SAN SEBASTIÁN · MADRID · BARCELONA · VALENCIA · MÁLAGA · PAMPLONA · LOGROÑO · QUERÉTARO (MX)

IFCT101PO - PLANIFICACIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

DURACIÓN: 80 HORAS

MODALIDAD: PRESENCIAL/AULA VIRTUAL

FECHA INICIO/FIN:

OBJETIVOS:

Planificar la seguridad informática en la empresa

PARTICIPANTES:

Personas trabajadoras OCUPADAS que han estado en ERTE

Personas trabajadoras DESEMPLEADAS inscritas en los servicios públicos de empleo.

Personas trabajadoras en situación de ERTE.

REQUISITOS DE ACCESO:

Cualquier persona que quiera adquirir y mejorar las competencias profesionales relacionadas con los cambios tecnológicos y la transformación digital. Es recomendable disponer de:

- Habilidades básicas de comunicación lingüística que le permitan el aprendizaje y seguimiento de la formación.

- Competencias básicas en el manejo de ordenadores.

- Manejo básico en entornos microinformáticos.

- Buen manejo del ordenador y software específico.

- Conocimientos de navegación en internet

CONTENIDOS:

1. DEBILIDADES, AMENAZAS Y ATAQUES
1.1. Tipos de atacantes.
1.2. Motivaciones del atacante.
1.3. Metodología de un atacante determinado.
1.4. Vulnerabilidades y ataques comunes.
1.5. Herramientas de hacking.
1.6. Ingeniería social.
1.7. Prevención de ataques.
1.8. Respuesta a contingencias

2. ADMINISTRACIÓN DE LA SEGURIDAD EN REDES.
2.1. Diseño e implantación de políticas de seguridad.

3. TECNOLOGÍAS CRIPTOGRÁFICAS.
3.1. Encriptación simétrica.
3.2. Encriptación asimétrica.
3.3. Firmas digitales.
3.4. Certificados digitales.
3.5. SSL/TLS. La herramienta de encriptación multiusos.
3.6. Navegación segura: HTTPS.

4. SISTEMAS DE AUTENTIFICACIÓN.
4.1. Tecnologías de Identificación.
4.2. PAP y CHAP.
4.3. RADIUS.
4.4. El protocolo 802.1X.
4.5. La suite de protocolos EAP: LEAP, PEAP, EAP-TLS.
4.6. Sistemas biométricos

5. REDES VIRTUALES PRIVADAS.
5.1. Beneficios y características.
5.2. IP Sec.
5.3. VPNs con SSL-TLS.

6. FIREWALLS
6.1. Arquitectura de Firewalls
6.2. Filtrado de paquetes sin estados
6.3. Servidores Proxy
6.4. Filtrado dinámico o ""stateful""
6.5. Firewalls de siguiente generación
6.6. Funciones avanzadas

7. DETECCIÓN Y PREVENCIÓN AUTOMATIZADA DE INTRUSIONES (IDS-IPS)
7.1. Arquitectura de sistemas IDS
7.2. Herramientas de software
7.3. Captura de intrusos con Honeypots.

PARA PODER TENER SUPERADO EL CURSO HAY QUE CUMPLIR LOS SIGUIENES REQUISITOS:

- TENER SUPERADAS TODAS LAS PRUEBAS DE EVALUACIÓN QUE SE REALICEN DURANTE EL PROCESO DE APRENDIZAJE Y LA PRUEBA FINAL DE LA ACCIÓN FORMATIVA.