Capítulo XII

Continuidad de los Servicios de TI

Continuidad de los servicios de TI

Tabla de contenido

Continuidad de los servicios de TI

1.- ¿Qué es administración de la continuidad?

La administración de la continuidad de los servicios de TI -IT Service Continuity Management- se encarga de prevenir y proteger a la empresa de los efectos que pudiera tener una interrupción de los servicios de TI, bien sea que haya sido ocasionada por alguna falla técnica o por causas naturales, o que haya sido provocada, voluntaria o involuntariamente, por alguna persona.

La administración de la continuidad de los servicios de TI debe combinar equilibradamente procedimientos:

- Preventivos:

  Medidas y procedimientos que buscan eliminar o mitigar los riesgos de interrupción y sus posibles efectos.

- Reactivos:

  Procedimientos cuyo propósito es reanudar el servicio tan pronto como sea posible después de cualquier interrupción.

No cabe duda que las políticas y procedimientos destinados a prevenir y limitar los efectos de un desastre son preferibles a las políticas para reaccionar frente a tales eventos, sin embargo la experiencia demuestra que debe disponerse de una juiciosa combinación de medidas.

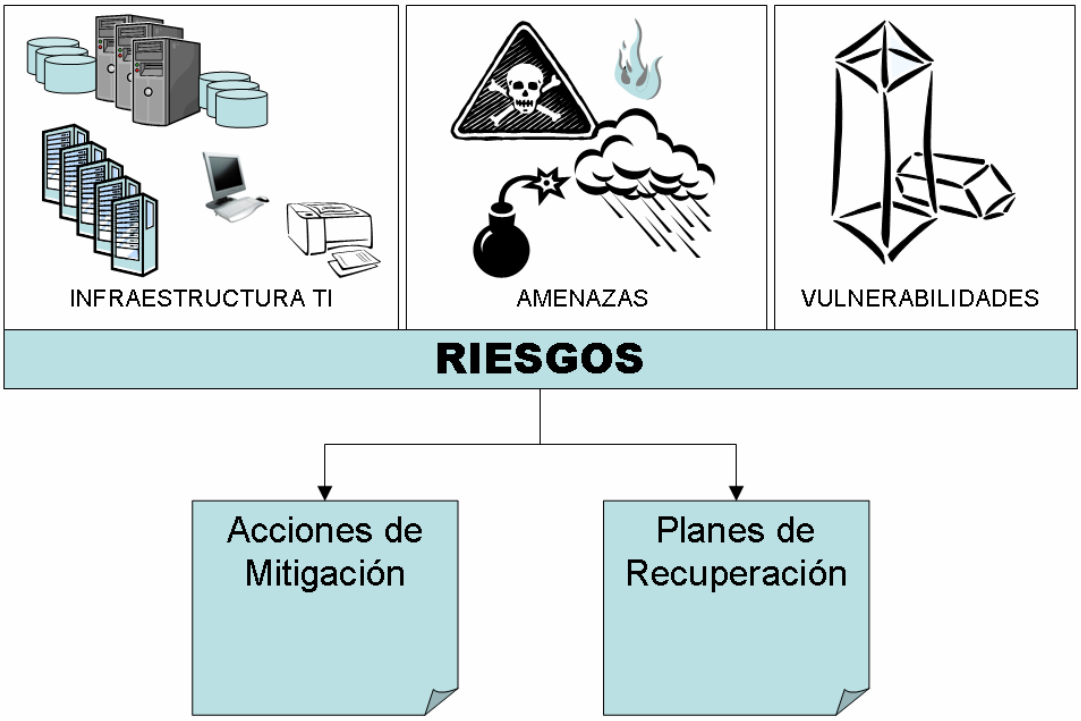
Los objetivos principales de la administración de la continuidad de los servicios pueden resumirse como:

- Asegurar la pronta recuperación de los servicios críticos de TI después de cualquier desastre.
- Establecer políticas, tomar medidas y desarrollar procedimientos para evitar, dentro de lo posible, las consecuencias de cualquier desastre natural -como terremoto-, evento accidental -como incendio- o actos de terrorismo –como explosivos-.

