una política claramente definida. La declaración de política de planificación de contingencia debe definir los objetivos de contingencia generales de la entidad y establecer el marco de organización y las responsabilidades de TI en la planificación de contingencia. Para tener éxito, la alta dirección debe apoyar un programa de contingencia. Los funcionarios deben ser incluidos en el proceso para desarrollar la política del programa, estructura, objetivos, roles y responsabilidades.

Las empresas deben evaluar sus respectivos sistemas de TI, operaciones y requerimientos para determinar que requisitos de planificación de contingencia son necesarios.

Elementos clave de políticas son los siguientes:

- Funciones y responsabilidades.

- Ámbito de aplicación, tipo de plataforma y funciones de la organización objeto de la planificación de contingencias.

- Recursos necesarios.

- Requisitos de formación.

- Ejercicios y horarios de las pruebas.

- Programa de mantenimiento del plan.

- La frecuencia de respaldos y almacenamiento de los medios de copia de seguridad.

A medida que se desarrollan la política de TI y un programa de contingencia, estos deben ser coordinados con las actividades relacionadas con la organización, incluyendo la seguridad de TI, la seguridad física, recursos humanos, operaciones y funciones de preparación para emergencias. Las actividades de contingencia para TI deberían ser compatibles con los requisitos del programa para estas áreas, y el personal de emergencia debe coordinarse con los representantes de cada área.

Los planes de contingencia deben ser escritos en coordinación con otros planes relacionados con los sistemas existentes.

2. EJECUCIÓN DEL BUSINESS IMPACT ANALISYS (BIA)

El BIA es un paso clave en el proceso de planificación de contingencia. El BIA permite al Coordinador de Planificación de Contingencia, reconocer plenamente los requisitos del sistema, los procesos, y las interdependencias, así como información vital para determinar las necesidades de emergencia y las prioridades. El objetivo del BIA es correlacionar los componentes específicos del sistema con los servicios esenciales que prestan, y con base en esa información, identificar las consecuencias de una interrupción de los componentes del sistema. Los resultados del BIA deben ser convenientemente incorporados en el análisis y los esfuerzos de desarrollo de la estrategia para el COOP, el BCP y el BRP de la organización.

2.1. Identificación de Recursos Críticos

Los sistemas de TI pueden ser muy complejos, con numerosos componentes, interfaces y procesos. Éste primer paso del BIA evalúa el sistema de TI para determinar las funciones críticas realizadas por el sistema y para identificar los recursos de sistema específicos necesarios para realizarlas.

Dos actividades por lo general son necesarias para completar este paso:

1. El Coordinador de Planificación de Contingencias debe identificar y clasificar los puntos internos y externos de contacto asociados con el sistema para determinar de que manera dependen de, o dan apoyo al sistema informático. Respecto a la identificación de contactos, es importante incluir a las organizaciones que proporcionan o reciben datos del sistema, así como a los diferentes sistemas que interactúan entre sí. Esta coordinación debe permitir que el administrador del sistema, especifique la gama completa de apoyo proporcionado por el sistema, incluida la seguridad, los requisitos de gestión, elementos técnicos y operativos.

2. El Coordinador de Planificación de Contingencia debe evaluar el sistema para vincular estos servicios críticos con los recursos del sistema. Este análisis suele identificar las necesidades de infraestructura, tales como energía eléctrica, conexiones de telecomunicaciones, y los controles ambientales. Equipos informáticos específicos, tales como routers, servidores de aplicaciones, y servidores de autenticación, generalmente son considerados críticos. También, el análisis puede determinar que ciertos componentes de TI, como una impresora o un servidor de impresión, no son necesarios para apoyar los servicios críticos.

2.2. Identificar el impacto de las interrupciones y el tiempo admitido

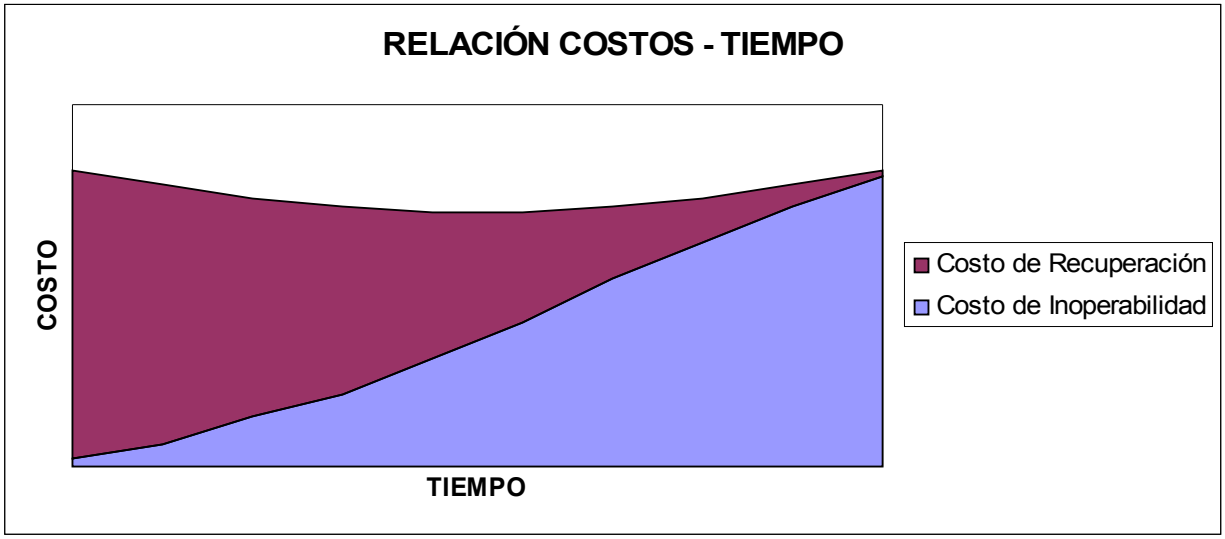
En este paso, el Coordinador de Planificación de Contingencias debe analizar los recursos críticos identificados en el paso anterior y determinar el impacto en las operaciones de TI, si un recurso determinado fuera interrumpido o deteriorado. El análisis debe evaluar el impacto de la interrupción de dos maneras.

1. Los efectos de la interrupción pueden ser rastreados a través del tiempo. Esto permitirá que el Coordinador de Planificación de Contingencia pueda determinar el tiempo máximo que un recurso puede ser negado antes de que inhiba el desempeño de una función esencial.

2. Los efectos de las caídas pueden ser rastreadas a través de los recursos relacionados y los sistemas dependientes, identificando todos los efectos en cascada que se pueden presentar (como un sistema alterado afecta a otros procesos que dependen de él).

El Coordinador de Planificación de contingencia debe determinar el punto óptimo para recuperar el sistema de TI, equilibrando el costo de la inoperancia del sistema contra el costo de los recursos necesarios para restaurar el sistema.

Figura 3.- Fuente: Contingency Planning Guide for Information Technology Systems.



2.3. Desarrollar prioridades de recuperación

El impacto de fallas y los tiempos de interrupción permisibles señalados en el paso anterior, son utilizados por el Coordinador de Planificación de Contingencia para desarrollar y dar prioridad a las estrategias de recuperación que el personal llevará a cabo durante el plan de contingencia.

Por ejemplo, si el paso de evaluación de los impactos determina que el sistema debe ser recuperado dentro de 4 horas, el Coordinador de Planificación de Contingencia tendría que adoptar medidas para cumplir ese requisito. Del mismo modo, si la mayoría de los componentes del sistema podrían soportar un corte de 24 horas, salvo un componente crítico que tendría que estar disponible a solo 8 horas, el Coordinador de Planificación de Contingencia dará prioridad a los recursos necesarios para el componente crítico. Al dar prioridad a estas estrategias de recuperación, el Coordinador de Planificación de contingencia, toma decisiones sobre la asignación de recursos a medidas de contingencia, ahorrando tiempo, esfuerzo y costos.

3. IDENTIFICAR CONTROLES PREVENTIVOS

Como indicamos anteriormente, el BIA puede proporcionar al Coordinador de Planificación de Contingencia información trascendente sobre la disponibilidad del sistema y los requisitos de recuperación. En algunos casos, las repercusiones identificadas en el BIA pueden ser mitigadas o eliminadas a través de medidas preventivas para retraer, detectar, y/o reducir los impactos en el sistema. Cuando sea viable y rentable, los métodos de prevención son preferibles a las acciones que sean necesarias para recuperar el sistema después de una interrupción.

Una gran variedad de controles preventivos están disponibles, dependiendo del tipo y configuración del sistema, sin embargo, algunas medidas comunes son enumeradas a continuación:

- UPS (Unidad de Alimentación Eléctrica Permanente) de tamaño adecuado para proporcionar energía de reserva a corto plazo a todos los componentes del sistema.

- Generadores diesel o a gasolina para proveer energía a largo plazo.

- Sistemas de aire acondicionado con exceso de capacidad.

- Sistemas de extinción de incendios.

- Detectores de humo e incendio.

- Sensores de agua en el techo y piso de la sala de informática.

- Lonas de plástico que pueden ser desenrolladas sobre los equipos de TI para protegerlos de los daños ocasionados por el agua.

- Recipientes resistentes al calor e impermeables para los medios de respaldo y de otros registros vitales no electrónicos.

- Sistema de apagado de emergencia.

- Almacenamiento externo de los medios de respaldo, los registros no electrónicos, y documentación del sistema.

- Controles de seguridad de carácter técnico, como la gestión de claves criptográficas y controles de acceso.

- Frecuentes respaldos programados.

Los controles preventivos deben estar documentados en el plan de contingencia, y el personal asociado con el sistema debe estar capacitado en cómo y cuándo usar los controles. Estos controles deben mantenerse en buen estado para garantizar su eficacia en una emergencia.

4. DESARROLLAR ESTRATEGIAS DE RECUPERACIÓN

Las estrategias de recuperación deben proporcionar un medio para restaurar las operaciones de TI con rapidez y eficacia tras una interrupción del servicio. Las estrategias deben abordar los impactos y los tiempos de interrupción permisibles identificados en el BIA. Varias alternativas se deben considerar en el desarrollo de la estrategia, incluido el costo, el tiempo de interrupción permisible y la seguridad.

La estrategia de recuperación seleccionada debe abordar los impactos potenciales identificados en el BIA y debe integrarse en la arquitectura del sistema durante el diseño y ejecución de las fases del ciclo de vida del sistema. La estrategia debe incluir una combinación de métodos que se complementan entre sí para proporcionar capacidad de recuperación ante todo el espectro completo de los incidentes.

4.1. Métodos de respaldo

Los datos del sistema deberían ser respaldados regularmente. Las políticas deben especificar la frecuencia de las copias de seguridad (por ejemplo, diaria o semanal, incremental o completa), sobre la base de datos de la criticidad y la frecuencia con que se introduce nueva información. Las políticas de respaldo de datos deben designar la ubicación de los datos almacenados, los códigos para nomenclatura de archivos y el método para el transporte de datos fuera del sitio. Los datos pueden ser respaldados en disco magnético, cinta o discos ópticos (como los CDs). El método específico elegido para la realización de respaldos debe basarse en el sistema y la disponibilidad de datos y los requisitos de integridad. Estos métodos incluyen la bóveda electrónica y réplicas de los discos.

Los métodos de respaldo, anualmente, deben ser testeados, es decir deben tomarse los respaldos y verificar que funcionen (ver ejemplo “J” del apartado “2” del capítulo X – Anexos).

Si se utiliza el almacenamiento fuera del sitio, los datos son copiados en las instalaciones de la organización, etiquetados, embalados y transportados a la instalación de almacenamiento. Si los datos son necesarios para la recuperación o realización de pruebas, serán transportados a la empresa. Los proveedores de estas prestaciones, a menudo ofrecen los medios de transporte y servicios de respuesta y recuperación.

Al seleccionar una instalación de almacenamiento externo y los proveedores, los siguientes criterios deben ser considerados; entre otros, distancia a la organización, accesibilidad, seguridad y confidencialidad, así como condiciones ambientales (temperatura, humedad, etc. de la instalación de almacenamiento). Otros factores no menores a considerar son el costo de envío, gastos de funcionamiento, respuesta a desastres y servicios de recuperación.

4.2. Sitios alternativos

A pesar de que las interrupciones importantes con efectos a largo plazo pueden ser poco frecuentes, deben tenerse en cuenta en el plan de contingencia. Así, el plan debe incluir una estrategia para recuperar y llevar a cabo las operaciones en una instalación alternativa durante un período prolongado. En general, tres tipos de sitios alternativos están disponibles:

- Pertenecientes o gestionados por la organización.
- De acuerdo con una entidad interna o externa.
- Alquilados.

Independientemente del tipo de sitio alternativo elegido, la instalación debe ser capaz de soportar las operaciones tal como se define en el plan de contingencia. Los tres tipos de sitios alternativos se pueden clasificar como sitios de frío, sitios cálidos, sitios calientes, sitios móviles, y sitios espejados. Se describen a continuación:

- **De frío.** Consisten normalmente en una instalación con suficiente espacio e infraestructura para soportar el sistema de TI. El sitio no contiene equipos de TI y en general no contiene equipo de oficina, tales como teléfonos, máquinas de fax, o fotocopiadoras. La organización que utilice el sitio frío es responsable de proveer e instalar los equipos necesarios y las capacidades de las telecomunicaciones.

- **Sitios cálidos.** Son parcialmente equipados, contienen todo o parte del hardware, software, telecomunicaciones, y fuentes de energía. El sitio cálido se mantiene en un estado de funcionamiento listo para recibir el sistema reubicado.

- **Sitios calientes**. Son espacios de oficina de tamaño adecuado para apoyar a los requisitos del sistema y se configuran con el hardware necesario, la infraestructura y personal de apoyo. Los sitios calientes suelen trabajar 24 horas al día, 7 días a la semana. El personal comienza a prepararse tan pronto como sean notificados de que el plan de emergencia ha sido activado.

- **Sitios móviles** son autónomos, con equipamiento de telecomunicaciones específicos y los equipos necesarios para cumplir con los requisitos del sistema. Estos están

disponibles para el alquiler a través de vendedores comerciales. Las instalaciones a menudo se encuentran en un tractor-remolque y pueden ser impulsados y puestos en marcha en la ubicación alternativa deseada. Los sitios móviles deben estar diseñados de antemano por el vendedor, y un contrato debe ser firmado entre las dos partes. Esto es se debe a que el tiempo necesario para configurar el sitio móvil puede ser amplio y sin coordinación previa, el plazo para presentar el sitio móvil puede exceder el tiempo de interrupción.

- **Sitios espejados**. Son completos, con las instalaciones listas. Son idénticos al sitio principal en todos los aspectos técnicos. Estos sitios ofrecen el más alto grado de disponibilidad, porque los datos son procesados y almacenados en el sitio principal y suplente. Estos sitios suelen ser diseñados, construidos, operados y mantenidos por la organización.

Hay costos obvios y diferencias de tiempo entre las cinco opciones. El sitio espejo es la opción más cara, pero se asegura una disponibilidad de casi el cien por ciento. Los sitios fríos son los menos costosos de mantener, sin embargo, puede requerir un tiempo considerable para adquirir e instalar el equipo necesario. Sitios parcialmente equipados, como los sitios cálidos, están en el medio del espectro. En muchos casos, los sitios móviles pueden ser entregados a la ubicación deseada dentro de las 24 horas. Sin embargo, el tiempo necesario para la instalación puede incrementar el tiempo de respuesta. La selección de ubicaciones fijas deberían representar el tiempo y el modo de transporte necesarios para trasladar al personal. Además, el sitio debe ser fijado en una zona geográfica que es poco probable que sea negativamente afectada por la misma catástrofe que el sitio principal de la organización (por ejemplo, los impactos relacionados con el clima o el fracaso de red eléctrica).

Los sitios deben ser analizados por la organización basada en los requisitos específicos definidos en el BIA.

Estos sitios alternativos pueden ser poseídos y operados por la organización, o sitios comerciales pueden estar disponibles bajo contrato. Para la contratación del sitio con un proveedor comercial, el tiempo de prueba suficiente, área de trabajo, requisitos de seguridad, requisitos de hardware, requisitos de las telecomunicaciones, servicios de apoyo, y días de recuperación (el tiempo que la organización puede ocupar el espacio durante el período de recuperación) deben ser negociados y claramente estipulados en el contrato.

Los clientes deben ser conscientes de que múltiples organizaciones podrán contratar con un proveedor alternativo para el mismo sitio, y como resultado, el sitio puede ser capaz de acomodar a todos los clientes, si un desastre afecta el suficiente número de clientes de forma simultánea. La política del vendedor sobre cómo esta situación se debe abordar y cómo se determina la prioridad debe ser negociada.

4.3. Reemplazo de Equipos

Si el sistema de TI está dañado o destruido, o el sitio primario no está disponible, hardware y software necesarios tendrán que ser activados o adquiridos de manera rápida y entregados a la ubicación alternativa. Existen tres estrategias básicas para prepararse para el reemplazo de equipos. Al seleccionar la estrategia más adecuada, hay que tener en cuenta que la disponibilidad de transporte puede ser limitada o detenida temporalmente en el caso de un desastre catastrófico.

Acuerdos con proveedores.

El contrato debe especificar la rapidez con que el proveedor debe responder después de haber sido notificado. El acuerdo también debería dar prioridad a la organización para el envío de equipos de sustitución del adquirido para las operaciones normales. El acuerdo debe discutir cuál es el estatus de prioridad que la organización recibirá en el caso de un desastre catastrófico que involucre múltiples clientes del mismo proveedor. Los detalles de estas negociaciones deben ser documentados en el contrato, que debe mantenerse con el plan de contingencia.

Inventario de equipamiento.

Medios materiales necesarios se pueden comprar por adelantado y almacenarse en una ubicación segura fuera de sitio, como un lugar alternativo, donde las operaciones de recuperación se llevarán a cabo, o en otro lugar donde serán almacenados y enviados al sitio alternativo. Esta solución tiene algunos inconvenientes. Una organización debe comprometer recursos financieros para adquirir este equipo con antelación, el equipo podría llegar a ser obsoleto o inadecuado para su uso con el tiempo, dadas las tecnologías de sistema y los requisitos de cambio.

Equipamiento compatible existente.

Al evaluar las opciones, el Coordinador de Planificación de Contingencia debe considerar que la compra de equipos cuando sea necesario es rentable, pero puede añadir un tiempo importante a la recuperación mientras se está en espera del traslado y la instalación; a la inversa, equipos de almacenamiento no utilizados es costoso, pero permite que las operaciones de recuperación comiencen más rápidamente. Independientemente de la estrategia seleccionada, listas detalladas de las necesidades de equipo y especificaciones deberían mantenerse dentro del plan de contingencia.

4.4. Roles y responsabilidades

Después de seleccionar y aplicar la estrategia de recuperación del sistema, el Coordinador de Planificación de Contingencias debe designar los equipos adecuados para aplicar la estrategia. Cada equipo debe estar capacitado y listo para la implementación de medidas en el caso de una situación perturbadora que requiera la activación del plan. El personal de recuperación debe ser asignado a uno de los varios equipos específicos, que responderá a la situación, y procederá a recuperar las capacidades, y devolver el sistema a las operaciones normales. Para ello, tendrán que comprender claramente la meta del

equipo en el esfuerzo de recuperación, cada paso que van a ejecutar, y cómo su equipo se refiere a otros equipos.

Los tipos específicos de equipos requeridos se basan en el sistema afectado. El tamaño de cada equipo, los títulos específicos de cada equipo, y los diseños dependen de la jerarquía de la organización. Además de un papel de autoridad única, una estrategia capaz requerirá algunos o todos de los siguientes grupos funcionales:

- Alto cargo directivo.
- Equipo de Gestión.
- Equipo de Evaluación de Daños.
- Equipo de Administración de Sistema Operativo.
- Equipo de Sistemas de Software.
- Equipo de recuperación de servidores (por ejemplo, servidor de cliente, servidor web).
- Equipo de recuperación LAN / WAN.
- Recuperación de base de datos.
- Equipo de recuperación de operaciones de red.
- Recuperación de aplicaciones.
- Equipo de telecomunicaciones.
- Equipo que coordine la recuperación en un lugar alternativo.
- Equipo de restauración.
- Equipo de pruebas.
- Equipo de Apoyo Administrativo.
- De transporte y mudanza.
- De asuntos jurídicos.

El personal que integrará esos equipos debe ser elegido en base a sus habilidades y conocimientos. Idealmente, los equipos estarían formados por personal que realice las

mismas o similares actividades en condiciones normales del negocio. Por ejemplo, el equipo de recuperación de los servidores debe incluir a los administradores del servidor. Los miembros del equipo deben comprender no sólo el propósito del plan de contingencia, sino también los procedimientos necesarios para la ejecución de la estrategia de recuperación. Los equipos deben estar preparados para que algún miembro no esté disponible o para que se designe un integrante alternativo. Del mismo modo, los miembros del equipo deben estar familiarizados con los objetivos y procedimientos de otros equipos para facilitar la coordinación "InterEquipos". El Coordinador de Planificación de Contingencias debe también considerar que un desastre puede ocurrir que haría que la mayoría o todo el personal no esté disponible para responder. En esta situación, la ejecución del plan sólo puede ser posible mediante el uso de personal contratado, o perteneciente a otra área geográfica de la organización. Dicho personal puede ser coordinado y entrenado como un equipo alternativo.

Cada equipo tiene un líder que dirige las operaciones del equipo en general y actúa como representante en la gestión y el enlace con otros líderes. El líder difunde información a los miembros del equipo y aprueba todas las decisiones que se deben tomar dentro del equipo. Los jefes de equipo deben tener un suplente designado para actuar como el líder si el principal no está disponible.

Para la mayoría de los sistemas, un equipo de gestión es necesario para proporcionar orientación general a raíz de una interrupción del sistema principal o de emergencia. El equipo es responsable de activar el plan de contingencia y supervisa la ejecución de las operaciones de contingencia. El Equipo de Gestión también facilita las comunicaciones entre los otros equipos de TI y supervisa las pruebas del plan de contingencia y ejercicios. Todos o algunos del equipo de gestión pueden integrar equipos de emergencia especializados. Un alto funcionario, tiene la autoridad final para activar el plan, y para tomar decisiones sobre los niveles de gasto, el riesgo aceptable, y la coordinación interinstitucional. Por lo general es quien lidera el equipo de gestión.

Una línea de planificación de sucesión puede ser incluida en el plan de contingencia. El orden de sucesión define quién asume la responsabilidad de la ejecución de los planes de contingencia en caso de que la máxima autoridad no está disponible o es incapaz de hacerlo.

4.5. Consideraciones de costo

El Coordinador de Planificación de Contingencias debe garantizar que la estrategia elegida se puede implementar de manera efectiva, con una adecuada disponibilidad de personal y recursos financieros. El costo de cada tipo de sitio alternativo, la sustitución de equipos, y la opción de almacenamiento en cuestión, deben "sopesarse" frente a las limitaciones presupuestarias (si fuese posible, los costos y beneficios de los métodos de recuperación deberían ser evaluados durante el desarrollo del sistema). El coordinador debe determinar los gastos conocidos del plan de contingencia, tales como gastos de contrato del sitio alternativo, y aquellos que son menos obvios, como ser el costo de la aplicación de un programa de alerta organizacional de emergencia. El presupuesto debe ser suficiente para

abarcar software, hardware, los viajes y el transporte, pruebas, programas de capacitación, programas de sensibilización, las horas de trabajo, otros servicios contratados, y cualquier otro recurso aplicable (por ejemplo, escritorios, teléfonos, máquinas de fax, bolígrafos y papel). La organización debe realizar un análisis costo-beneficio para determinar la estrategia de recuperación óptima.

Las tecnologías cambian rápidamente, como así también sus costos; esto determina que deba reverse periódicamente la relación costo-beneficio del desarrollo y alcance de los planes. Dicho proceso forma parte de la etapa de mantenimiento.

El siguiente cuadro proporciona un modelo para la evaluación de las consideraciones de costo.

Figura 4.- Fuente: Contingency Planning Guide for Information Technology Systems.

	Costos de:	Proveedores	Hardware	Software	Viajes/Transporte	Horas	Serv. Contratados	Pruebas	Suministros
Sitio Alternativo	Sitio Frío								
	Sitio Cálido								
	Sitio Caliente								
	Sitio Móvil								
	Sitio Espejado								
Almacenamiento fuera del sitio	Comercial								
	Interior								
Reemplazo del equipamiento	Almacenamiento								
	De uso actual								

5. PRUEBAS, CAPACITACIÓN Y EJERCICIOS DEL PLAN

El testeo del plan es un elemento crítico para la viabilidad de la capacidad de contingencia. A su vez permite que las deficiencias puedan ser identificadas y abordadas. Las pruebas también ayudan a evaluar la capacidad del personal de recuperación para aplicar el plan con rapidez y eficacia. Cada elemento del plan de contingencia debe ser analizado para comprobar la exactitud de los procedimientos individuales de recuperación y la eficacia global del plan. Las siguientes áreas deben tratarse en una prueba de contingencia:

- Recuperación del sistema en una plataforma alternativa a partir de los respaldos.

- Coordinación entre los equipos de recuperación.
- La "conectividad" interna y externa.
- El rendimiento del sistema mediante el uso de un equipo alternativo.
- Restauración de las operaciones normales.
- Procedimientos de notificación.

Para obtener el máximo valor de la prueba, el Coordinador de Planificación de Contingencia debe desarrollar un plan de pruebas diseñadas para probar el/los elemento(s) seleccionado(s) frente a los objetivos explícitos de prueba y criterios de éxito. El uso de objetivos de prueba y criterios de éxito permite evaluar la eficacia de cada elemento del plan y del plan en general. El plan de pruebas debe incluir un calendario que detalla los plazos para cada prueba y los participantes en la prueba. El plan de prueba también debe delimitar claramente el alcance, el escenario, y la logística. El escenario elegido puede ir desde el peor incidente hasta un caso de mayor probabilidad de ocurrencia. Se debe imitar la realidad lo más fielmente posible. Existen dos formatos básicos para los ejercicios:

1) **"Ejercicios de aula"**. Son llamados a menudo "de mesa", sin que ningún tipo de procedimientos de recuperación real ocurra. Los ejercicios en clase son los más básicos y menos costosos de los dos tipos de ejercicios y deben llevarse a cabo antes de realizar un ejercicio funcional.

2) **"Ejercicios funcionales"**. Son más amplios que los de "mesa", lo que requiere que el evento sea falsificado. Los ejercicios funcionales incluyen simulaciones y "juegos de guerra". A menudo, los guiones se escriben para los jugadores de rol simulando ser contactos de la organización externa, o puede ser más real, con participación interorganizacional y de proveedores. Un ejercicio funcional podría incluir la reubicación en sitios alternativos y/o corte y cambio de sistema.

El anunciar la prueba de antemano es beneficioso para los miembros del equipo, ya que pueden prepararse mentalmente y tener tiempo para dar prioridad a su carga de trabajo. Es probable que algunos miembros del equipo no estén disponibles debido a la ausencia o porque la prueba puede ser perjudicial para su carga de trabajo. Los problemas de disponibilidad de personal son útiles para evaluar como puede resultar el plan en una situación de éste tipo, aportando así una crítica a las modificaciones del plan. Es importante que un ejercicio no interrumpa las operaciones normales. Los resultados de las pruebas y las "lecciones" aprendidas deben ser documentados y revisados por los participantes en la prueba y demás personal, según corresponda. La información recopilada durante y luego de la prueba, que pueda mejorar la eficacia del plan, debe ser incorporada a éste.

Capacitación para el personal con responsabilidades en el plan de emergencia debe realizarse para complementar las pruebas. La formación debería ser proporcionada al menos anualmente, las nuevas contrataciones que tendrán responsabilidades en el plan deberían recibir una formación poco después de ser contratados. En última instancia, el personal abocado al plan de contingencia debe estar entrenado en la medida que sea capaz de ejecutar sus respectivos procedimientos de recuperación, sin la ayuda de documento alguno. Esta es una meta importante en el caso de que el papel o las versiones electrónicas del plan no están disponibles al principio como consecuencia del desastre. El personal de recuperación debe estar capacitado en los siguientes puntos:

- Propósito del plan.
- La coordinación del equipo y la comunicación.
- Los procedimientos de presentación de informes.
- Los requisitos de seguridad.
- Equipo de procesos específicos (notificación/activación, recuperación y fases de reconstitución).
- Responsabilidades individuales (notificación/activación, recuperación y fases de reconstitución).

6. PLAN DE MANTENIMIENTO

Para ser eficaz, el plan debe mantenerse de manera que pueda reflejar con precisión los requisitos del sistema, los procedimientos, estructura organizativa y las políticas. Los sistemas sufren cambios frecuentes debido al cambio de necesidades de la empresa, actualizaciones tecnológicas o de nuevas políticas internas o externas. Por lo tanto, es esencial que el plan de contingencia sea revisado y actualizado regularmente como parte del proceso de gestión de la organización, para asegurarse que la información nueva se documenta y se revisan las medidas de contingencia en caso necesario. Como regla general, el plan debe ser revisado con exactitud e integridad por lo menos anualmente o cada vez que se produzcan cambios significativos a cualquier elemento del plan. Ciertos elementos pueden requerir revisiones más frecuentes, como ser, listas de contactos. Basado en el tipo de sistema y de la criticidad, puede ser razonable que se evalúe el plan de contenidos y procedimientos con más frecuencia. Como mínimo, los elementos a relevarse deben ser los siguientes:

- Requisitos de funcionamiento.
- Requisitos de seguridad.

- Procedimientos técnicos.
- Hardware, software y demás equipamiento (tipos, especificaciones y cantidad).
- Costos.
- Nombres e información de contacto de los miembros del equipo.
- Nombres e información de contacto de proveedores.
- Requerimientos de las instalaciones fuera de sitio.
- Registros vitales (electrónicos y en papel).

Debido a que el plan de contingencia contiene información confidencial de funcionamiento y de personal, su distribución debe ser cuidadosamente controlada. Normalmente, las copias del plan se proporcionan al personal de recuperación para el almacenamiento en el hogar y la oficina. Una copia también debe ser almacenada en el lugar alternativo y con los medios de respaldo. El almacenamiento de una copia del plan en el sitio alternativo garantiza la disponibilidad y buen estado, en el caso de que no se pueda acceder a las copias del plan por causa del desastre. El Coordinador de Planificación de Contingencias debe mantener un registro de las copias del plan así como quienes las poseen. Otra información que se debe guardar con el plan incluye los contratos con los proveedores de servicio, licencias de software, manuales de usuarios del sistema, manuales de seguridad, y procedimientos operativos.

Los cambios realizados en el plan, las estrategias y las políticas deben ser coordinadas a través del Coordinador de Planificación de Contingencia, quien, según sea necesario debe comunicar los cambios a los representantes de los planes o programas asociados. Asimismo debe registrar modificaciones al plan, pudiendo serle útil el uso de un registro de los cambios (que muestre por ejemplo el número de página, el comentario del cambio, y la fecha del cambio.

Ejemplo:

Figura 5.- Fuente: Contingency Planning Guide for Information Technology Systems.

Registro de Cambios			
Nro. De página	**Comentario**	**Fecha**	**Firma**

El Coordinador de Planificación de Contingencia también debe evaluar la información de apoyo para garantizar que la información es actual y sigue cumpliendo con los requisitos del sistema de manera adecuada. Esta información incluye lo siguiente:

- Contrato del sitio alternativo, incluyendo los tiempos de prueba.
- Contrato de almacenamiento fuera de sitio.
- Las licencias de software.
- Requerimientos de hardware y software.
- Acuerdos de interconexión del sistema.
- Los requisitos de seguridad.
- Estrategia de recuperación.
- Políticas de contingencia.
- Entrenamiento.
- Ámbito de aplicación de las pruebas.

