FIRMA DIGITAL Y SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. Firma electrónica / firma digital.

UNIDAD DIDÁCTICA 2. Tipos de certificados:

1. Certificados de Servidor (SSL: Capa de zócalos seguro)
2. Microsoft Server Gated Cryptography Certificates (Certificados de CGC-una extensión del protocolo
3. SSL- ofrecida por Microsoft).
4. Certificados Canalizadores.
5. Certificados de Correo Electrónico.
6. Certificados de Valoración de páginas WEB.
7. Certificados de Sello, Fecha y Hora

UNIDAD DIDÁCTICA 3. Sistemas de seguridad en la empresa.

1. Sistemas pasivos y reactivos.
2. Suplantación o spoofing:
3. - SET (Secure Electronic Transaction).
4. - PGP (Enterprise Security).
5. - SSL (Secure Socket Layout).

UNIDAD DIDÁCTICA 4. 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.

UNIDAD DIDÁCTICA 5. 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.

UNIDAD DIDÁCTICA 6. Auditoria 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.

UNIDAD DIDÁCTICA 7. 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.

UNIDAD DIDÁCTICA 8. 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.

UNIDAD DIDÁCTICA 9. 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?

UNIDAD DIDÁCTICA 10. 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.

UNIDAD DIDÁCTICA 11. 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.

UNIDAD 12. 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.