La administración de la continuidad de los servicios de TI requiere de una labor de “evangelización” a todo lo largo de la organización, pues es

difícil de justificar, es costosa y sus beneficios sólo se perciben a largo plazo. Implementar la administración de la continuidad de los servicios de TI equivale a la contratar un seguro, ya que cuesta dinero y parece inútil mientras no ocurre ninguna eventualidad; sin embargo, resulta sumamente valioso frente a cualquier contingencia.

La administración de la continuidad de TI no puede concebirse como una disciplina exclusiva de TI, sino que debe formar parte de la disciplina de continuidad del negocio y debe estar en perfecta coordinación con esa disciplina. Obsérvese, que no tendría ningún sentido que se hagan esfuerzos para que un sistema de entrada de órdenes esté funcionando y disponible bajo cualquier condición, si no se toman las medidas para que el personal de atención al cliente esté listo para operarlo, aunque sea prestando un nivel mínimo de atención.



Existe una diferencia entre desastres tales como terremotos, incendios, inundaciones, etc. y desastres informáticos, tales como los que generan las fallas de equipos, de software, los virus o los ataques de hackers. Para ambos tipos de eventualidades, la disciplina de administración de la continuidad de los servicios debe incluir los procedimientos para mantener el negocio en funcionamiento. Sin embargo, en el último caso –falla informática- además de buscar la restauración del servicio TI con

prontitud, se deben prever las consecuencias en el funcionamiento del negocio ya que:

- Sólo se afectan los servicios TI, pero pueden paralizar toda la organización.
- Son más previsibles y más comunes.
- La percepción del cliente es diferente, pues los desastres naturales se aceptan con resignación y no se asocian a una actitud negligente de los técnicos de TI.

1.1.- Ventajas

La implementación adecuada de la disciplina de administración de la continuidad de los servicios de TI tiene una gran cantidad de ventajas, entre las cuales cabe destacar las siguientes:

- Se manejan y se mitigan los riesgos.
- Se reducen los periodos de interrupción no planificados del servicio de TI.
- Se fortalece la confianza en la calidad del servicio, por parte de usuarios y clientes.
- Se constituye en el apoyo indispensable que requiere el proceso continuidad de las operaciones del negocio.

1.2.- Barreras

La implementación de la disciplina de administración de la continuidad de los servicios de TI es una tarea compleja y laboriosa y, además, normalmente tropieza con diferentes obstáculos como los siguientes:

- Hay resistencia a realizar inversiones que no van a tener una rentabilidad inmediata, por lo que no se presupuestan ni asignan suficientes recursos.
- No existe un compromiso dentro de la organización a cumplir con las tareas y actividades que requiere la disciplina, por lo que continuamente se demoran los planes, para atender otras tareas de mayor prioridad.
- No se actualizan los procedimientos y guías cada vez que se realiza un cambio en la plataforma de servicios de TI.
- No se cumple con un análisis completo de riesgos y se dejan de lado amenazas y vulnerabilidades importantes.

- No se prepara convenientemente el personal, ni se realizan simulacros que permitan que toda la organización esté familiarizada con los procedimientos a seguir en caso de presentarse cualquier contingencia que interrumpa los servicios.
- Falta de coordinación con los planes de continuidad del negocio -Business Continuity Plan (BCP)-.

2.- El plan de continuidad del negocio - (BCP)

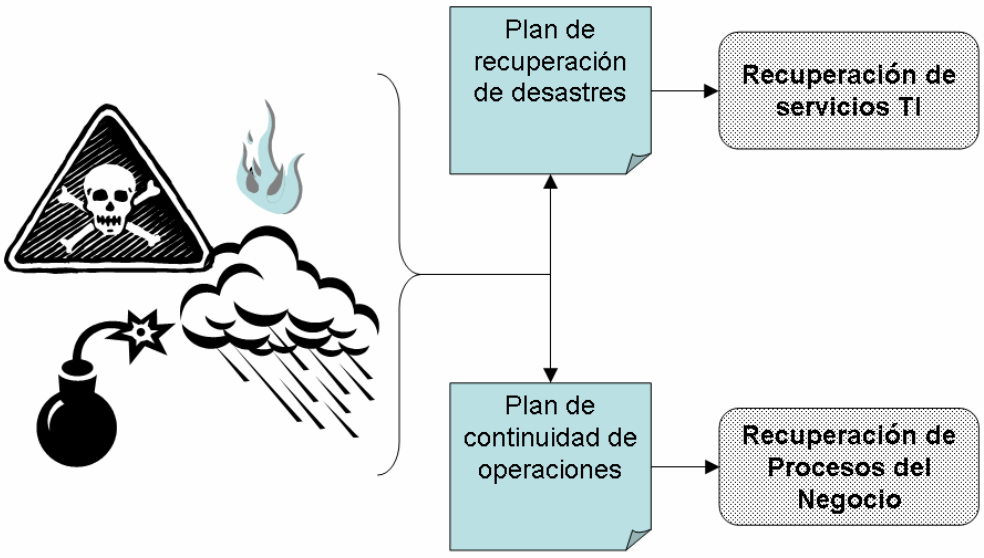
Es importante conocer un poco la terminología y los temas más relevantes de los planes de continuidad del negocio, con el fin de entender el contexto en el que se debe desarrollar la disciplina de administración de la continuidad de los servicios de TI:

