

Curso Gestión de la seguridad informática en la empresa



Duración
100 horas



Dirigido a
Trabajadores en activo -
Autónomos - ERE-ERTE



Ubicación
Estatat



Modalidad
Presencial (aula
virtual en directo)

Objetivos:

Con este curso aprenderás a desplegar, controlar y mejorar la gestión de la Seguridad Informática en la Empresa.

Requisitos:

Nivel académico o de conocimientos generales:

- Título de FP Grado superior, bachillerato.
- Dominio de inglés a nivel de lectura.
- Conocimientos básicos sobre el sistema operativo Windows.
- Experiencia profesional mínima de 6 meses en puestos relacionados con la especialidad.
- Conocimientos profesionales referidos a la especialidad.





Contenido del Programa:

1. Introducción a la Seguridad

- Introducción a la Seguridad de Información.
- Modelo de Ciclo de Vida de la Seguridad de la Información.
- Confidencialidad, Integridad y Disponibilidad. Principios de Protección de la Seguridad de la Información.
- Políticas de Seguridad.
- Tácticas de Ataque.
- Concepto de Hacking.
- Árbol de Ataque.
- Lista de Amenazas para la Seguridad de la Información.
- Vulnerabilidades.
- Vulnerabilidades en Sistemas Windows.
- Vulnerabilidades en Aplicaciones Multiplataforma.
- Vulnerabilidades en Sistemas Unix y Mac OS.
- Buenas Prácticas y Salvaguardas para la Seguridad de la Red.
- Recomendaciones para la Seguridad de su Red.

2. Políticas de Seguridad

- Introducción a las Políticas de Seguridad.
- ¿Por qué son Importantes las Políticas?
- Qué debe de contener una Política de Seguridad.
- Lo que No debe contener una Política de Seguridad.
- Cómo conformar una Política de Seguridad Informática.
- Hacer que se cumplan las Decisiones sobre Estrategia y Políticas.

3. Auditoría y Normativa de Seguridad.

- Introducción a la Auditoría de Seguridad de la Información y a los Sistemas de Gestión de Seguridad de la Información.
- Ciclo del Sistema de Gestión de Seguridad de la Información.
- Seguridad de la Información.
- Definiciones y Clasificación de los Activos.
- Seguridad Humana, Seguridad Física y del Entorno.
- Gestión de Comunicaciones y Operaciones.
- Control de Accesos.
- Gestión de Continuidad del Negocio.
- Conformidad y Legalidad.

4. Estrategias de Seguridad.

- Menor Privilegio.
- Defensa en Profundidad.
- Punto de Choque.





- El Eslabón más Débil.
- Postura de Fallo Seguro.
- Postura de Negación Establecida: lo que No está Prohibido.
- Postura de Permiso Establecido: lo que No está Permitido.
- Participación Universal.
- Diversificación de la Defensa.
- Simplicidad.

5. Exploración de las Redes.

- Exploración de la Red.
- Inventario de una Red. Herramientas del Reconocimiento.
- NMAP y SCANLINE.
- Reconocimiento. Limitar y Explorar.
- Reconocimiento. Exploración.
- Reconocimiento. Enumerar.

6. Ataques Remotos y Locales.

- Clasificación de los Ataques.
- Ataques Remotos en UNIX.
- Ataques Remotos sobre Servicios Inseguros en UNIX.
- Ataques Locales en UNIX.
- ¿Qué Hacer si recibimos un Ataque?

7. Seguridad en Redes Inalámbricas.

- Introducción.
- Introducción al Estándar Inalámbrico 802.11 – WIFI
- Topologías.
- Seguridad en Redes Wireless. Redes Abiertas.
- WEP.
- WEP. Ataques.
- Otros Mecanismos de Cifrado.

8. Criptografía y Criptoanálisis.

- Criptografía y Criptoanálisis: Introducción y Definición.
- Cifrado y Descifrado.
- Ejemplo de Cifrado: Relleno de una sola vez y Criptografía Clásica.
- Ejemplo de Cifrado: Criptografía Moderna.
- Comentarios sobre Claves Públicas y Privadas: Sesiones.

9. Autenticación.

- Validación de Identificación en Redes.





- Validación de Identificación en Redes: Métodos de Autenticación.
- Validación de Identificación Basada en Clave Secreta Compartida: Protocolo.
- Establecimiento de una Clave Compartida: Intercambio de Claves Diffie-Hellman.
- Validación de Identificación usando un Centro de Distribución de Claves.
- Protocolo de Autenticación Kerberos.
- Validación de Identificación de Clave Pública.
- Validación de Identificación de Clave Pública: Protocolo de Interbloqueo.





Contacta con nosotros:

¡Te lo ponemos fácil!

Ponemos a tu disposición los siguientes medios de contacto para resolver cualquier duda sobre nuestros cursos.

- Por correo electrónico: **formacionsubvencionada@cas-training.com**
- Por teléfono: llámanos gratis al **(+34) 91 553 61 62**
- Por nuestro **sitio web**: Visita nuestra página de contacto **aquí**.

