IFCT116. Gestión de la seguridad informática en la empresa

Sku: 114242IN

Horas: 60

Formato: HTML

OBJETIVOS

- Gestionar la seguridad informática en la empresa, adquiriendo los conocimientos necesarios para poder establecer protocolos adecuados de seguridad sobre los equipos informáticos de la empresa y redes empresariales.
- Diseñar e implementar políticas de seguridad informática eficaces que protejan los activos digitales de la empresa, garantizando la confidencialidad, integridad y disponibilidad de la información frente a posibles amenazas.
- Desarrollar habilidades para implementar auditorías de seguridad de la información y gestionar la normativa de seguridad en las organizaciones, garantizando la protección de activos, la continuidad del negocio y el cumplimiento legal.
- Afrontar los elementos relativos a las estrategias de seguridad informática, a fin de obtener una visión global de las maniobras de seguridad como respuesta a los peligros a los que se enfrentan diariamente las organizaciones.
- Arrojar elementos que determinen la importancia de gestionar adecuadamente tanto los canales de transmisión de los activos de información, como las infraestructuras físicas y digitales que dan soporte a toda la operatividad de una empresa, con el fin de sentar unas bases de seguridad a fin de obtener criterios claros de las maniobras básicas como respuesta a las amenazas o imprevistos.
- Abordar los elementos relativos a ataques informáticos remotos y locales, su clasificación y tipología, con el fin de definir las maniobras oportunas para que las organizaciones puedan gestionar adecuadamente la seguridad de sus activos.
- Examinar los elementos relativos a la seguridad en redes inalámbricas, encaminadas estas a proveer a las organizaciones de un recuso de inestimable valor para su quehacer diario.
- Abordar los elementos relativos al estudio de las complejas técnicas criptográficas y de criptoanálisis en un entorno de innovación tecnológica constante.
- Conocer los procesos de autenticación, como medio de someter la identidad de un posible usuario, a las pruebas necesarias para autorizar y confirmar el acceso a recursos.

CONTENIDOS

Unidad 1. Gestión de la Seguridad Informática en la empresa. Aproximación hacia los elementos que intervienen en la seguridad

Introducción

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.

Resumen

Unidad 2. Gestión de la Seguridad Informática en la empresa. Identificación de las políticas de seguridad

Introducción

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.

Resumen

Unidad 3. Gestión de la Seguridad Informática en la empresa. Caracterización de la auditoría de seguridad y gestión de la normativa de seguridad

Introducción

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.

Resumen

Unidad 4. Gestión de la Seguridad Informática en la empresa. Aplicación de estrategias de seguridad

Introducción

Aplicación de 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.

Resumen

Unidad 5. Gestión de la Seguridad Informática en la empresa. Exploración de las redes

Introducción

Exploración de la red.

- Inventario de una red. Herramientas del reconocimiento.
- NMAP Y SCANLINE.
- Reconocimiento. Limitar y explorar.
- Reconocimiento. Exploración.
- Reconocimiento. Enumerar.

Resumen

Unidad 6. Gestión de la Seguridad Informática en la empresa. Clasificación de ataques remotos y locales

Introducción

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?

Resumen

Unidad 7. Gestión de la Seguridad Informática en la empresa. Profundización en la 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.
Resumen

Unidad 8. Gestión de la Seguridad Informática en la empresa. Utilización de criptografía y criptoanálisis

Introducción
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.
Resumen

Unidad 9. Gestión de la Seguridad Informática en la empresa. Implementación de autentificación

Introducción
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.
Resumen