- Plan de recuperación de desastres - Disaster Recovery Plan (DRP)

  El plan de recuperación de desastres centra su atención en la recuperación de los servicios de TI y sus recursos, para aquellos casos en los que algún evento ocasione una interrupción significativa en su funcionamiento; por ejemplo, explosión, falla prolongada de electricidad, incendio, inundación, terremoto, etc.

- Plan de continuidad de operaciones - Continuity of Operations Plan (COOP)

  El plan de continuidad de operaciones incluye las guías y procedimientos para la recuperación de los procesos críticos y estratégicos de una empresa. Si bien el plan de continuidad del negocio es la integración todos los planes de recuperación, es frecuente que al plan de continuidad de operaciones se le de esa denominación –BCP-.



- Plan de contingencia - Contingency Plan (CP)

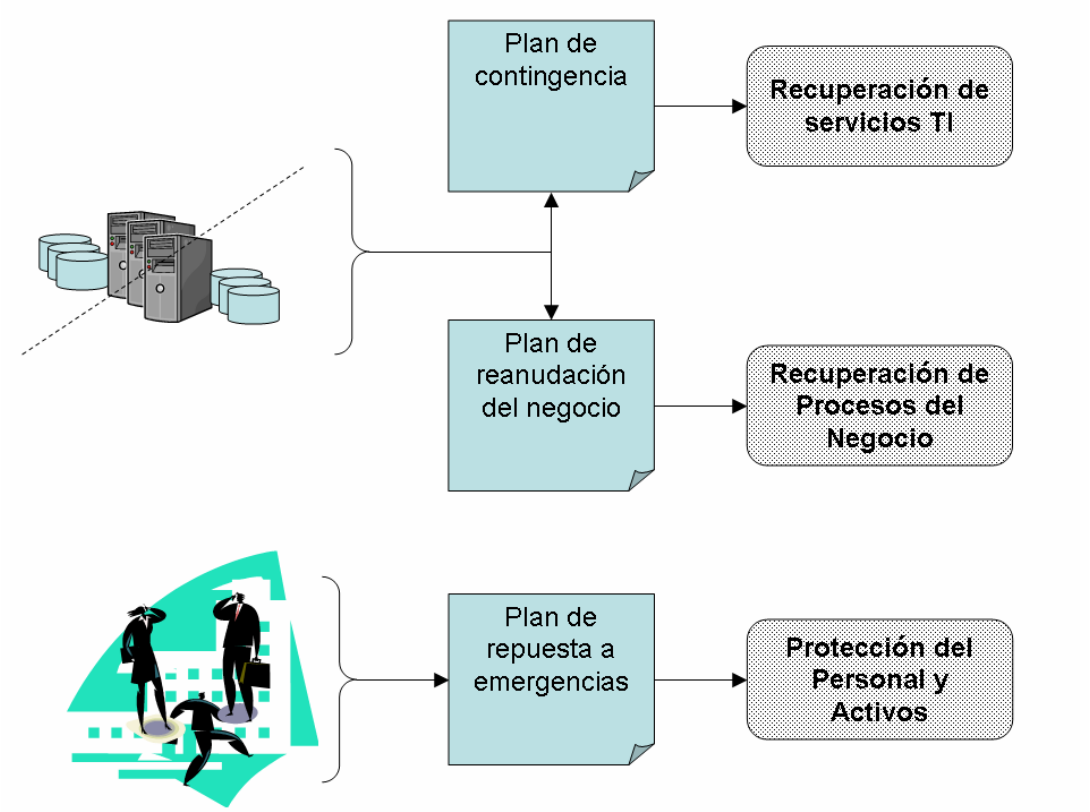
  El plan de contingencia centra su atención en la recuperación de los servicios y recursos de TI después de una falla, independientemente de su magnitud, mayor o menor. Establece procedimientos y lineamientos para la recuperación de equipos y servicios, así como también para las áreas de la empresa que puedan resultar afectadas.

