Sistema de gestión de continuidad o BCMS - Primera Parte

Tomasi, Susana Noemí

INTRODUCCIÓN

El Sistema de Gestión de Continuidad es un procedimiento que abarca una serie de actividades a través de las cuales se obtiene una previsión eficaz para afrontar situaciones que lleven a interrumpir el normal funcionamiento de la organización y por lo tanto la operatividad del ente se encuentre en peligro.

Su principal objetivo es que el organismo obtenga a través del BCMS un marco organizativo, tecnológico, funcional y operativo, que garantice y asegure la continuidad de las actividades del negocio y mejore la disponibilidad global de los recursos en consonancia con los criterios de integridad, confidencialidad y disponibilidad en el tratamiento y gestión de la información.

Incorpora los aspectos que la organización debe tener en cuenta para evitar interrupciones en el funcionamiento de su negocio.

En (1) se explica que: "... La Gestión de Continuidad de Negocio es un proceso integral de gestión que identifica los posibles impactos que amenazan a una organización y ofrece un marco para proporcionar robustez y disponer de una respuesta efectiva que salvaguarde los intereses de los principales proveedores, clientes y demás partes interesadas, la reputación, la marca y las actividades creadoras de valor.

"No nos pasará", "Aguantaremos, como siempre lo hemos hecho", "Somos demasiado grandes para fracasar" y "No somos un objetivo para los terroristas" son algunas de las respuestas más frecuentes que dan las empresas cuando se les cuestiona acerca de su falta de preparación. Otros creen que las empresas de seguros van a pagar por todo. La mayoría piensa que no dispone de tiempo para prepararse para algo que nunca sucederá.A pesar de los efectos negativos en las organizaciones, muchas empresas aún no toman medidas para contar con planes que les permitan lograr la Continuidad del Negocio.El 72% de todos los negocios tienen alguna de estas condiciones:

— No tienen Plan de Continuidad del Negocio— Si lo tienen, nunca lo han probado— Su Plan falló cuándo lo probaron

Para dar una idea de su importancia: De cada 100 empresas que afrontan un desastre sin contar con un Plan de Continuidad: 43% nunca reabren el negocio 51% sobrevive, pero están fuera del mercado en 2 años y sólo el 6% logra sobrevivir a largo plazo (Emergency Management Forum)..."

Un BCMS, abarca las siguientes fases:

* Análisis del impacto de una interrupción en el normal funcionamiento del negocio
* Plan de Continuidad del Negocio o BCP (Business Continuity Planning)
* Recuperación de Desastres
* Gestión de Incidentes.

El Sistema de Gestión de la Continuidad describe una filosofía o metodología de la manera de desarrollar la actividad del negocio, mientras que el Plan de Continuidad del Negocio es la actividad que determina cual debe ser esta metodología a utilizar para que la organización continúe en actividad si ocurre un desastre, siendo que la Recuperación de Desastres es una parte pequeña del Sistema de Gestión de la Continuidad y es la habilidad de recuperarse de un evento que impacta el funcionamiento de su organización lo más rápido y completo posible. El tipo de desastre puede variar, pero el objetivo final es siempre el mismo, volver a estar operativo.

Y a través de la Gestión de Incidentes, se obtiene recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan, para posteriormente conocer los responsables del mismo y atacar las fallas.

PRIMERA FASE: ANÁLISIS DEL IMPACTO DE UNA INTERRUPCIÓN EN EL NORMAL FUNCIONAMIENTO DEL NEGOCIO

Toda organización no importa el tamaño que tenga, si ve interrumpido su normal funcionamiento, tiene un impacto respecto a la operatoria que realiza, por lo tanto es dable analizar cómo sería el golpe que le

ocasionaría a la misma según el tipo contingencia que hubiera ocurrido.

Utilizando como herramienta el ANÁLISIS DEL IMPACTO DE UNA INTERRUPCIÓN EN EL NORMAL FUNCIONAMIENTO DEL NEGOCIO se podrá recopilar información respecto a la criticidad de cada sector de la misma y el tiempo necesario para conseguir la recuperación en caso de falla.

Nos muestra el costo que ocasionaría una suspensión total o parcial en la operatoria del negocio, se ubica la criticidad de cada proceso, la importancia de la operación de los mismos, y la prioridad de restablecimiento de los servicios y de la recuperación de la operatividad de la organización.

Se puede utilizar, también si existen cambios significativos en la operatoria del negocio, por ampliación del mismo, modificación en los mercados, en la financiación etc.

