GESTIÓN DE INCIDENTES Y GESTIÓN PARA LA CONTINUIDAD DEL NEGOCIO, ¿DOS PROCESOS IGUALES, PARALELOS O COMPLEMENTARIOS?

Carlos Javier Calderón Martínez, Leonardo Castro Ordóñez
carlosjtel@gmail.com
lcastroo75@gmail.com
Universidad Piloto de Colombia

Resumen- Como parte fundamental de las operaciones de negocio, la información ha tomado un papel determinante, convirtiéndose en activo crítico de los procesos y por tanto requiere de protección; involucrando tecnologías de información, recursos tanto de TI como organizacionales, los cuales deben ser sometidos a procesos de gestión y mejora continua que les permitan operar con un mínimo de interrupción ante la ocurrencia de un evento crítico.

En este artículo se pretende dar un enfoque comparativo entre los procesos de gestión de incidentes y gestión de la continuidad del negocio, teniendo en cuenta su interoperabilidad en la respuesta y la recuperación ante la ocurrencia de un evento o incidente.

Abstract- As a fundamental part of the business operation, the information had took an important role, converting it in critical asset of the processes, that require protection, involving information technologies, TI resources and organizational resources, those must be submitting to management process and continuous improvement that allow it to operate with a minimal interruption in front to occurrence of a critical event.

In this article is pretending to give a comparative approach between the incidents management process and business continuity management, taking into account the interoperability in the answer and the recovery in front the occurrence of an event or incident.

Palabras claves: BIA, continuidad, gestión, incidente, riesgo.

I. INTRODUCCIÓN

Este artículo trata de la comparación de dos procesos que si bien son necesarios en cada organización para garantizar la continuidad del negocio, son dos procesos diferentes que en la vida real deben estar separados y que se desarrollaran paralelamente ante la ocurrencia de un evento o incidente que afecte las operaciones críticas de la organización.

II. GESTION DE INCIDENTES

Los incidentes de seguridad informática son eventos inesperados que pueden causar daño o pérdida en los recursos de la organización, comprometiendo la seguridad de los sistemas; confidencialidad, integridad y disponibilidad, generando interrupción en las operaciones del negocio.

La gestión de incidentes busca detectar y dar solución a los incidentes de seguridad apoyado en un conjunto de acciones y procesos que permitan responder de forma rápida y adecuada ante la ocurrencia de un evento que ponga en riesgo parcial o total los servicios y/o productos brindados por la organización.

Dada la importancia y el papel determinante en los procesos del negocio ofrecido por los sistemas de información se debe garantizar su correcto funcionamiento, proceso que por el volumen de integración y la naturaleza de los negocios se hace cada vez más crítico, siendo necesario trazar un plan que soporte la gestión y solución de los incidentes. En este orden, la gestión de incidentes debe apoyarse en la gestión del riesgo y el análisis de impacto sobre el negocio (BIA), para conocer las áreas y procesos críticos del negocio y establecer así sus prioridades de solución y restauración.

A. *El papel del análisis de riesgos y el análisis de impacto sobre el negocio en la gestión de incidentes.*

El proceso de análisis del riesgo es un punto clave para poder definir una estrategia de seguridad informática que esté alineada con los objetivos del negocio ya que permite identificar los activos que forman parte de los procesos críticos de la organización como la información y su clasificación, dispositivos de Hardware y Software y aplicaciones del Core del negocio, así como identificar sus amenazas y vulnerabilidades que nos permitan conocer el nivel de riesgo sobre los procesos para seleccionar las medidas adecuadas enfocadas a mitigar el impacto en los sistemas de información y la tecnología que los soportan.

Así mismo, la gestión de incidentes debe apoyarse en el análisis de impacto sobre el negocio (BIA), el cual permite identificar los eventos que podrían afectar la continuidad de los sistemas críticos de la información y su impacto mediante la identificación de instalaciones físicas, identificación de sistemas de información, valoración de la criticidad de los sistemas de información y la estimación del tiempo de recuperación objetivo, punto de recuperación de cada proceso, que nos permita determinar las estrategias de recuperación a partir de la prioridad y criticidad del proceso y su impacto sobre las operaciones.

B. *Plan de gestión de respuesta ante incidentes.*

El plan de gestión de respuesta ante incidentes de seguridad define el conjunto de actividades que deben ser realizadas por el equipo de respuesta independientemente de que se esté respondiendo a un incidente o no. Este plan agrupa actividades y procesos tendientes a dar respuesta y resolución a incidentes de seguridad de manera rápida y eficaz para garantizar una correcta gestión de incidentes.

