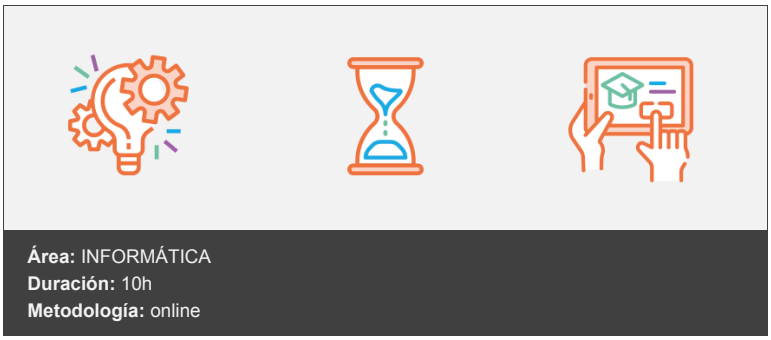
Protección de equipos en la red (IFCT106PO)



Área: INFORMÁTICA
Duración: 10h
Metodología: online

Objetivos

Prevenir los ataques de la red en equipos a partir de la comprensión de los riesgos, las vulnerabilidades y los ataques en la red; lo que nos permita una correcta selección de soluciones de seguridad.

Contenidos y estructura del curso

La necesidad de protegerse en la red
Redes abiertas basadas en la arquitectura TCP/IP
La actualidad: redes basadas en arquitecturas abiertas
Direcciones IP, puertos y conexiones lógicas
Direcciones IP
Arquitectura Cliente / Servidor
Interacción entre las diferentes capas TCP/IP y su impacto en la seguridad
Vulnerabilidades presentes en una red
Vulnerabilidades zero day
Endurecimiento de los dispositivos de red
Seguridad en redes inalámbricas
Resumen

Los peligros posibles: los virus informáticos
Definición de virus informático
Un poco de historia
Tipos de virus
Malwares
Puertas traseras
Ataques de ciberseguridad
Ataques por capas o niveles
Algunos ataques conocidos
Detectando un ataque
Indicios de un ataque de ciberseguridad en curso
Métodos para detectar un ataque
Medidas de contención
Recuperación de la normalidad
Resumen

Las soluciones: el antivirus
Los peligros informáticos
Definición de Antivirus
Virus total
Antivirus de sistemas operativos
Antivirus para Windows
Antivirus para Linux

Métodos de rescates externos para situaciones de desastre
Impacto de las vulnerabilidades "zero day" sobre los antivirus
La importancia de las salvaguardas de información
Definición de información digital
Salvaguarda de la información sensible
Salvaguarda de la configuración de los dispositivos de red
Resumen

Otros conceptos sobre seguridad informática
Ataques a la red desde la capa de aplicación
Ataques a la capa de aplicación desde la capa de red
DoS
DDoS
Firewalls
Conociendo los Firewalls
Cortafuegos de aplicaciones WEB
Limitaciones de un cortafuegos
Protección de accesos
Soluciones avanzadas para proteger la red
Monitoreo de red
IDS
IPS
Spam
Phishing
Ingeniería social
Resumen

Actualizaciones del software
Las políticas de actualización
Los peligros de un sistema desactualizado
Las alertas de seguridad
Solucionando las vulnerabilidades de los sistemas
Actualización del software de los dispositivos de red
Actualización de un enrutador de red
Actualización de un cortafuegos
Actualización del software de los sistemas operativos
Actualizaciones en Windows
Actualizaciones en Linux
Actualizaciones en Android
Actualizaciones de dispositivos pertenecientes a la IoT
Resumen

Metodología

En Criteria creemos que para que la formación e-Learning sea realmente exitosa, tiene que estar basada en contenidos 100% multimedia (imágenes, sonidos, vídeos, etc.) diseñados con criterio pedagógico y soportados en una plataforma que ofrezca recursos de comunicación como chats, foros y conferencias...Esto se logra gracias al trabajo coordinado de nuestro equipo e-Learning integrado por profesionales en pedagogía, diseño multimedia y docentes con mucha experiencia en las diferentes áreas temáticas de nuestro catálogo.

Perfil persona formadora

Esta acción formativa será impartida por un/a experto/a en el área homologado/a por Criteria, en cumplimiento con los procedimientos de calidad, con experiencia y formación pedagógica.