ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS

LA FORMACIÓN ES LA CLAVE DEL ÉXITO

Guía del Curso
Curso Práctico Online Gestión de Incidentes y Antivirus

Modalidad de realización del curso: Online
Titulación: Diploma acreditativo con las horas del curso

OBJETIVOS

Hoy en día la seguridad informática es un tema muy importante y sensible, que abarca un gran conjunto de aspectos en continuo cambio y constante evolución, que exige que los profesionales informáticos posean conocimientos totalmente actualizados. Con la realización del presente curso online de Gestión de Incidentes y Antivirus el alumno aprenderá los conocimientos necesarios para detectar alguna incidencia y virus para garantizar la seguridad informática.

CONTENIDOS

MÓDULO 1. GESTIÓN DE INCIDENTES Y ANTIVIRUS

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los sistemas de detección de intrusos

4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. 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

1. Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL DE CÓDIGO MALICIOSO

1. Sistemas de detección y contención de código malicioso
2. 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
3. Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
5. 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
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
7. Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE ANTIVIRUS

1. Virus informáticos
2. - Software malicioso: Conceptos y definiciones
3. . Evolución
4. . Virus, gusanos, troyanos, otros
5. . Vulnerabilidades en programas y parches
6. . Tipos de ficheros que pueden infectarse
7. . Medios de propagación
8. . Virus en correos, en programas y en documentos
9. . Ocultación del software malicioso
10. . Páginas web
11. . Correo electrónico
12. . Memoria principal del ordenador
13. . Sector de arranque
14. . Ficheros con macros
15. - Efectos y síntomas de la infección

16. - Virus informáticos y sistemas operativos
17. - Actualizaciones criticas de sistemas operativos
18. - Precauciones para evitar infección
19. Definición de software antivirus
20. Componentes activos de los antivirus
21. - Vacuna
22. - Detector
23. - Eliminador
24. Características generales de los paquetes de software antivirus
25. - Protección anti-spyware
26. - Protección contra el software malicioso
27. - Protección firewall
28. - Protección contra vulnerabilidades
29. - Protección contra estafas
30. - Actualizaciones automáticas
31. - Copias de seguridad y optimización del rendimiento del ordenador
32. Instalación de software antivirus
33. - Requisitos del sistema
34. - Instalación, configuración y activación del software
35. - Creación de discos de rescate
36. - Desinstalación
37. La ventana principal
38. - Estado de las protecciones. Activación y desactivación
39. - Tipos de análisis e informes
40. - Actualización automática y manual
41. - Actualización de patrones de virus y/ o ficheros identificadores de malware
42. - Configuración de las protecciones. Activación y desactivación
43. - Análisis, eliminación de virus y recuperación de los datos
44. - Actualizaciones
45. - Acceso a servicios
46. . Soporte
47. . Obtención de información
48. - Otras opciones

C/ San Lorenzo 2 - 2
29001 Málaga

Tlf: 952 215 476
Fax: 951 987 941

www.academiaintegral.com.es
E-mail: info@academiaintegral.com.es

ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS