PERFIL PROFESIONAL

UC0487_3

AUDITORÍA REDES DE COMUNICACIÓN Y SISTEMAS INFORMÁTICOS

MF0487_3

AUDITORÍA DE SEGURIDAD INFORMÁTICA (90 horas)

Realizaciones profesionales y criterios de realización

- **RP1**. Realizar **análisis de vulnerabilidades,** mediante programas específicos para controlar posibles fallos en la seguridad de los sistemas según las necesidades de uso y dentro de la organización
- **RP2**. Verificar el cumplimiento de la normativa y **requisitos legales** en materia de protección de datos personales para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización
- **RP3**. Comprobar el cumplimiento de la **política de seguridad** establecida para afirmar la integridad del sistema según las necesidades de uso y dentro de las directivas de la organización

RP1. Análisis de vulnerabilidades

- CR1.1 Las herramientas y tipos de pruebas de análisis de vulnerabilidades se seleccionan y adecuan al entorno a verificar según las especificaciones de seguridad de la organización
- CR1.2 Los programas y las pruebas se actualizan para realizar ensayos consistentes con los posibles fallos de seguridad de las versiones HW y SW instaladas en el sistema informático
- CR1.3 Los resultados de las pruebas se analizan y documentan conforme se indica en la normativa de la organización
- CR1.4 Los sistemas de acceso por contraseña se comprueban mediante herramientas específicas según las especificaciones de la normativa de seguridad
- CR1.5 La documentación del análisis de vulnerabilidades contiene referencias exactas de las aplicaciones y servicios que se han detectado funcionando en el sistema, el nivel de los parches instalados, vulnerabilidades de negación de servicio, vulnerabilidades detectadas y mapa de red

RP2. Requisitos legales

- CR2.1 Los ficheros con datos de carácter personal son identificados y tienen asignado un responsable de seguridad según normativa legal
- CR2.2 El listado de personas autorizadas a acceder a cada fichero existe y se encuentra actualizado según la normativa legal
- CR2.3 El control de accesos a los ficheros se comprueba siguiendo el procedimiento establecido en la normativa de seguridad de la organización
- CR2.4 La gestión del almacenamiento de los ficheros y sus copias de seguridad se realiza siguiendo la normativa legal y de la organización
- CR2.5 El acceso telemático a los ficheros ser realiza utilizando mecanismos que garanticen la confidencialidad e integridad cuando así lo requiera la normativa
- CR 2.6 El informe de la auditoría recoge la relación de ficheros con datos de carácter personal y las medidas de seguridad aplicadas y aquellas pendientes de aplicación

RP3. Política de seguridad

- CR3.1 Los procedimientos de detección y gestión de incidentes de seguridad se desarrollan y se incluyen en la normativa de seguridad de la organización
- CR3.2 Los puntos de acceso de entrada y salida de la red son verificados para que su uso se circunscriba a lo descrito en la normativa de seguridad de la organización
- CR3.3 Los programas de seguridad y protección de sistemas se activan y actualizan según las especificaciones de los fabricantes
- CR3.4 Los puntos de entrada y salida de la red adicionales son autorizados y controlados en base a las especificaciones de seguridad y al plan de implantación de la organización
- CR3.5 Los procesos de auditoría informática son revisados, tanto de carácter internos, como aquellos realizados por personal externo a la organización
- CR3.6 Los procedimientos de las políticas se verificarán en su cumplimiento por parte de los usuarios

Contexto profesional
Medios de producción

- Aplicaciones ofimáticas corporativas
- Analizadores de vulnerabilidades
- Herramientas para garantizar la confidencialidad de la información
- Programas que garantizan la confidencialidad e integridad de las comunicaciones
- Aplicaciones para gestión de proyectos
- Programas de análisis de contraseñas

Contexto profesional
Productos y resultados

- Informes de análisis de vulnerabilidades
- Relación de contraseñas débiles
- Registro de ficheros de datos de carácter personal, según la normativa vigente
- Informe de auditoría de servicios y puntos de acceso al sistema informático

Contexto profesional
Información utilizada o generada

- Normativa sobre protección de datos personales
- Política de seguridad de la empresa
- Metodologías de análisis de seguridad
  - OSSTM
  - BS7799/ISO17799
- Boletines de seguridad y avisos de vulnerabilidades disponibles en formato electrónico
- Topología del sistema informático a proteger