Aunque algunos cambios pueden ser muy visibles, otros requieren un análisis adicional. El BIA debe revisarse periódicamente y actualizarse con nueva información para determinar las necesidades imprevistas o nuevas prioridades.

A medida que nuevas tecnologías estén disponibles, los controles preventivos pueden ser mejorados y las estrategias de recuperación ser modificadas.

CAPITULO IV - DESARROLLO DEL PLAN DE CONTINGENCIA

El desarrollo del plan de contingencia es un paso crítico en el proceso de aplicación de un programa integral de planificación de contingencia. El plan contiene las funciones, responsabilidades, los equipos y procedimientos asociados con la restauración de un sistema a raíz de una interrupción. El plan de contingencia debe documentar la capacidad técnica destinada a apoyar las operaciones de contingencia; y debe además adaptarse a la organización y sus necesidades. Los planes necesitan equilibrar los detalles con flexibilidad, por lo general cuanto más detallado el plan, menos escalable y versátil, el enfoque. El formato del plan puede ser modificado según sea necesario para satisfacer mejor las necesidades específicas del usuario, de funcionamiento y los requisitos de la organización.

A continuación se identifican cinco componentes principales del plan de contingencia:

- El plan de apoyo a la información.
- Fase de activación.
- Fase de recuperación.
- Fase de reconstitución.
- Apéndices.

Los planes deben tener el formato ideal para proporcionar una orientación rápida y clara en el caso de que el personal familiarizado con el plan o los sistemas sean "llamados" a realizar operaciones de recuperación. Los planes deben ser claros, concisos y fáciles de aplicar en caso de emergencia.

1. INFORMACIÓN DE APOYO

Éste componente incluye conceptos que proporcionan información fundamental o contextual que hace que el plan de contingencia sea más fácil de comprender, implementar y mantener. Estos detalles facilitan la comprensión de la guía, la toma de decisiones sobre cómo utilizar el plan, y contribuyen también al suministro de datos sobre dónde puede ser encontrada la información, fuera del ámbito de aplicación del plan.

En general éste componente incluye varias subsecciones:

- **Propósito**. Este apartado establece el motivo para el desarrollo del plan de contingencia y define los objetivos del plan.

- **Aplicabilidad**. Todos los planes relacionados que apoyan o son apoyados por el plan de contingencia deben ser identificados y su relación debe ser descrita.

- **Ámbito de aplicación**. La sección identifica el destino y los lugares cubiertos por el plan de contingencia si el sistema se distribuye entre múltiples ubicaciones. Por ejemplo, el plan no puede tratar las perturbaciones a corto plazo que se espera duren menos de cuatro horas, o no puede resolver las catástrofes que resultan en la destrucción de las instalaciones de TI.

El ámbito de aplicación debería abordar las hipótesis formuladas en el plan, tales como el supuesto de que las personas clave estarán disponibles en caso de emergencia. Sin embargo, las hipótesis no deben utilizarse como sustituto de una planificación cuidadosa. Por ejemplo, el plan no debe asumir que las interrupciones se producen sólo durante el horario comercial; ya que mediante el desarrollo de un plan de contingencia sobre la base

de tal supuesto, el Coordinador de Planificación de Contingencia puede ser incapaz de recuperar el sistema de manera eficaz si la interrupción se produjera en horas no comerciales.

- **Registro de los cambios**. El plan de contingencia debe ser un documento vivo que se modifica a fin de reflejar cambios operacionales, de sistemas u organizacionales. Las modificaciones realizadas al plan deben ser registradas en el registro de los cambios.

- **Descripción del Sistema**. Es necesario incluir una descripción general del sistema de TI. La misma debe incluir la arquitectura del sistema, la ubicación, y cualquier otra consideración técnica importante. Un diagrama del sistema, incluidos los dispositivos de seguridad (por ejemplo, cortafuegos, conexiones internas y externas) es útil. El contenido de la descripción del sistema generalmente se puede extraer del plan de seguridad del sistema.

- **Línea de sucesión**. El orden de sucesión identifica el personal responsable para asumir la autoridad para ejecutar el plan de contingencia en caso de que la persona designada no está disponible o no puede hacerlo.

- **Responsabilidades**. Esta sección presenta la estructura general de los equipos de contingencia, incluyendo la jerarquía, los mecanismos de coordinación y los requerimientos de los equipos. La sección también ofrece una visión general de las funciones y responsabilidades de los miembros del equipo en una situación de contingencia. Los equipos y los miembros de éstos deben ser designados para la respuesta con funciones específicas de recuperación durante la activación del plan de contingencia. Las funciones deben ser asignadas a los equipos en lugar de a un individuo específico. Listar los miembros de los equipos por rol y no por nombre, no sólo reduce la confusión si el miembro no está disponible para responder, sino que también ayuda a reducir el número de cambios que tendrían que ser realizados en el documento debido a la rotación de personal.

2. FASE DE ACTIVACIÓN

Ésta fase define las medidas iniciales a ser adoptadas una vez que una emergencia o interrupción del sistema se ha detectado o parece ser inminente. Esta fase incluye actividades para notificar al personal de recuperación, evaluar los daños del sistema, y aplicar el plan. Al término de la fase de activación, el personal de recuperación está preparado para llevar adelante medidas de contingencia para restablecer las funciones del sistema sobre una base temporal.

2.1. Procedimientos de notificación

Un evento puede ocurrir con o sin previo aviso. Por ejemplo, un aviso por adelantado puede ser que un huracán afectará un área puntual o que se espera un virus informático en una fecha determinada. Sin embargo, puede no haber algún aviso de fallo del equipo o de un acto criminal. Los procedimientos de notificación deben ser documentados en el plan para los dos tipos de situación y describir los métodos utilizados para notificar al personal de recuperación durante el negocio y las horas no comerciales. Una notificación rápida es importante para reducir los efectos sobre el sistema de TI; en algunos casos, se podrá disponer de tiempo suficiente para permitir que el personal de sistemas apague el sistema con comodidad y así evitar un "choque duro". Tras el desastre, la notificación debe ser enviada al Equipo de Evaluación de Daños para que pueda determinar el estado de la situación y las próximas medidas apropiadas. Cuando se haya completado la evaluación de daños, la recuperación adecuada y equipos de apoyo deben ser notificados.

Las notificaciones se pueden lograr a través de una variedad de métodos, incluyendo el teléfono, buscapersonas, correo electrónico, o teléfono celular. Las notificaciones enviadas vía mail deben hacerse con precaución, porque no hay forma de garantizar una retroalimentación positiva, ya que si bien el correo electrónico tiene un gran potencial como método eficaz de difusión de información, no hay manera de asegurar que el mensaje será leído. Si se utiliza un método de notificación vía mail, el personal de recuperación debe ser informado de la necesidad e importancia de chequear sus mails con bastante frecuencia y regularidad. Las notificaciones enviadas durante el horario comercial deben ser enviadas a la dirección del trabajo, mientras que el uso de correos electrónicos personales puede ser útil en el caso de que la LAN esté caída. Algunas herramientas de notificación que son también eficaces en caso de desastres generalizados son los anuncios de radio, televisión y sitios web.

La estrategia de comunicación debe definir los procedimientos que deben seguirse en caso de que el personal específico no puede ser contactado. Los procedimientos de notificación deben ser documentados claramente en el plan de contingencia. Un método común de notificación es un "árbol de llamadas" (o call tree, en inglés). Esta técnica consiste en la asignación de obligaciones de notificación a personas concretas, que a su vez son responsables de notificar al personal de recuperación.

El personal a ser notificado deberá estar claramente identificado en las listas de contactos anexas al plan. Esta lista debería organizar al personal por su posición de equipo, el nombre y datos de contacto (por ejemplo, dirección, teléfono, direcciones de correo electrónico, etc.).

El tipo de información a ser transmitida a los que están siendo notificados debe estar documentada en el plan. La cantidad y detalle de la información transmitida puede depender del equipo específico que está siendo notificado. Siendo necesario, debería notificarse la siguiente información:

- Naturaleza de la emergencia que se ha producido o es inminente su ocurrencia.
- La pérdida de vidas o lesiones.
- Estimaciones de los daños conocidos.

- De respuesta y recuperación de datos.

- Dónde y cuándo convocar para dar más información o instrucciones de respuesta.

- Instrucciones para una reubicación en un período de tiempo estimado, si fuese necesaria.

- Instrucciones para completar las notificaciones utilizando el árbol de llamadas (si corresponde).

2.2. Evaluación de Daños

Para determinar cómo el plan de contingencia se llevará a cabo después de una emergencia, es esencial evaluar la naturaleza y el alcance de los daños al sistema. Esta evaluación de los daños debe completarse tan pronto como las condiciones lo permitan. Por lo tanto, cuando sea posible, el equipo de evaluación de daños debe ser el primero en ser notificado del incidente. Los procedimientos de evaluación de daños pueden ser únicos para un sistema en particular, sin embargo, las siguientes áreas deberían ser abordadas:

- Causa de la emergencia o la interrupción.

- Área afectada por la emergencia

- Estado de la infraestructura física (por ejemplo, la integridad estructural de la sala de informática, estado de la energía eléctrica, las telecomunicaciones y la calefacción, ventilación y aire acondicionado, etc.).

- Inventario y el estado de los equipos informáticos.

- Tipo de daño a los equipos informáticos o de datos (por ejemplo, daños por agua, fuego, calor, el impacto físico, o producto de la electricidad).

- Artículos a ser sustituidos (por ejemplo, hardware, software, firmware y materiales de apoyo).

- Tiempo estimado para restablecer los servicios con normalidad.

El personal con responsabilidades en la evaluación de daños debe entender y ser capaz de llevar adelante estos procedimientos en el caso de que el plan de trabajo no está disponible durante la situación. Una vez que el impacto sobre el sistema ha sido determinado, los equipos adecuados deben ser notificados.

En el Capítulo X – Anexos, se pueden apreciar distintos tipos de situaciones que causaron daños de diversa magnitud, afectando a diferentes organizaciones.

2.3. Plan de Activación

El plan de contingencia debe ser activado sólo cuando la evaluación de los daños indica que se cumplen uno o más de los criterios de activación de dicho sistema. Si un criterio de activación se cumple, el Coordinador de Planificación de Contingencia debe activar el plan. Los criterios de activación son únicos para cada organización y deben figurar en la declaración de política de planificación de contingencia. Los criterios pueden basarse en:

- Seguridad del personal y/o magnitud de los daños a las instalaciones.
- Extensión del daño al sistema (por ejemplo, físico, operacional, o el costo).
- Criticidad de los activos.
- La duración prevista de la interrupción.

Una vez que el daño en el sistema se ha caracterizado, el Coordinador de Planificación de Contingencia puede seleccionar la estrategia de recuperación adecuada, y los equipos asociados de recuperación deben ser notificados

3. FASE DE RECUPERACIÓN

Las operaciones de recuperación comienzan luego que el plan de emergencia ha sido activado, la evaluación de daños se ha terminado (si es posible), el personal ha sido notificado, y los equipos apropiados se han movilizado. Las actividades de la fase de recuperación se centran en las medidas de contingencia para ejecutar temporalmente la capacidad de procesamiento, reparar el daño al sistema original, y restaurar la capacidad operativa en el original o nueva instalación. En la finalización de la fase de recuperación, el sistema de TI estará en funcionamiento y realizando las funciones designadas en el plan. Dependiendo de las estrategias de recuperación definidas en el plan, estas funciones podrían incluir temporalmente el procesamiento manual, la recuperación y el funcionamiento de un sistema alternativo, o la reubicación y la recuperación en un sitio alternativo. Los equipos con responsabilidades en la recuperación deben comprender y ser capaces de llevar a cabo estas estrategias de recuperación de manera tal que si el plan de trabajo no está disponible durante las etapas iniciales del evento, aún puedan realizar las actividades necesarias.

3.1. Secuencia de actividades de recuperación

Cuando la recuperación corresponde a un sistema complejo, como una red WAN, la cual engloba una participación de múltiples componentes independientes, los procedimientos de recuperación deben reflejar las prioridades identificadas en el BIA. La secuencia de actividades debe reflejar el tiempo permitido de interrupción, para evitar impactos significativos a los sistemas y su aplicación. Los procedimientos deben ser escritos "paso por paso", en un formato secuencial de manera que los componentes del sistema puedan ser restaurados de una manera lógica. Por ejemplo, si una red LAN está siendo recuperada después de una interrupción, los servidores más críticos deben ser recuperados antes que los dispositivos menos críticos, tales como impresoras. Del mismo modo, para recuperar un servidor de aplicaciones, los procedimientos primero deben abordar la restauración del sistema operativo y su verificación. Los procedimientos también deben incluir instrucciones para la coordinación con otros equipos cuando se producen determinadas situaciones, tales como:

- Una acción no se complete en el plazo previsto.
- Un paso fundamental ha sido completado.
- Artículos determinados deben ser adquiridos.

Si las condiciones requieren que el sistema se recupere en un sitio alternativo, ciertos materiales deberán ser transferidos o adquiridos. Estos elementos pueden incluir el envío de datos de respaldo desde el almacenamiento externo, hardware, copias del plan de recuperación, y programas de software. Los procedimientos deben designar el equipo adecuado o los miembros del equipo para coordinar el envío de equipamiento, datos y registros vitales. Los procedimientos deben describir claramente los requisitos para el transporte y compra de los materiales necesarios para recuperar el sistema.

3.2. Procedimientos de recuperación

Para facilitar las operaciones de la fase de recuperación, el plan de contingencia debe prever procedimientos detallados para restaurar el sistema o los componentes del este. Dada la amplia variedad de tipos de sistema, configuraciones y aplicaciones, los procedimientos deben ser asignados al equipo de recuperación correspondiente y suelen abordar las siguientes acciones:

- La obtención de la autorización para acceder a las instalaciones dañadas.
- Notificación a interesados internos y externos asociados con el sistema.
- La obtención de material de oficina necesario y los espacios de trabajo.

- Obtener e instalar los componentes de hardware necesarios.

- La obtención y "levantamiento" de los respaldos.

- Restaurar el sistema operativo y software de aplicación críticos.

- Restaurar datos del sistema.

- La funcionalidad del sistema de análisis que incluye los controles de seguridad.

- Sistema de conexión a la red u otros sistemas externos.

Los procedimientos de recuperación deben ser escritos paso por paso. Para evitar dificultades o confusión en caso de emergencia, ningún "paso" debe ser asumido u omitido. El uso de una lista de verificación (check list) es útil para documentar los procedimientos de recuperación secuenciales y para solucionar problemas si el sistema no puede ser recuperado correctamente.

4. FASE DE RECONSTITUCIÓN

En la fase de reconstitución, se da término a las actividades de recuperación y las operaciones normales son transferidas de vuelta a las instalaciones de la organización. Si la instalación original es irrecuperable, las actividades en esta fase también se pueden aplicar a la preparación de una nueva instalación para soportar los requerimientos de la organización. Una vez que se restablezca el nivel que puede soportar el sistema de TI y sus procesos normales, se puede hacer la transición al original o al nuevo sitio. Hasta que el sistema principal sea restaurado y probado, el sistema de contingencia debe seguir operativo. La fase de reconstitución debe especificar los equipos responsables de la restauración y/o sustitución de la ubicación y el sistema de TI. Las siguientes actividades se producen en esta fase:

- Lograr el apoyo de una infraestructura adecuada, como la energía eléctrica, agua, telecomunicaciones, seguridad, controles ambientales, equipos de oficina y suministros.

- Instalación de sistema de hardware, software y firmware. Esta actividad debe incluir los procedimientos detallados de restauración similares a los seguidos en la fase de recuperación.

- El establecimiento de la conectividad y las interfaces con los componentes de red y sistemas externos.

- Testeo del sistema para garantizar un pleno funcionamiento.

- Respaldo de los datos operacionales en el sistema de contingencia y carga de los mismos al sistema de restauración.

- "Apagado" del sistema de contingencia.

- Finalización de las operaciones de contingencia.

- Protección, eliminación y/o reubicación de todos los materiales sensibles en el sitio de contingencia.

- Organización para que el personal de recuperación pueda volver a la instalación original.

Estos equipos deben entender y ser capaces de cumplir con sus funciones sin un plan de trabajo en el caso de que esa documentación no esté disponible.

5. APÉNDICES

Los apéndices al plan de contingencia proporcionan detalles clave que no figuran en el cuerpo principal del plan. Los apéndices deben reflejar la técnica, operativa, y los requisitos de manejo de contingencias del sistema dado, sin embargo, algunos de los apéndices se encuentran con frecuencia dentro de los planes de contingencia de TI. En general los apéndices incluyen lo siguiente:

- Información de contacto para el personal del equipo de planificación de contingencia.

- Información de contacto de proveedores, incluyendo el almacenamiento fuera de la organización e información sobre un eventual sitio alternativo.

- Procedimientos operativos estándar y listas de comprobación (check lists) para la recuperación del sistema y/o procesos.

- Listas de requisitos del sistema del hardware, software, firmware y otros recursos necesarios para apoyar las operaciones del sistema. Se facilitarán detalles para cada entrada, incluyendo el modelo o número de versión, las especificaciones y cantidades.

- El BIA, llevado a cabo durante las fases de planificación, contiene información valiosa acerca de las interrelaciones, los riesgos, el establecimiento de prioridades, y los impactos a cada elemento del sistema.

CAPITULO V - CONSIDERACIONES TÉCNICAS DE CONTINGENCIA

Este capítulo apunta a brindar información para la selección, desarrollo y aplicación de estrategias específicas de contingencia basadas en el tipo de sistema de TI. Toda la información presentada puede no ser aplicable a un sistema específico de TI, por lo tanto, el Coordinador de Planificación de Contingencia debe basarse en la información que corresponda y modificarla para satisfacer las necesidades de contingencia del sistema. Las siguientes plataformas se abordan en esta sección:

- Computadores de escritorio y sistemas portátiles.
- Servidores.
- Sitios Web.
- Redes LAN.
- Redes WAN.
- Sistemas distribuidos.
- Sistemas mainframe

Para cada plataforma de TI, las medidas técnicas son consideradas desde dos perspectivas. En primer lugar, se examinan los requisitos técnicos o los factores que el Coordinador de Planificación de Contingencia debe considerar al elaborar una estrategia de recuperación del sistema. En segundo lugar, las soluciones basadas en la tecnología se proporcionan para cada plataforma. Varias de estas medidas de contingencia son comunes a todos los sistemas de TI. En general incluyen lo siguiente:

- Frecuencia de los respaldos y almacenamiento fuera del sitio de los datos, las aplicaciones y el sistema operativo.
- Importancia de los componentes críticos del sistema.
- Documentación de las configuraciones y requisitos del sistema.
- “Interoperabilidad” entre los componentes del sistema, y entre los equipos del sitio principal y suplente para acelerar la recuperación del sistema.
- Controles ambientales, y configuración apropiada de las fuentes de energía.

1. COMPUTADORAS DE ESCRITORIO Y SISTEMAS PORTÁTILES

Un ordenador de escritorio o sistema portátil (por ejemplo, laptop o dispositivo de mano) por lo general consiste de una unidad de procesamiento central (CPU), memoria, almacenamiento en disco, y la entrada de diversos dispositivos de salida. Un PC está diseñado para su uso por una persona a la vez.

Los PCs son omnipresentes en la mayoría de las organizaciones. Debido a que las computadoras de escritorio y portátiles son la plataforma más común para la rutina de los procesos automatizados, es que resultan ser elementos importantes en un plan de contingencia. En principio son los que aparecen como más expuestos (no cuentan con las medidas de seguridad de los servidores) a accidentes físicos, como ser robos (ver ejemplo "A" del apartado "2" – Capítulo X - Anexos); y por ello no debería guardarse información considerada crítica para la organización en los mismos.

1.1. Consideraciones de Contingencia

Las consideraciones de contingencia deben hacer hincapié en la disponibilidad de datos, la confidencialidad y la integridad. Para abordar estas necesidades, el administrador de sistemas debe considerar cada una de las siguientes prácticas:

- **Almacenar los respaldos fuera de la organización**. Los medios de copia de seguridad deben guardarse fuera del lugar en una instalación, segura, ambientalmente controlada; ya que si no lo hacen se corren riesgos de sufrir las mismas consecuencias que la empresa del Ejemplo "G" (apartado "2", Capítulo X – Anexos). Una copia del plan de contingencia, licencias de software, contratos y otros documentos importantes deben guardarse con los respaldos. El BIA realizado por el Coordinador de Planificación de Contingencias debe ayudar a determinar con qué frecuencia deben enviarse los respaldos fuera de la organización.

- **Alentar a las personas a respaldar datos**. Si el proceso de respaldo del PC no es automático, los usuarios deben ser alentados a realizar una copia de seguridad de datos regularmente. Esta tarea puede ser realizada a través del entrenamiento del personal y como medida de prevención. La no realización de respaldos puede traer altos costos de recuperación e inoperancia, ver ejemplo "D" (apartado "2", Capítulo X – Anexos).

- **Proporcionar orientación sobre almacenamiento de datos en computadoras personales**. Instruir a los usuarios a que guarden los datos en una carpeta en particular facilita las necesidades de apoyo del departamento de TI. Si un equipo debe ser reconstruido, el técnico sabrá qué carpetas copiar y conservar al mismo tiempo que el sistema se vuelve a cargar.

- **Estandarización de hardware, software y periféricos**. La recuperación del sistema es más rápida si el hardware, el software y los periféricos son uniformes en toda la organización. Si las configuraciones estándar no son posibles en toda la organización,

entonces las configuraciones deben ser normalizadas por departamento o por el tipo de máquina o modelo, si es posible.

- **Documentar las configuraciones del sistema e información de proveedores**. Configuraciones bien documentadas facilitan la recuperación. Del mismo modo, los nombres de los proveedores y la información de contacto de emergencia debe incluirse en el plan de contingencia para que el equipo de reemplazo pueda ser adquirido rápidamente.

- **Coordinar las políticas de seguridad y el sistema de controles de seguridad**. Las soluciones de contingencia para los equipos portátiles y de escritorio deberían coordinarse con las políticas de seguridad y los controles de seguridad del sistema. Por lo tanto, al elegir la solución apropiada de contingencia, controles de seguridad similares y otras actividades relacionadas (por ejemplo, la evaluación del riesgo, la vulnerabilidad de exploración), deben aplicarse en la solución de contingencia para garantizar que, durante una interrupción del sistema, la ejecución de dicha solución no comprometa o revele datos sensibles.

- **Utilizar los resultados del BIA**. Impactos y prioridades descubiertos a través del BIA de las aplicaciones más importantes y sistemas de apoyo en general deben ser revisados para determinar los requisitos relacionados.

1.2. Soluciones de Contingencia

Amplias gamas de soluciones de contingencia técnica están disponibles para computadoras de escritorio, varias prácticas de eficiencia se discuten aquí. Datos del BIA de las principales aplicaciones y sistemas de apoyo se deben utilizar para determinar los requisitos de recuperación y las prioridades de implementación.

Las copias de seguridad son los medios más comunes para garantizar la disponibilidad de datos en los ordenadores. Existen ciertos factores que deben considerarse al elegir la solución de copia de seguridad apropiada:

- Volumen de almacenamiento.

- Tiempo de almacenamiento.

- Software utilizado para realizar los respaldos.

- Unidades de cinta. Las unidades de cinta no son comunes en computadoras de escritorio, pero son una opción para una solución de alta capacidad de copia de seguridad. Los costos de éstos medios son relativamente bajos.

- Cartuchos extraíbles.

- Disco compacto (CD). En general la mayoría de los ordenadores están equipados con unidades de CD grabable. Los CDs son de bajo costo de almacenamiento y tienen una mayor capacidad de almacenamiento que los disquetes (los cuales prácticamente se ha discontinuado su uso).

- Almacenamiento en red. Los datos almacenados en los ordenadores en red pueden ser respaldados en un disco de red o un dispositivo de almacenamiento en red:

- **El disco en red**. Un servidor con capacidad de almacenamiento de datos es un disco de red. La cantidad de datos que puede ser respaldada desde un PC está limitada por la capacidad de almacenamiento de disco o de asignación de disco para el usuario particular. Sin embargo, si se instruye a los usuarios a que guarden archivos en un disco en red, el disco en sí debe ser respaldado a través de la red o un programa de copia de seguridad del servidor.

- **Dispositivo de almacenamiento en red**. Un sistema de copia de seguridad en red se puede configurar para respaldar las unidades locales en los ordenadores conectados en red.

- Replicación o Sincronización. La replicación de datos o la sincronización es un método de respaldo común para ordenadores portátiles. Los equipos portátiles pueden conectarse a un PC y reproducir los datos deseados desde el sistema portátil a la computadora de escritorio.

- Respaldo en Internet. Los respaldos vía Internet, o en línea, es un servicio comercial que permite a los usuarios de PCs realizar una copia de seguridad de datos a una ubicación remota a través de Internet por una tarifa. Una aplicación se instala en el PC que permite al usuario programar copias de seguridad, seleccionar los archivos y carpetas que se respaldan, y establecer un "sistema de archivo" para evitar que los datos se sobrescriban. Los datos pueden ser encriptados para su transmisión. La ventaja del respaldo en Internet es que el usuario no está obligado a comprar hardware de respaldo o medios de comunicación.

Además de respaldar datos, las organizaciones también deben respaldar los controladores del sistema. Las organizaciones deben almacenar software y las licencias de los mismos en una ubicación secundaria. Si el software es comercial, se puede adquirir a través de un proveedor, en caso de que la copia o la licencia instalada antes de la destrucción no esté disponible.

La "popularidad" del cifrado como una herramienta de seguridad utilizada en los ordenadores portátiles está creciendo. Con el uso cada vez mayor de firmas digitales y el uso del cifrado, las organizaciones deberían considerar la inclusión de pares de claves de encriptación en su estrategia de respaldo.

Debido a que los ordenadores portátiles son vulnerables al robo, la encriptación se puede utilizar para proteger la información de ser divulgada si un equipo es robado. Los usuarios de computadoras portátiles también pueden usar un segundo disco duro en caso que estén de viaje. El segundo disco duro debería contener sólo las aplicaciones y los datos

mínimos necesarios. Al usar un segundo disco duro, si le roban la computadora portátil, la cantidad perdida de datos se minimiza.

2. SERVIDORES

Servidores de apoyo para compartir archivos y almacenamiento, procesamiento de datos, la aplicación central de alojamiento (como el correo electrónico o una base de datos central), la impresión de control de acceso, la autenticación de usuario, conectividad de acceso remoto, y otros servicios de red compartida. Los usuarios locales inician sesión en el servidor a través de PCs en red para acceder a recursos que el servidor ofrece. Un servidor es un equipo que ejecuta un software para facilitar el acceso a un recurso o una parte de la red y recursos de red, tales como el almacenamiento en disco, impresoras y aplicaciones de red. Un servidor puede ser cualquier tipo de equipo que ejecuta un sistema operativo de red. Un servidor puede ser un PC estándar, o puede ser un equipo grande que contiene varias unidades de disco y una gran cantidad de memoria que permitirá a la computadora procesar cientos de peticiones a la vez.

2.1. Consideraciones de Contingencia

Dado que los servidores pueden soportar numerosas aplicaciones críticas, la pérdida del servidor puede causar problemas significativos a los procesos de negocio. Debemos considerar las siguientes prácticas para enfrentar las vulnerabilidades que presenta el servidor:

- **Almacenar los medios de respaldo y el software fuera de sitio**. Como se describió anteriormente, los medios de comunicación y el software de copia de seguridad deben guardarse fuera del lugar en una instalación segura, ambientalmente controlada. La instalación de almacenamiento debe estar ubicada lo suficientemente lejos del sitio original para reducir la probabilidad de que ambos sitios sean afectados por el mismo evento.

- **Estandarización de hardware, software y periféricos**. La recuperación del sistema puede ser acelerada si el hardware, el software y los periféricos son uniformes en toda laorganización o el sitio. Las configuraciones estándar deben ser documentadas en el plan de contingencia.

- **Documentación de configuraciones del sistema y proveedores**. Mantener un registro detallado de las configuraciones del sistema mejora las posibilidades de recuperación del mismo. Además, los proveedores de hardware, software y otros elementos deben ser identificados en el plan de contingencia.

- **Coordinación con las políticas de seguridad y los controles de seguridad de sistema**. Las soluciones de contingencia del servidor deben coordinarse con las políticas de seguridad y los controles de seguridad del sistema. De este modo, al elegir la solución apropiada de contingencia técnica, los controles de seguridad similares y las actividades

relacionadas con la seguridad (por ejemplo, evaluación de riesgos, el análisis de vulnerabilidad) en el entorno de producción deberían aplicarse en la solución de contingencia para garantizar que, durante una interrupción del sistema o emergencia, la ejecución de la solución de contingencia técnica no comprometa o revele datos sensibles.

- **Utilizar los resultados del BIA**. Impactos y prioridades descubiertos a través del BIA de las aplicaciones más importantes y los sistemas de apoyo en general deben ser revisados para determinar los requisitos relacionados.

Adjunto se puede apreciar un cuadro ejemplo de Análisis de Servidores y Servicios realizado por la A.N.P.

2.2. Soluciones de Contingencia

El BIA de las principales aplicaciones y sistemas de apoyo, en general debe proporcionar información para determinar los requisitos de recuperación y las prioridades. La planificación de contingencia del servidor debe hacer hincapié en la fiabilidad y la disponibilidad de los servicios de red proporcionados por el mismo. Cuando se selecciona la solución apropiada de contingencia, se debe tener cuenta la confidencialidad de los datos y los requisitos de sensibilidad.

Además, al seleccionar la solución apropiada de la contingencia del servidor, los requisitos de disponibilidad para el servidor, sus aplicaciones y los datos deben ser evaluados. Como medida de emergencia las funciones críticas no deben ser co-ubicadas en los servidores con funciones no críticas, si es posible. Por ejemplo, un servidor que aloja una aplicación crítica debe dedicarse a esa solicitud y no proporcionar otros recursos.

Al igual que para los PC, los servidores deben ser respaldados regularmente. Los servidores pueden ser respaldados a través de un sistema distribuido, en el que cada servidor tiene su propio impulso, o por medio de un sistema centralizado, en donde un dispositivo de copia de seguridad centralizada está conectado a un servidor.

El respaldo se puede realizar por tres métodos:

- **Completo.** Copia completa de todos los archivos en el disco o dentro de la carpeta seleccionada para la copia de seguridad. Dado que todos los archivos respaldados se registraron en un único medio o conjunto de medios, la localización de un archivo en particular o grupo de archivos es muy sencilla. Sin embargo, el tiempo necesario para realizar una copia de seguridad completa puede ser largo. Además, copias de seguridad

completas de archivos que no cambian con frecuencia (como los archivos de sistema) podría conducir a un excesivo e innecesario gasto en medios de almacenamiento.

- **Incremental.** Una copia de seguridad incremental captura archivos que fueron creados o modificados desde la última copia de seguridad. Copias de seguridad incrementales permiten el uso más eficiente de los medios de almacenamiento, así como también reducen los tiempos de copia de seguridad. Como punto negativo encontramos que para recuperar un sistema desde una copia de seguridad incremental serán necesarias diferentes copias de seguridad incrementales.

- **Diferencial.** Una copia de seguridad diferencial captura los archivos que fueron creados o modificados desde la última copia de seguridad completa. Por lo tanto, si un archivo se cambia después de la copia de seguridad completa anterior, una copia de seguridad diferencial guardara el archivo hasta la próxima copia de seguridad completa. La copia de seguridad diferencial toma menos tiempo que una copia de seguridad completa. La restauración de una copia de seguridad diferencial puede requerir menos medios que una copia de seguridad incremental ya que sólo se necesitarían los medios de la copia de seguridad completa y los de la última copia diferencial. Como desventaja, las copias de seguridad diferenciales toman más tiempo para terminar que las incrementales.

Una combinación de las operaciones de copia de seguridad se puede utilizar en función de la configuración del sistema y los requisitos de recuperación. Por ejemplo, una copia de seguridad completa en el fin de semana y copias de seguridad diferenciales durante la semana al fin de cada jornada. En el desarrollo de la programación de copia de seguridad del servidor, las siguientes preguntas deben ser consideradas:

- ¿Dónde se almacenarán los medios de comunicación?

- ¿Qué información debe ser respaldada?

- ¿Con que frecuencia se realizan las copias de seguridad?

- ¿Con qué rapidez las copias de seguridad permiten volver a una situación normal en caso de una emergencia?

- ¿Quién está autorizado para ejecutar la recuperación de los datos?

- ¿Cuánto tiempo se tardará en recuperar los datos?

- ¿Dónde deben ser entregados?

- ¿Cuál es el régimen de etiquetado de los medios de respaldo?

- ¿Cuánto tiempo se mantendrán los medios de respaldo?

- Cuando los datos son almacenados fuera sitio, ¿que controles ambientales se proporcionan para preservar los medios?

- ¿Cuál es el medio adecuado de respaldo?

- ¿Qué tipos de lectores de datos se utilizan en el sitio alternativo?

Los medios de copia de seguridad deben guardarse fuera del sitio de operaciones de la empresa en un lugar seguro. Al seleccionar la ubicación fuera de sitio, la distancia de la ubicación, la facilidad de acceso a los medios de copia de seguridad, las limitaciones de almacenamiento físico y las condiciones del contrato deben tenerse en cuenta. Es importante que los medios de comunicación sean recuperados en una base regular de almacenamiento fuera del sitio, todo esto debe ser testeado para asegurar que las copias de seguridad responden correctamente. El Coordinador de Planificación de Contingencia deberá tomar en cuenta el BIA para ayudar a determinar la frecuencia con la cual la copia de seguridad de los medios de comunicación debe ser probada. Cada cinta, cartucho o disco debe ser etiquetado solo una vez y siempre en la misma ubicación, esto para asegurar que los datos requeridos puedan ser identificados rápidamente en una emergencia. Esto requiere que la organización desarrolle una eficaz estrategia de marcado y rastreo. Un método podría ser la etiqueta de los medios de comunicación por mes, día, y el año que se creó la copia de seguridad. Otras estrategias pueden ser más complejas, con varios conjuntos de medios de comunicación que se rotan. La estrategia de marcar debe ser coherente con las directrices de retención de medios que dictan el tiempo que los mismos deben ser almacenados antes de su destrucción.

Aunque el almacenamiento fuera del sitio de los datos de respaldo permite la recuperación del sistema, los datos que se cargaron en el servidor desde la copia de seguridad anterior podrían haberse perdido durante una interrupción o un desastre. Para evitar esta posible pérdida de datos, una estrategia de copia de seguridad puede necesitar ser complementada por soluciones de redundancia, como el **reflejo de disco, RAID, y balanceo de carga**. Estas soluciones se discuten a continuación. Los datos del BIA pueden ayudar al Coordinador de Planificación de Contingencia en la determinación de la longitud de tiempo adecuado para la rotación de datos.

RAID (Redundant Array of Independent Disks)

Proporciona tolerancia a fallos de disco para almacenamiento de datos y disminuye el tiempo medio entre fallos (MTBF). Se utiliza para impulsar la máscara de disco y de controlador de disco. Además, RAID aumenta el rendimiento y la fiabilidad mediante la difusión de almacenamiento de datos a través de varias unidades de disco, en lugar de un solo disco. RAID se puede implementar a través de hardware o software, en cualquier caso, la solución convierte al sistema operativo en una única unidad lógica. Con un sistema RAID, unidades intercambiables en caliente pueden ser utilizadas, es decir, unidades de disco se pueden intercambiar sin apagar el sistema cuando una unidad de disco falla. La tecnología RAID utiliza tres técnicas de redundancia de datos: la creación de reflejo, la paridad y la creación de bandas.

- **De reflejo (Mirroring)**. Con esta técnica, el sistema escribe los datos de forma simultánea para separar por un lado unidades de disco duro y por otro la matriz de discos. Las ventajas de esta técnica son, menor tiempo de inactividad, simple recuperación de datos y mayor rendimiento en la lectura del disco. Si un disco duro o una matriz de discos falla, el sistema puede funcionar desde el disco duro de trabajo, funcionar desde la matriz de disco o utilizar un disco para procesar una solicitud de lectura y otro disco para otra petición de procesamiento. La desventaja de reflejar es que tanto las unidades de disco como las matrices trabajan al mismo tiempo, lo que puede obstaculizar el rendimiento del sistema. El sistema de espejo tiene una alta tolerancia a errores.

- **De paridad.** La paridad se refiere a una técnica de determinar si los datos se han perdido o se han sobrescrito. La paridad tiene menor tolerancia a errores que la técnica de espejo. La ventaja de la paridad es que los datos pueden ser protegidos sin tener que guardar una copia de los mismos como se requiere con el sistema de espejo.

- **Segmentación**. La segmentación mejora el rendimiento de la matriz controladora de hardware mediante la distribución de datos a través de todas las unidades. En la segmentación, un elemento de datos está dividido en varias piezas, y una pieza es distribuida a cada unidad de disco duro. El rendimiento de transferencia de datos se incrementa, porque las unidades pueden tener acceso simultáneamente a cada pieza de datos. La segmentación se puede implementar en bytes o bloques. En el nivel byte se dividen los datos en bytes y se almacenan en las unidades de disco duro. En el nivel de bloques se dividen los datos en un bloque de determinado tamaño, y cada bloque se distribuye en un disco.

RAID es una estrategia efectiva para la redundancia de disco. Sin embargo, la redundancia de otras partes críticas de servidor, tales como el suministro de energía también debe ser aplicada. El servidor puede estar equipado con dos fuentes de alimentación, de modo que la segunda fuente de alimentación puede continuar apoyando el servidor si la fuente principal se sobrecalienta o queda inutilizable.

Aunque una segunda fuente de energía puede proteger contra fallos de hardware, no es una medida preventiva eficaz contra la falta de alimentación de energía. Para garantizar a corto plazo y para proteger contra las fluctuaciones de potencia es necesaria una terminal UPS (Unidad de Alimentación Eléctrica Permanente). Una UPS a menudo proporciona suficiente energía para permitir que el sistema se cierre correctamente. Si se requiere una alta disponibilidad de energía se puede utilizar un generador. El generador puede conectarse directamente al sistema de energía del sitio o puede ser configurado para iniciarse automáticamente cuando se detecta una interrupción de energía.

Bóveda electrónica y diario remoto

Son tecnologías similares que proporcionan capacidades adicionales de copia de seguridad, con respaldos realizados a las unidades de cinta remota a través de enlaces de comunicación. Permiten tiempos de recuperación más cortos y reducción de la pérdida de

datos si el servidor se dañase entre respaldos. El sistema de bóveda electrónica permite que se creen copias de seguridad fuera de sitio de forma automática. La bóveda electrónica podría utilizar los discos ópticos, discos magnéticos, dispositivos de almacenamiento masivo, o una librería robotizada de cintas como dispositivos de almacenamiento. Con esta tecnología, los datos se transmiten a la bóveda electrónica, tal como se producen cambios en los servidores de copias de seguridad. Estas transmisiones entre copias de seguridad se refieren a veces como un diario electrónico.

Con el diario remoto, registros de transacciones o revistas se transmiten a una ubicación remota. Si el servidor necesita ser recuperado, los registros se podrían utilizar para recuperar las transacciones, las aplicaciones, bases de datos o los cambios que se produjeron después de la última copia de seguridad del servidor. Diario remoto y bóveda electrónica requieren una ubicación fuera de sitio dedicada a recibir las transmisiones. Dependiendo del volumen y la frecuencia de las transmisiones de datos, pueden ser llevados a cabo durante una conexión con ancho de banda limitado.

"**Server Load Balancing" (Balanceo de Carga)**

Aumenta la disponibilidad del servidor y la aplicación. El tráfico se puede distribuir de forma dinámica a través de grupos de servidores que ejecutan una aplicación común de modo que ningún servidor sea sobrecargado. Con esta técnica, un grupo de servidores aparece como un único servidor a la red. El sistema monitorea cada servidor para determinar el mejor camino para enrutar el tráfico de manera de aumentar el rendimiento y la disponibilidad para que ningún servidor sea sobrecargado. El balanceo de carga se puede implementar entre los servidores dentro de un sitio o los servidores en sitios diferentes. El uso de "Server Load Balancing" puede permitir que la aplicación siga funcionando hasta que uno o más sitios vuelvan a estar funcionando. Así, el equilibrio de carga podría ser una medida de contingencia viable en función de los requisitos de disponibilidad del sistema.

Replicación de Disco

Con la replicación de disco la recuperación se minimiza porque los datos se escriben en dos discos diferentes para garantizar que dos copias válidas de los datos están siempre disponibles. Los discos se llaman: servidor protegido (el servidor principal) y servidor de replicación (el servidor de respaldo). La replicación de disco puede aplicarse a nivel local o entre distintas ubicaciones. Existen dos técnicas diferentes de replicación de disco, y cada uno proporciona diferentes RTO (Recovery Time Objetives - objetivos de tiempo de recuperación) y RPO (Recovery Point Objetives - objetivos de punto de recuperación). El RTO es la longitud máxima aceptable de tiempo que transcurre antes de que la falta de disponibilidad del sistema afecte gravemente a la organización. El RPO es el momento (punto en el tiempo) en que los datos deben ser restaurados con el fin de reanudar el procesamiento.

Las técnicas de replicación de disco son las siguientes:

- Sincronizado o de Espejo (Mirroring). Este método utiliza un sistema de copia disco a disco y mantiene una réplica de la base de datos. Aplica cambios en el servidor réplica al mismo tiempo que se efectúan en el servidor protegido. El modo sincronizado puede degradar el rendimiento en el servidor protegido y debe aplicarse sólo a corta distancia física donde el ancho de banda no va a restringir las transferencias de datos entre servidores. Con la réplica sincronizada, el RTO puede llevar desde algunos minutos a varias horas y el RPO podrá reducirse a la pérdida de trabajo comprometido. El mirroring se debe utilizar para las aplicaciones críticas que pueden aceptar poca o ninguna pérdida de datos.

- No sincronizado. Esta técnica mantiene una réplica de la base de datos o sistema de archivos mediante la continua captura de los cambios en el registro, y la aplicación de los mismos en el servidor de replicación. Con ésta técnica, el RTO puede durar desde unas horas a un día, dependiendo del tiempo que se requiere para implementar los cambios en los registros sin aplicación.

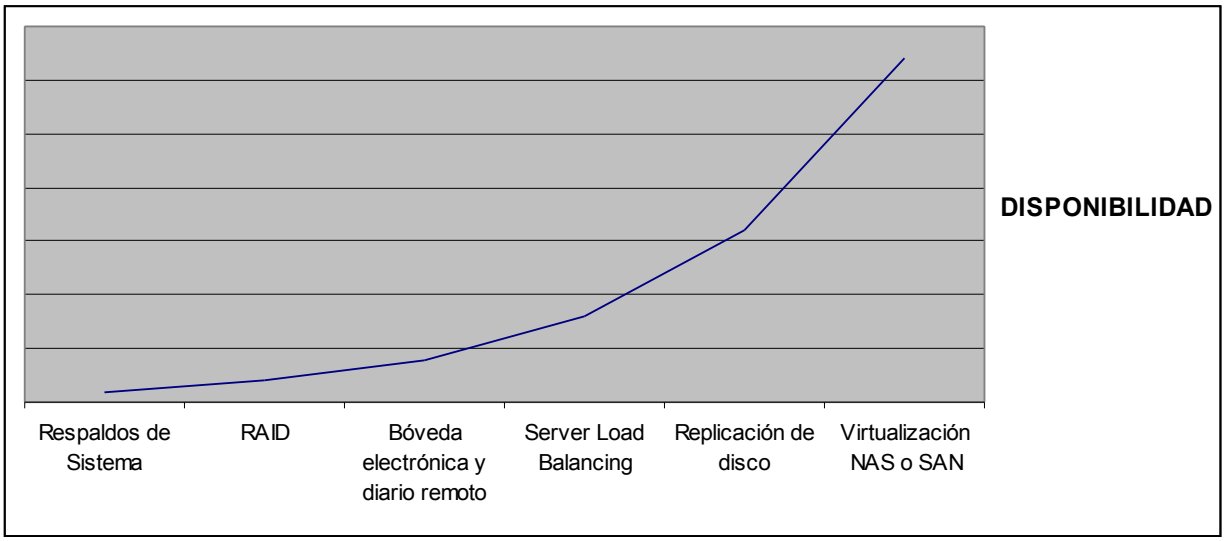
Virtualización de almacenamiento

El concepto de virtualización de almacenamiento es el proceso de combinar múltiples dispositivos de almacenamiento físico en un dispositivo lógico, el almacenamiento virtual puede ser gestionado de forma centralizada y se presenta a las aplicaciones de red, sistemas operativos y usuarios, un grupo de almacenamiento único. Las tecnologías de virtualización pueden ser “Network Attached Storage” (NAS), o “Storage Area Network” (SAN). Entornos NAS son de archivo y orientados a ofrecer un área de almacenamiento común para múltiples servidores. Los mismos son beneficiosos para el archivo de las aplicaciones de servidor o de almacenamiento. Un dispositivo NAS, o un servidor, va desde un sistema operativo mínimo, y está diseñado para facilitar el movimiento de datos. Con el archivo, protocolos orientados, que residen en cualquier aplicación, usando virtualmente cualquier sistema operativo pueden enviar datos o recibir datos desde un dispositivo NAS.

El entorno SAN, es una red de alta velocidad y alto rendimiento que permite a los equipos con sistemas operativos diferentes, comunicarse con un dispositivo de almacenamiento. A diferencia de un NAS, una SAN proporciona acceso a los datos en bloques y está construida para manejar el almacenamiento y el tráfico de copia de seguridad en lugar de archivo de tráfico orientado. Una SAN puede ser local o remota (a una distancia limitada) y generalmente se comunica con el servidor a través de un canal de fibra.

La siguiente gráfica presenta una escala de la disponibilidad relativa de las soluciones de contingencia discutidas. Alta disponibilidad se mide en términos de tiempo de pérdida de datos o cuelgue del servidor, la baja disponibilidad implica que la recuperación del servidor podría requerir días para ser completada.

Figura 6.- Fuente: Contingency Planning Guide for Information Technology Systems.



3. SITIOS WEB

Sitios web presentan información al público o personal autorizado a través de la World Wide Web (WWW) o una intranet privada. Un sitio web externo también puede ser un comercio electrónico (e-commerce) del portal, a través del cual la organización puede proporcionar servicios a través de Internet. Un sitio Web puede ser utilizado internamente dentro de una organización para proporcionar información, tales como las políticas corporativas, recursos humanos o un directorio telefónico a sus empleados.
Un sitio Web se utiliza para la difusión de información en Internet o una intranet. El sitio Web se crea en "Hypertext Markup Language" (HTML) que pueden ser leídos por un navegador Web en un equipo cliente. Un sitio web está alojado en un ordenador (servidor Web) que sirve las páginas Web al navegador del cliente solicitante. El servidor Web aloja los componentes de un sitio Web (por ejemplo, páginas, scripts, programas y archivos multimedia) y les sirve con el protocolo de transferencia de hipertexto (HTTP). Los sitios Web pueden presentar el contenido estático o dinámico. Un sitio Web puede ser interno a una organización (una intranet) o publicado a través de Internet.

3.1. Consideraciones de Contingencia

Prácticas para la planificación de contingencias de sitios Web incluyen las siguientes medidas:

- **Documento del sitio Web**. Documentar el hardware, el software y las configuraciones utilizadas para crear y alojar el sitio Web.

- Programación del sitio. Al igual que con otras aplicaciones, los sitios Web deben ser sometidos a pruebas exhaustivas en los servidores de prueba antes de la producción. Un programa de gestión de la configuración debe mantenerse, y los cambios deben estar documentados apropiadamente. Versiones aprobadas deberán ser grabadas en CDs para un fácil almacenamiento.

- **Sitio Web de codificación**. Un sitio Web está alojado en un servidor que se le asigna una dirección IP. Debido a que la dirección IP y el nombre de dominio pueden ser asignados al azar, el sitio Web no debe tener direcciones IP o nombres de dominio programados en el código. Si el sitio Web fue recuperado en un sitio alternativo, al servidor le puede ser asignada una dirección IP diferente. Si el sitio Web contiene direcciones codificadas de IP, nombres de dominio, o letras de unidad, la recuperación del sistema podría ser retrasada.

- **Coordinar soluciones de contingencia.** Con políticas adecuadas de seguridad y controles de seguridad. Un sitio Web es a menudo el punto de entrada de un hacker en la red de una organización. Así, el servidor Web y la infraestructura de apoyo deben ser protegidos a través de controles de seguridad fuertes. Las medidas de planificación de contingencia deben coordinarse con estos controles para garantizar que la seguridad no esté comprometida en la recuperación del sistema. Así, los controles de seguridad adecuados y los parches deben aplicarse en los sitios Web reconstruidos.

- **Coordinar con los procedimientos de contingencia soluciones de respuesta a incidentes**. Debido a que un sitio Web externo proporciona una imagen de la organización para el público, la imagen pública de la organización puede ser dañada si el sitio Web es afectado por un ataque cibernético. Para reducir las consecuencias de tal ataque, las soluciones de contingencia que figuran a continuación deberían coordinarse estrechamente con los procedimientos de respuesta a incidentes destinados a limitar los efectos de un incidente cibernético.

- **Utilizar los resultados del BIA.** Impactos y prioridades descubierto a través del BIA de las aplicaciones más importantes y sistemas de apoyo en general deben ser revisados para determinar los requisitos relacionados.

3.2. Soluciones de Contingencia

Las soluciones de contingencia deberían garantizar la fiabilidad y disponibilidad del sitio Web y sus recursos. El contenido presentado en las páginas dinámicas puede ser almacenado en un servidor distinto del sitio Web, como un servidor protegido detrás de un firewall. Así pues, a la hora de elegir las soluciones de contingencia para un sitio Web, la infraestructura de soporte del sitio Web debe ser considerada cuidadosamente. Además de los servidores, la infraestructura de apoyo podría incluir la red local que aloja el sitio Web.

Debido al número de solicitudes que los sitios Web podrían recibir y procesar, el balanceo de carga es una solución de contingencia popular.

4. REDES DE ÁREA LOCAL (LAN)

Una LAN es propiedad de una sola organización, puede ser tan pequeña como dos PC conectados a un solo eje, o puede soportar cientos de usuarios y servidores.

LAN también puede ser aplicado en dos arquitecturas principales:

- Peer-to-Peer. Cada nodo tiene capacidades y responsabilidades equivalentes. Por ejemplo, cinco computadoras pueden conectarse en red a través de un centro para compartir datos.

- Cliente / Servidor. Cada nodo en la red sea un cliente o un servidor. Un cliente puede ser un PC o una impresora, cuando un cliente se basa en un servidor de recursos. Una topología LAN, el protocolo, la arquitectura, y los nodos pueden variar dependiendo de la organización. Por lo tanto, las soluciones de contingencia para cada organización serán diferentes.

4.1. Consideraciones de Contingencia

- **Documentación de LAN**. El diagrama de LAN físico y lógico debe estar al día. El diagrama físico debe mostrar la disposición física de la instalación que alberga a la LAN, y los números de conector del cable deben ser documentados en el mismo. El diagrama lógico deberá presentar a la LAN y sus nodos. Los software de descubrimiento de red pueden proporcionar una imagen precisa de la LAN. Ambos diagramas ayudan al personal de recuperación a restaurar los servicios LAN más rápidamente.

- **Configuración del sistema e Información y Documentación del Distribuidor.** Documentación de configuraciones de la red de dispositivos de enlace que faciliten la comunicación LAN (por ejemplo, interruptores, puentes y concentradores) para una recuperación más rápida. Proveedores y su información de contacto debe ser documentada en el plan de contingencia para proporcionar el hardware y el reabastecimiento del sistema de software.

- **Coordinar las políticas de seguridad y controles de seguridad.** Las soluciones de contingencia para LAN, deben coordinarse con las políticas de seguridad de la red de protección contra las amenazas que podrían perturbar la red. Por lo tanto, al elegir la técnica adecuada de solución de contingencia, y los controles y las actividades relacionadas con la seguridad (por ejemplo, la evaluación del riesgo, la vulnerabilidad de

exploración) en los sistemas de producción, se debe garantizar que durante una interrupción de la red, la solución técnica no comprometa o revele datos sensibles.

- **Utilizar los resultados del BIA.** Impactos y prioridades descubiertos a través del BIA de las aplicaciones más importantes, y los sistemas de apoyo en general deben ser revisados para determinar las prioridades de la recuperación de LAN.

4.2. Soluciones de Contingencia

En el desarrollo del plan de contingencia para LAN, el Coordinador de Planificación de Contingencias debe identificar los puntos de falla que afectan a los sistemas críticos o procesos descritos en el BIA. Este análisis podría incluir amenazas para el sistema de cableado, tales como cortes de cable, los riesgos de interferencias electromagnéticas y de radiofrecuencia, y los daños resultantes de fuego, el agua, y otros. Como solución, los cables redundantes pueden ser instalados en su caso. Por ejemplo, no sería rentable instalar cables duplicados a los escritorios. Sin embargo, podría ser rentable instalar un cable de 100 megabits entre los pisos, de modo que los huéspedes en ambas plantas podrían ser vueltos a conectar si se corta el cable primario.

A menudo, no es rentable instalar cables duplicados a cada toma de ordenador. Sin embargo, cada toma de escritorio usualmente está equipada con al menos una toma de teléfono y una toma de ordenador. Cuando se instalan los cables, una organización puede elegir instalar un conjunto de tomas adicionales, y luego, si un problema se produce en un tramo de cable, un conector adicional a poca distancia estaría disponible como copia de seguridad. En este caso, el cable temporal se puede ejecutar desde el escritorio a la toma adicional para ofrecer conectividad para el escritorio hasta que un nuevo cable se pueda ejecutar a la toma de problema. Además, si el sistema de conectividad del teléfono se encuentra en la misma ubicación que los centros de columna vertebral, una toma de teléfono se puede convertir fácilmente en una toma de datos, si la toma de teléfono proporciona el ancho de banda adecuado.

La planificación de contingencia debe considerar también los dispositivos de red de conexión, tales como concentradores, conmutadores, enrutadores y puentes. El BIA debe caracterizar el papel que cada dispositivo tiene en la red, y una solución de contingencia debe ser desarrollada para cada dispositivo en función de su criticidad. Como ejemplo de una estrategia de emergencia para la conexión de dispositivos de red, routers redundantes de red inteligente pueden ser instalados, permitiendo a un router asumir la carga de trabajo total si el otro router falla.

El acceso remoto es un servicio proporcionado por los servidores y dispositivos en la LAN. El acceso remoto ofrece una comodidad para los usuarios que trabajan fuera de sitio o permite un medio para que los servidores y dispositivos estén comunicados entre los sitios. El acceso remoto se puede realizar a través de diversos métodos, como el acceso telefónico y red privada virtual (VPN). Si ocurre una emergencia o interrupción del sistema grave, el acceso remoto puede servir como una importante capacidad de contingencia mediante el acceso a los datos de toda la organización, tanto para los equipos de recuperación como para los usuarios. Si el acceso remoto se establece como una

estrategia de contingencia, los requisitos de ancho de banda deben ser identificados y utilizados a escala de la solución de acceso remoto. Además, los controles de seguridad tales como contraseñas y el cifrado de datos deben llevarse a cabo si la comunicación contiene información confidencial.

Redes de área local inalámbricas pueden servir como una solución de contingencia eficaz para restablecer los servicios de red luego de una interrupción de LAN cableada. Las redes inalámbricas no requieren la infraestructura de cableado de redes LAN convencionales, por lo tanto, se puede instalar rápidamente una solución provisional o permanente. Sin embargo, las redes inalámbricas transmiten los datos a través de una señal de radio, permitiendo a los mismos ser interceptados. Al implementar una red inalámbrica, los controles de seguridad, como encriptación de datos, deben aplicarse si el tráfico de comunicaciones contiene información confidencial.

Para reducir los efectos de una interrupción de la red LAN a través de la detección del sistema, software de monitoreo puede ser instalado. El software de control da una alerta si un nodo comienza a fallar o no responde. Además puede facilitar la solución de problemas y, a menudo proporciona al administrador un aviso antes que los usuarios puedan detectar el problema. Muchos tipos de software de monitoreo puede ser configurados para enviar una alerta electrónica a una persona designada automáticamente cuando un parámetro del sistema se sale de su rango de especificaciones.

5. REDES DE ÁREA EXTENSA (WAN)

Una red de área extensa (WAN) es una red de comunicaciones de datos que consta de dos o más LANs que se encuentran dispersas en una amplia zona geográfica. Enlaces de comunicaciones, por lo general proporcionada por un transportador público, permiten que una LAN interactúe con otras LAN.

Además de la conexión LAN, una WAN también puede conectarse a otra WAN, o puede conectar una red local a Internet. Los diversos tipos de enlaces WAN de comunicación incluyen los siguientes métodos:

1) De acceso telefónico. Pueden proporcionar un mínimo de transferencia de datos mediante una conexión de no permanentes. La velocidad dependerá de los módems que se utilizan, de hasta 56 kilobits por segundo (kbps).

2) Red Digital de Servicios Integrados (RDSI). RDSI es un estándar internacional de comunicaciones para el envío de voz, vídeo y datos a través de líneas telefónicas digitales o estándar. RDSI soporta transferencia de datos de 64 o 128 kbps.

3) T-1. T-1 es una conexión telefónica dedicada que soporta velocidades de datos de 1.544 Megabits por segundo (Mbps). Una línea T-1 consta de 24 canales individuales de 64 kbps, y cada canal puede ser configurado para llevar señales de voz o datos.

4) T-3. T-3 es una conexión telefónica dedicada que soporta velocidades de datos de alrededor de 43 Mbps. Una línea T-3 consiste de 672 canales individuales, cada uno de los cuales soporta 64 kbps.

5) Frame Relay. Frame Relay es un protocolo de paquetes para conectar dispositivos en una WAN. En frame relay, los datos se enrutan a través de circuitos virtuales. Redes Frame Relay soportan transferencia de datos a velocidades T-1 y T-3.

6) ATM. ATM es una tecnología de red que transfiere datos a altas velocidades con paquetes de tamaño fijo. Las implementaciones de soporte de datos ATM soportan tasas de transferencia de datos que van desde 25 hasta 622 Mbps.

7) Wireless (Inalámbricos). Un puente de LAN inalámbrico puede conectar varias LAN para formar una WAN. Las mismas soportan distancias de 20 a 30 millas con una línea directa de visión.

8) Red Privada Virtual (VPN). Una VPN es un canal cifrado entre los nodos de Internet.

5.1. Consideraciones de contingencia.

Las consideraciones de contingencia deberían aumentar la capacidad del personal de recuperación para restaurar los servicios WAN después de una interrupción. A continuación se mencionan algunas prácticas que complementan las estrategias de recuperación de la WAN que mencionaremos como soluciones de contingencia.

- **Documentación**. El diagrama de la arquitectura WAN debe mantenerse al día y debe identificar la conexión de dispositivos de red, direcciones IP, y los tipos de enlaces de comunicaciones y proveedores.

- **Documentación, configuraciones de sistemas y proveedores.** El plan de contingencia debe incluir una lista de proveedores para permitir la rápida sustitución de hardware, software y otros componentes de la WAN a raíz de una interrupción. El plan también debe documentar los proveedores de comunicaciones.

- **Coordinar las políticas de seguridad y controles de seguridad.** Las soluciones WAN de contingencia, deben coordinarse con las políticas de seguridad de la red para protegerla contra las amenazas que podrían comprometer la disponibilidad de la red. De este modo, al elegir la solución apropiada de contingencia, controles de seguridad similares y las actividades relacionadas con la seguridad (por ejemplo, evaluación de riesgos, el análisis de vulnerabilidad) en el entorno de producción, deberían aplicarse para garantizar que, durante una interrupción de la conectividad WAN, la ejecución de la solución de contingencia técnica no comprometa o revele datos sensibles.

- **Utilizar los resultados del BIA.** Impactos y prioridades descubiertos a través del BIA de las aplicaciones más importantes en general deben ser revisados para determinar los requisitos relacionados.

5.2 Soluciones de Contingencia

Las soluciones de contingencia para WAN incluyen todas las medidas discutidas para PCs, servidores, sitios Web, y redes de área local (LAN). Además, deben considerar los vínculos de comunicaciones que conectan las LAN dispares. Las estrategias de contingencia WAN están influidas por el tipo de datos enviados en la red. Una WAN que aloja una misión crítica en un sistema distribuido puede requerir una estrategia de recuperación más robusta que una red WAN que conecta varias LAN de recurso simple.

Las organizaciones deberían considerar las siguientes soluciones de contingencia para garantizar la disponibilidad de la WAN:

Enlaces de comunicaciones redundantes. Por lo general son necesarios cuando la red procesa datos críticos. Los enlaces redundantes podrían ser del mismo tipo, tales como dos conexiones T-1, puede además proporcionar un ancho de banda reducido para dar cabida sólo a las transmisiones críticas en una situación de contingencia. Por ejemplo, una línea RDSI puede utilizarse como un enlace de comunicaciones de emergencia para una T-1 primaria. Si se utilizan enlaces redundantes, el Coordinador de Planificación de Contingencias debe garantizar que los enlaces tienen una separación física y no siguen el mismo camino, de lo contrario, un solo incidente, como un corte de cable, podría interrumpir los vínculos.

Red redundante de proveeduría de servicios. Si se requiere el cien por ciento de disponibilidad de datos, los enlaces de comunicaciones redundantes pueden proporcionarse a través de múltiples proveedores de servicios de red. Si se opta por esta solución, el administrador debe asegurarse de que la solución no comparte atributos comunes en ningún punto.

Redundancia en Dispositivos de conexiones de red. Duplicar la conexión de dispositivos de red, como routers, switches y firewalls puede crear una alta disponibilidad en las interfaces LAN y proporcionar redundancia si un dispositivo falla. Duplicar los dispositivos también proporciona equilibrio de carga en rutas de tráfico.

Redundancia de NSP o ISP. El Coordinador de Planificación de Contingencias debe consultar con el NSP (Network Service Provider) seleccionado o con quien proporciona servicios de Internet (ISP) para evaluar la robustez y fiabilidad de sus redes básicas (por ejemplo, la conexión de dispositivos de red redundante y la protección de energía).

Para proporcionar redundancia adicional, conexiones a internet independientes pueden ser establecidas desde dos redes LAN separadas geográficamente. Si una conexión fallara, el tráfico de Internet podría ser encaminado a través de la conexión alternativa. Sin embargo, para aplicar esta estrategia debemos tener en cuenta el equilibrio que debe mantenerse entre seguridad y disponibilidad, no perdiendo de vista que conexiones a Internet múltiples incrementan la vulnerabilidad de una red.