Un plan de respuesta ante incidentes debe contemplar los siguientes puntos [3]:

- Definición de una Política.
- Especificación de Responsabilidades.

- Definición de Procedimientos Operativos y Canales de Comunicación.
- Estrategia para el Escalamiento de Incidentes.
- Establecimiento de Prioridades.
- Metodología para la Investigación y Evaluación de Incidentes.
- Implementación de Medidas de Respuesta ante Incidentes.
- Notificación a Terceras Partes Afectadas.
- Evaluación del Incidente.
- Uso de Medidas de Detección de Incidentes.
- Pruebas de Funcionamiento.
- Monitoreo.
- Análisis y mejora continua del plan.

El plan de respuesta es único para cada negocio determinado por su naturaleza, tamaño y objetivos del negocio y por tanto es la organización quien debe decidir los recursos dedicados para la defensa, respuesta y recuperación ante incidentes.

C. *Conformación del Grupo de Respuesta de Gestión de Incidentes.*

El equipo de respuesta debe estar conformado por al menos dos personas, el responsable del proceso y punto de comunicación con la dirección y el técnico. Dada la complejidad de los procesos es necesario involucrar personal de otras áreas tales como la Gerencia, personal de TI, recursos humanos, sistemas, área jurídica, entre otros [3].

Las responsabilidades y actividades del grupo deben estar alineadas con las estrategias del negocio. Las actividades incluyen:

- Definición y clasificación de incidentes.
- Determinar las tecnologías y herramientas a utilizar.
- Desarrollar actividades de sensibilización.
- Determinar si un incidente debe ser investigado y el alcance de dicha investigación.
- Aseguramiento de la red.
- Realizar revisiones de seguimiento.
- Desarrollar y mantener los mecanismos de respuesta y el plan.

III. GESTION DE CONTINUIDAD DEL NEGOCIO

Para el desarrollo y entendimiento de esta gestión es necesario dar un marco de entendimiento sobre la continuidad del negocio. Para todas las empresas como ya es conocido uno de sus activos más importantes es la información, pero para poder procesar este activo también se necesita analizar otros factores sin los cuales sería muy complicado realizar dicho procesamiento; la Continuidad del negocio es la capacidad de reacción de una organización para que no dejen de funcionar los procesos más críticos del negocio frente a la presentación de un evento o incidente que causa interrupción en su forma de operar normalmente y así el impacto de dicho incidente pueda reducirse.

Dado lo anterior es necesario realizar una Gestión de la Continuidad del Negocio

para determinar las amenazas y vulnerabilidades que puedan causar interrupciones y crear un plan que permita minimizar el impacto llevando acabo la recuperación de los procesos en un tiempo mínimo.

A. Ventajas de la Implementación de un Plan de Continuidad del Negocio.

La ocurrencia de un incidente que interrumpa el normal desarrollo de las operaciones del negocio puede afectar no solo dichas operaciones sino también el buen nombre de la compañía y causar un impacto financiero para la organización, derivando en la pérdida de negocios, clientes y en si la confianza del sector en el que se desarrolle la organización, lo cual puede incluso causar la quiebra de la misma. Por lo tanto una de las ventajas de la implementación de un Plan de Continuidad del Negocio es que mejora la imagen pública de la organización y garantiza en parte la tranquilidad de los clientes, proveedores, inversionistas y de los mismos accionistas de la organización.

Por otra parte las acciones preventivas que ayuden a identificar los riesgos a través del Plan de Continuidad del negocio generarán proactividad frente a cómo se pueden enfrentar las amenazas y los riesgos para evitar el impacto en las operaciones.

Otra de las ventajas y dependiendo del objeto de la organización, es que minimiza la aplicación de sanciones económicas o puede llegar a evitar demandas de tipo legal a la entidad por concepto de la no prestación de servicios a los cuales se haya comprometido o que sean parte del contrato con sus clientes.

La capacidad de recuperación de las operaciones y/o actividades del negocio es una de las ventajas más importantes que debe ser considerada en el Plan de Continuidad del Negocio dado que dicho plan ayuda a visualizar los tiempos y costos de dicha recuperación para la continuidad del negocio.

