Anticipando la Crisis

Luis A. Blanco Colón
Ciencias de Computadoras
Juan Ramirez, PE, Ph.D
Departamento de Ciencias de Computadora
Universidad Politécnica de Puerto Rico

Abstracto *— Este proyecto tiene como meta orientar sobre los objetivos necesarios que una empresa debe establecer, para implementar un plan de contingencia para evitar interrupciones parciales o prolongadas de sus actividades de negocio. En el ambiente riesgoso y competitivo en que vivimos, muchas empresas están optando por establecer planes de continuidad de negocio, para mejorar su habilidad de responder o mitigar estas interrupciones. Este plan es una herramienta que permite a las empresas reconocer sus vulnerabilidades, e implementar procesos que le permitan responder de manera eficiente para mantener operando a una empresa, antes, durante o después de un desastre o evento que pueda afectar sus operaciones de negocio.*

INTRODUCCIÓN

A partir de los actos terroristas del 11 de septiembre de 2001, muchas empresas han notado lo vulnerable que estas pueden estar y han comenzado a implementar planes de continuidad para responder a cualquier acto, ya sea por causa natural, tecnológica o humana. Los avances tecnológicos, la innovación en los servicios, el deseo de toda empresa de competir en el mundo globalizado, han dirigido a las empresas a crear una gran dependencia de los sistemas de información y las comunicaciones. Esta necesidad de competencia ha expuesto a sus sistemas, creando la necesidad de protegerlos de diferentes ataques. Los empresarios deben comprender la necesidad de mantener a la empresa operando ante cualquier adversidad, y adaptar e implementar planes de continuidad que permitan proteger a sus activos de cualquier desastre o evento que los pueda afectar. En este proyecto, exploramos algunos de los componentes claves para establecer un plan de continuidad de manera efectiva en una empresa, que servirá de guía para la creación, implementación y mantenimiento del mismo.

JUSTIFICACIÓN DEL PLAN

Antes de entrar en los componentes necesarios para establecer el plan, debemos comprender la necesidad de establecer el plan. Un estudio hecho sobre empresas que habían tenido una pérdida masiva de información, demuestra que 43% de éstas nunca restablecieron su actividad de negocio, 51% cerraron en los siguientes dos años, y solamente 6% lograron sobrevivir[2]. Estos análisis han demostrado, además, que cuando el período de funcionalidad de la empresa se extiende por periodos prolongados, una gran mayoría de estas empresas han tenido que acogerse a la quiebra parcial o total. Es por esta razón que un plan de continuidad del negocio es primordial para toda empresa. En el evento de los World Trade Center, el 11 de septiembre de 2001, 150 empresas de 350 afectadas no pudieron sobrevivir al evento, solo aquéllas con un plan de continuidad bien desarrollado, lograron restablecer sus operaciones en días [1].

OBJETIVO DEL PLAN

La seguridad de los sistemas de informática se ha convertido en uno de los asuntos primordiales de las empresas en los pasados años, esto debido a la necesidad de competir más efectivamente ante los mercados competitivos. Los avances tecnológicos que hemos experimentado en los pasados años, han expuesto a los sistemas de información a ataques cibernéticos, hackers, espionaje, sabotaje y otros. Los objetivos primordiales del plan de Continuidad

de Negocio es proteger la vida de sus empleados, sus activos fijos y la integridad de sus sistemas computadorizados. Este plan debe ser diseñado tomando en consideración las necesidades particulares de la empresa que lo desarrolle. Esto significa que aunque dos empresas pudiesen encontrarse con el mismo desastre, sus respuestas al mismo podrían ser diferentes, ya que sus necesidades, no necesariamente son similares. Tomando esto en consideración, podemos establecer que no existe un solo plan que albergue todas las soluciones posibles. Pero en muchas ocasiones es casi imposible definir todas las posibles soluciones para evitar o prevenir el suceso.