6. SISTEMAS DISTRIBUIDOS

Los sistemas distribuidos se ejecutan cuando los clientes y usuarios están muy dispersos. Estos sistemas se basan en los recursos de LAN y WAN para facilitar el acceso de los

usuarios. Los elementos que componen el sistema de distribución requieren de sincronización y coordinación para evitar interrupciones y errores de procesamiento. Una forma común de los sistemas distribuidos es un gran sistema de gestión de base de datos (DBMS), que soporta las funciones de negocios en múltiples ubicaciones geográficas. En este tipo de aplicación, los datos se replican entre los servidores en cada lugar, y los usuarios pueden acceder al sistema desde su servidor local.

Un sistema distribuido es un conjunto interconectado de múltiples elementos de proceso autónomo, configurado para el intercambio y proceso de datos para completar una función de negocio única. Para el usuario, un sistema distribuido parece ser como un solo recurso. Sistemas distribuidos utilizan la relación cliente-servidor para que la aplicación sea más accesible a los usuarios en diferentes lugares.

6.1. Consideraciones de Contingencia

Las consideraciones de contingencia para sistemas distribuidos se basan en los conceptos discutidos para las plataformas anteriores. Debido a que el sistema distribuido se basa ampliamente en redes LAN y WAN las medidas de contingencia del sistema son similares al de las redes mencionadas.

- **Estandarización de hardware, software y periféricos.** La recuperación del sistema puede ser acelerada si hardware, software y periféricos están estandarizados en todo el sistema distribuido. Los costos de recuperación pueden ser reducidos, las configuraciones estándar podrán ser designadas y los recursos pueden ser compartidos. Los componentes estandarizados también reducen el mantenimiento del sistema a través de la organización.

- **Documentación de sistemas configuraciones y proveedores.** Documentación de la arquitectura de sistemas distribuidos y las configuraciones de sus diversos componentes. Además, el plan de contingencia debe identificar a los proveedores y especificaciones del modelo (de los equipos) para facilitar la rápida reposición de equipos después de una interrupción.

- **Coordinar las políticas de seguridad y controles de seguridad.** La solución de contingencia del sistema distribuido, debe coordinarse con las políticas de seguridad de la red donde los controles de seguridad similares y las actividades relacionadas con la seguridad (por ejemplo, evaluación de riesgos, el análisis de vulnerabilidad) en el entorno de producción deberían aplicarse en la solución de contingencia para garantizar que, durante una interrupción del sistema, la ejecución de la solución de contingencia técnica no comprometa o revele datos sensibles.

- **Utilizar los resultados del BIA.** Impactos y prioridades descubiertos a través del BIA de LAN y/o WAN deben ser revisados para determinar las necesidades de recuperación y prioridades.

6.2. Soluciones de Contingencia

Debido a que un sistema distribuido se extiende por múltiples lugares, los riesgos para el sistema y su infraestructura de apoyo deben ser analizados a fondo en el proceso BIA. Como se mencionó anteriormente, las estrategias de contingencia del sistema suelen reflejar la dependencia de la LAN y de la WAN. Basado en este hecho, para el desarrollo de una estrategia de contingencia de un sistema distribuido, las tecnologías a considerar son las siguientes:

- Sistema de copias de seguridad.
- RAID.
- Respaldo (redundancia) de los componentes críticos del sistema.
- Bóveda electrónica y diario remoto.
- Replicación de discos.
- Virtualización, NAS o SAN.
- Acceso remoto.
- Redes inalámbricas.
- Redundancia del sistema LAN.
- Redundancia del enlace de comunicación WAN.

Las soluciones de contingencia pueden ser incorporadas en el diseño y aplicación. Un sistema distribuido, por ejemplo, puede ser construido de manera que todos los datos residen en un lugar (como la sede de la organización) y se replica a los sitios locales. Los cambios en los sitios locales podrían ser replicados a la sede. Si los datos se replican en los sitios locales como de sólo lectura, los datos en el sistema distribuido están respaldados en cada sitio local. Esto significa que si el servidor de la sede falla, los datos aún se podían consultar en los sitios locales de la WAN. Por el contrario, si los datos se cargan desde los sitios locales al sitio sede, entonces el servidor de la sede actuaría como una copia de seguridad para los servidores locales.

Como ilustra el ejemplo anterior, el sistema distribuido normalmente proporciona algún nivel de redundancia inherente que puede ser incorporado en la estrategia de contingencia (si consideramos un sistema crítico que se distribuye entre una sede del organismo y una pequeña oficina). Suponiendo que los datos se replican en ambos sitios, una estrategia efectiva de recuperación puede ser establecer un acuerdo de reciprocidad entre los dos sitios. En virtud de éste, en el caso de una interrupción en una oficina, el personal esencial se trasladaría a la otra oficina con las funciones del sistema. Esta estrategia podría ahorrar gastos imprevistos importantes, evitando la necesidad de adquirir y equipar sitios alternativos.

7. SISTEMAS MAINFRAME

A diferencia de la arquitectura cliente-servidor, se centraliza la arquitectura mainframe. Los clientes que ingresan a los mainframe son terminales "tontas" sin capacidad de procesamiento. Las terminales tontas aceptan solamente salidas del mainframe. Sin embargo, las computadoras también pueden acceder a un ordenador central mediante un software de emulación de terminal.

7.1. Consideraciones de Contingencia

Aunque la computadora central es grande y más poderosa que las plataformas discutidas anteriormente, comparte muchos de los requisitos de contingencia. Por el hecho de que una unidad central utilice una arquitectura centralizada, no tiene la redundancia que un sistema distribuido o la red proporcionan. Como resultado, la disponibilidad del mainframe y las copias de seguridad de datos son críticos. Las siguientes medidas deben ser consideradas al determinar las necesidades de emergencia de un computador mainframe:

- **Respaldo de medios externos.** Los respaldos de los medios de comunicación deben ser etiquetados, registrados y almacenados fuera del sitio en un lugar seguro, en un medio ambiente controlado. La instalación de almacenamiento debe estar ubicada lo suficientemente lejos del sitio original para reducir la probabilidad de que ambos sitios se vieran afectados por el mismo evento.

- **Documentación de configuraciones del sistema y proveedores.** Mantener un registro detallado de las configuraciones del sistema mejora las posibilidades de recuperación del sistema. Además, los proveedores de hardware esencial, software y otros elementos deben ser identificados en el plan de contingencia.

- **Coordinación entre la red de seguridad común y el sistema de controles de seguridad.** Las soluciones de contingencia para los mainframes deben coordinarse con las políticas de seguridad de red, tales como los controles de acceso estrictos. Los controles de seguridad de red pueden ayudar a proteger contra los ataques que podrían comprometer la disponibilidad de los mainframes.

- **Utilizar los resultados del BIA.** Impactos y prioridades descubiertos a través del BIA de las aplicaciones más importantes, en general deben ser revisados para determinar las necesidades de recuperación y prioridades.

7.2. Soluciones de Contingencia

Los mainframes requieren diferentes estrategias de contingencia para los sistemas de distribución porque los datos se almacenan en un solo lugar. Las estrategias de contingencia deben hacer hincapié en las capacidades de almacenamiento de datos del mainframe y la arquitectura subyacente. Los componentes del sistema redundante son críticos para asegurar que un fallo de un componente, como puede serlo una fuente de alimentación, no cause un fallo al sistema. UPS (Unidades de Alimentación Eléctrica Permanentes) y sistemas de gestión también deben utilizarse para garantizar que la fluctuación de energía no afectará a la mainframe. Debido a que normalmente los mainframes procesan grandes aplicaciones críticas, un respaldo de largo plazo de energía puede ser necesario. Un generador de gas o diesel puede garantizar que el procesamiento de mainframe no es interrumpido por un corte de energía.

Debido a que cada arquitectura mainframe es única y centralizada, una estrategia de contingencia es contar con un sistema de reemplazo disponible en un sitio cálido o caliente suplente. Sin embargo, las plataformas de mainframe de copia de seguridad resultan muy onerosas para comprar y mantener, por eso algunas organizaciones comparten “sistemas comerciales”. Las organizaciones también suelen mantener los contratos de mantenimiento con el proveedor para reparar la unidad dañada. Sin embargo, el soporte del proveedor por sí solo no puede restablecer las funciones del sistema dentro del tiempo permitido de corte. En todos los casos, los acuerdos de servicios con proveedores deben mantenerse actualizados y revisados para garantizar que el proveedor proporciona el apoyo adecuado a las necesidades del sistema.

Copias de seguridad deberían hacerse con regularidad y, los medios guardarse fuera. Los respaldos y los planes de conservación deben basarse en la criticidad de los datos procesados y la frecuencia con la que se modifican los mismos. Además, la replicación de disco, o el uso de tecnologías NAS o SAN (que replican varias plataformas a una réplica del servidor), pueden ser útiles en algunos casos.

CAPÍTULO VI – LA CONTINUIDAD DEL NEGOCIO

ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS

Objetivo: contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios, de los efectos de fallas significativas o desastres.

Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, entre otros, desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas), así como también analizarse las consecuencias ocasionadas. Planes de contingencia deberán desarrollarse para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.

La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Proceso de Administración de la Continuidad de los Negocios

Debe implementarse un proceso que contemple los siguientes aspectos:

- Análisis de los riesgos a los que está expuesta la organización, su probabilidad de ocurrencia e impacto.

- Identificación y priorización de los procesos críticos de negocio.

- Importancia que puede tener una interrupción en los negocios.

- Elaboración y documentación de una estrategia de continuidad de los negocios.

- Elaboración y documentación de un plan de continuidad de los negocios alineada con la estrategia.

- Pruebas y actualizaciones del plan.

- Asegurar que la estrategia de continuidad de los negocios se incorpore a lo que es la organización.

CONTINUIDAD DEL NEGOCIO Y ANÁLISIS DE IMPACTO

Ésta etapa debe iniciarse por la identificación de eventos o situaciones que amenacen la continuidad de los negocios. Luego deben evaluarse los riesgos para intentar estimar el impacto de las posibles interrupciones. Es una evaluación que considera todos los procesos de negocio, no limitándose a las instalaciones de procesamiento de la información.

De acuerdo a lo que resulte de la evaluación, deberá proceder a desarrollarse un plan estratégico para determinar el enfoque con el que se abordará la continuidad del negocio.

ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES

Los planes deben desarrollarse con el objetivo de restablecer las operaciones en los plazos requeridos, una vez ocurrida la "situación de contingencia". En la etapa de planificación deben considerarse los siguientes aspectos:

- Identificación de todas las responsabilidades y procesos de emergencia.

- Establecimiento de procedimientos de emergencia que permitan la recuperación en los plazos requeridos.

- Documentación.

- Entrenamiento del personal en materia de procesos y situaciones de emergencia.

- Prueba y actualización de lo planes.

El proceso de planificación debe centrarse en los objetivos de negocio requeridos, por ejemplo establecer los servicios a clientes en un plazo aceptable.

MARCO PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS

Se debe mantener un solo marco, a fin de garantizar la uniformidad de los planes e identificar prioridades de prueba y mantenimiento.

Cada plan debe especificar con claridad las personas responsables de ejecutar cada parte, así como las condiciones de la puesta en marcha.

El marco debe tener en cuenta los siguientes puntos:

- Las condiciones de implementación, como ser qué personas están involucradas, cómo evaluar la situación, etc.

- Procedimientos de emergencia que describan las acciones a seguir una vez ocurrido un evento que haga peligrar al negocio o la vida humana. Esto debe incluir disposiciones respecto a la gestión de las relaciones públicas con las autoridades pertinentes, por ejemplo bomberos y autoridades locales.

- Procedimientos que describan las acciones a seguir en caso de que haya que trasladar actividades esenciales de la organización o servicios de soporte a ubicaciones alternativas.

- Procedimientos de recuperación, que describan las acciones a seguir para recuperar la operativa normal.

- Un diagrama de mantenimiento que especifique instancias de prueba y mantenimiento del plan.

- Actividades de capacitación y concientización.

- Responsabilidades y responsables de la ejecución de cada parte del plan.

PRUEBA, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES

Los planes pueden fallar al ser probados, ya sea por negligencia, suposiciones incorrectas, o cambios. De ahí la importancia de la realización de pruebas periódicas para garantizar que estén actualizados y sean eficaces.

Debe establecerse un cronograma de pruebas que indique cómo y cuándo debe probarse cada elemento del plan. Diversas técnicas deben utilizarse para garantizar que los planes funcionen en la realidad. Éstas deben incluir:

- Pruebas de discusión de diversos escenarios, discutiendo medidas para la recuperación del negocio con la utilización de ejemplos de interrupciones.

- Simulaciones enfocadas a entrenar al personal en sus roles durante y luego del incidente o la crisis.

- Pruebas de recuperación técnica (que garanticen que los sistemas de información puedan ser recuperados con eficacia).

- Pruebas de recuperación en un sitio alternativo.

- Pruebas de instalaciones y servicios de proveedores (que garanticen que los productos y servicios de proveedores externos cumplan con el compromiso contraído).

- Ensayos completos.

Mantenimiento y reevaluación del plan

Los planes de continuidad de los negocios deben mantenerse mediante revisiones y actualizaciones periódicas para garantizar su eficacia permanente.

Deben asignarse responsabilidades por las revisiones periódicas de cada uno de los planes de continuidad del negocio. Así es que si se identificaran cambios en el negocio aún no reflejados en los planes de continuidad, debe revisarse y proceder a la actualización del plan. Es un proceso formal (proceso de control de cambios) que debe garantizar que se distribuyan los planes actualizados, e imponga el cumplimiento de los mismos mediante revisiones periódicas de todos los planes.

Hay varios ejemplos de situaciones que podrían requerir la actualización de los planes:

- Adquisición de nuevo equipamiento.

- Actualización de los sistemas operativos.

- Cambios en:

a) Personal.

b) Direcciones y/o números telefónicos.

c) Estrategia de negocios.

d) Ubicación, instalaciones.

e) Legislación.

f) Contratistas.

g) Proveedores.

h) Clientes clave.

i) Procesos.

j) Riesgos (tanto operativos como financieros).

CAPÍTULO VII - TRABAJO DE CAMPO

Éste trabajo se abordó desde dos perspectivas.

Por un lado, investigando en el mercado local, se contactaron un número importante de empresas, a las que se le planteó la posibilidad de colaborar con nuestra investigación; muchas de ellas valoraban el esfuerzo realizado pero no estuvieron dispuestas a brindar información. Sí obtuvimos respuestas de once organizaciones, de las cuales adjuntamos resultado de la entrevista.

Por otro lado recopilamos el enfoque utilizado sobre ésta temática, por empresas consultoras especialistas en brindar soluciones en continuidad operativa.

ENFOQUE DE CONSULTORA W

ETAPA DE ORGANIZACIÓN DEL PROYECTO

La etapa inicial de este proyecto implica realizar una serie de actividades para la organización, asignación de recursos, programación de tareas, etc. para lograr la mejor puesta en marcha del proyecto:

- Presentación de los equipos.
- Validación de los roles de cada equipo.
- Revisión de los objetivos del proyecto.
- Establecer los requerimientos de participación individual y conjunta.

- Elaboración y validación de los planes de trabajo.
- Selección de los participantes de la organización para cada etapa.
- Organizar el cronograma de entrevistas y visitas a los puntos de alta criticidad.
- Proveer un formato para el relevamiento de la información clave requerida para iniciar el servicio.

ETAPA DE ANÁLISIS

La etapa de Análisis normalmente se inicia con el Análisis de Impacto al Negocio a través del cual se identifican los procesos críticos del negocio. Una vez identificados dichos procesos críticos, se identifican los recursos que los mismos utilizan para su ejecución, sea un centro de procesamiento, un edificio o un área administrativa. Esta etapa, si bien a priori parece muy sencilla, no lo es, puesto que en muchas organizaciones resulta ser una actividad compleja, debido a que no se tienen bien identificados los procesos críticos, e incluso en ocasiones a falta de una dirección firme y consciente, el personal tiende a considerar su propio trabajo como crítico.

ANÁLISIS DE RIESGOS (CUALITATIVO)

Descripción

El análisis de riesgos permitirá a la organización conocer su capacidad para afrontar y responder a situaciones que potencial o realmente afecten su capacidad de operar y mantener el nivel de servicio comprometido con sus clientes y/o con la organización, mediante la identificación de las amenazas, con una estimación de probabilidad de ocurrencia e impacto, que puedan afectar a los recursos del negocio y en consecuencia a su operación.

Es un análisis cualitativo, que asigna impactos leves, medios y altos a las potenciales amenazas a los activos de la empresa. Algunos de los puntos a ser revisados son: la ubicación física, la seguridad de los accesos, las políticas y prácticas corporativas y las

capacidades edilicias. El estudio también evalúa las medidas de seguridad y controles existentes, identifica los expuestos remanentes y recomienda las técnicas de mitigación para eliminar, transferir o reducir riesgos para aquellos que se califiquen como inaceptables.

Objetivo

El objetivo es evaluar los riesgos a los que está sometido cada uno de los puntos de alta criticidad en función de las amenazas y vulnerabilidades existentes, generando las recomendaciones aplicables.

Este estudio del ambiente físico de los puntos de alta criticidad se desarrolla con la finalidad de:

- Identificar y analizar la exposición a amenazas.
- Relevar la situación actual de los puntos de alta criticidad en materia de seguridad física.
- Evaluar las vulnerabilidades para amenazas cuya ocurrencia y magnitud derive en consecuencias inaceptables.
- Sugerir acciones adicionales de mitigación para salvaguardar dichos activos.

Este estudio habilitará al ente a tomar acciones de corto, mediano y largo plazo, que protejan su negocio de ciertos riesgos que, potencialmente podrían provocar una indisponibilidad de los Puntos de Alta Criticidad considerados, situación que podría implicar una interrupción o degradación en el volumen de operaciones, disponibilidad de procesos y/o información crítica u otras consecuencias, pudiendo afectar su nivel de servicio.

ANÁLISIS DE IMPACTO AL NEGOCIO

Descripción

Una vez realizado el Análisis de Riesgos recomendamos el Análisis de Impacto al Negocio, conocido como BIA. Este estudio identifica y evalúa los recursos y estima los impactos financieros y no financieros resultantes de la indisponibilidad de los procesos críticos que soportan las diferentes unidades de negocio.

El fin último del BIA es entender que sucedería en las unidades de negocio de la empresa, en el caso de un desastre.

El estudio consiste en examinar cada proceso de negocio, seleccionado por el cliente, e identificar sus procedimientos administrativos y tecnologías asociadas.

Este análisis identifica las interdependencias específicas entre los procesos de negocio, y de estos con los recursos disponibles de TI. Genera una visión de las vulnerabilidades y requerimientos de recuperación del negocio a nivel de la corporación para mitigar una interrupción prolongada.

En general, este análisis abarca:

- El tiempo máximo que un determinado proceso de negocio crítico pueda estar indisponible sin que impacte severamente a la compañía, según sus valores de RPO y RTO.

- El impacto sobre el negocio que pudiere generar una interrupción severa.

- Las prioridades en la recuperación de los procesos de negocio críticos, según sus respectivos grados de criticidad e interdependencias funcionales.

- Los registros de la empresa que son críticos para la recuperación exitosa de la operación del negocio.

- Los recursos requeridos para recuperar los procesos de negocio críticos, que incluyen al personal que se considere estratégico.

Objetivos

Los objetivos básicos consisten en:

- Brindar una visión estructurada sobre los procesos críticos del negocio relacionados con los puntos de alta criticidad.

- Identificar y cuantificar de acuerdo a los requerimientos del cliente, a las exigencias del mercado, regulaciones, etc., los respectivos niveles de criticidad de cada uno de los procesos identificados.

- Establecer las ventanas de recuperación de cada proceso de negocio crítico identificado (RPO y RTO).

- Determinar los recursos de personal, tecnológicos, de infraestructura y de oficina críticos para operación bajo contingencia.

- Contar con los elementos de juicio para decidir sobre la estrategia de recuperación y niveles de Servicio que se ajusten a los requerimientos del negocio.

ANÁLISIS DE LA CAPACIDAD ACTUAL DE RECUPERACIÓN (ACAR)

Descripción

En forma conjunta con los resultados del Análisis de Riesgo y del Impacto al Negocio, se analizará y evaluará la capacidad de recuperación actual de los puntos de alta criticidad definidos por el cliente.

Objetivo

Analizar y evaluar las diferentes capacidades de recuperación de recursos, que puedan ser aplicables a cada punto de alta criticidad seleccionado, abarcando:

- Identificar las interfaces y requerimientos de recursos críticos.

- Identificar los registros vitales.

- Identificar las facilidades de oficina requeridas para los puestos de operación y trabajo.

- Determinar el tiempo actual de recuperación y establecer el desvío con los plazos requeridos por el negocio.

RELEVAMIENTO DE NIVELES DE SERVICIO ACTUALES

En función de los resultados que arrojen las actividades realizadas a este momento del proyecto (Relevamiento Inicial, Análisis de Riesgos, Análisis de Impacto al Negocio y Análisis de Capacidad Actual de Recuperación), se relevarán los niveles de servicio que presenten en la actualidad los procesos y/o procedimientos de cada punto de alta criticidad, los cuales se podrían categorizar según una escala a definir.

No se diseñarán, en esta instancia, nuevos niveles de servicio, ni se desarrollarán modificaciones a los vigentes, tarea que quedará a cargo de la organización como parte de la implementación de mejoras.

Los niveles de servicio actuales se referirán a los que se hayan obtenido con respecto a la situación actual correspondientes a:

- Riesgos.
- Ventanas de recuperación.
- Recursos de recuperación.

Los 3 criterios de evaluación mencionados se utilizarán para establecer el nivel de servicio actual de un determinado punto de alta criticidad, cuyas conclusiones serán presentadas al cliente, para que la organización pueda conocer su estado actual.

DEFINICIÓN DEL NIVEL DE SERVICIO OBJETIVO

En este punto del proyecto, y con la información disponible, la empresa deberá establecer los niveles de servicio objetivo que concuerden con su política corporativa, estableciendo así la estrategia de la organización en esta materia.

Con los resultados de los niveles de servicio actuales determinados por los estudios previos, el nivel de servicio objetivo deberá ser expresado por el cliente en términos de:

- Niveles de aceptación, mitigación y/o transferencia de riesgos, que se determinarán sobre las respectivas matrices de riesgo de cada punto de alta criticidad.
- Ventanas de recuperación requeridas por un determinado punto de alta criticidad, con información dada por las matrices de impacto.
- Recursos adicionales, sobre la base de los análisis de capacidad actual de recuperación correspondiente a cada punto de alta criticidad.

La organización, en base a su Visión, Misión y Políticas Empresariales, deberá fijar los Niveles de Servicio Objetivo para cada Punto de Alta Criticidad, en base a valores o índices referidos a los 3 criterios utilizados que cumplan con sus objetivos de negocio.

Nuestra intervención en este punto será la de asesorar, sobre aspectos relativos a la definición de los niveles de servicio objetivo, teniendo en cuenta el cronograma propuesto.

La identificación de las posibles brechas entre los niveles de servicio actual y objetivo, dará paso a las siguientes etapas de Diseño e Implementación de las soluciones que permitan mantener la continuidad operativa a los niveles adecuados para la empresa.

DEFINICIÓN DE MÉTRICAS

El objetivo principal de los proyectos de Continuidad Operativa es el de relevar, evaluar y proponer las acciones que sean necesarias para mantener y/o mejorar el nivel de servicio actual que la organización brinda a sus clientes.

Para monitorear los resultados que resulten del desarrollo de este proyecto, se deberán establecer ciertos parámetros de comparación, que reflejen la evolución desde la situación actual hacia el futuro, mediante indicadores que representen atributos específicos.

Para ello se utilizarán los Indicadores Clave de Performance, también conocidos como "Key Performance Indicators" (KPIs), que consisten en una medida cuantificable para representar los factores de éxito de un programa, sistema o servicio que se lleva a cabo en una organización.

Las métricas se centran en las acciones (y resultados de dichas acciones) que las organizaciones implementan para reducir y administrar los riesgos (por ejemplo: deterioro de la reputación, robo de información o dinero, interrupciones de los procesos de negocio) que puedan surgir cuando las defensas de seguridad (y otras acciones) son vulneradas. Son herramientas útiles para los altos ejecutivos, gerentes, administradores y otras personas con responsabilidad en los objetivos y resultados del negocio.

Proponemos un esquema de métricas que evalúen varios aspectos de la continuidad operativa actual y futura del organismo:

- Un conjunto de métricas, tales como índices estadísticos, que se refieran a la evolución en el tiempo de los riesgos y vulnerabilidades.

- KPIs para Riesgos.

  En esta actividad del proyecto, se identificará la información histórica disponible en la empresa, que pudiere ser utilizada como punto de partida para la definición de las métricas, cuya evaluación se llevará a cabo al final del proyecto, y que una vez finalizado el mismo, la organización pueda continuar con su monitoreo, evaluación y control.

  En función de lo que resulte del estudio de Análisis de Riesgos, se propondrá un conjunto de métricas basadas en los indicadores de los Puntos de Alta Criticidad, los cuales se podrían referir a, sin que la presente enumeración sea taxativa:

- Estadísticas de eventos significativos que hayan impactado el nivel de servicio por punto de alta criticidad en un determinado período.

- Nivel de vulnerabilidad de las instalaciones de seguridad física.

- Nivel de vulnerabilidad de las instalaciones de servicios generales.

KPI para Continuidad y Recuperación

Objetivos

La aplicación de esta herramienta persigue varios objetivos:

- Proveer un método estandarizado de comparación de la gestión de continuidad del negocio.

- Permitir a la organización evaluar su competencia actual, su grado de madurez y su capacidad en administración de la continuidad del negocio.

- Permitir a la organización contar con una herramienta para la creación de un tablero de control de la evolución de los Indicadores Clave de Performance ("Key Performance Indicators" - KPI's) de su administración de continuidad del negocio.

- Identificar los desvíos y temas pendientes referidos a la competencia y capacidad de gestión de la continuidad del negocio de la organización.

- Trabajar sobre la provisión y priorización de los recursos para resolver dichos desvíos y asignaturas pendientes.

- Facilitar el conocimiento y la administración de los perfiles y apetitos de riesgo de la organización.

- Demostrar en forma clara y proporcionar evidencias específicas que la organización está cumpliendo con sus requerimientos y responsabilidades referidas a riesgos, exigencias legales y regulatorias y de gobierno corporativo.

ETAPA DE DISEÑO

PRIORIZACIÓN PARA LA MITIGACIÓN DE RIESGOS IDENTIFICADOS

Durante la etapa de análisis se identifican los principales riesgos que afectan a los puntos de alta criticidad. Como parte del estudio se señalan una serie de recomendaciones a fin de mitigar los mismos. En la etapa de diseño de nuestra metodología y con el conocimiento de la brecha que pudiere existir entre los Niveles de Servicio Actuales y

Objetivo respectivamente, se realiza una priorización de las recomendaciones de mitigación.

Esta priorización de las recomendaciones puede realizarse en base a diferentes criterios que se establecerán en forma conjunta con el cliente, como ser niveles de criticidad, costo/beneficio de su implementación, impacto, factibilidad de su implementación, etc.

La priorización de estas acciones se convertirá en la base para el desarrollo del Plan de Mitigación de Riesgos, el que será instrumentado mediante el Plan de Adquisiciones.

FORMULACIÓN DE ESTRATEGIAS DE RECUPERACIÓN

Descripción

En base a la brecha que se identifique en los Niveles de Servicio, y con el completo entendimiento de la situación actual de la organización obtenida a partir de los estudios de Análisis de Riesgos, Impacto al Negocio y Capacidad Actual de Recuperación, se elaborarán opciones de estrategias factibles para la recuperación de los recursos, que den respuesta a cada escenario de potencial pérdida, es decir la indisponibilidad de los Puntos de Alta Criticidad definidos por el cliente.

A esta altura del proyecto, se podrán presentar dos situaciones, que requerirán acciones diferentes:

- En caso que los niveles de servicio actual y objetivo coincidan, o sea, no exista una necesidad de mejora, se mantendrá la estrategia de continuidad y recuperación vigente, por lo cual no será necesario proponer nuevas opciones, y se iniciará en la etapa correspondiente el desarrollo del Plan de Recuperación de Recursos sustentado en dicha estrategia.

- Para los casos en que exista un requerimiento de mejora en el nivel de servicio, se construirán diferentes soluciones que puedan mejorar la capacidad de recuperación, y se evaluarán las mismas desde el punto de vista de rango estimado de inversión, esfuerzo requerido, tiempo de implantación, beneficios, limitaciones y complejidad entre otros.

Objetivo

Evaluar y diseñar las diferentes estrategias de recuperación de recursos, que puedan ser aplicables a cada Punto de Alta Criticidad seleccionado, teniendo en cuenta:

- Los niveles de servicio objetivo.

- Las interfaces y requerimientos de recursos críticos.
- Los registros vitales.
- Las facilidades de oficina requeridas para los puestos de operación y trabajo.

ETAPA DE IMPLEMENTACIÓN

Selección de soluciones de continuidad y recuperación

En esta etapa la organización deberá seleccionar las soluciones de continuidad y recuperación a implantar para cada uno de los Puntos de Alta Criticidad basadas en una de las opciones de recuperación. Las diferentes soluciones elaboradas en la Etapa de Diseño son comparadas y la empresa seleccionará las que serán implementadas.

Se define entonces la Estrategia de Recuperación para cada Punto de Alta Criticidad.

Esta selección de soluciones de continuidad y recuperación establecidas por la empresa se convertirá en la base para el diseño y desarrollo del Plan de Continuidad Operativa, que integrará a las siguientes categorías de planes:

- Plan de Administración de Crisis.
- Plan de Recuperación de Recursos para Puntos de Alta Criticidad.
- Plan de Evacuación para un determinado PAC y/o edificio.

Tanto la solución de recuperación seleccionada como los pasos de recuperación tendrán como premisa el logro de los niveles de servicio objetivo definidos previamente.

El Plan de Continuidad Operativa documentará la estructura organizacional encargada de llevar adelante la recuperación, así como los diferentes equipos que deben formarse en el momento de manejar una contingencia, identificando roles y responsabilidades e interrelaciones.

El Plan de Continuidad Operativa permitirá a la organización:

- Reaccionar, en caso de desastre, de acuerdo con la estrategia, los criterios y las pautas enunciadas en el plan.
- Acotar la cantidad de decisiones a tomar.
- Documentar los procedimientos que deberán seguirse.

DISEÑO DEL PLAN DE ADMINISTRACIÓN DE CRISIS

Descripción

El Plan de Administración de Crisis consiste en un documento que contiene las responsabilidades y acciones a seguir por las Gerencias de la empresa en caso de que ocurra un desastre en alguno de los puntos de alta criticidad definidos.

Este plan permitirá a la organización contar con un conjunto de definiciones realizadas en forma previa que habilitará a la alta dirección a:

- Tomar decisiones oportunas.
- Facilitar la recuperación.
- Manejar apropiadamente la imagen institucional frente a la ocurrencia de un evento imprevisto
- Manejar la crisis para contribuir en el cumplimiento de los Niveles de Servicio definidos.
- Gestionar los recursos excepcionales requeridos por la crisis.