De tenerse en cuenta en el análisis:

* La clasificación de todos los activos de la organización y de los procesos productivos, de servicios, etc.

* Evaluar la criticidad de los recursos ya sean de equipos, instalaciones, personal, etc., que forman parte de esos activos y procesos.

* Para no incurrir en pérdidas significativas, cual es el período de recuperación razonable y prioridades de reparación.

* Clasificación de los riesgos, en (2), expreso que "... El objetivo de éste trabajo es mostrar la manera de llevar a cabo un análisis del riesgo respecto a la seguridad informática, de un Organismo correspondiente al sector público, que puede adaptarse a cualquier organización.

Para efectuar el análisis del riesgo de una organización es necesario:

1. Evaluar la normativa vigente.

2. La organización de un comité de seguridad.

3. Un relevamiento de los sistemas informáticos, clasificándolos, armando una planilla con el nivel de riesgo e importancia que poseen.

4. Determinar que contingencias pueden surgir a través del contrato con terceros contratados.

5. Evaluación del riesgo a través de la confección de:

a. Una tabla de amenazas.

b. Una tabla de vulnerabilidades — probabilidad de ocurrencia — impacto

c. Una tabla de controles.

d. Una tabla de riesgos

6. Reunión del comité de seguridad a fin de decidir respecto a las modificaciones propuestas por las distintas gerencias y sub gerencias...."

En éste tema se desarrollo en forma práctica un análisis de riego de los activos informáticos, pero de la misma manera se debe elaborar el análisis de riesgo de todos los activos y procesos involucrados en una organización, evaluando las vulnerabilidades existentes, cuales son las fuentes de amenazas, que incidentes pueden ocurrir y que consecuencia se tendría en la operatividad de la organización si sucedieran, la probabilidad de ocurrencia (es decir, si la organización se encuentra en una zona sísmica, la posibilidad de ocurrencia de un terremoto es mucho mayor que en una zona que no lo es), y que impacto y riesgo tendría el suceso en la empresa.

En la evaluación del riesgo de que la organización se encuentre inactiva por determinados períodos de tiempo, se deberán analizar los distintos escenarios posibles y el impacto ocasionado por el evento sobre los negocios del ente.

Efectuar el análisis del riesgo que tiene una organización no es una tarea sencilla, pero debería llevarse a cabo para prevenir eventos que afecten el normal desempeño de la empresa de que se trate.

SEGUNDA FASE: PLAN DE CONTINUIDAD DEL NEGOCIO

El BCP (3), es una guía para contrarrestar las interrupciones de las actividades comerciales, de organismos públicos o privados, ya sean personas individuales o sociedades, y que sirva para proteger los procesos críticos de los negocios o de las actividades involucradas en organizaciones gubernamentales, de los efectos de fallas significativas o desastres, asegurando el alineamiento con las actuales normas BS25999 e ISO 22301.

Lo que se debe garantizar es la prosecución de las actividades de la organización, cuando un evento que afecta la actividad de la misma ocurre, (como ser un terremoto, inundaciones, incendio, un atentado, huelgas, un virus informático grave, etc.), y por lo tanto impacta en el normal funcionamiento de la organización, logrando perderse documentación valiosa, o no pudiendo operar durante un tiempo prolongado afectando el patrimonio de la misma.

Lo que se pretende es a través de determinados procesos preservar el normal funcionamiento de la organización, recuperar a la misma de un desastre no previsto, contando con toda la información necesario para realizar su operatoria, en la menor cantidad de tiempo posible.

La norma ISO 22301 del 15 de mayo del 2012 especifica los requisitos para planificar, establecer, implementar, operar, monitorizar, revisar, mantener y mejorar continuamente un sistema de gestión documentado para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de incidentes perturbadores cuando los mismos surgen.

Los requisitos especificados en la norma ISO 22301/2012 son genéricos y se pretende que sean aplicables a todas las organizaciones, o sus partes, independientemente del tipo, tamaño y naturaleza de la organización.

La extensión de la aplicación de estos requisitos depende del entorno operativo de la organización y la complejidad de la misma.

Tanto los gobiernos como los organismos reguladores de bancos, compañías de seguros, etc., reconocen la importante contribución de las normativas respecto a la continuidad de los negocios.