- Plan de reanudación del negocio - Business Resumption Plan (BRP)

  El plan de reanudación del negocio centra su atención en la reanudación de los procesos del negocio que resulten afectados por una falla en los servicios de TI. Focaliza su atención en establecer los procedimientos y guías de trabajo para el funcionamiento de las áreas del negocio en situación de contingencia.

- Plan de respuesta a emergencias - Emergency Response Plan

  El objetivo del plan de respuesta a emergencias es brindar protección a los empleados, al público, el ambiente y los activos de la empresa. En última instancia, busca poner bajo control cualquier situación de crisis de manera inmediata.



Cada una de estas disciplinas se centran en la protección de aspectos específicos de la organización, integrándose entre si, para poder proteger el personal y todas las áreas críticas de la organización. El plan de continuidad del negocio es el concepto que integra el alcance y los objetivos de todas estas disciplinas.

3.- Terminología

Dentro de las diferentes disciplinas arriba descritas, se manejan varios términos de importancia, como son:

- Objetivo de tiempo de recuperación -Recovery Time Objetive (RTO)

  El objetivo de tiempo de recuperación es un resultado fundamental del análisis de impacto –Business Impact Análisis (BIA)-, que establece el intervalo de tiempo en el cual un servicio, proceso o actividad crítica de la empresa debe ser recuperado. En términos del Instituto de Continuidad del Negocio -Business Continuity Institute (BCI)- es “el período de tiempo en el que un proceso puede estar inoperativo”.

- Centro de operaciones alternas del negocio –COAN-

  El centro de operaciones alternas del negocio es el local escogido por la empresa para cumplir con sus operaciones en caso de que, por cualquier motivo, no pueda tenerse acceso a las oficinas de la empresa. Normalmente el centro alterno debe ubicarse en una localidad que no esté cercana a las oficinas regulares, previendo los estragos que un terremoto o motín político pudiera generar. En él se deberá disponer de los recursos necesarios para hacer funcionar el negocio, aunque sea en una mínima versión: mobiliario, suministros, equipos, teléfonos, etc.

- Centro Alterno de Operaciones de Tecnología -CAOT-

  El centro alterno de operaciones de tecnología es el local escogido por la empresa para operar los servicios de TI en caso de que, por cualquier motivo, no pueda tenerse acceso a las instalaciones normales. Es muy frecuente que el CAOT se ubique en un centro de procesamiento contratado, ya que en el mercado existen varios excelentes proveedores de servicios de recuperación y soporte.

4.- Preparación

La preparación de la disciplina de administración de la continuidad de operaciones requiere el cumplimiento de varias actividades bastante complejas y laboriosas, como son:

- Revisar los procesos del negocio y evaluar los riesgos
- Identificar procesos críticos y analizar el impacto que sufrirán esos procesos si faltan los servicios de TI
- Seleccionar las estrategias de recuperación

4.1.- Evaluación de riesgos

Las actividades de evaluación de riesgos en los diferentes procesos del negocio determinan las amenazas de un desastre, pormenorizan las vulnerabilidades existentes, permiten visualizar los posibles impactos de los diferentes eventos de desastre e identifican los controles necesarios para prevenir o mitigar los riesgos de cada evento.

Al realizar una evaluación de riesgos se desarrolla un informe de riesgos y controles que establece recomendaciones y plan de acciones para controlar y mitigar los riesgos que pudiesen alterar el normal desempeño del negocio

Para la elaboración de este informe es necesario:

- Revisar los procesos del negocio y sus dependencias de los servicios de TI
- Identificar los puntos más vulnerables
- Analizar las posibles amenazas sobre estos procesos y estimar su probabilidad

Gracias a los resultados de este análisis detallado, se dispondrá de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio.