Otra ventaja de la implementación del plan es que permite visualizar cuales son los procesos en los cuales se requiere mayor inversión priorizando los esfuerzos y los presupuestos en las áreas en las que más se necesitan de acuerdo con el objeto del negocio.

B. *Características para el Plan de Continuidad del Negocio.*

Para la implementación de un Plan de Continuidad del Negocio es importante tener en cuenta previamente los siguientes aspectos:

- Conocer la Empresa: Es importante conocer y conceptualizar los objetivos del negocio para ello se requiere conocer la empresa, sus productos, procesos, cuáles de estos procesos se apoyan en la tecnología y Sistemas de Información, quienes son los dueños de los procesos, proveedores, servicios que brinda y las metas de la organización para alinear el plan con los objetivos del negocio.

- Participación y Compromiso de la Gerencia y/o Presidencia: Antes de desarrollar cualquier plan es necesario obtener el compromiso de la dirección de la empresa, dado que la sensibilización no es una tarea fácil ya que la comunicación entre la parte técnica de la empresa y la gerencia no siempre es muy clara y para captar su atención es necesario explicar el por qué es necesario para la empresa invertir tiempo, dinero y recursos para la implementación del plan y de cómo se verá retornada esa inversión, por lo tanto debe expresarse en términos que sean digeribles para ellos y buscando siempre estar alineados con los objetivos y estrategias del negocio.

- Áreas Críticas del Negocio: Luego de conocer la empresa y de captar la atención de las directivas de la organización es de suma importancia contar con la colaboración de las áreas del negocio, tanto de las críticas como las que no lo son, ya que los procesos pueden verse afectados si no se obtiene dicha colaboración para perseguir los objetivos del negocio.

- Alcance: En este punto es importante establecer cuales productos y/o servicios, áreas que intervienen y sus procesos estarán contemplados en el plan ya que dependiendo del objeto del negocio y del tamaño de la organización (en cuanto a sus procesos), no todos sus procesos estarán incluidos en el Plan de Continuidad del negocio, adicionalmente por los costos que esto implicaría para la empresa, por lo tanto se debe definir un alcance del plan de continuidad para soportar los procesos que son críticos en su organización y sin los cuales no podría continuar.

- Recursos: Para este aspecto se debe tener en cuenta la estrategia para la implementación del Plan de Continuidad ya que requiere de recursos tanto en tiempo como en recursos de tipo económico, humano y tecnológico y sirve también para identificar qué recursos hacen falta en las áreas comprometidas y determinadas o incluidas en el plan de continuidad del negocio.

- Asesoría de Terceros: Es importante conocer si en algunos de los procesos hay una dependencia de un tercero y/o proveedor ya que con ellos también se debe contar en la implementación del Plan de Continuidad de Negocio.

C. Plan de Continuidad del Negocio.

La gestión de continuidad del negocio se desarrolla a través del ciclo para los Sistemas de Gestión, PHVA (Planear, Hacer, Verificar y Actuar), por lo tanto dentro del desarrollo del plan de continuidad

del negocio se contemplan las siguientes fases:

- Diseño y Política de Continuidad del Negocio.
- Conocimiento de los Procesos y Análisis de Riesgos.
- Medidas Preventivas.
- Estrategia de Recuperación.
- Desarrollo e Implantación del Plan de Continuidad del Negocio.
- Mantenimiento del Plan de Continuidad del Negocio.

1) Diseño y Política de Continuidad del Negocio.

En esta fase se determinan las actividades a realizar en la Implantación del Plan de Continuidad del Negocio, con las cuales se realizará el Diseño de dicho plan y como primera actividad se debe conformar un equipo con un líder y el personal necesario para realizar dichas actividades.

Posteriormente de se debe definir con la Dirección y/o Gerencia el alcance, los objetivos del plan y la identificación de los procesos críticos del negocio incluyendo las áreas en donde el proceso se considera crítico (No solamente Tecnología), definir Funciones y Responsabilidades.

También se debe contar con una Política para la continuidad del negocio que sea clara, precisa y concisa para que cualquier persona que la lea esté en capacidad de interpretar dicha política, identificar roles, responsabilidades y pueda ser aplicada buscando favorecer los objetivos del Negocio.

Por último se debe contar con un cronograma de actividades a desarrollar buscando lograr los objetivos descritos en la política del plan de Continuidad del Negocio, en donde también se debe identificar claramente los responsables de las actividades, plazos, tiempos de realización de las actividades, eventos de alcance de objetivos (hitos) y los indicadores de las actividades alcanzadas o indicador del estado de dichas actividades.

2) Conocimiento de los Procesos y Análisis de Riesgos.

Para el desarrollo de esta fase se debe entender claramente el objeto que persigue el negocio así como los productos y servicios críticos que realiza o brinda la organización, incluyendo las actividades realizadas de dichos productos y servicios junto con los recursos que lo soportan. También se debe identificar el impacto que genera al negocio los fallos en las actividades y recursos determinados como críticos.

Por otro lado se debe identificar y dar valor a los riesgos que podrían causar la interrupción en la producción de los productos y servicios de la organización.

Adicionalmente se debe establecer si se depende de proveedores o terceros para el cumplimiento de las actividades para que se puedan producir dichos productos y servicios, y determinar si la responsabilidad

es transferida, aunque por lo general para la Gestión de Continuidad del Negocio las responsabilidades no son transferidas.

Es importante resaltar que todas las organizaciones son al interior un conjunto de áreas, procesos, personas, equipos informáticos, dispositivos, comunicaciones, etc. que deben interactuar entre si y se puede tener los sistemas con los más altos estándares en tecnología y personal entrenado, pero si no se conoce la forma en que todos estos componentes interactúan para generar el producto y/o servicio, actividad, proceso, etc. para el negocio, cualquier esfuerzo por mantener la continuidad del negocio será inservible.

Una vez identificados los procesos críticos del Negocio junto con todas sus actividades, procesos y recursos, se debe realizar un análisis de los riesgos asociados y priorizar (Valorar) de acuerdo al impacto que genera en el caso en que se presente un evento que interrumpe el normal desarrollo de los procesos y/o actividades. Este impacto debe traducirse en la relación de costo – beneficio para la organización, es decir, el impacto será medible referente a cuanto representa económicamente a la organización en el caso de que se presente un evento de interrupción de sus actividades y se vean afectados sus procesos y la relación o el beneficio de poseer un plan de continuidad del negocio representado en la capacidad de recuperación del retorno a sus actividades normales y la buena imagen ante su competencia y la tranquilidad de sus clientes, inversionistas, accionistas y proveedores.

Dado lo anterior en donde se han verificado las actividades, estudiado los procesos, los riesgos de estos y calcular el impacto es normalmente lo que se conoce como el Análisis de Impacto del Negocio (BIA), el cual brinda una guía o base para armar un Plan de Continuidad del Negocio; dicho análisis permitirá a las organizaciones identificar qué perdidas podría llegar a tener si alguno de sus procesos o actividades y recursos que apoyan los mismos tiene una interrupción, así mismo permitirá conocer con qué recursos cuenta y los que harían falta para que el Plan de Continuidad del Negocio sea exitoso, de la misma forma permitirá conocer y poner en práctica la recuperación y en qué orden se deben restablecer las actividades y procesos de la operación después de la ocurrencia de un evento.

3) Medidas preventivas.

En esta fase deben ser consideradas las medidas de seguridad que deben ser aplicadas para tratar de evitar que se presenten incidentes o eventos, los cuales si no son bien gestionados hagan necesario la activación del Plan de Continuidad del Negocio.

Para realizar lo anteriormente expuesto se toma como base el Análisis de Riesgos y los resultados obtenidos del Análisis del Impacto del Negocio (BIA), para aplicar los controles que sean necesarios de forma tal que se aumente la fortaleza del negocio, reduciendo la probabilidad de ocurrencia de un evento que interrumpa el normal desarrollo de las actividades y que de

presentarse dicho evento limite el impacto a la organización y se minimice el tiempo de la interrupción.

En síntesis lo que se requiere es adoptar un plan de acción para los riesgos que no fueron considerados pero que de alguna forma se deben prevenir y evitar para tratar de no afectar la disponibilidad de los productos y servicios que brinda la organización, esto podría traducirse en algún momento en un beneficio en la relación costo – beneficio, ya que disminuye la posibilidad de enfrentar amenazas y vulnerabilidades aún mayores generando costos extras para la organización.

Algunas medidas preventivas, de acuerdo al objetivo del negocio, podrían ser que existiese redundancia de los sistemas de información, canales de comunicación con diferentes proveedores de servicio, copias de seguridad de la información sensible para la organización, sistemas de detección y prevención de intrusos, políticas de control de acceso, sistemas de seguridad física correctamente implementados y sensibilización y capacitación del personal de la organización.

4) Estrategia de Recuperación.

Partiendo de los resultados del BIA y el análisis de riesgos ya mencionados, en esta fase se identifican las alternativas de recuperación de los procesos críticos de la organización, teniendo en cuenta los tiempos definidos y aceptados de indisponibilidad de cada proceso.

Para garantizar que las soluciones y alternativas de recuperación sean las más adecuadas, los resultados del BIA deben contemplar los posibles daños potenciales sobre los activos y que se ajusten a la operación del negocio, es decir, las necesidades de la organización, contemplando factores como el costo asociado a la implementación, los beneficios de la estrategia a implementar, el tiempo de recuperación objetivo, la perdida máxima de información que una empresa puede asumir y el tiempo máximo permitido de interrupción del proceso crítico, partiendo del hecho que cada proceso tiene diferente prioridad de recuperación en función del impacto en las operaciones del negocio. Las estrategias de recuperación deben contemplar las personas, instalaciones, tecnología, información y proveedores como los principales recursos organizacionales para garantizar la continuidad del negocio.

Una vez analizadas y seleccionadas las estrategias de recuperación que serán empleadas como respaldo en caso de interrupción de las actividades críticas de negocio, es necesario documentar debidamente todas las soluciones y pasos a abordar en un plan que permita su implementación, seguimiento y mejora continua.

5) Desarrollo e Implementación del Plan de Continuidad del Negocio.

Una vez se han definido las estrategias, estas deben ser documentadas y se deben verificar colocándolas en acción por cada

uno de los responsables definidos en el Plan de Continuidad del Negocio en la organización y de esta forma se pasa de la fase de planificación a la fase de implementación realizando las acciones previamente definidas en las que se debe confirmar que existan los mecanismos que adviertan la ocurrencia de un evento y se active la Gestión de respuesta a Incidentes.

Por otra parte se debe verificar la continuidad de las actividades críticas del negocio, es decir, que se debe garantizar que el Plan de Continuidad del Negocio se está ejecutando y está siendo realizado por los responsables designados junto con los recursos asignados tanto humanos como tecnológicos hasta el retorno a la normalidad.

Dado lo anterior es entonces necesario definir los equipos y responsables que se necesitan para realizar la activación y la ejecución del Plan de Continuidad del Negocio, dichos equipos y responsables encargados de la puesta en marcha del plan pueden variar en cuanto a la cantidad de personas que lo componen de acuerdo a la estrategia de recuperación, a la cantidad de procesos y actividades a recuperar y al tamaño de la organización; por lo tanto es importante resaltar y clarificar las actividades identificadas como claves que se realizarán junto con sus responsables, quienes las llevaran acabo y el orden con que estas deben hacerse, como por ejemplo el equipo encargado de la gestión de respuesta a incidentes, en donde se analizará y se definirá el impacto de la incidencia a la organización y se verificará si es necesario activar el Plan de Continuidad del Negocio.

También se debe tener en cuenta los otros equipos que ayudarán a complementar la atención del incidente de ser necesario como son los Servicios de Emergencia (Policía, Bomberos, Asistencia Médica), Equipo de Manejo de Crisis, Equipo de Servicios de Soporte, Equipo de Logística, Equipo de Relaciones Públicas o de Comunicaciones, etc.

Una vez se han definido estos equipos, los responsables y las funciones a realizar por cada uno de ellos, la organización debe desarrollar los procesos y procedimientos a seguir. Estos últimos permitirán la ejecución del plan de continuidad del negocio, ya que poseen las características y el conocimiento para realizar la activación, ejecución y minimizarán el tiempo para la toma de decisiones críticas y el tiempo de reacción.

Dichos procesos y procedimientos deben ser claros, precisos, concisos, que se puedan realizar, que sean conocidos por los integrantes de los equipos que deben actuar en el plan de continuidad y deben estar elaborados en un lenguaje que todos los integrantes entiendan. Deben incluir las actividades, procesos, recursos críticos a recuperar, los tiempos de recuperación, situaciones en las que debe ser activado el plan de continuidad del negocio y deben tener la información que sea de utilidad para la Gestión de Continuidad del Negocio, como números de teléfono de terceros o proveedores, direcciones tanto físicas como lógicas, listas de chequeo, inventarios de

equipos necesarios para desarrollar el plan, etc.

