

CURSO: DISEÑO DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES

En las últimas décadas, las entidades a nivel nacional, han concedido una importancia creciente a la implementación de planes detallados y precisos que garanticen la continuidad de sus procesos ante eventualidades de diversa índole que afecten la prestación de sus servicios. Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos como el terrorismo, han mostrado la necesidad de incorporar nuevas amenazas en el proceso de gestión del riesgo. Es así, que los denominados Planes de Recuperación ante Desastres (DRP)¹ buscan sostener las funciones de TI de una entidad durante y después de una interrupción.

Es así que, por medio de la implantación de medidas o controles que de alguna forma mitigan el impacto producido por un evento determinado, se puede lograr confianza de parte de una comunidad específica a los servicios ofrecidos. En este punto, es importante considerar que no sólo debemos tener en cuenta en nuestro Plan de Recuperación ante Desastres, aspectos solamente económicos, sino, que temas como la reputación y la credibilidad de una compañía, pueden poner en peligro su funcionamiento a futuro, si ante un desastre o evento adverso no se responde con la adecuada estrategia y acciones debidamente soportadas por un plan previamente diseñado e implementado.

Ante un desastre uno de los principales problemas con que el que tendremos que enfrentarnos es el hecho que los usuarios tanto internos como externos no podrán acceder a sus sistemas de soporte o sistemas críticos. Este tipo de demoras o inclusive la imposibilidad de entregas de productos o de la prestación de un servicio pueden ser ocasionadas por ejemplo por el fuego, una falla prolongada de potencia, una inundación o un terremoto, entre otros eventos.

Recapitulando, el objetivo del Plan de Recuperación ante Desastres es, pues, sostener los sistemas de información críticos durante y después de una interrupción a través de la definición de estrategias de continuidad, recursos, procesos y sus respectivos roles y responsabilidades. Por otro lado, el Plan de Recuperación ante Desastres busca respaldar integralmente los intereses de las diferentes partes que conforman las entidades, así como preservar los indicadores de generación de valor (reputación, marca, confianza, etc.). Asimismo, se busca optimizar la capacidad de recuperación ante pérdidas significativas en recursos productivos (maquinaria y equipo) u operativos (personal). Por último, el DRP hace parte integral del BCP (Plan de Continuidad del Negocio) y permite recuperar las operaciones, recursos y procesos críticos asociados al área de TI. Este curso sigue las metodologías recomendadas por el Disaster Recovery Institute (www.drii.org) y el Business Continuity Institute (www.thebci.org).

¹ Referidos en la literatura como Planes de Recuperación ante Desastres (DRP, por su sigla en inglés).

DESCRIPCIÓN DEL CURSO

1. Introducción
 - a. Componentes de la organización
 - i. Personas
 - ii. Procesos
 - iii. Tecnología
 - b. Diferencias entre BCP y DRP
 - c. Planes complementarios
 - d. Tipos de desastres a considerar
2. Inicio del proyecto
 - a. Elementos para el éxito del proyecto
 - b. Equipo de trabajo
 - c. Roles y responsabilidades
 - d. Riesgos del proyecto
3. Análisis de impacto sobre el negocio
 - a. Introducción
 - b. Identificar funciones del negocio
 - c. Obtener información para el BIA
 - i. Cuestionarios
 - ii. Entrevistas
 - iii. Talleres
 - d. Determinar tiempos de recuperación
 - i. RTO
 - ii. RPO
 - e. Preparación del reporte
4. Análisis de riesgo
 - a. Introducción
 - b. Amenazas naturales
 - c. Amenazas accidentales
 - d. Amenazas intencionales
 - e. Identificar vulnerabilidades
 - f. Calificar el riesgo
 - g. Gestión del riesgo
 - i. Métodos cuantitativos
 - ii. Métodos cualitativos
 - iii. Análisis de disponibilidad y desempeño
 - h. Preparación del reporte
5. Estrategias de mitigación (personas, aspectos físicos, infraestructura)
 - a. Hot sites: Normalmente esta configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.
 - b. Warm sites: En esta opción no se incluyen servidores específicos de alta capacidad.
 - c. Cold sites: En esta opción sólo se tiene aire acondicionado, potencia, enlaces de telecomunicaciones, y otros.

- d. Sitios móviles
 - e. Acuerdos recíprocos con otras organizaciones
 - f. Mirror site: Se procesa cada transacción en paralelo con el sitio principal.
 - g. Múltiples centros de procesamiento internos con el fin de distribuir el procesamiento y de esta forma lograr un mejor nivel de disponibilidad.
6. Desarrollo del plan DRP
- a. Fases
 - i. Activación
 - ii. Recuperación
 - iii. Restauración
 - b. Definición de roles y responsabilidades
 - c. Definición de tareas
 - d. Plan de comunicaciones
7. Entrenamiento
- a. Objetivos
 - b. Tiempos
 - c. Desarrollo
 - d. Monitoreo
8. Pruebas
- a. Diseño de las pruebas
 - b. Confirmar actividades
 - c. Confirmar recursos
 - d. Analizar riesgos
9. Auditorías
- a. Planeación
 - b. Ejecución
10. Mantenimiento del Plan
- a. Gestión del cambio
 - b. Estrategias para el manejo del cambio
 - c. Evaluar e incorporar cambios
11. Conclusiones
- a. Integración del DRP con ISO 27001
 - b. Integración del DRP con ITIL v3
 - c. Integración del DRP con COBIT 4.1
 - d. Costos aproximados de un DRP
 - e. Herramientas de software para el DRP
 - f. Beneficios de contar con un DRP

DURACIÓN DEL CURSO

16 HORAS

CUPO ESTIMADO DE ASISTENTES

16 ASISTENTES