PLANES DE RECUPERACIÓN DE RECURSOS PARA PUNTOS DE ALTA CRITICIDAD

Descripción

El Plan de Recuperación de Recursos consiste en un documento que se diseña basado en la Estrategia de Recuperación de Recursos seleccionada e implementada para proveer la continuidad operativa del punto de alta criticidad de acuerdo a los niveles de servicio objetivos previamente definidos.

Este desarrollo permite la organización del personal en equipos de respuesta y contar con los recursos y las actividades clave para lograr la continuidad operativa del punto de alta criticidad, ante un evento inesperado que implique una interrupción prolongada.

De esta forma el personal responsable del punto de alta criticidad podrá:

- Reaccionar, en caso de desastre, de acuerdo con la estrategia, los criterios y las pautas enunciadas en el plan.

- Acotar la cantidad de decisiones a tomar.

- Reanudar lo antes posible la operatividad del mismo de acuerdo a los procedimientos que se desarrollen al efecto.

- Identificar cuál es el personal propio y cuáles son los proveedores que deben participar en el proceso de recuperación.

- Identificar cuáles son los registros vitales a resguardar, así como también los componentes críticos para el correcto funcionamiento de la operativa del punto de alta criticidad.

PLANES DE EVACUACION

Objetivo

Dado que consideramos que el personal de la empresa es su activo más importante, el mismo debe contar también con un "plan de recuperación" en caso que se presentare una contingencia que pudiere poner en peligro su integridad física.

En consecuencia, está previsto desarrollar los Planes de Evacuación para los PAC (puntos de alta criticidad) y/o edificios que no cuenten con éste, y revisar los existentes.

GESTIÓN DEL CAMBIO: PLAN DE CAPACITACIÓN Y DE COMUNICACIÓN

El Plan de Continuidad Operativa es de valor limitado a menos que esté explícitamente documentado, claramente comunicado, comprendido y ejecutado fielmente por todos los que conforman la organización. Como parte de las actividades de implementación de las actividades de continuidad operativa, se considera la definición, diseño y ejecución de un plan de capacitación y comunicación a los participantes del proceso con respecto a la importancia de la continuidad de negocio en función del logro de las metas de negocio. Así, la implementación del proceso de capacitación se efectuará sobre la base de los roles que cada uno de los participantes debe desempeñar en su ejecución, abarcando el desarrollo de sesiones de entrenamiento, talleres de simulación y otros ejercicios que le otorguen al participante la destreza requerida para cumplir con sus responsabilidades en el proceso.

Para llevar adelante la implantación de una cultura de continuidad operativa en la empresa, nuestra solución utiliza metodología de Gestión del Cambio.

La Gestión del Cambio es un conjunto de actividades orientadas a encauzar las transiciones de las personas, la cultura y la organización para lograr que comprendan, acepten e implementen los cambios requeridos para alcanzar una mejora en el desempeño de la organización.

Basados en nuestra experiencia, observamos que este tipo de proyectos y cambios generan muchos interrogantes, que de no ser atendidos con un apropiado sentido de urgencia, transparencia, importancia y claridad, pueden convertirse en verdaderas resistencias en las personas. Por ello, es importante anticiparse a las interrogantes que puedan emerger en la implantación de los proyectos, responderlas oportunamente validarlas, anticiparlas y/o diluirlas si es necesario.

Descripción

Para esta etapa inicial en cuanto a la Continuidad Operativa de la organización, proponemos acciones de gestión del cambio orientadas a la sensibilización, formación, capacitación y entrenamiento, que se deben realizar para tener un impacto sobre los componentes del comportamiento, tanto en la parte cognoscitiva como en lo sensitivo/emocional.

Objetivo

El objetivo es generar conciencia de prevención y compromiso, a partir de la capacitación y comunicación a las personas involucradas.

ETAPA DE SOPORTE A LA IMPLANTACIÓN Y MANTENIMIENTO

La metodología de nuestra consultora, para el soporte a la implementación y el mantenimiento de los Planes de Continuidad Operativa prevé una serie de actividades como ser:

- Pruebas o simulaciones.

- Mantenimiento.
- Auditoria.

Las pruebas de los planes nos permiten demostrar que han sido debidamente documentados y que permitirán una adecuada recuperación de los recursos críticos en el caso de ocurrir un desastre en los puntos de alta criticidad.

Asimismo las pruebas permiten corregir desvíos y mejorar los planes para que solucionen los problemas que se hayan encontrado durante las mismas y asegurar que el personal se familiarice con el proceso de recuperación.

El mantenimiento debe hacerse de dos formas: permanente y periódico. Sobre una base permanente, para cualquier cambio en el ambiente se necesitarán mecanismos que permitan saber cómo se modificarán los planes para reflejar este cambio. Por cada nueva oficina que se instale, se deberá preguntar: ¿esta oficina es un punto de alta criticidad? y ¿cómo aseguramos la continuidad operativa de esta locación? En cada nuevo sistema informático que se desarrolle o instale, se deberá preguntar: ¿Deberíamos planificar recuperar esta aplicación? De ser así, ¿cómo? ¿cuáles son los cambios que deberíamos introducir en nuestro plan de recuperación recursos para posibilitar la recuperación?

Y, además, periódicamente se deberán revisar los planes en forma completa. Ambos mantenimientos, el permanente y el periódico, son igualmente importantes. Posiblemente existan deficiencias en el plan que cada uno de estos enfoques de mantenimiento reflejarán.

Dado el volumen de planes, actividades, equipos de trabajo e información involucrados, resulta imprescindible la consolidación de una oficina de proyecto que haga el seguimiento y de soporte metodológico a todas las tareas relacionadas con la continuidad operativa de la organización.

PROGRAMA DE PRUEBAS DE LOS PLANES DE CONTINUIDAD OPERATIVA

Descripción

Uno de los éxitos de la Continuidad Operativa de una organización es su capacidad de mantener o continuar con los procesos de negocio y servicios durante eventos inesperados, tales como desastres. Cuando los procesos de negocio y servicios críticos pueden seguir funcionando y operando, dentro de los parámetros establecidos de continuidad operativa, con independencia del tipo de evento, la organización habrá alcanzado la posición de “lista para la recuperación”.

Alcanzar este logro requiere planificación, definiciones, responsabilidades asignadas y aceptadas, pruebas y un respaldo gerencial en todos los niveles.

Objetivo

El objetivo es establecer, mediante una política de pruebas que fije guías claras referidas a la frecuencia, alcance, criterios de medición y comunicación de los resultados de los ejercicios el programa de actividades correspondiente.

Un programa de pruebas consiste en la planificación, administración, desarrollo y evaluación de diversos tipos de ejercicios, mediante los cuales se validen la estrategia y sus ventanas de recuperación, los procedimientos y el entrenamiento del personal.

Un programa de pruebas del Plan de Continuidad Operativa debe:

- Demostrar la viabilidad del Plan y de la estrategia de recuperación implementada, validando los Niveles de Servicio establecidos.

- Llevar a cabo un entrenamiento periódico de los integrantes de los Equipos de Recuperación y personal involucrado en el Plan.

- Educar a los nuevos ejecutivos y empleados que se vayan incorporando a los equipos de recuperación y personal involucrado en el plan.

- Proveer a los participantes el beneficio psicológico de estar preparados para llevar a cabo las tareas de recuperación durante una crisis.

- Promover el trabajo en grupo.

- Simular condiciones similares a una situación real de recuperación.

- Detectar posibles desviaciones o modificaciones en uno o más componentes que afecten los procedimientos del plan, identificando las revisiones y actualizaciones que requiera el mismo.

- Comunicar a los participantes qué actividades y tareas deben completar para que el ejercicio sea válido.

- Ilustrar sobre el valor de la totalidad del Programa de Continuidad Operativa.

- Proveer evidencias a terceros y auditores que la Continuidad Operativa es posible.

PROGRAMA DE MANTENIMIENTO DE LOS PLANES DE CONTINUIDAD OPERATIVA

Descripción

El Programa de Mantenimiento de los Planes de Continuidad Operativa es un documento que resume las actividades y tareas que se deban ejecutar para mantener su vigencia, en base a dos modalidades de trabajo:

- Permanente (generado por eventos que impacten el contenido de los Planes de Continuidad Operativa).

- Periódico (generado por revisiones en lapsos prefijados).

Objetivo

El mantenimiento de los Planes de Continuidad Operativa es de vital importancia, ya que permite asegurar la vigencia de los elementos a recuperar y de los procedimientos que gobiernan esta recuperación. Por lo tanto es necesario mantener actualizados los distintos capítulos y sus respectivas secciones y sincronizados con los cambios en el negocio. Es necesario también el control de los mismos para validar la ejecución y calidad del mantenimiento.

¿Por qué se debe mantener el Plan? Las razones se resumen en:

- Asegurar que el Plan considere y responda a los cambios que se produzcan en el negocio por medio de una revisión periódica.

- Incorporar permanentemente los cambios relacionados con los sistemas de información, a través del proceso de Administración de Cambios y Problemas.

- Mantener al personal familiarizado con el plan.

El objetivo principal del mantenimiento es no tener que volver a desarrollar el Plan. De hecho, un plan pobremente mantenido es peor que la ausencia total del mismo, porque el que existe no es exacto y puede conducir a elecciones erróneas.

Esto obliga entonces a:

- Identificar la necesidad de actualizaciones permanentes y revisiones periódicas.

- Definir las responsabilidades para el mantenimiento del plan.

- Desarrollar procedimientos para detectar alteraciones que deban figurar en el plan en base a modificaciones en el desarrollo de sistemas, cambios en el ambiente de producción, cambios en el personal, etc.

- Mantener el Plan.

- Probar el Plan

Esto es un ciclo continuo que se retroalimenta.

A modo de ejemplo se listan una serie de tópicos que deberán considerarse para el mantenimiento de los Planes de Continuidad Operativa:

- Procesos, prácticas y procedimientos operacionales documentados.
- Incorporación de nuevas actividades ejecutadas en el punto de alta criticidad.
- Cambios en los recursos utilizados en producción y para la recuperación.
- Nuevos controles de seguridad.
- Cambios en las prioridades de recuperación.
- Procedimientos de prueba del plan.
- Cambios de personal y sus asignaciones a los equipos de recuperación.
- Procedimientos de respuesta a la emergencia.

Debe trabajarse con un cronograma que asegure la revisión periódica del plan.

ENFOQUE DE CONSULTORA X

¿Por qué es necesario el desarrollo de un Plan de Contingencias?

Las organizaciones se enfrentan a una creciente exposición a nuevos riesgos y a una disminución de la tolerancia a las interrupciones en las operaciones, y es por ello que se hace necesaria la evaluación de sus capacidades para hacer frente a las crisis y mitigar los riesgos futuros. Las organizaciones deben aceptar el desafío de proteger a su gente y comprender que la habilidad pasa satisfacer a sus clientes de forma continua es fundamental pasa sostener su ventaja competitiva.

Si un desastre se presenta y una organización no puede recuperarse en un plazo prudencial, puede traer consecuencias como disminuciones en los ingresos, pérdidas de clientes, deterioro de la marca, pérdida permanente del valor de la empresa.

Tradicionalmente las empresas planeaban contra los desastres naturales o los ocasionados por el hombre, que interrumpían la producción, distribución o procesamiento de datos. Estas amenazas son cada vez más frecuentes y de mayor impacto.

Al mismo tiempo, las amenazas a los activos de información están haciéndose más significativas, independientemente del tamaño de las empresas. Los virus de computadoras, los problemas de seguridad de la información, la calidad del software, el almacenamiento de datos inadecuado y las prácticas inadecuadas de administración de activos de información, pueden abrir puertas a catástrofes e interrupciones con el mismo o mayor impacto para los negocios que los provenientes de amenazas físicas.

Por lo tanto parece ser que ahora la pregunta no es más “¿Cómo responder en caso de una crisis?”, sino, “¿Cómo administrar los riesgos de manera de siempre estar disponible para los clientes?”

El desafío es establecer una estrategia tomando en cuenta la totalidad de los riesgos, que garantice la seguridad de las personas, balanceando los costos de administración de los riesgos, con los costos de oportunidad de no tomar las acciones adecuadas.

METODOLOGÍA DE TRABAJO

El objetivo de un servicio de Administración de Continuidad del Negocio (BCM) es asistir a las organizaciones a obtener una certeza razonable de que sus plataformas tecnológicas son de alta disponibilidad, y que además son capaces de restablecer las operaciones críticas dentro de un lapso de tiempo aceptable luego de una interrupción de negocio o de sistema.

Los proyectos de BCM pueden desarrollarse en forma integral o a través de la descomposición en algunos de los siguientes temas:

- **Planificación de la recuperación ante Desastres**. Desarrollo de estrategias y planes que soporten la recuperación de los sistemas en caso de una interrupción. Provee la metodología para identificar y mitigar potenciales puntos de falla.

- **Desarrollo del Plan de Continuidad del Negocio**. Consiste en la elaboración de políticas y estrategias enfocadas en el restablecimiento de las funciones de negocio en caso de interrupción. Provee la metodología y herramientas para la realización de un análisis detallado del impacto en el negocio.

- **Alta Disponibilidad de Sistemas y Datos**. Implementación de componentes tecnológicos redundantes para asegurar la disponibilidad continua de sistemas críticos.

- **Administración de Niveles de Servicio**. Incorporar los requerimientos de disponibilidad y recuperación a los procesos diarios y los niveles de servicio.

En la administración de la continuidad del negocio, las interrupciones se anticipan y mitigan antes de que ocurran. Así, se consideran factores como el nivel de mitigación del riesgo requerido, la exposición actual al riesgo y los costos de mitigación del riesgo.

El Ciclo de Vida de la Administración de la Continuidad de los Negocios tiene cuatro fases:

1) Diagnóstico y Perfil de Riesgo

2) Desarrollo de Estrategias

3) Elaboración de Planes de Continuidad

4) Administración de la Implementación

FASE 1

Evaluación de Riesgos e Impactos en el Negocio (BIA)

La evaluación de riesgos consiste en identificar las potenciales amenazas o riesgos que pueden afectar a las funciones críticas del negocio. Evalúa la probabilidad de ocurrencia de cada amenaza, así como el impacto cualitativo y cuantitativo de la interrupción.

El BIA tiene como objetivo identificar a alto nivel los requerimientos de continuidad operativa de las funciones críticas del negocio.

Actividades:

- Identificar para cada unidad de negocio, los procesos, funciones y/o servicios de alta criticidad que deben tener un alto nivel de continuidad y resistencia.

- Identificar los activos de alta criticidad, como ser personas, equipos, facilidades, aplicaciones de TI, etc., utilizados por el negocio; así como estimar los requerimientos de recuperación mínimos en caso de desastre.

- Evaluar los riesgos que pueden afectar a éstos recursos y su probabilidad de ocurrencia.

- Comparar los tipos de riesgos y priorizar.

- Determinar la probabilidad de ocurrencia de una interrupción de las funciones de negocio a través de la probabilidad de ocurrencia de los riesgos asociados.

Se lleva adelante un enfoque “top-down” con lo que se apunta a facilitar la determinación de los factores claves de éxito para la organización, así como la estimación del impacto en el negocio que puede ser experimentada ante una interrupción.

Comenzar el BIA con una perspectiva de la alta dirección permite validar el nivel de conciencia sobre riesgos e inculcar una misión y visión de una administración efectiva de la continuidad del negocio.

Niveles de servicio objetivo

Consiste en determinar los requerimientos de continuidad operativa para cumplir los niveles de servicio objetivo (tiempo y punto de recuperación objetivo), basados en métricas e indicadores.

Deben establecerse niveles de servicio objetivo para cada riesgo identificado.

Análisis de brecha

El objetivo de este apartado es evaluar el impacto tanto cuantitativo como cualitativo de la interrupción del negocio. Pueden establecerse también penalidades por no conformidad con las reglamentaciones, perdida de oportunidades o el impacto negativo en la satisfacción del cliente.

La identificación de las funciones críticas del negocio permite priorizar los recursos financieros y humanos asignados a los requerimientos de continuidad operativa.

Actividades:

- Revisar la capacidad actual de continuidad (resistencia a fallas y capacidad de recuperación) y su eficiencia en la reducción del nivel de exposición.

- Posteriormente, este proceso permitirá desarrollar las estrategias de continuidad (mitigación, recuperación) para los procesos, funciones y activos clave, enfocándose en eliminar o mitigar la exposición al riesgo o mejorar la capacidad de recuperación.

FASE 2

Estrategia del equipo de trabajo

En este modulo se determinaran los roles y responsabilidades requeridos, así como las competencias a desarrollar para cumplirlos adecuadamente.

Los altos ejecutivos de la empresa y los líderes de las unidades de negocio son los responsables de las políticas generales, toma de decisiones y la comunicación del programa de BCM en sus respectivos ámbitos. Utilizando el mismo enfoque que la continuidad del negocio podemos decir que los líderes son los responsables de la "resistencia" de su área. Los beneficios y costos de su unidad son sopesados contra los requerimientos de recuperación de la misma.

BCM es una disciplina basada en riesgos y usa un criterio de análisis similar.

Las principales decisiones a cargo del equipo de BCM incluyen:

- Políticas: determinar estándares, reglas y protocolos requeridos, así como los principios operativos de BCM.

- De monitoreo y control: determinar cómo deben ser los reportes periódicos de avance y las revisiones; acciones correctivas que deban tomarse; establecer cómo se asegura la organización que las correcciones son realizadas.

- Conformidad con normas: ¿Que procesos deben implementarse para asegurar la conformidad con estándares y obligaciones?

- Asignación de capital: ¿Como deben asignarse eficientemente los limitados recursos? ¿Que capital esta disponible como inversión? ¿Que procesos se deben utilizar para revisar los gastos?

- Planeamiento: Determinar que debe incluir la estrategia de recuperación. ¿Cuales deberían ser los objetivos de recuperación de TI?

Estrategia de asignación de recursos

El personal y otros recursos requeridos para la ejecución de los procesos críticos deben poder ser asignados de manera tal que frente a un desastre en cualquier sitio (ubicación del negocio) no dificulte la capacidad de la empresa de ejecutar sus funciones críticas.

Actividades:

- Identificar las funciones críticas del negocio (resultado del análisis BIA).
- Tiempo de recuperación objetivo: ¿Cuando las funciones deben estar "up and running" para soportar los procesos críticos?
- Determinar el número suficiente de personal.
- Desarrollar las vías para que la gerencia pueda tomar las decisiones de asignación.
- Selección del criterio para la reasignación de los recursos después de la crisis
- Administración de los riesgos claves del personal.
- Evaluación de personal adicional que pueda ser requerido.
- Comunicación, coordinación y entrenamiento.
- Determinar la estrategia de asignación por tipo de recuperación (instantánea, demorada).

Estrategias de recuperación técnica y del trabajo

Las estrategias de recuperación técnica y alta disponibilidad buscan mitigar los posibles riesgos identificados y reducir el tiempo de recuperación ante la interrupción del servicio. Tales estrategias dependerán de los niveles de servicios deseados.

Este análisis permitirá posteriormente adquirir los recursos necesarios para mantener los niveles de continuidad requeridos.

Actividades:

- Confirmar los requerimientos de continuidad obtenidos en el BIA.

- Estimar los costos de las alternativas evaluadas.
- Comparar el costo con el beneficio de la mitigación.
- Determinar estrategias de recuperación

Estrategias de comunicación y capacitación

Tiene como objetivo generar una conciencia de la importancia de la correcta administración de la continuidad del negocio en la empresa y en el equipo de BCM. Equiparlos de herramientas y la información que necesitan en caso de interrupción del negocio

Actividades:

- Establecer procesos de comunicación
- Analizar la infraestructura actual de capacitación.
- Desarrollar una guía de introducción al lenguaje de BCM.
- Desarrollar un conjunto de herramientas de capacitación en continuidad del negocio.

FASE 3

Plan de administración de crisis

Consiste en administrar la coordinación integral y global de la respuesta de la organización a la interrupción del negocio en tiempo y forma, con el objetivo de evitar o minimizar daños a la rentabilidad, reputación o habilidad de operar de la organización.

Esto incluye el establecimiento de una cadena de comando para incidentes que permita la efectiva toma de decisiones.

Se determinan roles y responsabilidades específicos y una clara estructura de reporte a seguir ante y durante el siniestro.

Actividades:

- Formar un equipo de administración de crisis con roles y responsabilidades claramente definidas.
- Diseñar e implementar un detallado plan de comunicaciones y acciones de respuesta al siniestro.

- Asegurar que las estrategias de respuesta al siniestro se mantengan eficientes con los cambios del negocio.

- Asegurar la disponibilidad de recursos.

- Formar conciencia dentro de la organización de la necesidad de un plan de administración de crisis.

Plan de Continuidad (BCP) y Recuperación de desastres (DRP)

A) Planes de continuidad y recuperación de las unidades de negocio.

Estos planes proveen el detalle de actividades a realizar para evitar la interrupción o para recuperar los recursos y servicios críticos de las unidades de negocio.

El proceso normalmente incluye los siguientes pasos:

1) Respuesta inmediata.

2) Recuperación ambiental.

3) Recuperación funcional.

4) Sincronización de datos.

5) Restauración de las funciones de negocio.

6) Sitio interino.

7) Retorno a situación normal.

Estos planes surgen de los procesos críticos del negocio.

B) Planes de recuperación de las aplicaciones de Sistemas.

Documenta los procedimientos a seguir ante una interrupción de TI y provee los pasos necesarios para minimizar el impacto en los procesos críticos de la organización.

Estos planes se orientan a la recuperación de las aplicaciones necesarias para llevar a cabo los procesos críticos de negocio, dentro de cada unidad. En estos se determinan como deben ser recuperados y reactivados los datos de la aplicación.

El plan de recuperación de aplicaciones sincroniza la tecnología (TI) con los requerimientos de negocio.

El plan incluye:

- Procedimientos de respaldo y restauración (backup, restore).
- Procedimientos de sincronización de datos.

C) Planes de recuperación de la infraestructura tecnológica.

Estos planes describen como se resguardan las configuraciones de hardware, software, redes, comunicaciones y otros recursos tecnológicos clave. Determinan como recuperar dichas configuraciones en caso de emergencia.

El plan contiene:

- Equipos de trabajo y responsabilidades.
- Lista de contactos de emergencia.
- Procedimientos de respaldo y restauración.
- Instalación de nuevos sistemas.
- Reemplazo del sistema existente.
- Plan de entrenamiento del equipo de trabajo.

Plan de recuperación del trabajo (WRP)

Provee los pasos detallados a seguir en la recuperación de los procesos clave de negocio. Busca ser una guía flexible para ser invocada en caso de una importante interrupción del negocio. Contiene los pasos a seguir para proteger la viabilidad del negocio proveyendo alternativas de ejecución de los procesos cuando el procesamiento normal no es posible.

Estos planes se basan en el perfil de riesgo de la empresa, el valor relativo de cada proceso y las opciones de recuperación disponibles dentro del presupuesto. La determinación de estas prioridades permite un BCM más eficiente, enfocado en la implementación de estrategias de recuperación para los procesos más críticos.

Generalmente se ordenan los procesos en bandas: siendo la banda 1 el 10 % de los procesos que deben ser soportados inmediatamente.

Actividades:

- Confirmar los procesos para el desarrollo del WRP.
- Confirmar las funciones críticas de cada proceso.
- Confirmar los elementos del BIA relevantes para el WRP.
- Identificar y formar al equipo de trabajo.
- Normalizar los datos y hacerlos de conocimiento en todas las unidades de negocio.

Plan de prueba

Busca llevar adelante la simulación de los planes y procedimientos de continuidad del negocio.

Actividades:

- Coordinar una programación de actividades que incluya todos los planes aplicables.
- Crear una programación detallada para cada plan.
- Determinar escenarios de prueba.
- Determinar los participantes.

FASE 4

Establece los lineamientos de cómo se llevara adelante la implementación del plan de continuidad. Esto implica adaptar las actitudes y aptitudes de las personas en la

organización para lograr el objetivo, sin perder de vista que involucrará a toda la organización.

Es necesario que la organización este preparada para adaptarse rápida y efectivamente a las nuevas situaciones.

ENFOQUE DE CONSULTORA Y

¿Por qué es necesario garantizar la Continuidad del Negocio?

La realidad actual pone a prueba a las organizaciones en relación a su capacidad de satisfacer las demandas de sus clientes, cumplir con los requerimientos de sus socios de negocio y adaptarse a las nuevas tecnologías y la realidad de sus mercados de manera eficiente y eficaz. Ésta situación se puede traducir en un medio ambiente muy dinámico y competitivo, en el cual es difícil mantener o lograr tener una ventaja competitiva.

Por eso, tener éxito en éstos aspectos está relacionado con las habilidades que puedan desarrollar las organizaciones para asegurar la continuidad en la prestación del servicio de manera satisfactoria.

La Continuidad Operativa es una característica de calidad muy relevante, ya que una interrupción en la misma puede tener un impacto importante con repercusiones económicas y de imagen para la organización.

Por ello es que contar con una solución puede significar un importante diferencial en materia de calidad de servicio y reforzaría además la imagen de solidez organizacional.

PREVENIR VS REMEDIAR

Al momento de determinar que hacer frente a un siniestro que pueda significar una interrupción no deseada de las operaciones de la organización surgen dos enfoques:

- Prevenir la ocurrencia del siniestro.

- En caso de ocurrencia, contar con un sistema de respuesta que permita restablecer la operativa a un nivel adecuado y en un lapso de tiempo aceptable.

Ambos aspectos son necesarios y complementarios a la vez; pero la implementación de medidas preventivas puede permitir la minimización de hechos que puedan interrumpir la continuidad del negocio. La prevención es más importante para aquellas actividades que son más difíciles de contar con medidas de respuestas previamente definidas.

De ésta forma, la definición de un Plan Preventivo se debe focalizar en mitigar aquellos riesgos que pueden significar pérdidas importantes a las empresas, y que les resulte beneficioso desde el punto de vista económico, ya que el costo de prevenir (costo de desarrollo y mantenimiento de un plan preventivo) en teoría, debe ser menor al que se incurriría en caso de contingencia (el de preparación y puesta en práctica de las medidas de respuesta y las perdidas asociadas)

A pesar de lo antes mencionado, trabajar solo en prevenir no es del todo correcto, atribuimos a esto las siguientes razones:

- Es imposible asegurar que se han identificado todos los posibles orígenes de continencias

- Hay riegos que no es rentable prevenir

- Aunque el Plan Preventivo sea excelente, sigue siendo preventivo, y las contingencias igual pueden suceder

Por esto es que es necesario el desarrollo de un plan que permita asegurar la recuperación de la actividad crítica de la empresa ante cualquier suceso que pueda provocar una interrupción en las operaciones de la organización, ya sea que esté previsto o no. Puede pasar también que la contingencia sea tal que obligue a la empresa a trabajar a un nivel operativo por debajo del previamente aceptado.

COMPONENTES DE UNA SOLUCIÓN DE CONTINUIDAD

Una solución de continuidad operativa adecuada debe permitir la recuperación de todos los procesos críticos del negocio, no solo su soporte informático y/o tecnológico, asegurando a su vez que protege la integridad de las personas y activos de la empresa, así como la salvaguarda de su imagen y reputación. Por ello es que las acciones de respuesta frente a contingencias pueden ser de naturaleza muy variada, por ejemplo:

- Procedimientos de evacuación.

- Administrar una crisis y mitigar su impacto.

- Gestionar las Comunicaciones hacia fuera de la organización (terceros interesados, ej. Los medios de prensa)

- Reubicación del personal.

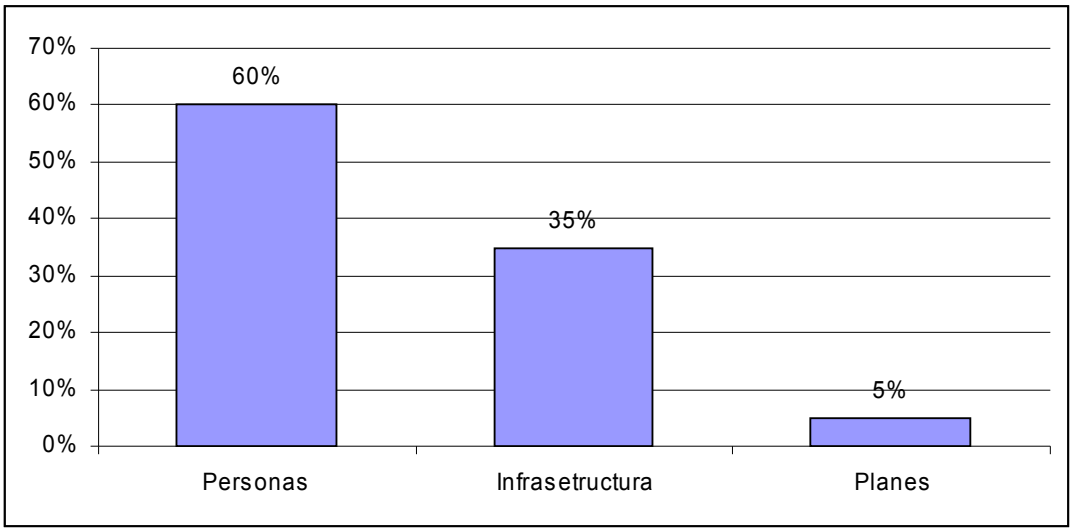
- Eventual cambio en los medios de atención al cliente
- Etc.

Como se ve, hay que estar "preparado para todo", tener todo previsto, desde la evacuación del edificio, hasta en caso de siniestro, quien va a ser el encargado de comunicar el suceso hacia el exterior de la organización. Lo que resulta evidente es que en las diferentes estrategias de recuperación que puedan existir, la tecnología juega un rol importantísimo.

Una cosa fundamental es nunca perder de vista la relación costo-beneficio de las posibles medidas a adoptar.

Para lograr una solución real frente a éste tema no basta solo con desarrollar un buen Plan de Contingencia, si no que hay que considerar otros 2 factores no menos importantes entre sí, por un lado la participación y el compromiso de los involucrados en los procesos del plan; y por el otro disponer de la infraestructura adecuada para sustentar los procedimientos establecidos en el plan.

La incidencia que pueden tener esos factores en el éxito de un plan de contingencias, la podemos esbozar de la siguiente manera.



PERSONAL

Son factores clave, contar con personal no solo capacitado, si no comprometido con las tareas que tienen que ver con responder ante una contingencia y con las acciones a seguir en caso de ser necesario. Por otra parte hay que buscar el no depender de ciertas personas para la ejecución de las medidas, para ello es necesario definir grupos de respuestas, para los cuales es necesario determinar las funciones y responsabilidades, así como el nivel de autoridad requerida para llevar adelante sus tareas. Si bien el "armado"

de esos equipos es responsabilidad de la organización, hay ciertos criterios que es recomendable seguir para llevar adelante esa tarea, como ser:

- Habilidades, conocimiento y experiencia sugeridos para los integrantes de cada equipo en función de sus responsabilidades.
- Existencia de líneas de reporte y mando claras.
- No colisionar con la estructura organizativa de la empresa, sin descuidar la flexibilidad que otorga el concepto de equipos de trabajo.
- Restricciones de acceso y confidencialidad respecto a la información que cada equipo maneja.
- Compromiso del personal.

INFRAESTRUCTURA

Se refiere tanto a la estructura edilicia, así como a los elementos tecnológicos y no tecnológicos, y demás recursos necesarios para mantener y llevar adelante los procesos del plan.