COMPROMISO AL PLAN

Desarrollar un plan de continuidad es un proceso que puede ser costoso, difícil de diseñar y de establecer. Para que este plan pueda tener éxito, el mismo debe de contar con la aprobación y el compromiso total de la alta gerencia de la empresa. Para establecer este plan la empresa tendrá que comprometer recursos económicos y de personal para su análisis, diseño y establecimiento. Así que un plan que no cuente con la aprobación y ayuda de los ejecutivos de la empresa, está destinado al fracaso. Una buena práctica para muchas empresas es el de elegir un alto ejecutivo como parte de los comités necesarios para el desarrollo del plan.

COMITÉS PARA EL PLAN

Para poder crear un plan de contingencia es necesario crear un comité que pueda servir de guía para el plan. Muchas empresas designan a un coordinador de proyecto, para que éste se haga cargo de la coordinación del plan, y de todas las actividades del comité o de los diferentes comités que puedan surgir. El coordinador de proyecto debe estar claro de los objetivos del plan, y además debe tener un amplio conocimiento de las operaciones de la empresa. En muchas ocasiones es el coordinador de proyecto, el que escoge al personal para el comité a cargo del establecimiento del plan. El comité debe contar con personal de cada una de las áreas operacionales de la empresa, de manera que éstos puedan contribuir en identificar procesos y funciones críticas dentro de su área operacional. Una vez constituido el comité, el coordinador de proyecto debe establecer una fecha para coordinar la agenda del plan. Algunos de los aspectos que se podrían atender en esta primera reunión son:

- Introducción al Plan de Continuidad
- Organización del proyecto
- Información inicial requerida
- Identificación de causas potenciales de desastre o amenaza
- Identificación de impacto a los potenciales desastres o amenazas
- Metodología y desarrollo del plan
- Pruebas del plan
- Entrenamiento del personal

El coordinador de proyecto debe de coordinar con la alta gerencia de la empresa, para identificar el alcance del plan y los recursos para el establecimiento del mismo.

DOCUMENTOS REQUERIDOS

El coordinador de proyecto junto con el comité designado para el desarrollo del plan deben de preparar una lista de documentos e información que serán parte del plan y contribuirán a su diseño y ensamblaje. Algunos de los documentos más usados para la elaboración del plan, lo son:

- Gráfica organizacional de la empresa incluyendo nombres y posiciones
- Información de contacto de los miembros de cada comité
- Lista de suplidores con teléfonos de emergencia
- Lista de servicios de emergencia con teléfonos (bomberos, policías, hospitales, etc.)
- Inventario de equipos del departamento de IT
- Lista de programas utilizados por la empresa con sus respectivos números de licencia
- Especificaciones de los sistemas de comunicaciones y sus respectivos manuales de usuarios

- Políticas de la empresa
- Procedimientos operacionales y administrativo
- Copia de los planos de piso de las facilidades
- Copia de Pólizas de seguros
- Copia de garantías o contratos de servicios de los sistemas de IT
- Lista de Regulaciones o guías relevante a la industria
- Procedimientos de Resguardo de información

La amenaza

Podemos definir la amenaza como "La posibilidad de incurrir en pérdida como resultado de un evento". Una amenaza es un evento o circunstancia con el potencial de causar daño a un sistema, una empresa o un ser humano. Estas amenazas regularmente tienden a tener resultado solo cuando una vulnerabilidad existe dentro de nuestros sistemas o procesos. Por ejemplo, una empresa que tenga una planta de energía eléctrica para reaccionar a una interrupción de energía, habrá eliminado una vulnerabilidad. Si esta planta eléctrica trabaja con diesel o gasolina, la falta de uno de éstos podría ser una vulnerabilidad durante una interrupción prolongada. El coordinador de proyecto, junto con el comité designado deben de identificar todas y cada una de las vulnerabilidades dentro de los procesos de la empresa. Esta fase es una compleja y se necesita tener un amplio conocimiento de las operaciones de la empresa para poder identificarlas. Las fuentes más comunes de amenaza son las naturales, las humanas y las tecnológicas. Algunas de las amenazas con las que muchas empresas deben lidiar son:

