Manual Online Gestión de Incidentes y Antivirus (60 horas)



Categoría: Informática, Programación y Comunicaciones
Página del curso: https://www.ensenanzadual.com/cursos/manual-online-gestion-de-incidentes-y-antivirus-60-horas/

Objetivo

Con el Curso de **60 horas** de **Manual Online Gestión de Incidentes y Antivirus** adquirirás los conocimientos necesarios para cambiar de carrera o actualizar tus competencias profesionales, no lo dudes más y solicita información sobre este curso.

Descripción

MÓDULO 1. GESTIÓN DE INCIDENTES Y ANTIVIRUS UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS) - Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención - Identificación y caracterización de los datos de funcionamiento del sistema - Arquitecturas más frecuentes de los sistemas de detección de intrusos - Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad - Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS **UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS** - Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio. - Definición de políticas de corte de intentos de intrusión en los IDS/IPS - Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS - Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión - Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS **UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO** - Sistemas de detección y contención de código malicioso - Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar - Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso - Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso - Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad - Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso - Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada **UNIDAD DIDÁCTICA 4. INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE ANTIVIRUS.**

Virus informáticos.

- Software malicioso: Conceptos y definiciones.
    - Evolución. - Virus, gusanos, troyanos, otros. - Vulnerabilidades en programas y parches. - Tipos de ficheros que pueden infectarse. - Medios de propagación. - Virus en correos, en programas y en documentos. - Ocultación del software malicioso. - Páginas web. - Correo electrónico. - Memoria principal del ordenador. - Sector de arranque. - Ficheros con macros. - - Efectos y síntomas de la infección. - - Virus informáticos y sistemas operativos. - - Actualizaciones criticas de sistemas operativos. - - Precauciones para evitar infección. - Definición de software antivirus.

Componentes activos de los antivirus.

- - Vacuna. - - Detector. - - Eliminador.

Características generales de los paquetes de software antivirus.

- - Protección anti-spyware. - - Protección contra el software malicioso. - - Protección firewall. - - Protección contra vulnerabilidades. - - Protección contra estafas. - - Actualizaciones automáticas. - - Copias de seguridad y optimización del rendimiento del ordenador.

Instalación de software antivirus.

- - Requisitos del sistema. - - Instalación, configuración y activación del software. - - Creación de discos de rescate. - - Desinstalación.

La ventana principal.

- - Estado de las protecciones. Activación y desactivación. - - Tipos de análisis e informes. - - Actualización automática y manual. - - Actualización de patrones de virus y/ o ficheros identificadores de malware. - - Configuración de las protecciones. Activación y desactivación. - - Análisis, eliminación de virus y recuperación de los datos. - - Actualizaciones.

- Acceso a servicios.
    - Soporte. - Obtención de información. - - Otras opciones.

Información adicional

- Online: Si
- Tipo: Profesiones
- Horas: 60
- Unidades: 4