PLANES

Planes que permitan hacer frente a una crisis, enfocados en asegurar la integridad de las personas y bienes de la organización; planes enfocados en recuperar la operativa del negocio, y mantenerla durante el período de contingencia, así como la ejecución de la vuelta a la normalidad en forma ordenada; planes que es necesario ejecutar para poder restablecer y mantener el soporte informático y tecnológico en general, requerido por el negocio para recuperar su capacidad operativa, y mantenerla durante el período que se prolongó la contingencia y su vuelta a la normalidad.

BENEFICIOS QUE PUEDE BRINDAR EL DESARROLLO DE UNA SOLUCIÓN DE CONTINUIDAD OPERATIVA

- Contar con medidas preventivas que permitan mitigar aquellas situaciones de riesgo que comprometen la operativa crítica de a organización.

- Lograr una detección oportuna de situaciones que puedan colocar a la empresa en una situación de contingencia.

- Lograr un nivel de preparación frente a incidentes tal que permita asegurar que se puede proteger la integridad de las personas y bienes de la organización de manera adecuada.

- Frente a cualquier contingencia, de cualquier magnitud, tener la capacidad de recuperar el nivel operativo definido como mínimo aceptable dentro del tiempo establecido.

- Minimizar las decisiones a tomar en caso de contingencia para evitar cometer errores.

- Minimizar el impacto de imagen negativo, y/o las pérdidas económicas, derivados de una interrupción en sus operaciones, a través de una respuesta rápida y adecuada.

- Planificar interrupciones puntuales de ciertos servicios en caso que lo estime necesario, conociendo como va a responder la organización, el nivel de respuesta a obtener, cómo se vería afectado el servicio, y eventualmente las pérdidas asociadas. Por ejemplo, si hubiera necesidad de refaccionar un local, ya estaría planificado dónde pueden operar las áreas afectadas y cómo.

OBJETIVOS Y ALCANCE DE ÉSTE TIPO DE TRABAJOS

Objetivos Primarios

- **Elaborar un plan preventivo**, cuya implementación permita minimizar la posibilidad que la organización se vea en una situación de contingencia, teniendo en cuenta que se mantenga una relación costo-beneficio para cada una de las medidas que formen parte del plan, respecto a la situación de no prevenir y tener que responder en caso de materializarse el riesgo en cuestión.

- **Elaborar una Solución de Continuidad Operativa**, que permita en primer lugar, detectar cualquier situación de contingencia, y en caso de que ocurra, asegurar la recuperación de las principales funciones de la organización, dentro de los parámetros de tiempo y calidad que se definan, sin dejar de prestar servicios a los clientes. En aquellos casos que la contingencia sea muy grande, el plan debe también incluir las acciones a seguir para salvaguardar la integridad de las personas que puedan verse afectadas (en primer lugar), y en segundo lugar, salvaguardar los activos de la organización. A su vez dentro de éste objetivo primario hay ciertos objetivos particulares que se persigue:

  - Instrumentar las acciones requeridas para administrar las crisis en caso de contingencia importante que adquiera la dimensión de desastre, priorizando lo relativo a la

seguridad de las personas y los activos de la organización (incluyendo especialmente la información).

- Administrar todo tipo de comunicaciones que deriven de la situación de contingencia, con los funcionarios, socios de negocio, clientes y el público en general.

- Minimizar las pérdidas, reduciendo la posibilidad de cometer errores y el tiempo de recuperación de las principales funciones de la organización, y del soporte informático /tecnológico que las mismas requieran, y que permita alcanzar un nivel operativo mínimo aceptable. En éste sentido se considerarán procesos críticos aquellos cuya interrupción puedan provocar pérdidas importantes tanto desde el punto de vista de imagen como económico, o coloquen a la empresa en una situación de incumplimiento respecto a la normativa interna o externa vigente.

- Administrar la operativa crítica durante el período de contingencia.

- Guiar la evaluación detallada de la situación para iniciar tareas de reconstrucción y/o reparación del origen de la interrupción.

- Planificar la vuelta a la operativa normal.

Objetivos Secundarios

- **Definir un Plan de Acción** para implementar el plan preventivo y la solución de continuidad operativa.

- **Definir los Equipos de Respuesta** necesarios para instrumentar la solución.

- **Capacitar al Personal** que participe en el desarrollo, mantenimiento, y eventual ejecución de la solución de continuidad operativa.

- **Elaborar un Plan de Pruebas** que permita verificar en forma periódica la adecuación de la solución de continuidad operativa.

- **Elaborar un Plan de Mantenimiento**, ya que son muchos los cambios que una empresa puede sufrir que impacten en su solución de continuidad operativa, como ser: creación/eliminación de unidades de negocio, cambios en el organigrama, cambios en el soporte tecnológico (tanto desde el punto de vista de la estructura del hardware como del software de aplicación), cambios en la estrategia de la organización, entre otros.

- Lograr el **Compromiso** de los funcionarios involucrados en el desarrollo y ejecución de la solución de continuidad.

ALCANCE

Aquí vamos a analizar tres puntos, a saber: Alcance del Plan Preventivo, Alcance de la Solución de Continuidad operativa, y Alcance de las tareas de soporte a la implantación.

Alcance del Plan Preventivo

Identificación de los riesgos

Se procederá a identificar aquellos riesgos frente a los cuales la organización tiene un grado de exposición importante, siendo más rentable trabajar en prevenir su ocurrencia, que tener que responder en caso de que efectivamente ocurran.

El análisis debe ser exhaustivo hacia todas las amenazas relativas a la seguridad física, lógica y ambiental, que puedan exponer una debilidad que presente la organización.

Medidas de Mitigación

El plan se elaborará en base a las medidas recomendadas para mitigar los riesgos mencionados anteriormente. Las recomendaciones se presentarán en relación al riesgo asociado según el nivel de criticidad, y al costo estimado de implementación.

Plan de monitoreo

Se deben identificar asimismo procedimientos para evaluar los controles establecidos a fin de poder probar su efectividad.

Capacitación

El personal debe capacitarse a fin de poder ejecutar las medidas de monitoreo establecidas. Parte de esa capacitación debe estar referida a la administración de riesgos en general y el resto a procesos específicos que formen parte del plan de monitoreo.

Alcance de la Solución de Continuidad Operativa

Se consideran 5 dimensiones: 1) Tipos de contingencias consideradas, 2) Desde la perspectiva de los procesos a recuperar, 3) Desde las perspectiva de las distintas etapas asociadas a una contingencia; 4) Desde la perspectiva de los edificios; 5) Desde la perspectiva de los componentes de la solución de continuidad.

1) La solución debe contemplar, debe proveer una respuesta adecuada a cualquier interrupción a los procesos críticos de la organización, de cualquier naturaleza y que no puedan ser resueltos aplicando los procedimientos habituales.

2) Se contemplará la recuperación de todos los procesos que se definan como críticos para la organización, con independencia de donde se lleven a cabo así como su naturaleza, por ejemplo procesos vinculados a la atención a los clientes, servicios de TI, etc. En líneas generales se puede decir que un proceso es crítico cuando su interrupción puede ocasionar a la empresa pérdidas directas o indirectas que ésta no esta dispuesta a asumir, coloca a la organización en una situación de incumplimiento y/o pérdida de imagen.

3) La solución debe contemplar varios aspectos: una detección oportuna de situaciones que puedan derivar en una contingencia que ponga en peligro la continuidad del negocio, dar una evaluación preliminar en forma rápida de manera de poder facilitar la decisión de poner en marcha el plan de contingencia, y en caso de hacerlo, que acciones seguir; en caso de que la contingencia sea de una importancia/magnitud tal que adquiera la característica de crisis, que medidas seguir para su administración (éstas tienen por objetivo contener el impacto de la crisis con una respuesta oportuna que permita proteger la integridad física tanto de las personas como de los bienes de la organización, y la realización de un buen manejo de las comunicaciones internas y externas). Particularmente para este último punto se debe tener previsto un plan de evacuación de edificios.

Otros aspectos no menores que deben también considerarse son: acciones para poder recuperar y volver a ejecutar los procesos críticos (en los tiempos que se establezcan y con el nivel operativo deseado); incluir procedimientos alternativos para ejecutar los procesos una vez recuperados y mientras dure el régimen de contingencia; establecer los procedimientos a seguir para recuperar el soporte informático-tecnológico que brinda soporte a los procesos críticos; incluir las acciones a seguir para solucionar el incidente que dio lugar a la interrupción; y por último se deben incluir las acciones a seguir para la planificación y vuelta a la operativa normal.

4) Algunas acciones incluidas dentro del plan de contingencias dependerán de las ubicaciones físicas donde se desarrollan las actividades y/o procesos que se desean recuperar.

5) En éste sentido la solución debe incluir:

- Planes de Contingencia, que serán desarrollados de acuerdo a actividades o tareas específicas que persiguen objetivos determinados y que serán ejecutados por un equipo determinado. Éste enfoque da la pauta de contar con varios planes organizados, en lugar de un único documento, lo que lo hace más ventajoso, ya que facilita la capacitación del personal y cada equipo conoce con seguridad las acciones a seguir. Estos planes se pueden clasificar en 3 tipos: planes para la administración de las crisis; planes para la recuperación del servicio/negocio; planes para la recuperación de las TI.

- Infraestructura: se deben considerar no solo la infraestructura edilicia sino tecnológica requerida para poder ejecutar los planes.

- Personas: deben definirse los equipos de respuesta necesarios para ejecutar el plan de contingencia. Además deben establecerse descripciones de tareas y responsabilidades de cada integrante de los equipos.

Alcance de las tareas de Soporte a la Implantación.

- **Capacitación**

Es de vital importancia lograr el compromiso de los empleados de la organización con relación al éxito de la solución de continuidad operativa en caso que deba ejecutarse la misma. Deben establecerse instancias de capacitación que permitan instruir al personal.

- **Prueba de la solución de continuidad operativa.**

Es una tarea muy compleja que puede traer un costo no menor a la empresa, aunque es un punto extremadamente importante a fin de poder establecer si los objetivos pueden alcanzarse o no.

- **Mantenimiento de la solución de continuidad operativa.**

Es una tarea que tampoco es sencilla, pero sí es muy importante, ya que la vigencia del plan de contingencias puede resultar vital para garantizar el éxito de su ejecución. Por ello es recomendable su revisión periódica por parte de los responsables. Como se puede ver éste punto está muy relacionado con el anterior.

ENFOQUE DE CONSULTORA Z

¿Por qué es necesario el desarrollo de un Plan de Contingencia?

En la actualidad el hecho de no contar con un esquema que garantice la continuidad del negocio ante la aparición de una falla o desastre es considerado un riesgo estratégico para las empresas; y es por ello es que se hace necesario definir el mejor nivel de recuperación con un enfoque de continuidad.

OBJETIVOS DE LA CONSIDERACIÓN DE UNA SOLUCIÓN DE ESTAS CARACTERÍSTICAS

- Realizar un diagnóstico de la situación actual, para hacer frente a fallas
- Realizar un análisis del impacto del negocio, el cual incluirá los niveles de respuesta objetivo: niveles mínimos de operación, procedimientos internos
- Realizar un análisis de impacto de riesgos
- Realizar un análisis de la estrategia de continuidad a implementar, que puede incluir un plan de adquisiciones con detalle de elementos y costos estimativos

- Desarrollar el plan de continuidad, el cual debe incluir la elaboración conjunta de los procedimientos de continuidad, recuperación, respuesta de emergencia, manejo de crisis, mantenimiento

- Desarrollar un plan de pruebas

- Elaborar un plan de capacitación

- En función de las revisiones que se realicen, diseñar los cambios que surjan

- Diseñar una oficina de Continuidad Operativa, que será responsable de "gerenciar" el plan de continuidad. Asimismo deben definirse roles, responsabilidades y actividades relacionadas.

ALCANCE

La metodología del trabajo se presenta mediante un enfoque "end to end", que va desde la detección y análisis de riesgos, hasta la implementación de los planes de mejora, y capacitación de los usuarios.

Hay que considerar ciertos componentes que resultan de vital importancia:

- Estructura física

- Infraestructura tecnológica

- Personal

- Telecomunicaciones

- Registros vitales

- Procesos de negocio

La relación costo beneficio, si bien es estimada, no debe perderse de vista. Los costos pueden ser tomados de precios de referencia del mercado, listas de precios, etc. El nivel de detalle va a depender de la necesidad, entendiendo que el objetivo del plan consiste en orientar, priorizar y definir estrategias de contingencia.

METODOLOGÍA DE TRABAJO

1. **Análisis del Impacto en el Negocio (BIA)**
2. **Análisis de Impacto de Riesgos (RIA)**
3. **Análisis de la Estrategia de Continuidad**
4. **Desarrollo del Plan de Continuidad y Pruebas**
5. **Capacitación e Implementación**

El plan de contingencia debe cubrir todos los eventos posibles, y por tanto debe ser guía de quién, qué y cómo proceder antes, durante y después de una contingencia.

Análisis del impacto en el Negocio (BIA)

El BIA identifica los impactos operacionales y financieros en caso de falla operativa o acceso a las funciones de negocio críticas, considerando tanto impactos cualitativos como cuantitativos.

El BIA da las bases para desarrollar la estrategia de continuidad del negocio, porque es el análisis que no solo determina las necesidades del negocio, sino que cuantifica los costos asociados a una interrupción de las operaciones. Esto se determina para cada proceso o función, y se establecen a su vez los tiempos de recuperación.

El BIA identifica y describe:

- Los procesos críticos de negocio
- Análisis del impacto operativo, identificando el impacto de las pérdidas de acceso, aplicaciones e infraestructura. Asimismo determina las funciones que pueden ser afectadas por éstas pérdidas y las consecuencias de la interrupción
- El impacto financiero, determinando el impacto económico que puede resultar de una contingencia. Esto es realizar la justificación de los costos de un plan de continuidad.

Para llevar adelante el BIA se recomienda realizar entrevistas, que incluyan:

- Objetivo y descripción de los procesos y funciones
- Impactos al negocio

- Tiempo de tolerancia
- Tiempo de recuperación
- Relación entre funciones y/o procesos
- Requerimientos mínimos de operación
- Información “vital”

Análisis de Riesgos (RIA)

El objetivo del RIA es la identificación y obtención de la información necesarios para conocer los riesgos potenciales sobre los recursos de los procesos críticos del negocio, lo cual servirá para identificar la criticidad de los recursos y establecer medidas de prevención.

Para cada uno de los recursos (infraestructura física, comunicaciones, informáticos y personas) se deberán evaluar los riesgos existentes ante amenazas naturales y/o humanas (errores, hackers, fraudes, atentados, robos, siniestros, etc.).

Así, en la evaluación de riesgos se deben tener en cuenta dos factores no menos importantes ni uno ni el otro: Probabilidad de Ocurrencia e Impacto.

Los recursos a considerar son entre otros:

- Gente
- Equipamiento de oficina
- Espacio físico
- Equipamiento informático
- Aplicaciones y software de base
- Datos en todo tipo de medios
- Formularios y suministros
- Equipamiento de comunicaciones
- Servicios y recursos de proveedores externos

Estrategia de Continuidad

Se evalúan diferentes alternativas de continuidad y recuperación de los recursos que soportan las funciones de negocio, considerando los requerimientos de tiempo que se establecieron al realizar el BIA.

Éstas alternativas pueden incluir servicios contratados y cambios operacionales internos. Para cada alternativa deben determinarse los costos y todo aquel factor que se considere relevante.

En cuanto a la recuperación de los recursos informáticos y de comunicaciones, se diseña la solución tecnológica expresada en el plan de recuperación de desastres (DRP).

Por último, se identifican las mejores alternativas para cada recurso y servicio, y se pasa a integrarlas en una única estrategia de continuidad organizacional.

Se realiza un análisis técnico y económico de las alternativas, incluyendo la justificación de la estrategia recomendada.

El Comité de Dirección del Proyecto deberá en éste momento determinar la estrategia de continuidad a implementar.

Hay un factor que no se puede dejar de mencionar por su importancia en éste tema; y es la organización del BCM (Businness Continuity Management).

Organización del BCM

Consiste en establecer la organización del plan de continuidad y elaborar los procedimientos de manejo de crisis.

La organización del BCM tiene como objetivo definir los grupos de personas, roles y actividades con respecto al proceso de continuidad (antes, durante, después de la crisis, y el mantenimiento). La organización BCM consta de los siguientes grupos:

- Alta gerencia: es el grupo que decide la estrategia de continuidad y establece el presupuesto destinado al proyecto. Toma decisiones de largo plazo enfocadas a temas de alto nivel.

- Manejo de Crisis: es el grupo que gerencia el proceso durante la continuidad y recuperación de los servicios, y es el que mantiene el relacionamiento de la organización con el exterior (clientes, proveedores, seguros, instituciones estatales, medios de comunicación, etc.). Enfocado en el corto y mediano plazo.

- Respuesta de emergencia: es el grupo de personas (potencialmente toda la organización), quienes detectan el inicio de la contingencia, dan la respuesta inicial y abordan el incidente (eventual evacuación, seguridad de las personas y servicios de emergencia). Se enfoca en el corto plazo.

- Continuidad de los procesos: es el grupo de personas responsables de mantener operativos los servicios críticos del negocio en los niveles mínimos requeridos, durante la recuperación de los procesos y servicios normales.

- Recuperación: es el grupo responsable de restablecer la infraestructura y soporte de TI a niveles normales de funcionamiento. Soluciones de corto plazo, enfocadas e la gente, instalaciones, equipos, proveedores, tecnologías de la información y comunicaciones.

Desarrollo del Plan

Ésta etapa consiste en documentar detalladamente la solución tecnológica, así como los procedimientos de continuidad y recuperación, tanto tecnológicos como operativos.

El plan DRP debe ser desarrollado dentro de la estrategia general de continuidad.

Las áreas de TI incluyen:

- Computación centralizada y descentralizada
- Aplicaciones
- Software de base
- Hardware
- Soporte técnico
- Comunicaciones de voz y datos
- Otros servicios tecnológicos

Pruebas del Plan

Se define la estrategia de pruebas y capacitación previa.

En lo relativo a la capacitación, se definen los requerimientos, se establece el plan, se elabora el material y se pone en práctica la actividad.

El proceso de pruebas del plan tiene como objetivo alcanzar un nivel aceptable de confianza en el mismo, mediante el mejoramiento progresivo del plan. Internacionalmente se cree que para lograr alcanzar un plan de continuidad adecuado se deben llevar a cabo pruebas periódicas, por lo menos dos veces al año.

El proceso de pruebas consiste en establecer el tipo y alcance de las pruebas y su frecuencia:

- Pruebas de escritorio
- Por componente
- Escenario específico
- Árbol de llamadas
- Prueba total del plan

Mantenimiento del plan

El plan de mantenimiento de contingencia alcanza todos los niveles de la organización y todas las tareas administrativas necesarias para la recuperación. Se establece la frecuencia de actualización de cada componente del plan de continuidad y el grupo responsable de su mantenimiento.

Podemos decir que el plan de mantenimiento incluye:

- Organización
- Análisis de impacto
- Análisis de riesgos
- Estrategia de continuidad
- Recuperación
- Respuesta de emergencia
- Manejo de crisis
- Plan de capacitación
- Procedimientos y guías del plan de pruebas
- Plan de mantenimiento

ENTREVISTAS CON EMPRESAS DEL MEDIO LOCAL

Este cuestionario sirve de base para nuestro trabajo monográfico, la información recabada será utilizada únicamente con fines didácticos colaborando con el proceso de formación de los estudiantes, futuros profesionales que se desempeñaran en nuestro medio. El trabajo monográfico busca el aporte de los estudiantes de acuerdo a la formación recibida y a la capacidad crítica desarrollada, de modo que este sea aplicable a la vida de las empresas.

El equipo se compromete a mantener absoluta reserva de la información identificatoria de la empresa.

Información básica de la empresa:

Denominación:

A) Milbourne Ltda.

B) U.T.E.

C) Zetasoftware

D) A.N.P. (Administración Nacional de Puertos) – Área Sistemas

E) Presentia S.R.L.

F) Laboratorio - Industria Farmacéutica

G) Unilever

H) Antel

I) Pequeña Empresa del Rubro Ferretería

J) Pequeña Empresa, Exportadora – Importadora

K) Estudio Contable

Giro:

A) Importación y Exportación

B) Empresa Eléctrica

C) Desarrollo y comercialización de software estándar para Pymes y profesionales

D) Administración de puertos.

E) Desarrollo de software

F) Industria farmacéutica

G) Bienes de consumo

H) Telecomunicaciones

I) Ferretería

J) Exportaciones, Importaciones

K) Estudio Contable

Cantidad de empleados:

A) 32

B) 6000

C) 9

D) 15 personas, Área Sistemas

E) 11

F) 30

G) No revelado

H) No revelado

I) 4

J) En zafra más de 50, regularmente 10

K) 2

Monto de facturación anual en $:

A) No revela

B) 22.500.000.000

C) 8.500.000

D) No revela

E) No revela

F) 160.000.000

G) No revela

H) No revela

I) 3.000.000

J) 6.000.000

K) No revela

CUESTIONARIO

- **¿Posee un equipo de TI? ¿Cuántas personas lo integran? ¿El servicio es tercerizado? ¿Qué incluye el mismo?**

A) No lo poseemos. Tenemos contratada una empresa que nos brinda servicios informáticos, consistentes en instalación de nuevo software, service a los equipamientos, mantenimiento de redes, reparación de hardware y asesoramiento sobre adquisición de equipos y programas.

B) Poseemos un equipo de TI integrado por doscientas personas, no es un servicio tercerizado. Se encarga de desarrollo y mantenimiento de aplicaciones, operación de las mismas y atención de problemas informáticos. Además se encarga de las compras e instalaciones de equipamiento informático.

C) Estoy contestando en base a que entiendo por “equipo”, personas y software, el hardware no es un problema. Podrían robarnos todas las máquinas, que no nos afectaría el funcionamiento, ya que todo lo que necesitamos está online, en datacenters externos de Google, Microsoft y Montevideo.com.

D) El departamento de TI está integrado por quince empleados: cinco ingenieros de sistemas, dos analistas de sistemas, cuatro técnicos helpdesk, tres programadores y un administrador de redes. El servicio es tercerizado, ya que es una licitación por seis años. La licitación a grandes rasgos, abarca un mantenimiento de todos los sistemas informáticos y de los servidores tanto de correo, dominio, web, firewalls, etc.

E) Cuenta con un equipo de TI integrado por dos personas de la empresa (los dos socios directores), que se dedican al mantenimiento de servidores y redes, así como a proveer soluciones a cualquier situación que se plantee.

F) Si. El departamento de sistemas lo integra solo una persona, que es contratada por la compañía, abocado al mantenimiento de software, hardware, administración de servidores, redes y comunicaciones. A su vez hay un programador externo que cuando sus servicios son requeridos el mismo está a la orden.

G) Poseemos un equipo de TI para el Cono Sur (Argentina, Bolivia, Chile, Paraguay, Perú y Uruguay). Trabajan en el equipo aproximadamente cuarenta personas entre personal propio y tercerizado.

H) Si. Conformado por personal propio y tercerizado; integran el mismo administradores de sistemas operativos, bases de datos y servidores de aplicaciones; desarrolladores, mantenimiento de equipos y redes; coordinadores.

I) No poseemos un equipo de TI.

J) No poseemos un equipo propio. Sí existe un servicio tercerizado, brindado por una empresa que es la que la proveedora de computadoras, impresoras, etc., y que se la requiere en caso de necesidad.

K) No hay equipo de TI.

- **¿Ha evaluado los riesgos a los que está expuesta su empresa?**

A) Los riesgos en nuestra empresa pueden deberse a muchos factores, al trabajar con comercio exterior, el tipo de cambio es una de las variables más riesgosas a las que nos enfrentamos, otras son las crisis mundiales, pero ambas son externas a la empresa. Dentro de la empresa los riesgos pueden venir por algún tipo de siniestro (incendio, inundación), por robos o virus informáticos.

B) Si.

C) Si.

D) Si.

E) Si.

F) Si.

G) Si, se hacen evaluaciones periódicas.

H) Si.

I) No.

J) Si, de manera general.

K) Si, sin duda.

- **¿Tiene identificados cuales pondrían en peligro la continuidad del negocio?**

A) Todos los antes mencionados pueden poner en riesgo la continuidad, dependiendo del grado de significación que tengan.

B) Si.

C) Si.

D) Si.

E) Si; rayos, incendios y pérdida de información.

F) Si, como por ejemplo fallas en los equipos, accidentes o sabotajes, entre otros.

G) Si, surgen de las evaluaciones.

H) Si, se realiza una matriz de riesgo y un plan de mitigación de los mismos.

I) No

J) Si, a grandes rasgos, no puntualmente.

K) Si.

- **¿En caso afirmativo, los tiene clasificados? ¿Con qué criterio? ¿Ha considerado probabilidad de ocurrencia, grado de fatalidad, áreas afectadas, impacto en el negocio?**

A) No los hemos clasificado.

B) Los tenemos clasificados. Hemos considerado probabilidad de ocurrencia, grado de fatalidad, áreas afectadas, e impacto en el negocio, determinando así las áreas y servicios críticos.

C) Si, lo evaluamos. De ahí que en el último año hemos migrado todo lo posible fuera de la empresa. Hemos cambiado hasta el eslogan de la empresa a “Administración Online”.

D) Si, perfectamente se tiene claro cuáles son los servidores de mayor importancia y cuales afectarían, son los más críticos.

E) No se ha cuantificado el impacto que puede tener en el negocio.

F) Se establece una clasificación por nivel de contingencia, y se le da una denominación que va desde contingencia menor (nivel 1) a máxima (nivel 4), para cada nivel se presenta una respuesta que varía de acuerdo a la gravedad.

G) Se clasifican según una matriz de riesgo. Donde se contempla la probabilidad de ocurrencia, si existe contingencia, el impacto, etc.

H) Del análisis de riesgos surgen (sin perjuicio de que se puedan realizar ajustes) cinco escenarios y un listado de riesgos a los cuales cada escenario puede ser expuesto. Escenarios: 1. Pérdida de edificio Aguada (incluido equipamiento y/o infraestructura), 2. Pérdida de edificio Unión (incluido equipamiento y/o infraestructura), 3. Pérdida de edificio Centro (incluido equipamiento y/o infraestructura), 4. Mail Server de Adinet fuera de línea, 5. Pérdida de equipo AAA de ADSL centro.

Amenazas: 1. Incendio, problemas eléctricos (cableado, equipamiento de aire acondicionado, generadores, etc.); 2. Accidentes ocasionados tanto por negligencia como por ignorancia; 3. Incendio, existen depósitos de combustible en el edificio (cuatro tanques más el tanque maestro); 4. Inundación; 5. Alta circulación de personal y terceros (Sabotaje, vandalismo, atentados); 6. Ingreso de personas no autorizadas a áreas restringidas; 7. Incapacidad de asegurar una respuesta oportuna ante incidentes de seguridad física y ambiental en todos los casos; 8; Falla del servidor; 9. Pérdida del servidor.

I) No.

J) No los he escrito como para clasificarlos tan detalladamente, pero sí soy consciente del riesgo que corro en ciertas áreas. El riesgo de robo es muy alto, ya que se trabaja fundamentalmente cerca de áreas muy marginadas de Montevideo; siendo el departamento de Administración el más afectado de la empresa, no solo por el volumen de información que genera, sino también por la importancia de la misma. De ocurrir algún inconveniente de pérdida de información, el impacto sería muy alto en éste departamento, donde se encuentra toda la información de proveedores y clientes, pudiendo llevar a perder el detalle de cuentas corrientes de ellos por ejemplo.

K) No están clasificados, puesto que toda la información es relevante. En caso de que no sea relevante, no se guardan registros, se los elimina.

- **En base a esto ¿Ha evaluado la necesidad de desarrollar un plan de acción ante eventuales sucesos que afecten la normal operativa de su empresa? ¿Cuándo surgió la necesidad de tal desarrollo?**

A) Plan de acción no, pero se trata de minimizar los riesgos por medio de seguros (incendio y hurto), por medio de antivirus, respaldo de la información, etc.

B) Luego del incendio de 1993, surgió la necesidad imperante de desarrollar un plan de acción para hacer frente a sucesos inesperados cómo el mismo incendio o cualquier otra catástrofe.

C) No es necesario.

D) La necesidad surgió en el momento del desarrollo del departamento, siempre tiene que haber un respaldo cuando se trabaja con tecnologías de información.

E) No se ha evaluado el desarrollo de un plan de contingencias hasta el momento, pero si se lleva adelante una política (no documentada) de respaldos, para disponer en todo momento de la información necesaria. No obstante no se ha llevado adelante un análisis del costo de tener que restablecer el normal funcionamiento de la empresa, en caso de siniestro, tanto el costo que puede insumir la restauración de información respaldada, así como los desembolsos en infraestructura, equipamiento, mano de obra específica, etc.

F) Si, se desarrolla un plan de contingencia, requerido por políticas organizacionales.

G) Se evalúan los planes y dos veces al año se hacen testeos de los mismos.

H) Focalizándose en mejorar sus sistemas de control interno, Antel entendió necesario llevar adelante un proyecto que permita a la organización contar con un plan para hacer frente a situaciones inesperadas y/o de desastre, logrando mantener la operación y la entrega de servicios.

J) Más de una vez hemos evaluado la generación de un plan de acción, pero por falta no solo de recursos económicos, sino también de tiempo, no lo hemos desarrollado. La necesidad del desarrollo surge a causa del crecimiento repentino que ha tenido la empresa, y el volumen de información que aumenta y que es necesario mantener día a día. También nos lo planteamos cuando estuvimos a punto de perder toda la información de uno de los directores de la empresa por rotura del disco duro y no teníamos respaldo de tal información vital.

K) Sí, fue evaluado y fue implementado un plan de acción. Surgió la necesidad en el inicio de actividades, como forma de salvaguarda de la información de los clientes.

- **¿Qué entiende por Plan de Contingencias?**

A) Entiendo que es la creación de un conjunto de medidas a llevar a cabo ante circunstancias que pueden poner en riesgo al negocio en sí.

B) Tener planificados los pasos a seguir en caso de ocurrir un siniestro.

C) Darle continuidad a la empresa en caso de accidentes o eventos inesperados. No nos referimos a hardware y equipos sino a software y personas.

D) El plan de contingencia es una guía que debe o debería tener todo departamento (no solamente una empresa TI sino en todas las ramas de la empresa), para solucionar cualquier eventualidad y que el mismo pueda ser interpretado por cualquier persona de la compañía.

E) Tener todos los planes y prácticas necesarias para hacer frente a los riesgos que puedan afectar la continuidad del negocio.

F) Conjunto de procedimientos que, tomando en cuenta los aspectos y funciones de negocio más críticos, contemplan la restauración de información y/o reanudación de los servicios en un plazo de tiempo y una calidad de prestación previamente definidos como admisibles.

G) Son las acciones que se deben llevar adelante cuando surge algún siniestro.

H) El objetivo es definir los planes y esfuerzos necesarios para asegurar el mejor nivel de recuperación y continuidad operativa de las distintas líneas de negocio frente a una falla o desastre. Un plan de contingencia comprende la capacitación, recuperación, comunicación, así como adecuación de instalaciones y procesos internos que permitan lograr el nivel de continuidad operativa que asegure la entrega de servicios a los clientes.

I) Un plan que especifique que hacer en caso de pérdida de información vital para la empresa, con el fin también de minimizar las consecuencias del problema ocurrido.

J) Un instructivo de que procesos realizar de manera habitual para que, en caso de inconvenientes de cualquier tipo que traiga como consecuencia una perdida de información, exista un Plan al que podamos recurrir para reconstruir todo en el menor tiempo posible y sin perdida de información.