- Naturales
  - Tormentas
  - Inundaciones
  - Terremotos
  - Tsunamis
- Tecnológicas
  - Interrupción de energía
  - Interrupción en las comunicaciones
  - Fallo de los sistemas de información
- Humanos
  - Virus
  - Hackers
  - Espionaje
  - Fraude

Análisis de Impacto

El análisis de impacto del negocio es el proceso mediante el cual identificamos las funciones críticas de la empresa, y sus efectos si estas funciones no estuvieran disponibles. Este análisis ayuda a identificar la pérdida que relacionada a la función, como pérdida de ingresos, pérdida de equipo, pérdida de reputación y otros. Otra de las ventajas de hacer un análisis de impacto es que ayuda a identificar cuán rápido necesita la empresa restablecer un proceso ante una amenaza, para evitar pérdida alguna. El análisis de impacto es confundido en ocasiones con la Evaluación de Riesgo. La evaluación de riesgo es utilizada para determinar la potencial pérdida de una función ante un riesgo, y evaluar ésta con el costo de proteger el activo vs el valor del activo.

Estrategias de Mitigación

Como hemos hablado anteriormente, es sumamente difícil identificar todas las vulnerabilidades a las que está expuesta una empresa. Las amenazas a las que sus procesos podrían estar expuestos, pueden ser tantas, que sería difícil poder identificar todas. Existen una serie de estrategias de mitigación que son básicas para toda empresa, y que no requieren un alto nivel de análisis para poder ser implementadas. Para muchos desarrolladores de planes de continuidad, estas estrategias pueden ser clasificadas en tres fases. La primera fase es la de seguridad física, esta regularmente puede ser implantada con un presupuesto bajo y muchas de las estrategias se pueden deducir con un poco de sentido común.

- Servicios eléctricos deben estar resguardado en cuartos con seguridad y el acceso debe ser para personal autorizado
- Equipos de Computadoras, como servidores, "routers", "switches", "gateways", cables y otros, deben estar en cuartos seguros y el acceso debe ser controlado. Además, estos equipos no deben tener acceso a través de plafones o pisos elevados
- Estas áreas deben de ser monitoreadas por personal de seguridad y cámaras de seguridad.
- El cuarto de cómputos debe estar en el centro de las facilidades, y si es un edificio, no debe de estar en el primer piso

La segunda fase es la de seguridad de los datos de información. La empresa debe poner mucho énfasis en proteger este activo ya que es uno irremplazable.

- Establecer políticas de resguardo de información, y si es posible, en facilidades alternas
- Establecer políticas de acceso a información utilizando métodos de autenticación y asignando privilegios por individuo, por grupo o por tipo de trabajo
- Cifrar cualquier información de carácter confidencial o clasificada

La tercera fase es la seguridad de la red. Esta regularmente es la más compleja ya que requiere de conocimientos técnicos, en algunos casos para configurar equipos. Alguna de las estrategias de mitigación más comunes, son:

- Instalar sistemas de 'firewall', para controlar el acceso desautorizado a la red
- Instalar suplentes de corriente eléctrica 'UPS' a equipos de cómputos
- Instalar planta eléctrica para la empresa
- Crear políticas de seguridad para el personal y orientar al personal sobre estas políticas

PASOS PARA ESTABLECER EL PLAN

No existe un diseño o un código formal de cómo establecer un plan. De hecho el plan puede ser desarrollado de muchas formas, siempre que el mismo cumpla con su cometido. Existe una gran deferencia entre compañías dedicadas a desarrollar planes de continuidad en cómo debe ser estructurado el plan, pero todas ellas concuerdan en que al menos deben de existir los siguientes seis pasos en todo plan de contingencia. Estos pasos, que son primordiales para que el plan sea uno efectivo y capaz de mitigar cualquier amenaza o de restituir un proceso a su condición natural, son:

- Planificar la metodología a utilizar para el plan y coordinar con el comité y los ejecutivos los pasos necesarios para la iniciación del plan.
- Identificar las amenazas potenciales que puedan afectar el funcionamiento del negocio.
- Evaluar el impacto de las potenciales amenazas y determinar el daño financiero que éstas puedan tener.
- Seleccionar las técnicas de manejo apropiadas para evitar o mitigar la amenaza.
- Diseñar el plan de contingencia utilizando las técnicas de manejo seleccionadas.
- Evaluar, revisar y probar que el plan sea efectivo.

