EC-Council Certified Incident Handler (ECIH)

Código: ECIH-001

Propuesta de Valor: EC-COUNCIL

Duración: 24 Horas

En el presente curso, el participante aprenderá la metodología para la creación de grupos de respuesta a incidentes, así como los procedimientos para realizar las actividades de un equipo de respuesta a incidentes. Este curso lo prepara para la Certificación: EC-Council Certified Incident Handler.

AUDIENCIA

- El curso está dirigido a profesionistas técnicos de la seguridad en TI encargados de atender incidentes en cómputo que afecten la seguridad en los sistemas en la organización.

PRE REQUISITOS

- No hay requisitos previos.

OBJETIVOS

- Describir los principios y técnicas que permiten detectar y manejar los diferentes incidentes de seguridad de la información que se presenten en una organización.
- Aplicar los diferentes procedimientos y metodologías que permiten manejar adecuadamente los incidentes de seguridad en cómputo, apegándose a las políticas de seguridad y la legislación informática existente, que reduzcan el impacto negativo.
- Crear grupos de respuesta a incidentes, especificando sus procedimientos, políticas y sus alcances.

CERTIFICACIÓN DISPONIBLE

- Título del examen: EC-Council Certified Incident Handler.
- Código de examen: 212-89.
    - Número de preguntas: 100.
    - Duración: 3 horas.
    - Disponibilidad de exámenes: EC-Council Exam Portal.
    - Formato de prueba: opción múltiple.
    - Puntaje de aprobación: 70%.

CONTENIDO

1. INTRODUCCIÓN A LA RESPUESTA DE INCIDENTES

2. EVALUACIÓN DEL RIESGO

3. RESPUESTA A INCIDENTES Y PASOS A SEGUIR

4. CSIRT

5. MANEJO DE INCIDENTES DE SEGURIDAD EN REDES

6. MANEJO DE INCIDENTES DE CÓDIGOS MALICIOSOS

7. MANEJO DE AMENAZAS INTERNAS

8. ANÁLISIS FORENSE Y RESPUESTA A INCIDENTES

9. REPORTE DE INCIDENTE

10. RECUPERACIÓN DE INCIDENTE

11. POLÍTICAS DE SEGURIDAD Y LEGISLACIÓN

BENEFICIOS

- Al terminar el curso el estudiante podrá aplicar la metodología para la creación de grupos de respuesta a incidentes, así como los procedimientos para realizar las actividades de un equipo de respuesta a incidentes.