Ciber Resiliencia

Ciber Resiliencia para el Profesional de Continuidad de Negocio
Duración: 4.5 días (cuatro días completos de instrucción), seguido de un medio día para examen.
Examen: Examen de Resiliencia
Costo: US$2,750.00

Descripción

Las organizaciones de hoy se enfrentan a una amplia gama de ataques cibernéticos y su organización no es una excepción. Hay innumerables oportunidades para que los piratas causen interrupciones masivas, por lo cual requerirá una respuesta que lo involucrará. Es por eso por lo que este curso es imprescindible. Más que una simple declaración del problema, el curso de Ciber-Resiliencia para Profesionales de Continuidad de Negocio es una experiencia de cuatro días repleta de información que proporcionará una comprensión de cómo abordar las interrupciones cibernéticas dentro de un marco de la Continuidad de Negocio.

Descubrirá cómo la Continuidad de Negocio y la Ciber seguridad deben integrarse dentro de cada organización, utilizando los cinco elementos de la Ciber Resiliencia: preparar / identificar, proteger, detectar, responder y recuperarse. Colectivamente, estos conceptos y los planes de acción resultantes ayudarán a desarrollar una estrategia para responder efectivamente a eventos imprevistos y hacer que su organización vuelva a funcionar lo más rápido posible. Estas dos funciones tradicionalmente separadas deben trabajar juntas, y con este curso, podrá tomar medidas para que eso suceda en su organización. Hacerlo agilizará la identificación y la respuesta bien coordinadas a ataques o violaciones de datos, minimizará los costos, protegerá la reputación de la organización y le brindará la ventaja profesional de aportar la información y las habilidades más actuales.

Objetivo

1. Proporcionar a los estudiantes la instrucción detallada, marco y orientación para implementar los conceptos esenciales para combinar la seguridad cibernética y la continuidad de negocio en un programa efectivo de Ciber Resiliencia.
2. Preparar a los estudiantes con recomendaciones prácticas para representar una "propuesta de valor" apropiada para la administración ejecutiva de una organización que ayudará a asegurar cualquier inversión necesaria para avanzar hacia un programa fuerte de Ciber-Resiliencia.
3. Haga que los estudiantes participen en ejercicios basados en Ciber / BCM para ayudar a comprender los problemas que enfrentará.
4. Compartir experiencias con otros profesionales.
5. Preparar para aprobar el Examen de Ciber Resiliencia, para que pueda ser Certificado como un Profesional de Ciber-Resiliencia Certificado por DRI International.

Contenido

DÍA 1

- Introducción al concepto de Ciber-Resiliencia.
- Tipos de eventos Cibernéticos.
- Cómo los eventos de Ciberseguridad impactan la Continuidad de Negocio.
- Integrar la Ciberseguridad en la Continuidad de Negocio.
- Consideraciones organizacionales.
- Avanzar desde la Ciberseguridad y la Continuidad de Negocio para lograr la Ciber-Resiliencia.

DIA 2

- Desarrollar una respuesta efectiva a incidentes.
- Identificar medios específicos para unir la Planificación de Respuesta a Incidentes de seguridad Cibernética y la Planificación de Continuidad de la entidad.
- Diseñar estrategias que mitiguen la pérdida en caso de incumplimiento.
- Identificar los parámetros críticos de las operaciones relacionadas con TI con una evaluación de impacto de la entidad.
- Enumerar las estrategias de recuperación de entidades cruciales para restablecer la tecnología y la continuidad de los procesos críticos de la entidad.
- Ventajas de identificar riesgos relacionados con Ciberseguridad e integrarlos en la planificación y administración de la entidad.

DÍA 3

- Crear marco de seguridad Cibernética.
- Examine el último marco de Ciberseguridad.
- Revise las reglamentaciones existentes que rigen la protección y los informes de seguridad Cibernética.
- Explicar cómo desarrollar e implementar la protección de salvaguarda para infraestructura y servicios tecnológicos críticos para contener el impacto de un ataque Cibernético.
- Discutir cómo detectar y monitorear los indicadores de ataque a la red para garantizar la efectividad de las salvaguardas.
- Describir la importancia de la capacitación periódica para la conciencia Cibernética.
- Monitorear los eventos de seguridad interna y correlacione con las amenazas externas.

DÍA 4

- Crear un plan de respuesta efectivo.
- Cómo restaurar datos y servicios que pueden haber sido afectados durante un Ciberataque.
- Comprender cómo la Ciberseguridad y la Continuidad de Negocios trabajan con la gestión de la reputación.
- Monitorear de Ciberseguridad.
- Crear planes efectivos de comunicación de crisis para incidentes Cibernéticos.
- Enumerar las recomendaciones para preparar proveedores clave en caso de un Ciberataque.
- Discutir cómo deberían emplearse iniciativas de capacitación y sensibilización para incorporar la Ciber Resiliencia dentro de toda la organización y garantizar que el personal conozca la función de los planes de respuesta.