K) Son planes que se efectúan para cuidar la información y resguardarla de posibles accidentes o siniestros.

- **¿Tiene usted un plan de contingencias?**

A) No.

B) SI, como ya dijimos desarrollado luego del incendio del 93, que ha sido una bisagra en la historia de nuestra institución.

C) No es necesario.

D) Si, se creó un plan de contingencia para todo el departamento de TI.

E) No.

F) Si.

G) Si.

H) Si.

I) No.

J) No, por el momento.

K) Si.

EN CASO AFIRMATIVO DE TENER UN PLAN DE CONTINGENCIAS

- **¿Existe documentación respaldante del plan? ¿Existen copias? ¿Dónde son guardadas? ¿Con que medidas de seguridad? ¿Quiénes lo conocen?**

B) Existe documentación respaldante del plan de contingencia que es guardada en la red y en bóveda externa, se cuenta con respaldo magnético y en papel, bajo medidas de seguridad de respaldos críticos. El plan es conocido por los responsables del mismo.

D) La documentación del plan de contingencias está respaldada digitalmente en los servidores y existen copias en papel guardadas en un sobre lacrado junto con las contraseñas de los servidores dentro de la oficina y otro fuera del departamento.

Todas las personas conocen ésta información pero no tiene acceso, solamente el Administrador de Redes, el Jefe de Operaciones y el Gerente del Área son los que conocen el procedimiento.

El sobre lacrado es por si en algún momento ninguna de las personas mencionadas se encuentra en la empresa y otro empleado necesita alguna clase de información, rompe el sobre y luego las claves se vuelven a cambiar.

F) Si, se conservan copias del plan de contingencias en: caja de seguridad del centro de cómputos, caja de seguridad de gerencia, caja de seguridad de depósito de TI (ubicada fuera del edificio).

Debe garantizarse en todo momento, la existencia de una única versión del plan, por lo que, ante cualquier modificación se realizará la correspondiente redistribución.

G) Existe documentación técnica y funcional del plan. Está publicado en la intranet y también existen copias. Solamente los usuarios involucrados pueden acceder a ellos y con diferentes niveles de autorización.

H) El plan es conocido por los responsables. Las copias se guardan en bóveda interna y externa.

K) No está documentado. Lo que se hacen son respaldos, en un sistema de hardware de almacenamiento portátil. Quienes están enterados de la existencia de esto son los dos integrantes del estudio y quien nos presta el servicio de almacenamiento.

- **¿Qué recursos tiene comprometidos con este plan?**

B) No contesta.

D) El plan de contingencias tiene comprometidos solamente los servidores con su información respectiva, pero no se compromete con la información personal que los funcionarios mantengan localmente en sus terminales.

F) Los recursos necesarios serían, los equipos, la gente, los últimos respaldos, los procedimientos, y no menos importante, documentación de las operaciones y/o información procesada entre la fecha y hora del último respaldo disponible y la fecha y hora de la ocurrencia de la contingencia. Asimismo puede ser necesario considerar un sitio alternativo para las operaciones dependiendo de la gravedad del siniestro.

G) Software, hardware y recursos humanos.

H) Hardware, software, instalaciones, equipamiento, y por supuesto, recursos humanos. Un comentario a destacar es la existencia de equipos de guardia (24 horas), cuya función si cae una aplicación de alta criticidad es de alto impacto, “todos se ponen a trabajar”, aunque el siniestro ocurra fuera del horario de oficina.

K) Recursos informáticos.

- **¿Qué áreas están involucradas?**

B) Los responsables de las aplicaciones críticas y de criticidad media, también las unidades de sistemas involucradas en el plan de contingencia.

D) Se involucran todas las áreas de la empresa, ya que el ochenta por ciento de la misma está digitalizada y la información se encuentra en la misma.

F) Todos los sectores de la empresa (normas de seguridad a observar en caso de evacuación del edificio), usuarios clave, equipo de soporte y equipo de contingencia.

G) Todas las necesarias dependiendo del plan.

H) Quien se encarga del plan de contingencia, de realizar la documentación con los pasos a seguir, evaluar e identificar los riesgos, así como determinar el tiempo que llevaría y los costos que tendría solucionarlos, son los ingenieros administradores de los equipos, ya que conocen las máquinas y la comunicación entre todas las partes involucradas.

Los servidores son Webphare y las bases de datos DB2, compradas a IBM, así que si existe un problema que excede al equipo de TI, se pide soporte a IBM.

K) Todas.

- **¿El personal ha sido capacitado especialmente para eso?**

B) Si.

D) Como se mencionó anteriormente, sólo el Administrador de Redes, el Jefe de Operaciones y el Gerente.

F) Si. Los integrantes del equipo de contingencia, son previamente entrenados y poseen la autoridad necesaria durante el manejo de la crisis. El personal afectado al citado equipo, dependerá del tipo de emergencia que se presente. Además, se han designado usuarios clave, personal externo al área de sistemas, con conocimiento de las aplicaciones críticas y un equipo de soporte encargado de proveer los recursos necesarios. Los responsables del equipo de contingencia convocarán a los miembros necesarios de cada equipo, según las características de la contingencia, y coordinarán su accionar.

G) Si.

H) Si. Hay cursos que mantienen actualizado a todo el personal. En adición, si se piensa desarrollar un plan de contingencia para una aplicación específica; reunidos administradores, desarrolladores, quienes mantienen los equipos y redes, coordinadores, jefes y gerentes, evalúan necesidades. En base a ello, se determinan los requisitos para poder llevar adelante el plan, y por último la aceptación de cada parte y de los distintos gerentes de la cadena. Lego el plan deberá ser documentado, comunicado, y el personal capacitado para el mismo.

K) Si.

- **¿Ha testeado el plan? ¿Realizado simulacros?**

B) Se ha testeado parcialmente el plan, solo se han realizado pruebas no simulacros, dado que éstos requieren una inversión importante de recursos.

D) El plan es testeado eventualmente para mantenerlo actualizado y tener la practicidad de hacerlo en el menor tiempo posible. Ya que si no se hacen simulacros o se testea, puede ser que en la realidad, los mismos fallen o no tengan un procedimiento correcto.

F) Si, una vez al año se realizan pruebas completas, que incluye la evacuación del edificio.

G) Si, dos veces al año.

H) Existe un grupo de "testing" que se encarga de probar el plan. También son realizados simulacros, y se va depurando el plan de contingencia de acuerdo a éstas experiencias.

K) Si; el plan funciona en caso de accidentes.

- **¿Podría darnos un esbozo del plan? Incluyendo inicio de la contingencia, preparación, acciones a seguir y finalización de la contingencia.**

B) Existen planes separados para las diferentes aplicaciones.

D) Se realiza un análisis de riesgo para cada uno de los servidores; teniendo en cuenta: servicios prestados, funcionalidad, medidas actuales (ej. respaldos), nivel de criticidad, etc.; y en base a esto se determinará el tipo de respuesta requerida.

Se adjunta documento anexo.

F) Se adjunta documento como anexo.

G) No revela.

K) Al ser una pequeña empresa, cada semana se respalda en disco, y cada cuatro semanas se respalda toda la información almacenada en los equipos en hardware externo. Este último se encuentra físicamente en otro lugar. En caso de siniestro, se restaura y se continúa con la operativa normal del negocio.

- **Procedimiento para la actualización del plan: ¿Existe, frecuencia, responsables, involucrados, en qué consiste?**

B) Sí, existe un procedimiento para la actualización del plan, y una aplicación que apoya el mismo: guarda la información y apoya en la gestión de la misma.

D) Generalmente se realiza una vez al mes, junto con el administrador de redes y el jefe de operaciones; consiste en apagar un servidor en particular y seguir el procedimiento descripto en el plan de contingencia.

F) Existe un procedimiento que contiene los pasos a seguir para la actualización del plan. Se establecen responsabilidades y rutas de aprobaciones de cada modificación.

G) Dos veces al año, se toma como base los responsables del último plan y se realiza una revisión y ejecución del mismo.

H) Los planes de contingencia se actualizan si existe algún cambio de hardware o software (incluidos cambios de versiones). Quienes están a cargo son los administradores.

K) Existe, quienes son responsables son los prestadores del servicio externo.

- **¿Tienen equipos para el reemplazo de los equipos que son críticos o dañados?**

B) Si en los casos en que así se definió la contingencia, no para los casos en los que se utilizará equipamiento de aplicaciones de menor prioridad.

D) Solamente tenemos reemplazo de los servidores y switches que son netamente críticos.

F) Si.

G) Si.

H) Si. Por ejemplo para las aplicaciones de alta criticidad, existen réplicas idénticas, que permiten que si se cae la aplicación por algún motivo, se levantan otras virtuales.

K) No; pero se cuenta con un seguro que posibilita el reemplazo de los equipos.

- **¿Dentro del plan de contingencias consideran el respaldo?**

B) Si.

D) El respaldo también se cuenta como una parte del plan de contingencia.

F) Si, los respaldos son parte importante del plan de contingencia.

G) Si como parte fundamental del mismo.

H) Se respalda absolutamente todo. Y en relación a las aplicaciones se lleva un versionado de las mismas, por si hay necesidad e volver a una versión anterior.

K) Por supuesto.

EN CASO NEGATIVO

- **¿Como enfrenta la empresa posibles problemas asociados a perdidas de información (corte de energía, inundaciones, etc.)?**

A) Se trata de concientizar a los empleados para que creen respaldos en el servidor de la información que consideren importante. Estamos estudiando la posibilidad de que además del respaldo en el servidor se realice también mediante algún otro medio, ya sea en dvd o cd.

Para los casos de corte de energía eléctrica poseemos un generador de energía, que alimenta el cincuenta por ciento de los equipos informáticos. Si bien se podrá perder la información que no fue guardada, podremos seguir trabajando "aunque sea a media máquina".

C) Ya no nos manejamos más con información en nuestros notebooks o PCS. Hemos migrado todo lo necesario e importante a datacenters externos; desde nuestro software de administración, nuestros correos, etc.

E) Hay una política de respaldos, como ya se mencionó, no documentada. Se evaluó la necesidad de un generador, pero dada la frecuencia y duración de cortes de energía eléctrica, no lo vemos como necesario, considerando el costo y beneficio de la inversión. Sí contamos con UPS, lo que nos permite en caso de corte, un lapso de tiempo que nos permite guardar la información y apagar los equipos con normalidad. Otro aspecto a destacar es que el setenta por ciento de los empleados trabajan con notebooks, lo que les permite también en caso de corte, contar con un tiempo de independencia de energía; la idea es que en el corto plazo, el cien por ciento de los equipos sean de éstas características.

Lo más crítico es la pérdida de información y es barato respaldarla. El servidor principal (al cual ingresan los usuarios locales, así como clientes del exterior) usa discos espejados.

Realizamos respaldos diarios automáticos, y semanales, que son guardados fuera de la oficina, en la casa de uno de los socios o del encargado de administración y finanzas. La información la podemos dividir en dos categorías, información de gestión (propuestas, contabilidad, documentación, etc.), que a nuestro entender no es lo más crítico, e información de programación, la cual sí es de una alta criticidad, son los llamados códigos fuente (la programación propiamente dicha). Para la información de programación hay respaldos automáticos diarios de cada máquina al servidor central y de éste a su vez diarios y semanales. Se hacen otros respaldos en un servidor "online" en Estados Unidos (información encriptada), ésta metodología nos permite el respaldo de grandes volúmenes de información, de manera segura y a un bajo costo.

En caso de un siniestro, se puede llegar a reconstruir la información recurriendo a los distintos respaldos, e incluso se puede solicitar a los clientes información para lograr una reconstrucción óptima.

I) Recolectando nuevamente la información, a partir de la documentación más reciente.

J) Tratamos de reconstruir la información de diferente manera, ya sea, vía papeles físicos, computadoras (en caso de tener la misma información en otra), solicitando información a terceros (clientes y proveedores; "el peor de los males", sobretodo si ellos tienen una deuda contigo y se dan cuenta de que perdiste la información).

- **¿Ha evaluado la posibilidad de que uno de estos problemas le afecte la continuidad del negocio en el corto, mediano y largo plazo?**

A) Sinceramente no lo hemos evaluado. Si bien como lo decía recién, poseemos medios como para seguir funcionando en caso de corte de energía; somos concientes de que queda mucho por hacer en lo que refiere a posible pérdida de información. Sabemos que muchas veces la recomendación de crear respaldos no son debidamente llevadas a cabo por los funcionarios, deberíamos no recomendar sino exigir.

C) Todo está online. Se puede trabajar desde cualquier lugar, al estar todo en datacenters externos, si se rompe una máquina se usa otra cualquiera. Por lo cual siempre se puede seguir trabajando.

E) En el corto plazo si, porque hay que "volver al ruedo"; a largo plazo se recupera la continuidad.

Lo peor puede ser un incendio, "si hay un incendio, ¿mañana a dónde vamos?" Pueden estar los equipos, pero lo más difícil es reubicar a la gente y volver a la normalidad en otro lugar físico.

I) Si, pero las soluciones pensadas requieren de capital para infraestructura y formación del personal, capital con el que hoy en día no cuenta la empresa.

J) Si, definitivamente. Ya estuvimos varias veces expuestos y por suerte las pérdidas fueron menores.

- **¿Considera necesario el desarrollo de un plan de contingencias? ¿Lo tiene previsto?**

A) No lo tenemos previsto.

C) No lo consideramos necesario.

E) Es necesario, está previsto, pero por el momento no se han podido asignar recursos a éste proyecto.

I) Si, lo considero muy necesario, pero por el momento no esta previsto. Al momento lo que intentamos es mitigar los posibles hechos que puedan llegar a generar problemas que requieran un plan de contingencia.

J) Si, definitivamente, ya estuvimos varias veces expuestos y por suerte las pérdidas fueron menores.

- **¿Que necesitaría para desarrollarlo?**

A) Tal vez no lo hemos llevado a cabo por no tener la real dimensión de la utilidad que nos pueda brindar. Pero espero en un futuro no muy lejano, podamos llegar a confeccionarlo.

I) Capital, asesoramiento y recursos humanos, tanto para un correcto diseño del mismo como para su consiguiente implementación.

J) Sin lugar a dudas que tiempo para poder desarrollarlo; y no menor es el factor económico, que en todo desarrollo de planes es vital.

CAPÍTULO VIII - CONCLUSIONES

CONCLUSIONES ACERCA DEL TRABAJO DE CAMPO

Se realizaron entrevistas en el mercado uruguayo, buscando abarcar un espectro lo más amplio posible. Pero dada la sensibilidad de la información solicitada, no todas las organizaciones están dispuestas a compartirla. Es por ello que de nuestro trabajo, surgen

once entrevistas, y dentro de las mismas se logró una muestra, que si bien es pequeña, resultó diversa.

Entre las once organizaciones que accedieron a colaborar con nuestro trabajo se encuentran: Ute, Antel, Administración Nacional de Puertos, Laboratorio del rubro farmacéutico, Unilever, Zetasoftware, Presentia S.R.L., Milbourne Ltda, una Ferretería, una Exportadora e Importadora y un Estudio Contable.

Ocho de once empresas cuentan con un equipo de TI, de las cuales dos cuentan con personal mixto (propio y tercerizado), tres con personal propio y tres tercerizado.

Diez de las once empresas afirman haber evaluado los riesgos a los que están expuestas, y los que puedan poner en peligro la continuidad del negocio; mientras que una no lo hizo.

Seis empresas son las que tiene los riesgos clasificados.

Tres empresas no evaluaron la necesidad de desarrollar un plan de acción frente a siniestros, mientras que las restantes afirman haberlo hecho.

La mitad de los entrevistados afirma tener un plan de contingencias.

A grandes rasgos, podemos observar que las organizaciones que cuentan con un plan de contingencias, que le asegure continuidad frente a siniestros que puedan afectar la normal operativa de los negocios, son las empresas estatales y multinacionales, mientras que las demás no lo poseen. Muchas veces por falta de recursos, o bien a raíz de su evaluación costo beneficio no les es rentable desarrollar un plan de éstas características. En otros casos pudimos observar carencias de políticas organizacionales que determinen el desarrollo de un plan de continuidad operativa.

En el caso de las empresas cuyas casa matrices están ubicadas en el exterior, cuentan con lineamientos que les exigen el desarrollo de políticas a nivel local en materia de contingencia. Muchas veces, filiales uruguayas se empapan de culturas organizacionales provenientes de mercados más maduros, primermundistas. En ellos los análisis acerca de la superación de situaciones críticas, a las que están expuestas las organizaciones, es una temática recurrente. El desarrollo de los planes viene dado por políticas corporativas, y su aplicación se adapta a las particularidades del mercado en el que se insertan.

Varios motivos llevan a que las organizaciones multinacionales trabajen sobre este tipo de políticas para todas sus filiales, entre ellos podemos identificar:

- Unificar criterios a nivel mundial, lineamientos iguales con el fin de lograr desarrollos similares, que luego serán auditados y evaluados por equipos abocados a esos fines. Esto facilita la gestión a nivel global.

- No perder competitividad.

- Cuidar la cartera de clientes, asegurando una prestación integral de los servicios, aún estando en situaciones anormales.

- Mantener una imagen positiva.

- Y sobre todo salvaguardar los activos organizacionales, entre ellos la gente, la información, el equipamiento, las instalaciones.

Otro sector analizado fue el de empresas estatales. Aquí la realidad es otra, ya que muchas de estas empresas configuran monopolio, y un siniestro que afecte la capacidad de prestar servicio repercute en toda la población. Al no tener competencia, éste no es un factor crítico al momento de desarrollar políticas de continuidad operativa, sino que lo que toma más relevancia es la no interrupción en la prestación de los servicios, junto a la salvaguarda de los activos de la organización. Aquí también comienzan a jugar temas de imagen, temas políticos, ya que se rigen por otro tipo de normativa, diferentes al sector privado y tienen un impacto a nivel nacional en toda la población.

Cabe destacar que éste es un sector muy sensible a la opinión pública ya que en general brindan servicios considerados básicos o de primera necesidad.

No podemos afirmar con exactitud en todos los casos, el momento en el que se toma conciencia de la necesidad de contar con planes de contingencia. Ya que observamos el caso de Ute, hasta que no sucedió el tan famoso incendio del Palacio de la Luz (año 1993), no se pensó en desarrollar un plan de continuidad operativa. Esto nos hace pensar en las demás, si en realidad surgen los desarrollos por concientización en continuidad o por "miedo" a que suceda lo mismo que con Ute. Éste es un tema en el que no pudimos ahondar ya que el acceso a la información es reservado, y no todas las respuestas posibles dejan "bien parada" a la institución frente a los ojos de terceros.

El restante grupo de empresas no cuentan con planes de contingencia, son empresas locales, de distintos sectores del mercado.

Igualmente tuvimos la oportunidad de entrevistar empresas con distintos tipos de percepciones de acuerdo a la temática. Pudimos observar que hay organizaciones que no ven necesario el desarrollo de planes de contingencia, otras que tienen una conciencia de continuidad pero no disponen de los recursos necesarios para desarrollarlos, y otras que si bien conocen del tema no ven como relevante el desarrollo de planes.

Una característica que todas tienen en común es la conciencia sobre la importancia del respaldo y la recuperación de la información, sobre todo en las empresas de software. Al comenzar a indagar observamos que entre las empresas pequeñas y medianas, muchas veces se confunde el concepto de plan de contingencia y continuidad operativa, con el de política de respaldos. Los respaldos son una parte importante de los planes, pero no el todo.

Otro punto a destacar es que hay empresas que sí tienen un conocimiento sobre la importancia y relevancia de la temática, pero carecen de los recursos para desarrollarlos; el caso de Presentia por ejemplo, en conversaciones con uno de los socios, nos manifestó el interés, el conocimiento y la perspectiva a mediano plazo de poder desarrollar un plan de contingencia, pero la imposibilidad hoy de lograrlo por la carencia de recursos, tanto económicos, como de tiempo y de recursos humanos, ya que en principio serían los socios mismos quienes deberían llevar adelante el proyecto, y no solo es una pequeña empresa sino que tiene pocos años de actividad. Similar es el caso de la empresa que se dedica a realizar exportaciones e importaciones, por carencia de recursos económicos y de tiempo

no han podido desarrollar un plan de contingencia, pero comprenden claramente su importancia.

Según se deja entrever, el activo más importante de estas organizaciones es la información, y por tanto se abocan a analizar los riesgos que amenazan la integridad, confiabilidad y seguridad de dicha información, dejando en un segundo plano factores como el equipamiento y las instalaciones. Asimismo en ningún caso tuvimos mención sobre medidas preventivas y de seguridad relativas a la gente, como sí se presenta en los casos de grandes empresas que sí disponen por ejemplo, de planes de evacuación de edificios y capacitación para ello, capacitación en respuesta a siniestros, etc.

Como ya hemos visto, hay empresas que brindan consultoría en el tema, con una vasta experiencia a nivel mundial.

Dadas las características de los mercados, cada vez más dinámicos, altamente competitivos y con una fuerte dependencia de la tecnología, aparecen nuevos actores que dedican sus esfuerzos a brindar soluciones de continuidad operativa a las empresas, con el fin de que las organizaciones puedan enfrentar de la mejor manera cualquier imprevisto que ponga en riesgo su negocio. De éste modo las empresas pueden centrar sus esfuerzos en sus procesos clave, en su misión y visión; dejando a los especialistas la planificación y el desarrollo de dichas soluciones.

Las organizaciones necesitan abocar sus energías y recursos en mantenerse operativas, protegiendo sus activos y buscando lograr una ventaja competitiva que las haga diferenciarse. Estas razones hacen que los especialistas vean una necesidad insatisfecha y provean soluciones para hacer frente a siniestros.

Para manejar una idea del impacto que un siniestro pueda tener en una organización, se afirma que dos de cada cinco empresas que sufren un imprevisto que afecte su continuidad operativa, y no cuentan con planes de contingencia, no logran sobrevivir los próximos cinco años (estudio realizado en los Estados Unidos por Vic Whitman – “Aftermath: Disaster Recovery”).

Las propuestas son coincidentes en muchos aspectos. EL BIA aparece como una etapa fundamental en los cuatro trabajos, así como la necesidad de realizar un análisis de riesgos, considerando probabilidad de ocurrencia e impacto, el desarrollo de un plan de contingencia, su puesta en práctica, pruebas periódicas, capacitación del personal, monitoreo y actualización. Asimismo plantean la creación de un departamento abocado a tales fines; vale destacar la apreciación que realiza la consultora Y acerca de la necesidad de conformar equipos de trabajo, los cuales si bien dan una noción de flexibilidad, no deben colisionar con la estructura organizacional.

Las metodologías de trabajo son similares, surgiendo alguna diferencia como en el enfoque de la consultora Y, que destaca la importancia del factor personas como pilar del éxito de un buen plan de contingencia. Además hace hincapié en la importancia de la prevención como factor fundamental para el logro de los objetivos.

Otra diferencia radica en el enfoque de la consultora X, cuando en su etapa de “diagnóstico y perfil del riesgo”, estudia la capacidad actual de continuidad de la

organización, es decir que toma en cuenta los trabajos ya realizados por la empresa para afrontar los riesgos a los que pueda estar expuesta.

RECOMENDACIONES

En la actualidad en nuestro país no existe una normativa, o disposiciones reglamentarias que obliguen a las empresas a desarrollar planes de contingencia y continuidad del negocio, y por lo tanto tampoco existen entes fiscalizadores. Creemos que es importante la intervención del estado en la materia, puesto que la práctica en el Uruguay demuestra que mientras no existe una norma, una fiscalización y sanciones (económicas y/o penales), la mayoría de los actores no se amoldan a las prácticas por más que sean beneficiosas para la sociedad. Por ejemplo, hasta hace un tiempo, no había ninguna normativa relativa a la prevención de muertes por ataques cardíacos en lugares públicos, y mediante decreto del Gobierno se logró que en lugares de gran concurrencia se coloquen desfibriladores.

Lamentablemente nuestra cultura, lejos de buscar el bienestar social, prioriza los beneficios individuales sin considerar el costo social por inoperancia que las empresas pueden generar a la sociedad en su conjunto. Supongamos una institución de salud que pierda las bases de datos con las historias clínicas de los pacientes, y no tenga manera de recuperar en un breve lapso de tiempo ésta información; aquí ya no hablamos de pérdidas económicas, sino de la salud de una persona.

CAPÍTULO IX - EL ROL DEL EGRESADO

La realidad actual de las empresas hace que el profesional deba estar más y mejor capacitado. Debe ser flexible, dispuesto al cambio, ya que existen diversos factores que

exigen que el profesional cada día esté mejor formado para contribuir al logro de los objetivos de las organizaciones.

Hace algunas décadas no se pensaba en planes de contingencia, pero los mismos cambios en la información, la globalización, y el desarrollo de las TI han generado una revolución en los procesos de negocio; asimismo han hecho que cada vez se considere más la importancia de salvaguardar la información y de contar con planes para ello. El Contador, como usuario de la información conoce la importancia que la misma reviste, y puede valorar el costo asociado a la pérdida de ella.

El Contador Público en su función de profesional, tiene implícito un rol social a desarrollar; volcar su conocimiento a la comunidad, es decir mirar el beneficio de la empresa y no el suyo propio. La idea no es necesariamente venderle a las organizaciones una solución, por el contrario sí lo es asesorarlas y advertirlas de los riesgos a los que puedan estar expuestas.

Nuestro rol como contadores es colaborar con la dirección para una correcta gestión de las organizaciones.

Del trabajo de campo realizado surge que la mayoría de las empresas (sobre todo pequeñas y medianas) no parecen tener conciencia de la importancia de la información, ni de los costos asociados que puede traer la pérdida de la misma. Más aún, varios creen tener conciencia, pero no logran demostrarlo, ya sea por incongruencias o desconocimiento.

Es importante también puntualizar las diferencias entre políticas de respaldos y planes de continuidad operativa, ya que son conceptos que en el ámbito de pequeñas empresas parecen confundirse.

Nuestro deber como asesores y/o miembros de las empresas, usuarios de la información, es concientizar a las mismas sobre los riesgos a los que están expuestas, los beneficios del desarrollo de planes de contingencia, así como los costos de desarrollarlos. Muchas veces se requiere trabajo interdisciplinario, formando equipos con otros profesionales.

Debemos proporcionarle a las organizaciones todos los elementos que éstas necesiten para poder realizar su propia evaluación de costos y beneficios de llevar adelante el plan, para que de éste modo puedan tomar una decisión con una base lógica y sólida.

La decisión de si llevar o no adelante un proyecto de desarrollo de un plan de continuidad operativa, recaerá siempre en la dirección de la empresa, quien en caso afirmativo deberá proveer todos los recursos necesarios para realizarlo. Además es quien evaluará las necesidades y la realidad actual, y decidirá si el desarrollo será propio o tercerizado.

CAPITULO X - ANEXOS

1) EJEMPLOS DE PLANES DE CONTINGENCIA

A) EJEMPLO DE PLAN DE CONTINGENCIA DE EMPRESA DE LA INDUSTRIA FARMACÉUTICA

1.- INTRODUCCIÓN

Las funciones de negocio dependiente del equipo informático de la compañía están permanentemente expuestas a fallas en los equipos, accidentes o sabotajes. Como medidas precautorias se definen políticas y procedimientos de seguridad de aplicación en el mencionado entorno, tendientes a garantizar un servicio adecuado. Sin embargo la seguridad total es casi imposible de alcanzar, por lo que la posibilidad de riesgo no debe ser subestimada.

A fin de contrarrestar los efectos producidos por hechos que representen la detención parcial o total de los sistemas de la compañía, es imprescindible definir un plan de contingencia. El mismo, consiste en un conjunto de procedimientos que tomando en cuenta los aspectos y funciones de negocio más críticos, contemplan la restauración de información y(o reanudación de los servicios, en un plazo de tiempo y una calidad de prestación, previamente definidos como admisibles.

De lo anterior se desprende que el plan de contingencia es, ante todo, un Plan de Continuidad de las Funciones de Negocio de la empresa.

2.- OBJETIVO

El objetivo del plan es asegurar a la compañía la capacidad de absorber el impacto provocado por una contingencia, a través de una estrategia que le asegure:

- Respuesta adecuada del personal ante la emergencia.
- Medios alternativos de funcionamiento
- Recuperación temprana y efectiva de sus funciones
- Minimización de inconvenientes operativos y del impacto en el negocio

La interrupción de los servicios de negocio pueden afectar la imagen de la compañía, y lo que es más importante aún, los costos de no tomar precauciones pueden ser mucho más perjudiciales que la más modesta preparación para una recuperación de contingencia.

3.- MARCO DE APLICACIÓN

3.1- Alcance

El presente plan se aplicará ante una emergencia que afecte las aplicaciones y servicios informáticos de la compañía en sus distintas plataformas. Esto es:

- Entorno AS-400 mod. 825 afectado a la administración.
- Servidores LAN destinados a mensajería, bases de datos, archivos de usuarios.

Aún con testeos regulares, los planes pueden tener deficiencias que se detectan sólo ante una situación de desastre. Debido a las variables comprendidas por los distintos escenarios en que puede desarrollarse una catástrofe y las diversas características que ésta puede presentar, éste procedimiento se ha elaborado en base a una situación que permita controlar tanto a eventos levemente perjudiciales, como a catástrofes de mayor magnitud.

Este plan se utilizará como guía y no como modelo, ya que está sujeto a cambios basados en las condiciones y consecuencias del desastre. El equipo de contingencia será quien determine, utilizando su criterio analítico, los puntos aplicables y no aplicables de este procedimiento ante la situación de emergencia que se presente.

Debe revisarse éste procedimiento al menos una vez al año, documentando los resultados y evaluando las necesidades de cambio y/o actualización.

3.2.- Sectores involucrados

- Todos los sectores de la compañía, (normas de seguridad a observar en caso de evacuación del edificio).
- Usuarios clave.
- Equipos de soporte.
- Equipo de contingencia.

3.3.- Definiciones

- Contingencia: se define así al evento que produzca la interrupción de los servicios de información críticos o de los procesos productivos, por un período de tiempo inaceptable. Se utilizan como sinónimos, desastre, catástrofe y emergencia. Ejemplos de contingencia son: inundaciones, equipamientos, etc. No constituyen contingencia aquellas interrupciones programadas a las disponibilidad de los servicios, tales como ejecución de respaldos, actualizaciones de hardware o software, reorganización de la información. El plan de contingencia se refiere a la restauración de las operaciones después de un evento inesperado que ocasione la salida de servicio de los sistemas críticos.

- Equipo de Contingencia: es el grupo de personas con conocimientos informáticos y entrenados en el plan de contingencia, asignados al esfuerzo de recuperar las funciones críticas de la compañía.

- Usuarios Clave: es el grupo de personas, con conocimientos generales del sistema crítico que les compete, que apoyarán al equipo de contingencia en la tarea de recuperación.

- Equipo de soporte: es el grupo de personas que brindan el soporte necesario en lo referido a infraestructura, logística y control de catástrofes.

- Sistemas: éste concepto abarca no solo a los programas y sus datos de entrada y salida, sino también a aquellos requerimientos de hardware, de comunicaciones y de energía que permiten la ejecución normal y confiable de los mismos. Nos referimos entonces a la recuperación de sistemas como a la recuperación total de las funciones y no sólo a restaurar la plataforma computacional.

3.4.- Conservación del plan

Se conservarán copias del plan de contingencia en las siguientes ubicaciones:

- Caja de seguridad de centro de cómputos:

- Caja de seguridad de gerencia.

- Caja de seguridad en depósito de TI.