Adicionalmente es importante tener en cuenta que dependiendo del tipo de desastre, los planes de continuidad del negocio también deben tener una copia o respaldo disponible en otro lugar diferente geográficamente a la ubicación de la organización y que deben estar en diferentes formatos (En papel y en medios electrónicos).

6) Mantenimiento del Plan de Gestión de Continuidad del Negocio.

Para garantizar que los procedimientos de recuperación establecidos permitan la continuidad de las operaciones a la hora de enfrentar un desastre, en esta fase deben trazarse los siguientes objetivos [1] :

- Inculcar y promocionar una cultura de continuidad de negocio en la organización de forma que paulatinamente se convierta en un proceso crítico a gestionar bajo un ciclo de mejora continua.
- Mejorar la eficiencia y eficacia del plan de continuidad de negocio.
- Transmitir fiabilidad a empleados, clientes, accionistas sobre la capacidad de la organización para superar posibles interrupciones de sus operaciones.
- Minimizar la probabilidad y el impacto de las interrupciones.
- Adaptar el plan de continuidad a los cambios de la organización y de negocio a los que se enfrentan las empresas, revisando periódicamente los análisis de riesgos, los Análisis de Impacto en el Negocio (BIA) y los contactos y responsabilidades asignados que deben mantenerse actualizados en las estrategias y los procedimientos [1].

Una vez desarrollado e implementado el plan de continuidad del negocio, la organización debe someterlo a pruebas sin que afecten las operaciones del negocio. Este objetivo se logra planificando cada aspecto y elemento involucrado; criticidad del proceso, alcance, secuencia de ejecución, duración, participantes, con el fin de cubrir aspectos propios de las organizaciones, tales como:

- Descubrimiento mejoras y eficiencias que al ser aplicadas, perfeccionan el plan.
- Los procesos de negocio, las interdependencias, el entorno tecnológico y otros componentes adicionales cambian con el paso del tiempo desactualizado los procesos que soportan los planes de continuidad de negocio y por tanto su eficacia.
- Evaluar de forma más veraz la capacidad de respuesta de una compañía ante un desastre (tiempos de respuesta, capacidad de los responsables implicados e idoneidad de los procedimientos desarrollados).

El mantenimiento del plan da a conocer el estado de madurez, la viabilidad y eficacia del plan, pero así mismo se deben

tener en cuenta los riesgos asociados al mantenimiento del plan.

Por otro lado, y como medida general, se recomienda que los planes de continuidad de negocio, aparte de ser flexibles, sean probados al menos una vez al año a través de la realización periódica de simulacros que reproduzcan de forma ficticia situaciones de emergencia o contingencia. Dicha periodicidad depende de las necesidades que determine la organización y el entorno en el que opera [1].

IV. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA Y GESTIÓN PARA LA CONTINUIDAD DEL NEGOCIO ¿DOS PROCESOS IGUALES, PARALELOS O COMPLEMENTARIOS?

La gestión de incidentes y la gestión de la continuidad del negocio son dos elementos principales de la parte operativa de un sistema de gestión. Estos elementos deben tener como objetivo alinear la resolución de incidentes y la continuidad de una organización con los objetivos del negocio.

El esquema de un incidente permite identificar etapas desde el momento que se presenta, su resolución y retorno a la normalidad, y en casos con altos niveles de afectación sobre las operaciones debe incluir la etapa de activación del plan de continuidad del negocio. Es por esto que el plan de gestión de incidentes debe garantizar la disponibilidad del servicio tan pronto como sea posible, evitando la necesidad de invocar el plan de continuidad. De ser necesaria su invocación, esta debe estar claramente definida dentro del plan de gestión de incidentes, apoyándose en el Plan de Continuidad del Negocio como proceso paralelo.

Partiendo de este hecho, ante un incidente estos dos planes se convierten en procesos independientes, paralelos que deben estar perfectamente integrados y coordinados para recuperar la normalidad de las operaciones en el menor tiempo posible.

Esta interoperabilidad se puede ilustrar basada en el objetivo de tiempo de recuperación tal como se muestra en la Fig.1.