PORQUE ES NECESARIO IMPLEMENTAR UN PLAN DE CONTINUIDAD DE NEGOCIOS:

Es necesario para en caso de un desastre o percance que afecte la continuidad de la organización, se cuente con una planificación que permita recuperarse rápidamente de la perdida permitiendo el normal funcionamiento de la empresa.

Es preferible:

— Anticiparse a los eventos que reaccionar en forma posterior a que ocurran los mismos.

— Mantener la organización operativa, con el ahorro que eso significa, que actuar una vez ocurrido el hecho.

— Existe además, un problema de imagen ante clientes, usuarios, proveedores, etc., y de seguridad de las personas involucradas en el acontecimiento ocurrido

Asimismo:

— Es necesario implementarlo para cumplimentar las normativas legales de los Bancos Centrales, Superintendencias de Seguros, Órganos Ministeriales y Provinciales, etc. y para que la organización siga en funcionamiento.

— Teniendo en cuenta que se requiere un compromiso de la más alta dirección del organismo de que se trate, ya que para su implementación se requiere de inversiones, pues se necesitan lugares físicos, recursos humanos y de sistemas, contratos con proveedores externos, consultores, etc.

LAS ETAPAS DE UN PLAN DE CONTINUIDAD DE NEGOCIOS SON LAS SIGUIENTES:

1. Coordinación General
2. Relevamiento, análisis y definición de un Plan de Continuidad de Negocios.
3. Proceso de puesta en marcha y avance del Plan de Continuidad de Negocios seleccionado.
4. Desarrollo e implementación del plan de continuidad de negocios, con programas de entrenamiento y concientización.

PRIMERA ETAPA: COORDINACIÓN GENERAL:

Se refiere al "Liderazgo", correspondiente al Plan de Continuidad de Negocios, reforzando la necesidad de compromiso de la Alta Dirección para establecer, controlar y revisar el sistema de gestión de continuidad de negocio, sin dicha conducción se hace imposible la implementación de dicho plan.

Teniendo en cuenta que el foco principal del Líder debería ser que si ocurre un desastre que deje inoperante a la organización, se perderán mercados, se deteriorará el valor de reputación de la empresa con la consiguiente disminución del valor de las acciones de la misma, y disminuirá la confianza de clientes y proveedores, y eso justamente es lo que el Director de una organización desea evitar, por lo cual las organizaciones deben estar preparadas para afrontar la próxima crisis.

Por lo cual se debe reconocer el importante papel que tiene el Plan de Continuidad de los Negocios, en la protección de la sociedad, y en asegurar la capacidad de la misma para responder a los incidentes, situaciones de emergencia y los desastres, como por ejemplo, el último sismo y tsunami ocurrido en Japón.

O sea, el Líder, Coordinador, Director, etc., debe ser priorizar, la continuidad del negocio, y llevar a cabo las acciones, los procesos necesarios para que ante el impacto de un eventual incidente, tengan la capacidad de reacción para estar fuera de servicio en tiempos aceptables, debe incorporar en todos los estamentos de la organización la conciencia de contar con un Plan de Continuidad del Negocio, que comprendan en la organización la necesidad de contar con el mismo, y de ejercitarlo.

El Coordinador es el responsable de tomar las medidas necesarias, de la implementación, publicación (para que el personal de la organización tome conocimiento) y la ejercitación de las mismas.

Prácticas de manejo de un Plan de Continuidad de Negocios:

Política y Gestión de Programas

Incorporación de un Plan de Continuidad de Negocios en la cultura de la Organización

Prácticas Técnicas de un Plan de Continuidad de Negocios:

Comprender la Organización

Determinar la estrategia de Plan de Continuidad de Negocios.

Desarrollo e implementación de un Plan de Continuidad de Negocios

Hacer ejercicio, mantenimiento y revisión de un Plan de Continuidad de Negocios.

SEGUNDA ETAPA: RELEVAMIENTO, ANÁLISIS Y DEFINICIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIOS:

Que abarca:

*** Determinación de los procesos que son necesarios para la continuación de la actividad del ente**, y cuáles de ellos deben ser abarcados por el Plan de Continuidad de los Negocios para la prosecución del trabajo, en caso de que ocurra un acontecimiento que impida el normal funcionamiento de la organización y que implique la utilización del Plan de Continuidad de los Negocios.

Dentro de ésta fase se deberá interactuar con las distintas áreas de la organización, a fin de evaluar correctamente todas las operaciones con que la firma debe contar a fin de seguir operativa.

