DATOS IDENTIFICATIVOS DEL MÓDULO FORMATIVO

MÓDULO FORMATIVO	AUDITORÍA DE SEGURIDAD INFORMÁTICA	Duración	90
Código	MF0487_3		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área profesional	Sistemas y telemática		
Certificado de profesionalidad	Seguridad informática	Nivel	3
Resto de formación para completar el certificado de profesionalidad	Seguridad en equipos informáticos	Duración	90
	Gestión de incidentes de seguridad informática		90
	Sistemas seguros de acceso y tratamiento de datos		60
	Gestión de servicios en el sistema informático (Transversal)		90
	Prácticas profesionales no laborales en seguridad informática		80

Apartado A: **REFERENTE DE COMPETENCIA**

Este módulo formativo se corresponde con la unidad de competencia UC0487_3: AUDITAR REDES DE COMUNICACIÓN Y SISTEMAS INFORMÁTICOS

Apartado B: **ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS**

Capacidades y criterios de evaluación

C1: Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática.

CE1.1 Explicar las diferencias entre vulnerabilidades y amenazas.

CE1.2 Enunciar las características de los principales tipos de vulnerabilidades y programas maliciosos existentes, describiendo sus particularidades.

CE1.3 Describir el funcionamiento de una herramienta de análisis de vulnerabilidades, indicando las principales técnicas empleadas y la fiabilidad de las mismas.

CE1.4 Seleccionar la herramienta de auditoría de seguridad más adecuada en función del servidor o red y los requisitos de seguridad.

CE1.5 A partir de un supuesto práctico, ante un sistema informático dado en circunstancias de implantación concretas:

- Establecer los requisitos de seguridad que debe cumplir cada sistema.
- Crear una prueba nueva para la herramienta de auditoría, partiendo de las especificaciones de la vulnerabilidad.
- Elaborar el plan de pruebas teniendo en cuenta el tipo de servidor analizado.
- Utilizar varias herramientas para detectar posibles vulnerabilidades
- Analizar el resultado de la herramienta de auditoría, descartando falsos positivos.
- Redactar el informe de auditoría, reflejando las irregularidades detectadas, y las sugerencias para su regularización.

C2: Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.

CE2.1 Explicar la normativa legal vigente (autonómica, nacional, europea e internacional) aplicable a datos de carácter personal.

CE2.2 Exponer los trámites legales que deben cumplir los ficheros con datos de carácter personal, teniendo en cuenta la calidad de los mismos.

CE2.3 Describir los niveles de seguridad establecidos en la normativa legal vigente asociándolos a los requisitos exigidos.

CE2.4 A partir de un supuesto práctico, en el que se cuenta con una estructura de registro de información de una organización:

- Identificar los ficheros con datos de carácter personal, justificando el nivel de seguridad que le corresponde.
- Elaborar el plan de auditoría de cumplimiento de legislación en materia de protección de datos de carácter personal.
- Revisar la documentación asociada a los ficheros con datos de carácter personal, identificando las carencias existentes.
- Elaborar el informe correspondiente a los ficheros de carácter personal, indicando las deficiencias encontradas y las correcciones pertinentes.

C3: Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.

CE3.1 Identificar las fases del análisis de riesgos, describiendo el objetivo de cada una de ellas.

CE3.2 Describir los términos asociados al análisis de riesgos (amenaza, vulnerabilidad, impacto y contramedidas), estableciendo la relación existente entre ellos.

CE3.3 Describir las técnicas de análisis de redes, explicando los criterios de selección.

CE3.4 Describir las topologías de cortafuegos de red comunes, indicando sus funcionalidades principales.

.

Contenidos

1. Criterios generales comúnmente aceptados sobre auditoría informática

- Código deontológico de la función de auditoría
- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- Criterios a seguir para la composición del equipo auditor.
- Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- Tipos de muestreo a aplicar durante el proceso de auditoría
- Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

2. Aplicación de la normativa de protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Normativa europea recogida en la directiva 95/46/CE
- Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
- Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

3. Análisis de riesgos de los sistemas de información

- Introducción al análisis de riesgos
- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- Particularidades de los distintos tipos de código malicioso
- Principales elementos del análisis de riesgos y sus modelos de relaciones
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Identificación de los activos involucrados en el análisis de riesgos y su valoración
- Identificación de las amenazas que pueden afectar a los activos identificados previamente
- Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
- Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
- Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
- Determinación de la probabilidad e impacto de materialización de los escenarios
- Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
- Relación de las distintas alternativas de gestión de riesgos
- Guía para la elaboración del plan de gestión de riesgos
- Exposición de la metodología NIST SP 800-30
- Exposición de la metodología Magerit versión 2

4. Uso de herramientas para la auditoría de sistemas

- Herramientas del sistema operativo tipo Ping, Traceroute, etc.
- Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
- Herramientas de análisis de vulnerabilidades tipo Nessus
- Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
- Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
- Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

5. Descripción de los aspectos sobre cortafuegos en auditorías de Sistemas Informáticos.

- Principios generales de cortafuegos
- Componentes de un cortafuegos de red
- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Arquitecturas de cortafuegos de red
- Otras arquitecturas de cortafuegos de red

6. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información

- Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
- Guía para la elaboración del plan de auditoría
- Guía para las pruebas de auditoría
- Guía para la elaboración del informe de auditoría

Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

– Estar en posesión del título de Bachiller
– Estar en posesión de algún certificado de profesionalidad de nivel 3.
– Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional
– Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior
– Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años
– Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad: Seguridad informática.