La prevención frente a riesgos genéricos y poco probables puede ser muy costosa y difícil de justificar, sin embargo, las medidas preventivas o de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente económicas.

4.2.- Identificar procesos críticos

Al identificar los procesos críticos, que contribuyen más a la misión de la empresa –mission critical-, se analiza en detalle el impacto que podría tener cualquier evento que impidiera su correcto funcionamiento y las pérdidas potenciales que podría acarrear esa interrupción.

Como resultado, se desarrolla el informe de análisis de impacto –Business Impact Análisis (BIA)- en el cual se identifican las áreas del negocio que son críticas, así como la magnitud de los impactos potenciales, tanto operativos como financieros, de una interrupción en su funcionamiento:

- Pérdida de rentabilidad
- Pérdida de participación de mercado
- Mala imagen
- Otros efectos

4.3.- Selección de estrategias de recuperación

Para establecer los planes de recuperación es necesario establecer el tipo de recuperación que puede adoptarse para cada área del negocio, en relación con la criticidad y las necesidades de recuperación que tenga el área.

En general, los tipos de recuperación que pueden adoptarse son:

- Manual

  Procedimientos manuales o semi manuales para llevar a cabo las tareas del área, como por ejemplo, para autorizar compras de los clientes, disponer de un listado de saldos y registrar los pedidos en una hoja de EXCEL. Una vez que se recupere la operación normal, se transferirán al sistema los pedidos registrados en EXCEL.

- Recuperación gradual –cold standby-

  El método de recuperación gradual consiste en poner a disposición del negocio las facilidades de oficina y de servicios de TI, en el COAN y CAOT, en forma gradual, con varios días de espera –hasta 4 días o más-.

- Recuperación intermedia –warm standby

  El método de recuperación intermedia consiste en recuperar las operaciones en la localidad de contingencia –COAN y COAT- dentro de un plazo de 2 ó 3 días. Muchas veces los locales para llevar a cabo la recuperación de las operaciones son facilidades que se comparte con otras empresas.

- Recuperación rápida – hot standby-

  El método de recuperación rápida busca recuperar las operaciones de los servicios más importantes, dentro de un plazo de 24 horas. Normalmente para este método, el CAOT asume la

modalidad de local “sombra”, en el que se dispone de los equipos necesarios y se pueden poner a funcionar con cierta rapidez, con una pequeña pérdida de información.

- Recuperación inmediata –también hot standby-

  Es un método que se utiliza para los procesos más críticos y requiere un local de contingencia –CAOT- en el que se encuentren instalados equipos “espejo”, que permiten reanudar operaciones en cuestión de minutos, sin pérdida de información.

Excepto para el método de recuperación manual, todos los restantes métodos requieren la elaboración de copias de bases de datos y librerías de software, que servirán como punto de arranque de los servicios y las operaciones.

En el caso de la recuperación inmediata, estas copias de respaldo se actualizan con cada operación que se registra, utilizando las nuevas tecnologías de arreglos de discos que permiten replicar instantáneamente cualquier operación en discos “espejo” ubicados en localidades distantes.

Para los otros métodos de recuperación, normalmente se elaboran copias de respaldo con la periodicidad requerida -diaria o semanal- que se almacenan en una localidad segura. Es bueno observar que, para estos métodos, la información de las operaciones que se ejecuten entre la última toma de respaldo y el momento en que ocurra un desastre, será información que no está respaldada y que, en algún momento u otro, habrá que incluir en los sistemas, a riesgo de tener unas bases de datos inexactas.