Se deben tener en cuenta los lugares físicos con que deben establecerse como optativos, el equipamiento y recursos humanos necesarios, disponer de personal que funcione como apoyo cuando sea necesario. etc.

*** Con la identificación de los recursos de la organización críticos** que fuera efectuada en el Análisis de Riesgo, ya sea de Tecnología de la Información, de Infraestructura necesaria para operar, Equipamiento, Recursos Humanos, Recursos financieros y de Protección civil, establecer las correlaciones mínimas entre los procesos y los recursos disponibles en la organización y desarrollar las alternativas factibles en caso de un evento, identificar las estrategias posibles para mantener operativo el negocio.

*** Determinación de los tiempos aceptables para estar fuera de servicio**, se deben definir los tiempos de recuperación deseables, luego de un evento, y contar con información sobre la asignación de prioridades en la recuperación, que fuera efectuada en el Análisis de Riesgo oportunamente desarrollado.

*** Definición de las prioridades de rehabilitación**, de cada sector de la organización, y dentro de los sectores, de los distintos procesos operativos. La evaluación de las prioridades debe ser efectuada en concordancia con los distintos sectores del ente.

*** Determinación de los procesos y equipamiento mínimos para sustentar el Plan de Continuidad del Negocio**, como objetivo determinado se deberá estipular las necesidades específicas de todos los recursos del ente que deben estar disponibles a fin de realizar el Plan de Continuidad del Negocio, con indicación de la correlación de procesos con equipamiento, recursos humanos y lugares físicos de implementación. Efectuando un relevamiento, análisis y evaluación de alternativas factibles. Como resultado se obtendrá una primera evaluación de los componentes necesarios para sustentar el BCP.

*** Evaluación y formulación de las posibles estrategias y técnicas para garantizar la continuidad operativa del negocio**, con análisis de sitios alternativos de operatividad, reemplazo de equipamiento,

(acuerdo con proveedores, inventario del equipamiento necesario y equipos compatibles) traslado de los recursos humanos si fuera necesario de ciudad, metodología de back — ups de los recursos de Tecnología de la Información, sin los cuales la operatividad sería imposible de realizar, desarrollo de estrategias que permitan operar en distintos escenarios, asignando un valor prioritario de simplicidad y confiabilidad de la operación a cada estrategia propuesta y factible. Como resultado se obtendrá un set de alternativas, analizadas y evaluadas en detalle para garantizar que cumplen con el objetivo propuesto.

* **Análisis de los costos**, de las diferentes alternativas viables, solicitando información técnica y comercial de proveedores de los distintos servicios involucrados, lugares físicos de traslado, en caso de ser necesario, con evaluación de los resultados obtenidos, y determinación de la opción económicamente más eficiente.

* **Selección de la estrategia más eficiente**, en relación con la posibilidad de la implementación de un Plan de Continuidad del Negocio a un costo razonable.

TERCERA ETAPA: PROCESO DE PUESTA EN MARCHA Y AVANCE DEL PLAN DE CONTINUIDAD DE NEGOCIOS SELECCIONADO:

Que abarca:

* **Avance con la táctica seleccionada**, con definición de los procedimientos que se utilizarán, crear una métrica clara, estructura de informes y la frecuencia y forma para comunicarse entre los distintos estamentos de la organización que formarán parte de éste proceso de forma regular, a fin de verificar el estado de desarrollo del programa elegido.

Entre otras conceptos es necesario que todo el personal de la organización comprenda qué procesos del negocio son los más importantes para la continuidad del ente, de manera tal que se pueda contar con diferentes individuos con el mismo conocimiento, sobre todo en momentos críticos cuando la persona experta del área involucrada no se encuentra disponible.

* **Elaboración primaria del escenario de contingencia**, que abarca el diseño de los elementos de la organización necesarios para soportar el Plan de Continuidad del Negocio elegido, con el diseño de la arquitectura de los componentes involucrados en los procedimientos de las distintas áreas de la organización, con énfasis en las Tecnologías de la Información, como indicáramos en (4) "...Revisar la seguridad física del Centro de Proceso de Datos, que se refiere a:

1. La protección del Hardware y de los soportes de datos,
2. La protección de los edificios e instalaciones que los albergan.
3. Abarca situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

— La seguridad lógica de datos, procesos y funciones informáticas, que debe abarcar la seguridad:

1. El cumplimiento de normas y estándares.
2. La protección:

a. Del Sistema operativo
b. Del Software.
c. De las Comunicaciones.
d. De la Base de Datos.
e. Del Proceso.
f. De las Aplicaciones.
g. De la Seguridad Física, del personal y las instalaciones correspondientes..."