El plan de gestión de incidentes debe iniciar en un tiempo muy cercano a la presentación del incidente o en el mismo instante en que es detectado (Punto 1 de la Fig. 1); en este punto las operaciones y/o actividades acaban de pasar de la normalidad a la degradación de dichas operaciones, por consiguiente se debe realizar el registro del evento, la evaluación del mismo y su clasificación de acuerdo al impacto; establecido esto se verifica si puede ser solucionado o si es necesario realizar el escalamiento definido en el plan de gestión de incidentes y como última opción para el Plan de incidentes se debe invocar el plan de gestión de continuidad del negocio como un proceso paralelo (Punto 2 de la Fig. 1).

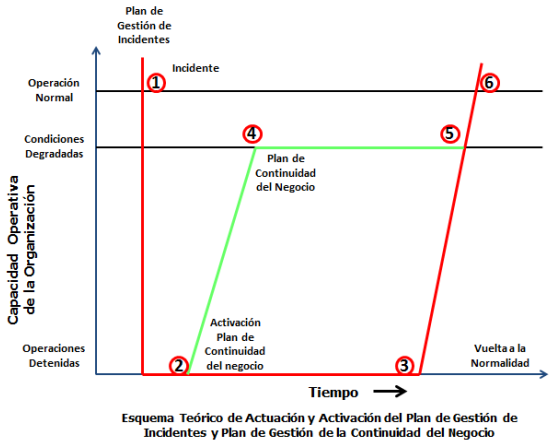

Fig. 1 Esquema teórico de actuación y activación del plan de plan de gestión de incidentes y plan de Gestión de la Continuidad del Negocio [2].

Una vez se ha puesto en marcha el plan de continuidad del negocio, este debe en el menor tiempo posible brindar las condiciones suficientes para que el negocio continúe en funcionamiento sin importar que el incidente no haya sido solucionado todavía (Punto 4 de la Fig. 1).

Es importante resaltar que el plan de continuidad del negocio debe estar en capacidad de soportar la operación mientras el plan de gestión de incidentes continúa trabajando en la búsqueda de la solución.

De manera alterna y paralela el equipo de gestión de incidentes debe estar realizando las gestiones necesarias para atender el incidente y tratar de llevar a la organización a su operación normal (Punto 3 de la Fig. 1).

Una vez se ha encontrado la solución al incidente presentado los dos equipos tanto de gestión de incidentes como de gestión de continuidad del negocio deben coordinar esfuerzos para la vuelta a la normalidad (Puntos 5 y 6 de la Fig. 1).

Como se puede observar en la Fig. 1 existen dos puntos críticos e importantes 2 y 6, dado que la toma de decisión de la activación del plan de continuidad de negocio debe hacerse en el momento preciso para que no derive en un problema mayor y también la vuelta a la normalidad puesto que es necesario coordinar los esfuerzos entre los dos equipos priorizando las actividades a realizar y hacerlo de forma ordenada para que no se convierta en un caos dicho retorno.

La identificación temprana de los incidentes es fundamental a la hora de responder a los mismos de forma ágil y efectiva. Un incidente que no es identificado, evaluado y gestionado adecuadamente puede derivar en un problema de mayor magnitud o incluso en una crisis [2].

V. RETORNO A LA NORMALIDAD

Una vez superado el incidente debe existir relación entre los grupos de los dos procesos (Gestión de Incidentes y Gestión de la Continuidad del Negocio), es decir, en este proceso debe participar personal de los dos grupos para realizar un retorno a la normalidad de forma coordinada y porque cada cual posee información de cada proceso importante y la prioridad con que los sistemas deben ser recuperados a su funcionamiento normal; lo cual no indica que deban participar todos los integrantes de los dos equipos. Para esto se deben definir

los responsables, canales de comunicación y el monitoreo de las actividades.

VI. ANÁLISIS Y MEJORA CONTINUA

Posterior al retorno a la normalidad es necesario evaluar los procesos involucrados para encontrar los puntos a mejorar y hacer mucho más eficaces y eficientes la gestión y el manejo ante eventos futuros.

A. La mejora continua de los procesos.

La mejora continua garantiza que los procesos involucrados alcancen un nivel de excelencia. El proceso de mejora continua relaciona todas aquellas actividades necesarias a implementar en la organización para enfrentar incidentes futuros. La organización debe apoyarse en los incidentes atendidos y la información obtenida para que mediante un plan de acción se tome medidas que permitan mejorar los mecanismos de protección para limitar la exposición al riesgo, evitando que incidentes similares se repitan.