Figura 1
Pasos del plan

Como podemos observar de la grafica en la Figura 1, este plan es uno cíclico, debido a que el

mismo debe de ser revisado y actualizado anualmente o cuando las condiciones organizacionales de la empresa así lo ameriten.

Planificación del Plan

El primer paso para establecer el plan es la planificación o metodología a utilizar por parte del coordinador de proyecto y el comité a cargo de desarrollar el plan de continuidad. Estos deben de establecer junto con los gerentes de la empresa, un itinerario de trabajo para el proyecto. Además, como parte de esta planificación se deben de establecer las políticas del plan, sus alcances, las reuniones con el personal, los documentos requeridos para el plan y cualquier otro asunto que sea necesario para los inicios de los trabajos.

Identificar las amenazas

El próximo paso en el proceso de desarrollo del plan, es identificar las funciones críticas de la empresa e identificar las posibles amenazas a los que éstas pueden estar expuestas. En esta fase el gerente del proyecto junto al comité, se reunirán con cada uno de los ejecutivos y directores de departamento de la empresa. El propósito es identificar los procesos fundamentales de cada uno de los departamentos para identificar aquéllos que son críticos para el departamento. Estos procesos críticos deben de ser clasificados por departamento y por su impacto en las operaciones de la empresa. Este comité debe de auditar el manejo de las operaciones, el uso de los sistemas de información, el manejo de documentos y cualquier otro proceso que desempeñe el departamento. Además, debe de analizar el impacto que un departamento pueda tener sobre otro en caso de una interrupción parcial o prolongada.

Evaluación del Impacto

El tercer paso es el de evaluar cómo afecta al negocio la pérdida o interrupción de cada una de las funciones críticas a que se hace referencia en la fase anterior. Esta fase es una de las más difíciles ya que se debe medir el costo o el impacto económico que éstas tienen sobre la empresa. Una pobre evaluación del impacto, podría hacer creer a la empresa que alguno de estos procesos no es vital para su funcionamiento y no tomarlo en consideración durante la elaboración del plan. Durante esta fase se debe evaluar la amenaza individual y colectiva de cada una de las operaciones de la organización y organizarlas en orden de mayor impacto. También, se debe de identificar el tiempo que tomaría restablecer el proceso, tomando en consideración el tipo de evento que lo afecte. Es imperante que el comité conozca el funcionamiento de la empresa y del sistema de información, y cómo éstas contribuyen al funcionamiento de cada uno de sus departamentos.

Técnicas de Manejo

En esta fase ya se ha identificado y analizado el impacto de los procesos medulares de la empresa. Los ejecutivos de la empresa, junto al comité constituido deben seleccionar aquellos procesos para los cuales desean tomar acción, tomando en consideración el impacto que cada uno de ellos tiene sobre la empresa. En esta fase se deben identificar las herramientas necesarias para prevenir o mitigar el impacto en el proceso, o para restituir el mismo. Muchas empresas dedicadas a la implementación de planes de contingencia, utilizan un análisis de costo beneficios para justificar la inversión de estas técnicas. También es importante durante esta fase, que se constituya el comité que estará a cargo del manejo e implementación del plan, de manera que estas técnicas de manejo cuenten con la aceptación de este nuevo comité. Además, es necesario que este comité, al igual que el comité anterior, cuente con personal de cada uno de los departamentos y con un ejecutivo de la organización.