* **Prueba inicial de la estrategia seleccionada**, con definición de los recursos necesarios para el desarrollo de las pruebas de factibilidad técnica del modelo seleccionado, y definición de los procedimientos de prueba del mismo.

* **Elaboración de los estándares técnicos para la selección de proveedores**, con las especificaciones técnicas necesarias para la implementación de todos los procesos de negocio de acuerdo al plan de continuidad seleccionado.

* **Documentación formal de la estrategia seleccionada**, el objetivo de documentar el plan seleccionado, es que en caso de una contingencia la manera de la intervención para volver a poner operativa a la organización esté suficientemente definidos y explicitados y hayan sido formulados en base a una evaluación inicial adecuada y suficiente de las necesidades operativas con que se va a desarrollar el

proceso.

CUARTA ETAPA: DESARROLLO E IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIOS, CON PROGRAMAS DE ENTRENAMIENTO Y CONCIENTIZACIÓN:

Que abarca:

*** Desarrollo en detalle del Plan de Continuidad del Negocio**, las actividades a elaborar se deberán ajustar a los protocolos delineados y escritos, implementados por equipos debidamente formados, y coordinados, que deberán entrenar al resto del personal de la organización, para garantizar en caso de un evento, que el organismo va a volver a ser operativo en la menor cantidad de tiempo posible.

*** Soporte técnico especializado en la instalación del Plan de Continuidad del Negocio**, contar con los expertos necesarios dentro de la organización (o consultores externos) que realicen la coordinación del Plan que sea requerido.

*** Diseño y desarrollo del plan de capacitación y prueba final de la aplicación del Plan de continuidad del Negocio**, el objetivo principal será probar con anticipación y coordinar ejercicios, documentando y evaluando los resultados obtenidos.

Para el logro de los objetivos se deberá establecer y ejercitar el Plan de Continuidad elegido, determinar cuáles son los requerimientos para la ejercitación adecuada, efectuar dicha ejercitación en escenarios realistas, para que el personal se encuentre correctamente entrenado, y preparar las planillas correspondientes de control de las ejercitaciones de manera tal que puedan posteriormente realizarse las evaluaciones convenientes a fin de realizar las modificaciones que sean necesarias.

*** Diseño de la documentación de detalle**, que abarca el diseño de los manuales de procedimientos, etapa por etapa, diseño de la lista de tareas para ser realizadas y chequeadas, organigrama de las funciones de cada persona dentro de la organización para el caso de que ocurra una contingencia y se deba actuar en base al Plan de Continuidad establecido.

*** Procedimientos de mejora continua**, a través de la obtención de la retroalimentación de los resultados obtenidos en las ejercitaciones y pruebas realizadas e implementar las mejoras necesarias, para ello se deberá tener en cuenta los siguientes componentes:

1. Gestión de las modificaciones ocurridas en la organización que puedan alterar el Plan de Continuidad de Negocios seleccionado, tales como cambios en el personal, desarrollo de nuevos emprendimientos o baja de alguno de los existentes, cambio de ubicación física de la empresa, alteración en Tecnología de la Información, etc.
2. Régimen de adiestramiento del personal en forma continua, con respecto al Plan de Continuidad de Negocios.
3. Definir un sistema de ejercitación del Plan de Continuidad de Negocios, al menos completo una vez al año, y por partes cada tres meses.
4. Estudio constante del Plan de Continuidad de Negocios, por parte del coordinador del mismo y su equipo de trabajo, para implementar mejoras operativas.

(1) http://www.adacsi.org.ar/es/content.php?id=412

(2) Tomasi, Susana Noemí, Análisis de riesgo respecto a la seguridad informática de una organización correspondiente al sector público— primera parte, http://www.magatem.com.ar/index_archivos/Page507.htm

(3) Ardita Julio, Castellanos Raúl, Apuntes de la materia: Gestión, Auditoria y Normas de Seguridad, de la Carrera de Especialización en Criptografía y Seguridad Teleinformática, Facultad de Ingeniería, Dto. De Posgrados, Instituto Universitario del Ejército Argentino, 08/09-2009.

(4) Tomasi, Susana Noemí, La Seguridad en el entorno informático, Revista Enfoques, Contabilidad y Auditoría, Editorial La Ley, 12-2009.