CURSO PLAN DE CONTINUIDAD DEL NEGOCIO (BCP, DRP)

PLAN DE CONTINUIDAD DEL NEGOCIO

Plan de Continuidad del Negocio

Un plan de continuidad del negocio PCN, se enfoca en sostener las funciones del negocio de una entidad durante y después de una interrupción a los procesos críticos del negocio.

Planes que complementan el Plan de Continuidad del Negocio

En la figura siguiente, se observa una versión completa de los diferentes tipos de planes, relacionados con la atención de emergencias, y que se interrelacionan con un Plan de Continuidad del Negocio (BCP, DRP).

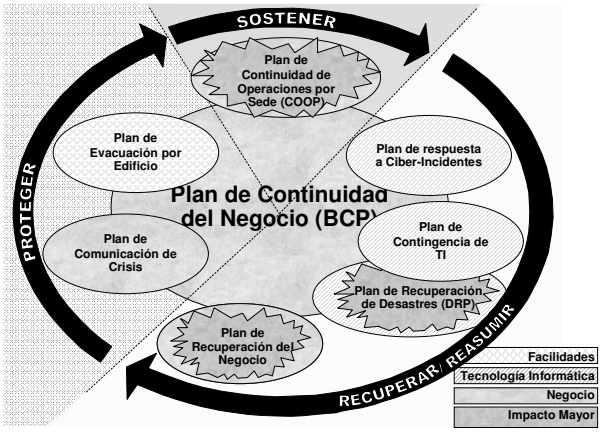

Figura 1. Plan de Continuidad del Negocio.(BCP, DRP)

Se desprende la conveniencia de que un Plan de Continuidad del Negocio se complemente con otros planes que ayudan a su efectividad. Sin embargo, debido a la carencia de definiciones estándar para estos tipos de planes, en algunos casos, el alcance de los mismos puede variar entre las diferentes organizaciones. Estos planes son:

- **Plan de comunicación de crisis**: documento que contiene los procedimientos internos y externos que las organizaciones deben preparar ante un desastre. Este plan debe estar coordinado con los demás planes para asegurar que sólo comunicados aprobados sean divulgados y que solamente personal autorizado sea el responsable de responder las diferentes inquietudes y de diseminar los reportes de estado al personal y al público.

- **Planes de evacuación por edificio:** contiene los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y seguridad del personal, el ambiente o la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica.

- **Plan de continuidad de operaciones por sede o filial (COOP por sus siglas en inglés – Continuity of Operations Plan):** orientado a restaurar las funciones esenciales de una sede o filial de la entidad (ej: una agencia, la fábrica, el almacén de ventas) en una sede alterna y realizar aquellas funciones por un período máximo de 30 días antes de retornar a las operaciones normales. Debido a que un COOP se enfoca en sedes o filiales, debe ser desarrollado y ejecutado independientemente del BCP. Interrupciones menores que no requieren reubicación en una sede alterna típicamente no son cubiertas en un COOP.

- **Plan de respuesta a ciber-incidentes**: Establece procedimientos para responder a los ataques en el ciberespacio contra un sistema de Tecnología Informática (TI) de una entidad. Estos procedimientos son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como: Acceso no autorizado a un sistema o dato, Negación de servicio, Cambios no autorizados a HW, SW o datos.

- **Planes de contingencia de TI**: orientado a ofrecer un método alterno para sistemas de soporte general y para aplicaciones importantes Debido a que un Plan de contingencia de TI debe ser desarrollado por sistema de soporte general y por cada aplicación importante, existirán múltiples planes de contingencia.

- **Plan de recuperación de desastres (DRP):** Orientado a responder a eventos importantes, usualmente catastróficos que niegan el acceso a la facilidad normal por un período extendido. Frecuentemente, el DRP se refiere a un plan enfocado en TI diseñado para restaurar la operabilidad del sistema, aplicación o facilidad de cómputo objetivo en un sitio alterno después de una emergencia. El alcance de un DRP puede solaparse con el de un Plan de Contingencia de TI; sin embargo, el DRP es más amplio en alcance y no cubre interrupciones menores que no requieren reubicación.

- **Plan de recuperación del negocio:** Permite restaurar un proceso de negocio después de una emergencia, pero al contrario del BCP, carece de procedimientos para asegurar la continuidad de procesos críticos durante una emergencia o interrupción.

Productos que componen el Plan de Continuidad (BCP,DRP)

El Plan de Continuidad del Negocio incluye los siguientes productos:

1. Business Impact Analysis (Impacto de Análisis del Negocio).
2. Risk Assesment (Evaluación o Valoración de Riesgos).
3. Estrategias de Continuidad.
4. Estructura Organizacional para la Continuidad (Roles, responsabilidades y procedimientos).
5. Procesos y Procedimientos de Continuidad.
6. Plan de Pruebas del Plan de Continuidad.

CONTENIDO DEL SEMINARIO

- Introducción al Plan de Continuidad
- Metodología para el Plan de Continuidad
- Realización del BIA
- Análisis de riesgo
- Estrategias de mitigación
- Desarrollo del Plan de Continuidad
- Pruebas del Plan
- Mantenimiento del Plan

Duración seminario: 20 horas

Máxima capacidad: 6 personas

Costo: 3000 U$ (No iva)

Conferencistas: ING: Fernando Ferrer CISA, PMP, Cobit
ING:Rodrigo Ferrer CISSP, CISA, ABCP, CST, CSSA.