Debe garantizarse en todo momento, la existencia de una única versión del plan, por lo que ante cualquier modificación, se realizará la correspondiente redistribución.

3.5.- Centro de Control

En caso de emergencia, las acciones a tomar serán dirigidas desde un centro de control situado en el centro de cómputos. Si el lugar estuviese afectado por la emergencia, se procederá al sitio de contingencia contratado.

Desde el centro de control se coordinará el manejo y la supervisión del presente plan, así como el correcto accionar del equipo de contingencia de la empresa.

4.- OBJETIVOS DE RECUPERACIÓN DEL PLAN DE CONTINGENCIA

El presente plan de contingencia se enfoca primordialmente en los denominados sistemas y/o servicios críticos dependientes de la plataforma computacional de la compañía. Es decir, aquellos que por el nivel crítico de la información que proveen, cumplen un papel preponderante en la continuidad de las funciones de la afiliada. Los así denominados para cada entorno son:

Entorno AS-400:

- Mantenimiento de routings.
- Transacciones y consultas de inventario.
- Ingreso y consulta de pedidos. Backorders. Precios.
- Pick y confirm de pedidos.
- Análisis y liberación de créditos. Facturación.
- Estadísticas de venta diaria.
- Sistema contable.

Entorno LAN:

- Lotus Notes.
- Aplicaciones.
- Archivos de usuario.

Se revisarán las listas precedentes como mínimo una vez por año para que, de común acuerdo entre las distintas gerencias, se verifique su validez y la posible incorporación de otras aplicaciones o servicios.

5.- PERSONAL INVOLUCRADO

El equipo de contingencia tiene a su cargo el restablecimiento total de los servicios críticos, el manejo de la situación de emergencia y posterior normalización de la totalidad de los

servicios. Los integrantes del equipo estarán previamente entrenados y la dirección de la empresa les otorgará la autoridad necesaria durante el manejo de la crisis.

El personal afectado al citado equipo dependerá del tipo de emergencia que se presente. Además se han designado usuarios clave, personal externo al área de sistemas, con conocimiento de las aplicaciones críticas y un equipo de soporte, encargado de proveer los recursos necesarios. Los responsables del equipo de contingencia convocarán a los miembros necesarios de cada equipo, según las características de la contingencia, y coordinarán su accionar.

6.- RECURSOS NECESARIOS ANTE CONTINGENCIAS

Para el entorno AS/400, procedimiento de contingencia; documentación de información procesada entre la fecha y hora del último respaldo disponible y la fecha y hora de ocurrencia de la contingencia; sitio de contingencia.

Para el entorno LAN, procedimiento de contingencia; respaldo de información en cinta de acuerdo al procedimiento de respaldos vigente; ID y contraseña de usuario administrados de la red en sobres cerrados ubicados en caja de seguridad del centro de cómputos, caja de seguridad de gerencia; listado de usuarios, grupos y permisos.

7.- ESCALAMIENTO DE CONTINGENCIAS

Para una mejor utilización de éste plan, los desastres serán catalogados por niveles de gravedad y en base a éstos se encaminarán las acciones correspondientes.

- Nivel 1: Contingencia Menor. Pérdida parcial o total de información en disco que requiere recuperación desde medios de respaldo.

- Nivel 2: Contingencia Mayor. Salida de línea de servidores, por pérdida en el vínculo de comunicaciones o averías que presuponen una inactividad no mayor de 24 horas.

- Nivel 3: Contingencia Grave. Salida de línea de servidores, por pérdida en el vínculo de comunicaciones o averías que presuponen el reemplazo de los mismos o una inactividad mayor a 24 horas.

- Nivel 4: Contingencia Máxima. Destrucción del centro de cómputos o instalaciones por siniestro que afecta equipamiento y la estructura de comunicaciones. Se establece un período de tiempo de 48 horas, desde la interrupción del servicio, para declarar la contingencia máxima. A partir de ese momento, contempla otro período de 48 horas para el restablecimiento de los sistemas críticos.

8.- PLAN DE ACCIÓN

8.1- Inicio de la Contingencia

- Principio de incendio en centro de cómputos: Dicha área está provista de detectores de humo, alarmas de incendio y sistema automático de extinción para afrontar este tipo de situaciones.

1. Dar el aviso correspondiente.

2. Activar la alarma de incendios.

3. Si la situación lo permite, desconectar la fuente de energía del sector.

- Inconvenientes en el suministro eléctrico en el área de sistemas.

1. Notificar al encargado del mantenimiento eléctrico inmediatamente.

2. Apagar los equipos, previo resguardo de la información crítica, antes del agotamiento de la UPS.

- Imposibilidad de acceso a aplicaciones.

1. Informar al soporte técnico local.

2. El soporte técnico evaluará la situación y en caso de ser necesario, activará el nivel de contingencia que corresponda.

- Interrupción de las comunicaciones: por caída de enlaces (locales y/o internacionales), falla en el hardware de la red o en el cableado de la misma.

1. Informar al soporte técnico de comunicaciones.

2. El soporte técnico evaluará la situación y en caso de ser necesario activara el nivel de contingencia 2.

- Principio de inundación.

1. Dar el aviso correspondiente.

2. Si la situación lo permite, desconectar la fuente de energía del sector.

8.2.- Preparación

- El encargado de seguridad detallará el estado de situación a los responsables del equipo de contingencia.

- Los responsables del equipo de contingencia se encargarán de convocar a los miembros necesarios del equipo.

- Una vez reunido el equipo, deberá evaluar la situación, el alcance de los daños y deberá determinar el plan de acción de acuerdo al nivel de contingencia. Además identificará relaciones de dependencia y establecerá prioridades de recuperación en base a la definición de aplicaciones críticas. De ser necesario, definirán la convocatoria de integrantes del equipo de soporte y usuarios clave.

- El equipo de contingencia informará a los usuarios afectados el tiempo aproximado que demandará la recuperación de la anomalía.

8.3.- Acciones a seguir

Contingencia de nivel 1.

Entorno AS/400 y comunicaciones.

- La gerencia de sistemas, en particular el área de desarrollos de sistemas, especificará la información total o parcial que debe ser restaurada.

- La recuperación estará a cargo de personal de operaciones haciendo uso de los medios detallados.

- Se informará a los usuarios la necesidad de reproceso de información ingresada con posterioridad al último respaldo.

Entorno LAN.

- Si el daño consistiera en la pérdida total o parcial de información almacenada, se procederá a la recuperación de la misma, mediante el último respaldo disponible, según se indique en el procedimiento de respaldos.

- En caso de que el daño implicara la pérdida de alguna aplicación, se evaluarán las acciones correctivas a tomar.

- Si se estima que dicha aplicación es irrecuperable, se procederá a la reinstalación de la misma, según se indique en el procedimiento correspondiente.

- Si correspondiera, se informará a los usuarios la necesidad de reproceso de información ingresada con posterioridad al último respaldo.

Contingencia de Nivel 2.

Entorno AS/400.

En caso de ser detectado, reportar el incidente. Operaciones iniciará las acciones correctivas pertinentes para restablecer el servicio dentro del tiempo estipulado.

Notificar la contingencia a los usuarios clave para que ejecuten las medidas alternativas, definidas previamente, para mantener las operaciones vitales hasta que se establezca un servicio de contingencia o se reanuden las operaciones.

Comunicaciones.

- Hardware local. Evaluar daños en el equipamiento afectado; activar el contrato de mantenimiento de equipamiento de comunicaciones.

- Caída del vínculo frame relay internacional. Activar el enlace de comunicación alternativo, e iniciar el reclamo al proveedor del vínculo principal.

Entorno LAN.

- Ejecutar el test de diagnóstico correspondiente al servidor.

- Proceder de acuerdo al test.

- De ser necesario, contactar al servicio técnico, indicando grado y localización de la avería o la presunción acerca de ésta.

- Localizar y chequear el estado del equipamiento de respaldo disponible y de backups a efectos de coordinar la restauración de la información y/o aplicaciones afectadas.

- Si la anomalía estuviese en el sistema operativo, utilizar los discos de recuperación correspondiente. Determinar si el problema puede ser resuelto con la reinstalación del sistema operativo.

- Si la anomalía está en una aplicación, determinar si puede solucionarse con la reinstalación de la misma.

- Si el daño consistiera en la pérdida total o parcial de información almacenada, se procederá a la recuperación de la misma mediante el último respaldo disponible.

- Establecer, de ser necesario, tiempos de proceso en horarios de emergencia.

Contingencia de Nivel 3.

Entorno AS/400.

Ídem a Contingencia de Nivel 3.

Comunicaciones.

Ídem a Contingencia de Nivel 3.

Entorno LAN.

Se identificarán los daños producidos, a fin de determinar los proveedores que deban ser contactados.

Deberán tomarse acciones para cada uno de los servidores durante el período que insuma la contingencia.

Contingencia de Nivel 4.

Activar el BRP (Business Recovery Plan) y proceder de acuerdo a las instrucciones del mismo.

Notificar la contingencia a los usuarios clave para que ejecuten las medidas alternativas, definidas previamente, a fin de mantener las operaciones vitales hasta que se establezca un servicio de contingencia o se reanuden las operaciones.

Determinar en conjunto con los usuarios clave, el personal que deberá trasladarse hasta el centro de operaciones alternativo. Proceder según el procedimiento de "Hot Recovery Site".

Para el caso de los servidores proceder de acuerdo al nivel de contingencia 3.

8.4.- Finalización de la Contingencia.

Una vez finalizado el proceso de recuperación, cualquiera haya sido el nivel de contingencia, se deberá:

- Informar a los usuarios el reestablecimiento del servicio.
- Realizar un informe de la situación acontecida, incorporarlo a la base "Incident Report", y en caso de ser necesario, actualizar o modificar el plan de contingencia u otras normas de seguridad que así lo requieran.

9.- PLAN DE ENTRENAMIENTO.

Todo el personal del departamento de sistemas, los usuarios clave e integrantes del equipo de soporte deben ser entrenados en la aplicación del plan de contingencia.

10.- PRUEBA DEL PLAN.

El éxito del plan recae en el grado de conocimiento y capacitación, que sobre él, tiene el personal involucrado, respecto de los procedimientos de emergencia y su ejecución. Para lograr éstos objetivos es necesario implementar una prueba del plan de contingencia en forma periódica, al menos una vez al año.

Para una prueba ordenada, que garantice el relevamiento de la información necesaria para la evaluación del plan, se utilizará un formulario ("Plan de Contingencia - Test").

11.- PROCEDIMIENTO PARA LA ACTUALIZACIÓN DEL PLAN.

El plan de contingencia consiste en un cuerpo principal que aborda aspectos generales referidos al tratamiento de los distintos niveles de contingencia que pueden afectar a la plataforma computacional de la compañía. Acompañando al mismo, se encuentran una serie de anexos específicos que detallan aspectos tales como especificaciones técnicas de equipos, recuperación de software de base y de aplicación, restauración de archivos, bases de datos y formularios.

Ante la necesidad de realizar un cambio, el responsable procederá de la siguiente manera:

1. Realizar las modificaciones necesarias en el procedimiento.

2. Indicar en el Panel de Control de Cambios, la fecha y responsable de la última modificación.

3. Guardar el archivo modificado y someterlo al circuito de autorizaciones.

4. Distribuir las copias autorizadas en los lugares detallados en el punto "3.4".

12.- CONCLUSIÓN

La implementación de todo procedimiento de seguridad significa un trabajo adicional para todos los sectores, lo que involucra tiempo y dedicación por parte del personal afectado. Es importante que todos comprendan la importancia y la necesidad de un plan de contingencia, así como la preponderancia de una política homogénea respecto a la seguridad.

Lo esencial es lograr la continuidad en el procesamiento de datos, y la mejor manera de lograrlo es con medidas de prevención que minimicen la posibilidad de contingencia. El uso apropiado de sistemas de alimentación ininterrumpida (UPS), detectores de humo, alarmas, copias de seguridad, etc., junto con la aplicación de políticas y procedimientos apropiados de seguridad, manuales de emergencia y planes de entrenamiento; forman una estrategia efectiva que redundará en la optimización de los servicios prestados por este departamento para la recuperación pronta y efectiva de las actividades críticas de la compañía.

B) ADMINISTRACIÓN NACIONAL DE PUERTOS

Análisis de servidores y servicios

Nombre	IP	Servicios	Bkps	Contingencia	Gravedad	Respuesta
Armageddon	17xxx	Base de Datos Informix	SI	SI	Alta	A determinar
Kwanyin	17xxx	Controlador Principal de Dominio	SI	SI	Media	3
Intranet	17xxx	Aplicación para insertar pie de página de ISA.	SI	SI	Media	ISA Ltda.
Pro-Sesos	17xxx	Procesos agendados automáticos	SI	SI???	Alta	A determinar
Qdocsserver	17xxx	Controlador secundario de Dominio	SI	SI	Media	3
Backinf	17xxx	Servidor Linux con Informix de Respaldo de Armageddon	N/A	N/A	Baja	4
Procesos	17xxx	Segundo equipo con procesos	SI	NO	Alta	A determinar
Buda	17xxx					
	17xxx	Servidor aplicación de Cubos O3	SI	NO	Media	4
	17xxx	Aplicación Lloyds	SI	NO	Media	3
Tacuabe	17xxx					
	17xxx	DHCP	SI	SI	Alta	2
	17xxx	DNS	SI	Si	Alta	2
	17xxx	WINS	SI	NO	Baja	3
Lhotse	17xxx					
	17xxx	Servidor de Respaldos (ArcServe)	SI	NO	Baja	3
	17xxx	DNS secundario	SI	SI	Media	2
	17xxx	WSUS	SI	NO	Baja	3
	17xxx	Servidor Virtual Producción y Contingencia	SI	SI	Baja	1
	17xxx	Consola de administración para Storage DS4300	SI	NO	Media	4
Exchange	17xxx	Servidor de exchange con funcionalidad Web Mail	SI	NO	Alta	4
Bi fang	17xxx					
	17xxx	Servidor de aplicaciones Web internas	SI	SI	Alta	2
	17xxx	Servidor Virtual Producción y Contingencia.	SI	SI	Media	2
Confucio	17xxx					
	17xxx	File Server para el CPD y Usuarios	SI	SI	Alta	1
	17xxx	SQL Server 2005 (BD Sharepoint)	SI	NO???	Media	3
	17xxx	Genexus Protección Server	NO???	NO???	Baja	2
Kwan kwong	17xxx	AS400				
	17xxx	SEE Producción	SI	SI	Alta	A determinar
	17xxx	Contingencia BDs Producción y Apps	N/A	N/A	Baja	4
Dayman	17xxx	AS400, BD y aplicaciones Desarrollo	NO???	NO???	Baja	A determinar
Uruguay	17xxx	AS400				
	17xxx	BDs Producción y Apps	SI	SI	Alta	1
	17xxx	SEE Contingencia	N/A	N/A	Baja	4
Micro	17xxx	Servidor Virtual, ejecuta el servicio de antivirus corporativo.	SI	SI	Baja	
Anpnet	17xxx	Servidor Virtual, contiene el sitio interno de ANP, ANPNET	SI	SI	Media	
Kwanyin2	17xxx	Servidor Virtual Windows 2000 de contingencia	N/A	N/A	Baja	
WEB1	17xxx	Servidor Web y de aplicaciones externo	SI	SI	Baja	

Nivel de respuesta

Id	Descripción
1	Se recupera en un tiempo estimado de 1 hora.
2	Se recupera en un tiempo estimado de 3 hs.
3	Se recupera en un tiempo estimado de 1 día.
4	Tiempo de recuperación indeterminado, posiblemente varios días.

***Nota:** el calculo de tiempos es estimativo, puede variar mucho dependiendo del tipo y alcance de las fallas.*

Gravedad

Id	Descripción
Alta	Perdida esencial para el funcionamiento de ANP, o de otros servicios importantes.
Media	Perdida importante que a largo plazo pueden perjudicar la operativa.
Baja	Perdida que no representa una emergencia inmediata.

***Nota:** el calculo de tiempos es estimativo, puede variar mucho dependiendo del tipo y alcance de las fallas.*

Glosario

Id	Descripción
Bkps?	Pueden ser respaldos a cinta, con Ghost, o copia a otro servidor.
Contingencia?	El equipo original tiene una falla grave, no se recuperara en corto plazo, si existe contingencia los servicios pueden ser recuperados en corto plazo, o en un plazo razonable teniendo en cuenta la importancia del servicio.
Respuesta	Calculo estimativo del tiempo de respuesta. Esta discriminado en varios niveles detallados en este documento.

2) EJEMPLOS DE CONTINGENCIAS OCURRIDAS

A) Pequeña empresa mejicana especializada en vender dulces (ejemplo extraído de la página de M&B IT Consultants)

Un comerciante cuya especialidad era vender dulces, estaba seguro que no requería ningún plan de contingencia ya que al ser una pyme y tener solamente 3 computadoras, toda la información que tenía en ellas era "prescindible", según sus propias palabras. Entonces paso lo impensable, un lunes cuando llegó a su negocio, alguien había abierto el mismo y se había robado las 3 computadoras. En un inicio no se dio cuenta del desastre, pero con el tiempo este demostró ser más importante que la misma perdida de mercancía que había sufrido.

Para comenzar, por lo menos tenía 5 años que su vendedor, almacenaba toda la información de sus clientes en Outlook, y bueno la última vez que había tenido problemas con su libreta de direcciones habían podido recuperar toda su información de la lista de

clientes que llevaba la contadora en Excel; solo que ahora, esa computadora estaba también desaparecida.

Eso significaba que de la noche a la mañana se habían perdido todos los datos del vendedor, ya no sabía más que por memoria, las llamadas que tenía pendientes y las citas que había que cumplir, pero más importante, no sabia que pedidos había que surtir, y en muchos de los casos requeriría ir a ver a los clientes una vez más para obtener sus datos, o hacer una cacería de datos en las copias de las facturas de la compañía. Meses de trabajo se habían perdido, y a cualquier cliente que no se le hubiera facturado, o cualquiera que hubiera cambiado sus datos desde su última factura, sería prácticamente imposible contactarlo. Esa recuperación de información tomaría al menos 15 días, dinero y esfuerzo extra.

Por otra parte la contabilidad estaba perdida. Cierto es que existía respaldo de toda la información del último año, pero la de los años anteriores había estado en aquella bodega que se inundó, y cuando fueron a buscarla, los papeles eran una masa incorpórea de pulpa y tinta, y nada se podría obtener de ellos.

Los históricos de compras y los inventarios estaban todos en la tercer computadora, así que de pronto no se tenía para la compra más que los recuerdos y decisiones del dueño. La complicada formula que se había realizado por 3 años y que ayudaba a mantener la rotación de inventarios, solo funcionaba con datos históricos, datos que no tenían, y los recuerdos de cuando se sobre inventariaban con artículos de temporada y la viabilidad de su negocio estaba en juego.

Era un verdadero desastre, y uno del que tardaría tiempo en recuperarse, ya que solo hemos mencionado lo que salió a la luz de inmediato, hubo procesos que requirieron interminables horas hombre, como la captura de toda la cartera y la conciliación bancaria para saber quien debía qué.

De pronto los 2,500 dólares que costaba haber realizado un plan de contingencia se habían convertido en más de 5,000 dólares solo en reprocesos, aunado a una pérdida de productividad que solo se solucionó al aumentar el personal para poder hacer frente a la restructuración y actualización del sistema.

B) Inundación en Banco Español

El Banco Guipuzcoano tuvo que poner en marcha su plan de contingencia cuando en el verano de 1997 un torrente de agua y barro, provocado por fuertes lluvias, inundó las instalaciones del Centro de Cálculo de la entidad en San Sebastián. El banco estuvo sin comunicaciones ni energía eléctrica y sus ordenadores quedaron sepultados. EDS, con quien esta entidad tenía contratado el servicio de recuperación informática, puso en marcha el plan de contingencia: la red de datos del banco se redireccionó hacia el Centro de Recuperación de Negocios de EDS en Barcelona y se llevó a cabo la reconstrucción de las bases de datos en este centro alternativo. De esta forma, el banco pudo recuperar la normalidad operativa en menos de 24 horas.

C) Caída del sistema en el sector "Atención de Emergencias" en una institución médica del interior del Uruguay (ejemplo obtenido de conversaciones con médico a cargo del sector).

La forma de trabajo es a través de la recepción de llamados de emergencia por parte de los usuarios; la llamada es recibida por un telefonista que lo ingresa la solicitud al sistema y verifica los datos del afiliado, para así enviarle un médico a su domicilio.

Un domingo a la 1 a.m. el sistema falló, por lo que se procedió a contactar al médico responsable del sector, ya que no existe ningún plan para hacer frente a una contingencia cómo ésta. La decisión tomada fue la de responder a todas las emergencias requeridas, sin verificar si era un afiliado quien la solicitaba. Esto pudo traer pérdidas no previstas a la institución, ya que se podría estar enviando un médico a un domicilio de una persona que no era usuaria de la mutualista.

Al día siguiente se contactó al proveedor de la aplicación para resolver el problema.

D) Rotura del disco duro de la máquina de uno de los socios de una pequeña empresa exportadora e importadora del Uruguay (caso mencionado por uno de los socios, titular de la empresa entrevistada en el capítulo II).

Sin saber por qué motivo, un día el PC de uno de los socios no encendía (por un problema en el disco duro). Este suceso, fue un golpe tremendo y que tomaba por sorpresa a los dueños de la empresa, porque en esa máquina estaba toda la información relativa a clientes y proveedores, información vital para la organización. Consultados sus asesores de sistemas, así como diversas empresas más, se les contestaba que era imposible repararlo. Hasta que un proveedor de sistemas argentino expreso que tal vez podría tener solución, pero había que hacerle llegar el disco dañado. A esto, uno de los socios, en persona viajó a Buenos Aires a llevarle el disco al mencionado proveedor, y éste pudo repararlo con el uso de un láser. Fueron días terribles porque en el disco había información muy valiosa y que no estaba respaldada, así que de ahí en más, la decisión (que hasta el momento es llevada adelante) tomada fue comprar un disco extraíble para cada equipo informático, con el fin de que todos los días se pueda realizar una copia de los archivos del disco duro de cada máquina al extraíble.

E) Muchas organizaciones se vieron afectadas a causa del atentado en el World Trade Center (Año 1993).

Luego del atentado en el estacionamiento del World Trade Center de Nueva York (26 de febrero de 1993), las pérdidas materiales fueron escasas, hubieron grandes destrozos en los sótanos del edificio pero las plantas superiores quedaron intactas. Sin embargo, se dieron dos circunstancias que representaron la banca rota y el cierre definitivo de decenas de empresas; la primera, que se trataba de una atentado terrorista; la segunda, fueron las características de los edificios: edificios de alto riesgo (rascacielos) que debían ser desalojados e inspeccionados por los servicios de seguridad, mientras duraran las investigaciones. El resultado fue, que durante un periodo que osciló entre uno y dos meses aproximadamente, numerosos CPDs con la más moderna tecnología quedaron totalmente aislados, sin posibilidad de que nadie pudiera entrar en ellos. El motivo fue que las torres fueron "selladas" durante ese periodo para facilitar las tareas de desescombro, los trabajos de investigación y poder garantizar los niveles mínimos de seguridad para los miles de ocupantes en ambas torres.

El restablecimiento de la seguridad, fue el causante de que muchas organizaciones no tuvieran acceso a su mayor activo que estaba perfectamente reservado: la información. Como consecuencia muchas de las empresas que no disponían de los datos fuera de los límites físicos del edificio, no tuvieron acceso a la información básica para gestionar la tesorería, atender a los clientes, etc. Y por ello en casos dónde no existía un plan de contingencia, o el mismo no incluía el caso de "pérdida de acceso", significó la desaparición de la compañía.

Un caso particular fue el de Tea Deloitte and Touch, ya que contaba con un plan de contingencia, lo que le permitió trasladar todas las operaciones desde el World Trade Center a un centro de oficinas alternativo en la ciudad de Nueva York, el fin de semana siguiente al atentado.

Años más tarde, el 11 de setiembre de 2001, los planes de contingencia eran una realidad en las mismas torres, y si bien los daños materiales y las pérdidas humanas fueron asombrosos, quedó marcada una importante diferencia entre las empresas que disponían de un plan y las que no; las primeras, tras un breve lapso de tiempo (desde horas a unos pocos días) estaban dando servicio desde los respectivos centros de respaldo alternativos.

F) Caso de una empresa que se le inundó el Centro de Procesamiento de Datos (suceso ocurrido en la ciudad de Barcelona).

Fue el caso de una organización que contaba con un moderno CPD, el cual estaba ubicado en el sótano de un céntrico edificio de Barcelona. Dicho sótano fue literalmente inundado por toneladas de agua que los bomberos vertieron para sofocar un incendio tres plantas más arriba. El resultado no fue muy distinto que si se hubiera quemado el CPD, solamente que no se quemó, fue inundado, nadie pensó en la contingencia ante una

inundación provocada por el cuerpo de bomberos. Actualmente ambas empresas disponen de un DRP.

G) Empresa que fue objeto de un robo (ciudad de Barcelona).

Determinada empresa, tenía todos los desarrollos de su programa de investigación y desarrollo en un servidor a parte y con sus copias de seguridad al lado. Meses de trabajo se perdieron cuando por ausencia no solo de una adecuada política de seguridad sino también de un plan de contingencia les fueron sustraídos los servidores y las copias de seguridad durante la noche.

H) Daño en fibra óptica complicó la prestación de servicios de Antel.

Una falla causada en maniobras con la fibra óptica de la Central Aguada de Antel, sumada a un corte realizado por una empresa en Vilardebó y Millán (a unos 200 metros de ese lugar) produjo el 17 de Setiembre de 20808, la suspensión de conexiones ADSL, autorizaciones de tarjetas de crédito y transacciones con cajeros automáticos en Montevideo y en el Interior del país. Más de 100 cajeros automáticos de la red Banred estaban fuera de servicios por éste problema. La solución de emergencia brindada por Antel consistía en realizar una especie de bypass, y unir fibra óptica de la central con un sitio donde estuviera sana, hasta encontrar exactamente el punto donde se produjo el daño. Esto no permitía recuperar todos los servicios, pero sí una gran cantidad (según declaraciones de Roberto Mourelle, Gerente de la División Operaciones y Mantenimiento de Redes de Antel, al diario El País).

Diez días antes los usuarios de Antel, ADSL y Ancel de Santa Lucía y zonas cercanas estuvieron incomunicados durante todo un día también por problemas en la fibra óptica; se supuso vandalismo pero no hubo avances en el caso.

I) Atentado de Bishopsgate, 24 de Abril de 1993.

El 24 de abril de 1993 el Ejército Republicano Irlandés Provisional (IRA) detonó un camión bomba frente al Hong Kong and Shangai Bank, en el distrito financiero de Londres, ubicado en Bishopsgate, dejando personas heridas y fallecidas.

Los edificios situados a 500 metros a la redonda sufrieron daños, la detonación afectó a 140.000 metros cuadrados de oficinas y rompió más de 500 toneladas de vidrio. El atentado provocó que varias compañías modificaran el ejercicio de sus operaciones, y confeccionaran planes para hacer frente a cualquier incidente futuro. La fuerza de la

explosión hizo volar un gran número de documentos por las ventanas de los edificios, por lo que la policía debió utilizar una cortadora para destruir todos los que encontraban. Esto a su vez causó que los administradores de riesgos demanden una política de "escritorios limpio" al final de cada jornada laboral, para aumentar la seguridad de la información. Otra consecuencia del ataque fue que las compañías financieras británicas y estadounidenses prepararon panes de recuperación ante desastres, en caso de futuros atentados terroristas.

Los daños estimados inicialmente (1.000.000 millones de libras) fueron rebajados, y el costo total de la reconstrucción fue de 350.000 millones, los subsiguientes pagos por parte de las compañías de seguros causaron que éstas sufrieran grandes pérdidas, lo que a su vez provocó una crisis en la industria, incluido el casi colapso del Lloyds of London. En consecuencia, el Reino Unido introdujo un plan de seguros respaldados por el Gobierno, dónde éste pasó a ejercer el papel de "reasegurador de último recurso" por pérdidas superiores a los 75 millones de libras.

J) Centro de Cómputos del Banco de Previsión Social.

Hace tiempo atrás, el B.P.S. tenía un sector de almacenamiento de respaldos seguro. Se hacían respaldos regularmente y se guardaban cuidadosamente varias copias. Un día sucedió un imprevisto (daño en un disco fijo); por lo que se tuvo que recurrir a los respaldos. Para gran sorpresa de los usuarios, la recuperación falló, pues si bien los procedimientos de respaldo eran correctos, no se verificaban, y las copias magnéticas habían sido afectadas por humedad sin que nadie lo percibiera.

BIBLIOGRAFÍA

- ISO 17799 – Código de Práctica para la Administración de a Seguridad de la Información - 2005.

- Contingency Planning Guide for Information Technology Systems - National Institute of Standards and Technology - Technolgy Administration, U.S. Department of Commerce - 2002.

- Contingency Planning Guide for Federal Information Systems - National Institute of Standards and Technology - Technolgy Administration, U.S. Department of Commerce - 2009.

- Manual de Buenas Prácticas - Guía para instaurar buenas prácticas globales en gestión de continuidad del negocio - Business Continuity Institute - 2007.

- Documento ERM, Cátedra Control Interno, facultad de CCEE - 2005.

- "Apreciación de Riesgos", Cátedra Control Interno, facultad de CCEE - 2003.
- Riesgo informático – Spyware, Adware, y Popup, Simon Mario Tenzer - 2004.
- Riesgo Informático – Nueva modalidad a través de Internet: "Phishing" - Simón Mario Tenzer - 2004.
- Respaldo y recuperación de datos Simón Mario Tenzer y Nelson Pequeño - 2000.
- Seguridad informática, Leonardo Sena - 2000.
- Riesgo Informático, Leonardo Sena y Simón Mario Tenzer - 2004.

PÁGINAS WEB

- http://www.tcpnetworks.net/GartnerDisaster.pdf
- http://www.gartner.com/5_about/news/disaster_recovery.html
- http://www.consultorias-it.com.mx/DRP/que-es-un-DRP.php
- http://www.interamerica.net/doc/contingenciaweb.pdf
- http://www.osinerg.gob.pe/newweb/uploads/GFH/08.-PCGrifoFlotante.pdf
- http://www.ocp.com.ar/plan-de-contingencia.php
- http://www.interamerica.net/esp/soluciones.html
- http://www.idg.es/computerworld/Desastre-en-el-CPD.En-marcha-el-Plan-de-Contingenc/seccion-/articulo-9306
- http://elcomercio.pe/edicionimpresa/Html/2007-11-03/local_no_tenia_plan_de_conting.html
- http://www.eluniverso.com/2003/03/07/0001/10/973156F4B16A4522BDCE53F7CA28C200.html
- http://www.consultorias-it.com.mx/DRP/que-es-un-DRP.php
- http://www.cibersociedad.net/congres2006/gts/comunicacio.php?llengua=es&id=309
- Cursos/InformaticaGestion_DAE/InformPara Gestion.htm

- http://www.lssi.es/HTML/Resources/SSICE.pdf
- http://www.cert.org/podcast/show/20071113wilson.html
- http://www.isaca.org
- http://www.informatica-juridica.com/trabajos/Proteccion_contra_los_delitos_informaticos_en_Cuba.asp
- http://www1.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5080/cap01.htm
- http://www.recoverylabs.com/prensa/2007/02_07_expansion.htm
- http://findarticles.com/p/articles/mi_mODUD/is_1_22/ai_68864006/