

IFCT050PO. Gestión de la seguridad informática en la empresa

Sku: 67140IN

Horas: 100

OBJETIVOS

- Gestionar la seguridad informática en la empresa.
- Generar consciencia empresarial sobre la importancia de contar con un sistema de seguridad informática que haga frente a los peligros y amenazas de la red.
- Asegurar el acceso a los equipos informáticos, dispositivos móviles y navegación por internet como herramientas de gestión empresarial, mediante la aplicación práctica de los conocimientos básicos sobre seguridad.
- Incorporar a la filosofía de la empresa una educación en el uso responsable de los recursos tecnológicos, basados en la información, y que facilitan la tarea diaria en la consecución de los objetivos empresariales.
- Acercar conocimientos en política de seguridad informática para profesionales autónomos, pymes, empresas, organizaciones públicas o privadas, empleados, usuarios y colaboradores con el fin de identificar los elementos claves para salvaguardar y proteger la integridad de los sistemas de información frente a la ciberdelincuencia.
- Abordar los elementos relativos a las diligencias de las organizaciones destinadas a velar por la buena gestión de los activos de la información y por el cumplimiento de la normativa en gestión de seguridad informática.
- 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 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.
- Abordar 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

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.

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.

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**.**

Estrategia 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.

Exploración de redes

Exploración de la red.

Inventario de una red. Herramientas del reconocimiento.

NMAP Y *SCANLINE.*

Reconocimiento. Limitar y explorar.

Reconocimiento. Exploración.
Reconocimiento. Enumerar.

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?

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.

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: sesione**s.**

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.