Con el fin de garantizar la madurez de los planes de gestión estos deben ser mantenidos a través de ciclos de mejora continua mediante la revisión constante de los cambios estratégicos, operacionales o tecnológicos que impacten los procesos del negocio y permita determinar qué ajustes se deben realizar en los procesos y procedimientos para mantener su capacidad y efectividad basados en los resultados de re-evaluar el análisis de riesgos y el análisis de impacto del negocio (BIA).

En cada uno de los ciclos de mejora los procesos deben mantener criterios que garanticen su funcionalidad y verifiquen que el proceso se encuentra alineado con la estrategia de la organización, resulta de utilidad para la toma de decisiones, responde a los requisitos legales y normativos, presenta criterios adecuados para el cálculo de riesgos, cuenta con los recursos necesarios, presenta una definición adecuada de nivel de riesgo aceptable [2].

Existen dos puntos importantes para garantizar la mejora continua de los procesos de gestión de incidentes y de continuidad del negocio: Su flexibilidad y Evaluación periódica. Las pruebas deben estar orientadas a obtener resultados que permitan su actualización con el objetivo de planificar las modificaciones necesarias para colaborar en la mejora continua de los mismos.

B. Revisar las políticas y mecanismos de respuesta.

Posterior al incidente y basados en las lecciones aprendidas durante la resolución, todas las partes involucradas deben revisar aspectos tanto del proceso de gestión de incidentes como de continuidad del negocio, principalmente procedimientos y mecanismos de respuesta tendientes a tomar las medidas de protección que mitiguen la exposición al riesgo y las políticas que nos permitan ajustar los controles obteniendo de esta forma un proceso de mejora continua.

VII. CONCLUSIONES

El plan y los elementos y de gestión deben alcanzar la madurez, capacidad operativa, de respuesta y resolución a un incidente, demandando en el menor tiempo y con la menor afectación posible, involucrando el menor número de recursos de la organización. Las medidas y respuestas del plan de gestión de incidentes deben obtener un nivel de solución capaz de enfrentar los eventos críticos sin la necesidad de invocar el plan de continuidad del negocio.

La gestión de incidentes y la gestión de continuidad del negocio no son dos procesos iguales, aunque similares ambos deben desarrollarse de forma paralela ante la presencia de un evento que genere interrupción total o parcial de las operaciones y/o actividades críticas del negocio; podría decirse también que son complementarios ante la ocurrencia del incidente.

Como se pudo observar en el desarrollo de este artículo en los dos procesos de gestión, el Análisis de Impacto del Negocio (BIA) es de suma importancia para realizar la valoración del impacto en cualquier proceso, por lo tanto debe considerarse como una herramienta imprescindible al momento de determinar los procesos críticos del negocio y su categorización.

REFERENCIAS

[1] Instituto nacional de Tecnologías de la información. Inteco. Guía práctica para Pymes: Cómo implantar un plan de continuidad del negocio. [Citado Octubre de 2010]. Disponible en [http://www.bsigroup.es/upload/docs/guia_practica_para_pymes_como_implantar_un_plan_de_continuidad_de_negocio.pdf].

[2] Lerma Agustín, Benito Gómez Mariano. Gestión de Incidentes y Gestión de la Continuidad del Negocio: Hermanos pero no gemelos. [Citado Agosto de 2010]. Disponible en [http://www.bsigroup.es/upload/Technical%20articles/Continuidad_de_negocioBS25999_Sept2011.pdf].

[3] Ramos Antonio. Gestión de Incidentes y planes de Continuidad de Negocio. [Citado Febrero de 2008]. Disponible en [http://www.aetical.com/aetical/images/contenidos/GLOBALTECH08_S21sec.pdf].

[4]Aquino Rubén, Chávez José Luis. Proyecto AMPARO. Manual de Gestión de Incidentes de Seguridad Informática. [Citado Marzo de 2010]. Disponible en [http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf].

Autores

Carlos Javier Calderón Martínez
Ingeniero en Telecomunicaciones
Universidad de Pamplona
2007
Analista Junior de Seguridad de la Información
Digiware de Colombia S.A
Estudiante Especialización en Seguridad Informática
Universidad Piloto de Colombia
2013

Leonardo Castro Ordóñez
Ingeniero de Sistemas
Universidad Antonio Nariño
2002
Analista Seguridad Informática
Banco GNB Sudameris
Estudiante Especialización en Seguridad Informática
Universidad Piloto de Colombia
2013