FORMACIÓN E-LEARNING

Curso Online de

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

Para elaborar, desarrollar y gestionar con garantías un plan de recuperación de desastres informáticos en su empresa.

CURSO BONIFICABLE

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

Tel. 900 670 400 - attcliente@iniciativasempresariales.com
www.iniciativasempresariales.com

BARCELONA - BILBAO - MADRID - SEVILLA - VALENCIA - ZARAGOZA

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

Presentación

Casi todo el mundo conoce de primera mano testimonios de personas que aseguran haber sufrido un problema de seguridad informática que, en mayor o menor medida, les ha afectado en su rutina diaria. Apagones, virus, borrado accidental de datos, rotura de tuberías o robos son solo algunas de las circunstancias más comunes a las que nos podemos enfrentar.

Otras menos habituales y que, generalmente, conocemos a través de las noticias (huracanes, terremotos, inundaciones, guerras y terrorismo) pueden también golpearnos de forma inesperada. Es lo que se conoce como contingencia o desastre y dependerá de lo preparados que estemos ante cualquiera de estos acontecimientos para que un simple borrado de ficheros pueda afectar o no al funcionamiento de nuestra empresa, o para que algo tan grave como un incendio o una inundación no supongan más que un leve contratiempo.

En este curso se mostrarán los estándares de la industria y las prácticas recomendadas para la implementación de un completo y detallado plan de recuperación de desastres informáticos adaptado a las necesidades de su organización.

La Formación E-learning

Los cursos online se han consolidado como un método educativo de éxito en la empresa ya que aportan flexibilidad al proceso de aprendizaje, permitiendo al alumno escoger los momentos más adecuados para su formación. Con más de 35 años de experiencia en la formación de directivos y profesionales, Iniciativas Empresariales y la Manager Business School presentan sus cursos e-learning. Diseñados por profesionales en activo, expertos en las materias impartidas, son cursos de corta duración y eminentemente prácticos, orientados a ofrecer herramientas de análisis y ejecución de aplicación inmediata en el puesto de trabajo.

Nuestros cursos e-learning dan respuesta a las necesidades formativas de la empresa permitiendo:

1. La posibilidad de *escoger* el momento y lugar más adecuado para su formación.
2. *Interactuar* con otros estudiantes enriqueciendo la diversidad de visiones y opiniones y su aplicación en situaciones reales.
3. *Aumentar sus capacidades* y competencias en el puesto de trabajo en base al estudio de los casos reales planteados en el curso.
4. *Trabajar* con los recursos que ofrece el entorno on-line.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

Objetivos del curso:

- Conocer todos los tipos de desastres a los que es susceptible nuestra empresa de estar expuesta.
- Saber en qué consiste un proyecto de elaboración de un Plan de Recuperación de Desastres Informáticos.
- Identificar todos los factores de éxito para la consecución de un proyecto.
- Conocer la utilidad del BIA (Análisis del Impacto de Negocio) dentro de una organización y qué relación tiene con la evaluación de riesgos.
- Conocer de qué técnicas disponemos para el diseño de un BIA.
- Clasificar nuestros procesos de negocio en función de su criticidad.
- Aprender a identificar los activos a proteger.
- Identificar y analizar los factores de riesgo que pueden afectar a nuestra empresa.
- Conocer por qué la evaluación y gestión de riesgos debería encabezar la lista de prioridades de cualquier compañía que desee subsistir a largo plazo.
- Aprender a elaborar, desarrollar y gestionar con garantías un plan de recuperación de desastres informáticos.
- Conocer cómo, cuándo y por quién serán implementadas las estrategias de mitigación diseñadas.
- Identificar en base a qué requisitos definiremos los grupos de trabajo que van a intervenir en la implementación y mantenimiento de nuestro plan.
- Conocer cuando activar el plan de recuperación de desastres informáticos.

> “Hoy en día toda empresa debe preparar y desarrollar un plan de contingencias para prevenir los efectos de un desastre informático”

Dirigido a:

Profesionales de los departamentos de informática que quieran mejorar la seguridad de su sistema y conocer cómo crear e implantar planes de recuperación de desastres informáticos.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

Estructura y Contenido del curso

El curso tiene una duración de 60 horas lectivas 100% online que se realizan a través de la plataforma e-learning de Iniciativas Empresariales que permite el acceso de forma rápida y fácil a todo el contenido:

Manual de Estudio
6 módulos de formación que contienen el temario que forma parte del curso y que ha sido elaborado por profesionales en activo expertos en la materia.