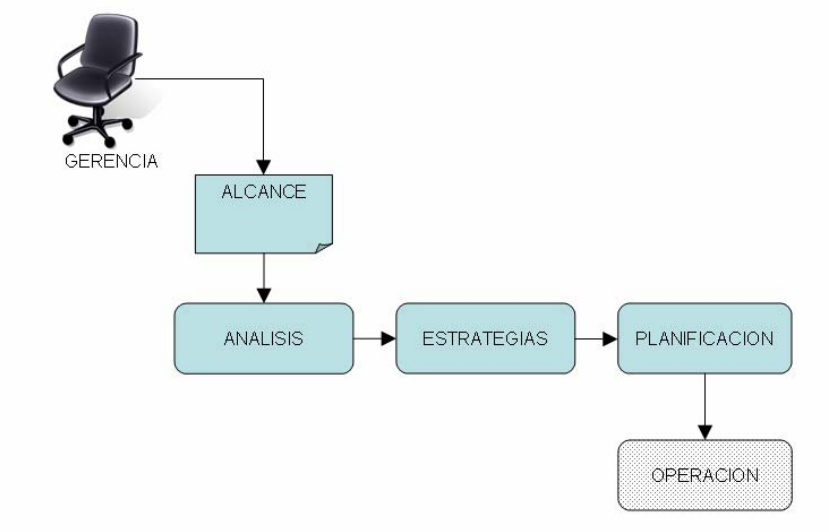
Por lo arriba señalado, algunos especialistas establecen que el objetivo de tiempo de recuperación –RTO- para un área del negocio debe estar dado por la cantidad de información que el área puede perder.

5.- Alcance de la continuidad de servicios

Uno de los pasos iniciales para desarrollar la disciplina de administración de la continuidad del servicio debe ser establecer claramente sus objetivos generales, su alcance y el compromiso de la organización TI.

También la dirección de la empresa debe demostrar su compromiso con el proceso, pues la implantación de la administración de la continuidad de servicios de TI puede resultar compleja y costosa sin una visible contraprestación o un retorno de inversión.

El énfasis de los alcances de la administración de la continuidad del servicio debe ser puesto en las prioridades del negocio; esto es, una vez establecidas cuáles son las áreas críticas y los servicios de TI que apoyan su funcionamiento, desarrollar los planes de continuidad y, una vez que las áreas más críticas se hayan asegurado, se pueden ir incluyendo paulatinamente otras áreas de menor prioridad.



Así pues, deben evitarse enfoques demasiado ambiciosos y establecer alcances realistas para la administración de la continuidad de servicios de TI en función de:

- Los servicios estratégicos de TI –requeridos por las áreas prioritarias del negocio-.
- Los planes generales de continuidad del negocio.
- La historia de interrupciones graves de los servicios TI.
- Las expectativas de negocio.
- La disponibilidad de recursos.

La administración de la continuidad del servicio estará destinada a fracasar si no se destinan suficientes recursos, tanto técnicos, como equipos –hardware y software-.

Será importante recordar que una buena cantidad del esfuerzo de desarrollo de la disciplina debe destinarse al adiestramiento del personal, con el fin de que, en momentos de crisis, conozca las responsabilidades que deberá asumir y las tareas que deberán ser cumplidas.

6.- Organización y planificación

Una vez determinado el alcance que habrá de dársele a la administración de la continuidad de servicios de TI, analizados los riesgos y vulnerabilidades y definidas unas estrategias de prevención y recuperación es necesario asignar y organizar los recursos necesarios. Con ese objetivo la administración de la continuidad del servicio debe elaborar una serie de documentos entre los que se incluyen:

- Plan de mitigación de riesgos
- Plan de manejo de emergencias
- Plan de recuperación

6.1.- Plan de mitigación de riesgos

Un plan de mitigación de riesgos tiene como objetivo principal evitar o minimizar el impacto de un desastre en la infraestructura TI. Entre las medidas se incluyen en este tipo de planes, pueden encontrarse las siguientes:

- Utilización de sistemas alternos de suministro eléctrico –plantas eléctricas alternas-
- Uso de unidades de electricidad ininterrumpibles –Uninterruptible Power Supply (UPS´s)–
- Políticas de respaldo y custodia para los archivos y las bases de datos.
- Duplicación de elementos críticos, como switches, canales de comunicación, etc.
- Utilización de sistemas de seguridad pasivos, como cajas de seguridad

6.2.- Plan de manejo de emergencias

Las crisis suelen provocar reacciones de pánico, que pueden ser contraproducentes que, en algunos casos, pueden causar mayores daños que el incidente que las haya podido causar. Por ello es imprescindible que estén claramente definidas las responsabilidades y funciones del personal en caso de alguna situación de emergencia, así como también deben estar definidas las guías de actuación correspondientes.

