IFCT050PO
Gestión de la seguridad informática en la empresa

Descripción: La seguridad informática es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o la que circula a través de las redes de computadoras. El objetivo de este curso será ofrecer una visión general de los riesgos a los que está expuesta una organización hoy día y brindar las técnicas, las herramientas y los conocimientos necesarios para gestionar la seguridad informática en la empresa.

Nº de horas:
100 horas

Objetivos:

- Gestionar la seguridad informática de la empresa.
- Conocer las políticas de seguridad.
- Estudiar la auditoría y normativa de seguridad.
- Aprender las estrategias de seguridad.
- Conocer la exploración de las redes.
- Estudiar los ataques remotos y locales y la seguridad en redes inalámbricas.
- Conocer la criptografía, el criptoanálisis y las técnicas de autenticación.

Contenido IFCT050PO

Gestión de la seguridad informática en la empresa

Unidad didáctica 1. Introducción a la seguridad
1.1 Introducción, modelo de ciclo de vida y principios de protección
1. 2. Políticas de seguridad.
1.3. Tácticas de ataque.
1.4. Concepto de hacking.
1.5. Árbol de ataque.
1.6. Lista de amenazas para la seguridad de la información.
1.7. Vulnerabilidades en sistemas Windows, en aplicaciones multiplataforma y en sistemas Unix y Mac OS.
1.8. Buenas prácticas, salvaguardas y recomendaciones para la seguridad de la red.

Unidad didáctica 2. Políticas de seguridad
2.1. Introducción a las políticas de seguridad.
2.2. ¿Por qué son importantes las políticas?
2.3. Qué debe contener una política de seguridad.
2.4. Lo que no debe contener una política de seguridad.
2.5. Cómo conformar una política de seguridad informática.
2.6. Hacer que se cumplan las decisiones sobre estrategia y políticas.

Unidad didáctica 3. Auditoría y normativa de seguridad
3.1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
3.2. Ciclo del sistema de gestión de seguridad de la información.
3.3. Seguridad de la información.
3.4. Definiciones y clasificación de los activos.
3.5. Seguridad humana, seguridad física y del entorno.
3.6. Gestión de comunicaciones y operaciones.
3.7. Control de accesos.
3.8. Gestión de continuidad del negocio.
3.9. Conformidad y legalidad.

Unidad didáctica 4. Estrategias de seguridad
4.1. Menor privilegio, defensa en profundidad, punto de choque y el eslabón más débil.
4.2. El eslabón más débil.
4.3. Postura de fallo seguro, de negación establecida y de permiso establecido.
4.4. Participación universal, diversificación de la defensa y simplicidad.

Unidad didáctica 5. Exploración de las redes
5.1. Exploración de la red.
5.2. Inventario de una red. Herramientas del reconocimiento.
5.3. NMAP Y SCANLINE.
5.4. Reconocimiento: limitar y explorar, exploración y enumerar.

Unidad didáctica 6. Ataques remotos y locales
6.1. Clasificación de los ataques.
6.2. Ataques remotos en UNIX y ataques remotos sobre servicios inseguros en UNIX.
6.3. Ataques locales en UNIX.
6.4. ¿Qué hacer si recibimos un ataque?

Unidad didáctica 7. Seguridad en redes inalámbricas
7.1. Introducción a las redes inalámbricas y al estándar inalámbrico 802.11 – WIFI.
7.2. Topologías.
7.3. Seguridad en redes inalámbricas (wireless). Redes abiertas.
7.4. WEP, Ataques WEP y otros mecanismos de cifrado.

Unidad didáctica 8. Criptografía y criptoanálisis
8.1. Criptografía y criptoanálisis: introducción y definición.
8.2. Cifrado y descifrado.
8.3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
8.4. Ejemplo de cifrado: criptografía moderna.
8.5. Comentarios sobre claves públicas y privadas: sesiones.

Unidad didáctica 9. Autenticación
9.1. Validación de identificación en redes y métodos de autenticación.
9.2. Validación de identificación basada en clave secreta compartida: protocolo.
9.3. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.