Material Complementario
En cada uno de los módulos que le ayudará en la comprensión de los temas tratados.

Ejercicios de aprendizaje y pruebas de autoevaluación
para la comprobación práctica de los conocimientos adquiridos.

Bibliografía y enlaces de lectura
recomendados para completar la formación.

Metodología 100% E-learning

Aula Virtual *
Permite el acceso a los contenidos del curso desde cualquier dispositivo las 24 horas del día los 7 días de la semana.
En todos nuestros cursos es el alumno quien marca su ritmo de trabajo y estudio en función de sus necesidades y tiempo disponible.

Soporte Docente Personalizado
El alumno tendrá acceso a nuestro equipo docente que le dará soporte a lo largo de todo el curso resolviendo todas las dudas, tanto a nivel de contenidos como cuestiones técnicas y de seguimiento que se le puedan plantear.

* El alumno podrá descargarse la APP Moodle Mobile (disponible gratuitamente en Google Play para Android y la Apple Store para iOS) que le permitirá acceder a la plataforma desde cualquier dispositivo móvil y realizar el curso desde cualquier lugar y en cualquier momento.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

Contenido del Curso

MÓDULO 1. Introducción a la recuperación de desastres informáticos

10 horas

1.1. Introducción:
1.1.1. Objetivos de este curso.

1.2. Definiciones básicas:
1.2.1. Plan de emergencias.
1.2.2. Plan de contingencias.
1.2.3. Plan de continuidad de negocio.
1.2.4. Plan de recuperación de desastres.
1.2.5. Plan de recuperación de desastres informáticos.
1.2.6. Relación temporal entre el BCP y el DRP.

1.3. Tipología de desastres:
1.3.1. Desastres naturales:
1.3.1.1. Desastres naturales biológicos.
1.3.1.2. Desastres naturales geofísicos.
1.3.1.3. Desastres naturales hidrológicos.
1.3.1.4. Desastres naturales meteorológicos.
1.3.1.5. Desastres naturales climatológicos.
1.3.1.6. Desastres naturales espaciales.
1.3.2. Desastres antropogénicos.
1.3.3. Desastres sinérgicos.

1.4. Desastres informáticos:
1.4.1. Desastres informáticos personales.
1.4.2. Desastres informáticos de infraestructura.

1.5. Los tres elementos clave de la empresa:
1.5.1. Las personas.
1.5.2. Los procesos.
1.5.3. La tecnología.

1.6. Las etapas de un Plan de Recuperación de Desastres Informáticos:
1.6.1. Inicio del proyecto.
1.6.2. Análisis del Impacto de Negocio (BIA).
1.6.3. Evaluación de riesgos.
1.6.4. Estrategias de mitigación.
1.6.5. Implementación del plan de recuperación.
1.6.6. Formación, pruebas y auditoría.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

1.6.7. Mantenimiento del plan.

1.7. Venta interna del proyecto:
1.7.1. Beneficios para las personas.
1.7.2. Beneficios para los procesos.
1.7.3. Beneficios para la tecnología.
1.7.4. Obligaciones legales.
1.7.5. Negligencias.
1.7.6. Beneficios competitivos.
1.7.7. Supervivencia.
1.7.8. Ejecución parcial del proyecto.

MÓDULO 2. Inicio del proyecto

10 horas

Esta primera fase es la encargada de iniciar el proceso de desarrollo de un plan de recuperación de desastres informáticos. El mismo nombre de la fase nos indica además que este desarrollo se tratará como un proyecto.

2.1. Introducción:
2.1.1. Definición de proyecto.

2.2. Objetivos, requisitos y ámbito de un proyecto:
2.2.1. Objetivos de un proyecto:
2.2.1.1. Specific (eSpecífico).
2.2.1.2. Measurable (Medible).
2.2.1.3. Achievable (Alcanzable).
2.2.1.4. Relevant (Relevante).
2.2.1.5. Time bounded (Temporal).
2.2.2. Requisitos de un proyecto:
2.2.2.1. Requisitos de negocio.
2.2.2.2. Requisitos funcionales.
2.2.2.3. Requisitos no funcionales (técnicos).
2.2.3. Ámbito de un proyecto:
2.2.3.1. Las 3 restricciones de un proyecto.

