ACADEMIA INTEGRAL
CENTRO DE NUEVAS TECNOLOGIAS

LA FORMACIÓN ES LA CLAVE DEL ÉXITO

Guía del Curso
UF1353 Monitorización de los Accesos al Sistema Informático

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

OBJETIVOS

Este curso se ajusta a lo expuesto en el itinerario formativo de aprendizaje perteneciente a la Unidad Formativa UF1353 Monitorización de los Accesos al Sistema Informático incluida en el Módulo Formativo MF0959_2 Mantenimiento de la Seguridad en Sistemas Informáticos regulada en el Real Decreto 1531/2011, de 31 de Octubre, modificado por el RD 628/2013, de 2 de Agosto que permita al alumnado adquirir las competencias profesionales necesarias para identificar los tipos de acceso al sistema informático así como los mecanismos de seguridad del mismo describiendo sus características principales y herramientas asociadas más comunes para garantizar el uso de los recursos del sistema e interpretar las trazas de monitorización de los accesos y actividad del sistema identificando situaciones anómalas, siguiendo unas especificaciones dadas.

CONTENIDOS

UNIDAD FORMATIVA 1. MONITORIZACIÓN DE LOS ACCESOS AL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. GESTIÓN DE LA SEGURIDAD INFORMÁTICA

1. Objetivo de la seguridad
2. Términos relacionados con la seguridad informática
3. Procesos de gestión de la seguridad
4. - Objetivos de la gestión de la seguridad
5. - Beneficios y dificultades
6. - Política de seguridad. La Ley Orgánica de Protección de Datos de carácter personal
7. - Análisis de riesgo
8. - Identificación de recursos
9. - Identificación de vulnerabilidades y amenazas: atacante externo e interno
10. - Medidas de protección
11. - Plan de seguridad
12. Interrelación con otros procesos de las tecnologías de la información
13. Seguridad física y seguridad lógica

UNIDAD DIDÁCTICA 2. SEGURIDAD LÓGICA DEL SISTEMA

1. Acceso al sistema y al software de aplicación
2. - Concepto de usuario, cuenta, grupo de usuario, permisos, lista de control de accesos (ACL)
3. - Políticas de seguridad respecto de los usuarios
4. - Autenticación de usuarios:
5. - Definición y conceptos básicos
6. - Sistemas de autenticación débiles y fuertes
7. - Sistemas de autenticación biométricos y otros sistemas
8. - Acceso local, remote y Single Sing-On
9. - Herramientas para la gestión de usuarios
10. - El servicio de directorio: conceptos básicos, protocolos e implementaciones
11. - Directorios: LDAP, X500, Active Directory
12. - Herramientas de administración de usuarios y equipos
13. - Administración básica del servicio de directorio
14. Confidencialidad y Disponibilidad de la información en el puesto de usuario final

15. - Sistemas de ficheros y control de acceso a los mismos
16. - Permisos y derechos sobre los ficheros
17. Seguridad en el puesto de usuario
18. - Tipología de software malicioso
19. - Software de detección de virus y programas maliciosos
20. - Antivirus, antispyware, firewall, filtros antispam, etc
21. - Técnicas de recuperación y desinfección de datos afectados
22. Herramientas de gestión remota de incidencias

UNIDAD DIDÁCTICA 3. PROCEDIMIENTOS DE MONITORIZACIÓN DE LOS ACCESOS Y LA ACTIVIDAD DEL SISTEMA

1. Objetivos de la monitorización y de la gestión de incidentes de seguridad
2. Procedimientos de monitorización de trazas
3. - Identificación y caracterización de aspectos monitorizables o auditables
4. - Clasificación de eventos e incidencias: de sistema, de aplicación, de seguridad
5. - Mecanismos de monitorización de trazas: logs del sistema, consolas de monitorización de usuarios
6. - Información de los registros de trazas
7. Técnicas y herramientas de monitorización
8. - Técnicas: correlación de logs, de eventos
9. - Herramientas de monitorización
10. - Herramientas propias del sistema operativo
11. - Sistemas basados en equipo (HIDS)
12. - Sistemas basados en red (NIDS)
13. - Sistemas de prevención de intrusiones (IPS)
14. Informes de monitorización
15. - Recolección de información
16. - Análisis y correlación de eventos
17. - Verificación de la intrusión
18. - Alarmas y acciones correctivas
19. Organismos de gestión de incidentes:
20. - Nacionales. IRIS-CERT, esCERT
21. - Internacionales. CERT, FIRST

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