En principio los planes de manejo de emergencias deben tomar en cuenta aspectos tales como:

- Evaluación del impacto de la contingencia en la infraestructura TI

- Asignación de funciones de emergencia al personal de servicio TI
- Comunicación a los usuarios y clientes en caso de una grave interrupción o degradación del servicio
- Procedimientos de contacto y colaboración con los proveedores involucrados
- Guías y protocolos para la puesta en marcha del plan de recuperación correspondiente

6.3.- Plan de recuperación

Cuando una interrupción del servicio es un hecho inevitable, es el momento de poner en marcha los procedimientos de recuperación. Para ello, el plan de recuperación debe incluir todo lo necesario para:

- Reorganizar al personal involucrado
- Reestablecer los sistemas de hardware y software necesarios
- Recuperar los datos y reiniciar el servicio TI

Los procedimientos de recuperación pueden depender de la importancia de la contingencia y de la opción de recuperación asociada –cold, warm o hot stand-by-, pero en general deben detallar:

- Asignación de personal y recursos
- Instalaciones y hardware alternativos
- Planes de seguridad que garanticen la integridad de los datos
- Procedimientos de recuperación de datos
- Acuerdos de colaboración con otras organizaciones
- Protocolos de comunicación con los clientes

Cuando se tiene que poner en marcha un plan de recuperación, no oportunidad para la improvisación, cualquier decisión puede tener graves consecuencias tanto en la percepción que los usuarios tengan del personal de TI, como en los costos asociados al proceso.

7.- Continuidad de servicios en el día a día

Una vez establecidas las políticas, estrategias y planes de prevención y recuperación es indispensable que estos no queden en carpetas “llevando polvo”, es necesario que la organización TI esté perfectamente preparada para su correcta implementación. Ello dependerá de dos factores clave, la adecuada preparación del personal y la continua adecuación a las necesidades reales del negocio, a medida que evolucione la infraestructura de TI y los procesos del negocio.

Uno de los factores clave para el éxito de la administración de la continuidad del servicio es mantener un interés permanente en la disciplina, ya que si el interés decayera, después de tener varios periodos en los que la prevención y la buena suerte hayan impedido que se presenten interrupciones graves, en el momento menos pensado podría presentarse alguna dificultad grave y no estar en condiciones de reaccionar adecuadamente frente a ella.

Es imprescindible llevar controles rigurosos que impidan que la inversión y compromiso inicial se diluyan o que la administración de la continuidad de servicios de TI no se mantenga al nivel adecuado para enfrentar cualquier situación. En todo momento, la administración de la continuidad de servicios de TI debe garantizar:

- La puesta en marcha de los planes preestablecidos.
- La supervisión de los mismos.
- La coordinación con la administración de la continuidad del negocio.
- La asignación de recursos necesarios.

7.1.- Adiestramiento

Es inútil disponer de unos planes de prevención y recuperación concienzudamente preparados, si las personas que deberán ponerlos en práctica no están familiarizadas con los mismos. Es indispensable que la administración de la continuidad de servicios de TI prepare al personal:

- Dando a conocer los planes de prevención y recuperación
- Ofreciendo adiestramiento en el uso de los diferentes procedimientos de prevención y recuperación.
- Realizando periódicamente simulacros de diferentes tipos de desastres, con el fin de asegurar la capacitación del personal involucrado.

7.2.- Actualización

Tanto las políticas, estrategias y planes han de ser actualizados periódicamente para asegurar que responden a los requisitos de la organización en su conjunto.

Cualquier cambio en la infraestructura TI o en los planes de negocio puede requerir de una profunda revisión de los planes en vigor y una consecuente auditoría que evalúe su adecuación a la nueva situación.

En ocasiones en que el dinamismo del negocio y los servicios TI lo haga recomendable, estos procesos de actualización y auditoria pueden establecerse de forma periódica.

La Gestión de Cambios juega un papel esencial en asegurar que los planes de recuperación y prevención estén actualizados manteniendo informada a la administración de la continuidad de servicios de TI de los cambios realizados o previstos.

8.- Evaluación de la disciplina

La administración de la continuidad del servicio debe elaborar periódicamente informes sobre su gestión que muestren información relevante para el resto de la organización TI.

Estos informes deben incluir:

- Análisis sobre nuevos riesgos y evaluación de su impacto.
- Evaluación de los simulacros de desastre realizados.
- Actividades de prevención y recuperación realizadas.
- Costes asociados a los planes de prevención y recuperación.
- Preparación y capacitación del personal TI respecto a los planes y procedimientos de prevención y recuperación.