2.3. Factores de éxito en la gestión de proyectos:
2.3.1. Factores organizativos.
2.3.2. Factores relacionados con la gestión de proyectos.
2.3.3. Factores relacionados con los gestores de proyectos.

2.4. Inicio del proyecto del Plan DR / BC:
2.4.1. Pasos previos:
2.4.1.1. Definición del ámbito general del proyecto.

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

2.4.1.2. Identificación del patrocinador del proyecto.
2.4.1.3. Formación del equipo de trabajo.
2.4.2. Definición del proyecto:
2.4.2.1. Definición del problema.
2.4.2.2. Declaración de intenciones.
2.4.2.3. Enumeración inicial de objetivos y requisitos.
2.4.2.4. Identificación de las restricciones.
2.4.2.5. Creación de la propuesta de proyecto.

MÓDULO 3. Análisis del impacto de negocio

8 horas

El análisis del impacto de negocio (BIA) es la base de nuestro plan DR/BC y determinará una vez finalizado qué necesita ser recuperado inmediatamente después de un desastre y cómo de rápido. Determinar ese "qué" y "cómo de rápido" es una de las tareas más difíciles y laboriosas que encontraremos en nuestro camino hacia la elaboración de un plan DR/BC y, sin embargo, es una de las más importantes.

3.1. Introducción:
3.1.1. Relación entre BIA y evaluación de riesgos.

3.2. Definiciones:
3.2.1. Unidad funcional.
3.2.2. Proceso / subproceso.
3.2.3. Activo.

3.3. Criticidad de los procesos:
3.3.1. Urgencia e impacto.
3.3.2. Categorías de criticidad.
3.3.3. Calculando el impacto.

3.4. Conceptos temporales asociados al impacto:
3.4.1. RPO.
3.4.2. MTPOD.
3.4.3. RTO.
3.4.4. WRT.

3.5. Elaborando el análisis del impacto de negocio:
3.5.1. Definición de ámbito, objetivo y definiciones.
3.5.2. Lista de procesos de negocio.
3.5.3. Detalle de cada proceso de negocio.

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

MÓDULO 4. Evaluación de riesgos

16 horas

Si los riesgos a los que se enfrenta un individuo son innumerables, los riesgos que afectan a una empresa pueden ser aún si caben más cuantiosos: defectos en los productos o servicios producidos, pérdida del valor de las acciones, aumento de los intereses de la deuda contraída, impagos de clientes, huelgas, etc. Es por ello, que la evaluación y gestión de riesgos (y, por tanto, un plan de recuperación de desastres) debería encabezar la lista de prioridades de cualquier compañía que desee subsistir a largo plazo.

4.1. Introducción.

4.2. Definiciones:
4.2.1. Activo.
4.2.2. Vulnerabilidad.
4.2.3. Amenaza.
4.2.4. Riesgo.
4.2.5. Contramedida.

4.3. El proceso de evaluación de riesgos:
4.3.1. Evaluación de riesgos frente a gestión de riesgos.
4.3.2. Clases de evaluación de riesgos:
4.3.2.1. Evaluación vertical / horizontal.
4.3.2.2. Evaluación cualitativa / cuantitativa.
4.3.3. Fuentes de información.

4.4. La evaluación de activos:
4.4.1. Identificación de los activos a proteger.
4.4.2. El proceso de valoración de activos (AV).

4.5. La evaluación de amenazas:
4.5.1. La cadena de amenazas.
4.5.2. Amenazas naturales:
4.5.2.1. Fuego.
4.5.2.2. Agua.
4.5.2.3. Tormentas eléctricas.
4.5.2.4. Terremotos.
4.5.2.5. Epidemias y pandemias.
4.5.2.6. Tormentas de nieve.
4.5.2.7. Otras amenazas naturales.
4.5.3. Amenazas antropogénicas:
4.5.3.1. Fuego.
4.5.3.2. Agua.
4.5.3.3. Terremotos.
4.5.3.4. Vandalismo, sabotajes y robos.