Diseño del Plan

En la fase de diseño, el comité presentará las técnicas de manejo diseñadas para el plan de

continuidad y comenzará a redactar el manual que servirá de guía. Este manual debe ser impreso y se deben mantener varias copias en la empresa, y al menos una en otra localidad segura. Entre las cosas más comunes que este manual puede contener, son:

- Procedimientos de Mitigación
- Procedimientos de Restauración
- Procedimientos de Remplazo
- Procedimientos de Auditoria
- Políticas de Seguridad
- Políticas de empleado
- Plan de Recuperación de Desastre
- Lista de contactos de los comités, la gerencia, suplidores y contratistas
- Plano general de la estructura o estructuras que contempla el plan
- Localizaciones y recursos de facilidades de resguardo.
- Lista de equipos y licencias

La empresa debe de asegurarse que el plan sea realista y fácil de entender durante una crisis.

EVALUACIÓN Y MANTENIMIENTO DEL PLAN

El propósito de probar el plan es lograr que la organización lo acepte porque sus soluciones satisfacen los requerimientos de recuperación. Muchos planes no logran cumplir sus expectativas debido a que son imprecisos, tienen boquetes en su diseño o errores de implementación. Se deben de crear unos escenarios para probar los procesos de recuperación y ejecución de los empleados y contratistas externos. El primer paso en la planificación de los procesos, es definir los objetivos de las pruebas. Estas pruebas deben de simular de la forma más precisa las condiciones reales a la que el proceso puede estar expuesto. Este paso es uno de mucho esfuerzo considerando que puede ser muy difícil simular alguna de las condiciones a las que pueden estar expuestos los procesos. Otro problema de esta fase es que algunas ocasiones envuelve la coordinación de más de un departamento, y de personal interno y externo de la empresa. Como parte del proceso de evaluación se deben de crear unos documentos de evaluación, que serán utilizados para medir la efectividad de la prueba. Estos documentos se utilizarán para identificar fallas en el proceso de recuperación, y servirán de guía para modificar y mejorar el proceso. Antes de comenzar cada prueba se debe de determinar el costo que la misma pueda tener sobre las operaciones de la empresa. Considerando que toda prueba tiene un costo envuelto, de éstas ser considerables, debiesen de contar con la aprobación de los altos ejecutivos. Antes de comenzar con las pruebas se debe entrenar al personal que formará parte de los comités de respuesta. Todo plan de continuidad de negocio debe ser probado periódicamente para asegurar que sus procesos de mitigación sigan siendo efectivos. Por tal razón se recomienda que el plan sea probado una o dos veces al año. También debemos de tomar en consideración que cualquier cambio de personal u organizacional dentro de la empresa puede tener un efecto adverso dentro de los procedimientos del plan, por tal razón éste debe de ser auditado constantemente. Algunas compañías contratan firmas de auditores para corroborar la efectividad del plan y evaluar los costos de impacto de cada uno de los procesos de recuperación.

CONCLUSIÓN

A principio de los años 90, la seguridad no era una prioridad para las empresas, debido a que sus sistemas de cómputos posiblemente no tenían una puerta abierta al mundo, como lo es el Internet. Aquellos que tenían conexión al Internet, regularmente lo lograban a través de una línea "dial-up" que en muchas ocasiones solo operaba por tiempos limitados. La necesidad de las empresas por competir y obtener mayores ganancias, junto a los avances tecnológicos de los pasados años, han creado una necesidad en la industria a invertir en seguridad para sus sistemas. Existen muchas condiciones que pueden poner en peligro los activos de una empresa. Si consideramos que el mercado es cambiante y

competitivo, y que cualquier interrupción del negocio pone en peligro su reputación, su existencia y sus finanzas, entonces debemos de reconocer la necesidad de crear un plan de continuidad de negocio.

INVESTIGACIONES FUTURAS

Para investigaciones futuras creo que se podría abarcar en las diferencias entre el Plan de Continuidad del Negocio y el Plan de Recuperación de Desastre. Existe una diferencia en la metodología y diseño de estos planes, la cual podría ser considerada para futuras investigaciones.

REFERENCIAS

[1] Federal Emergency Management Agency, *"Purpose of Standard Checklist Criteria for Business Recover",* March 2006.

[2] Rittinghouse, John W., Ransome, James F., "*Business Continuity and Disaster Recovery for the InfoSec Managers"*, Maryland: Elsevier Digital Press, 2005