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

4.5.3.5. Suspensión de la actividad empresarial.
4.5.3.6. Terrorismo.
4.5.3.7. Guerra.
4.5.3.8. Amenazas biológicas, químicas o nucleares.
4.5.4. Amenazas informáticas:
4.5.4.1. Averías informáticas. Amenazas físicas.
4.5.4.2. Pérdida de datos o aplicaciones. Amenazas lógicas.
4.5.4.3. Infraestructura IT. Electricidad y aire acondicionado.
4.5.5. La probabilidad de ocurrencia de una amenaza:
4.5.5.1. Cálculo de la Tasa Anual de Ocurrencia.

4.6. La evaluación de vulnerabilidades:
4.6.1. Recalculo de la Tasa Anual de Ocurrencia.
4.6.2. Factor de Exposición (EF).
4.6.3. Expectación de Pérdida Unitaria (SLE).
4.6.4. Expectación de Pérdida Anual (ALE).

4.7. Software para la gestión de riesgos:
4.7.1. Pilar.
4.7.2. Practical Threat Analysis (PTA).

MÓDULO 5. Estrategias de mitigación

12 horas

Al conjunto de contramedidas a aplicar en nuestra organización con el objeto de paliar los riesgos detectados es lo que denominamos estrategias de mitigación. Esta fase es lo que convierte una evaluación de riesgos en una gestión de riesgos.

5.1. Introducción.

5.2. Tipos de estrategias de mitigación:
5.2.1. Aceptación del riesgo.
5.2.2. Evitación del riesgo.
5.2.3. Limitación del riesgo.
5.2.4. Transferencia del riesgo.

5.3. Desarrollando la estrategia de mitigación:
5.3.1. Tipos de contramedidas.
5.3.2. Valoración de las contramedidas.

5.4. Contramedidas IT:
5.4.1. Contramedidas frente a amenazas físicas:
5.4.1.1. La importancia del CPD.

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

5.4.1.2. Discos en RAID.
5.4.1.3. Discos en spare o de repuesto.
5.4.1.4. Réplicas de cabinas de almacenamiento SAN.
5.4.1.5. Réplicas de bases de datos.
5.4.1.6. Cluster de servidores.
5.4.1.7. Virtualización.
5.4.2. Contramedidas frente a amenazas lógicas:
5.4.2.1. Backups o copia de seguridad.
5.4.2.2. Snapshots.
5.4.2.3. Antivirus.
5.4.3. Combinar contramedidas ante amenazas físicas y lógicas.

MÓDULO 6. Implementación y mantenimiento del plan

4 horas

Una vez analizado el impacto de negocio (BIA), realizar la evaluación de riesgos y definir las estrategias de mitigación que mejor se adaptan a nuestra organización, llega el momento de implementar el plan, realizar la formación, pruebas y auditorías, para finalmente mantener el plan con el que iniciar una nueva iteración en el bucle del proceso continuo de adaptación y mejora de un plan DR/BC.

6.1. Introducción.

6.2. Implementación del plan de recuperación:
6.2.1. Desarrollo de un plan de recuperación:
6.2.1.1. Desastres o interrupciones críticas.
6.2.1.2. Desastres o interrupciones graves.
6.2.1.3. Desastres o interrupciones leves.
6.2.1.4. ¿Cuándo activar el plan de recuperación?
6.2.2. Desarrollo de un Plan de Continuidad de Negocio:
6.2.2.1. ¿Cuándo activar el plan de continuidad de negocio?
6.2.3. Definición de los equipos de trabajo.
6.2.4. Implementación de las estrategias de mitigación.

6.3. Formación, pruebas y auditoría.

6.4. Mantenimiento del plan:
6.4.1. Principales tipos de cambio que afectan a nuestro plan:
6.4.1.1. Cambios organizativos.
6.4.1.2. Cambios en los procesos de negocio.
6.4.1.3. Cambios en la tecnología.
6.4.1.4. Cambios legales.

Elaboración de un Plan de Recuperación de Desastres Informáticos (DRP)

Autor

Francisco Javier Roldán
Ingeniero Superior en Informática, cuenta con una amplia experiencia en Arquitectura de Sistemas y Gestión de Proyectos Informáticos, así como en diseño, implementación y mantenimiento de Sistemas Hardware y Software en Alta Disponibilidad (HA) y en configuraciones de recuperación de desastres (DR), orientados a entornos críticos donde el RPO (Recovery Point Objective) y el RTO (Recovery Time Objective) es igual a cero.

Titulación

Una vez finalizado el curso el alumno recibirá el diploma que acreditará el haber superado de forma satisfactoria todas las pruebas propuestas en el mismo.