MF0487_3: AUDITORÍA DE SEGURIDAD INFORMÁTICA

Certificado de Profesionalidad IFCT0109 SEGURIDAD INFORMÁTICA

Lugar de impartición: Aemta, C/ Roa de la Vega 14, ent.dcha, León
Dirigido prioritariamente a trabajadores (por cuenta ajena y autónomos) y desempleados

Acción gratuita financiada por el Servicio Público de Empleo Estatal

Objetivo: Auditar redes de comunicación y sistemas informáticos.
Duración: 90 horas presenciales.
Nivel del Certificado: 3

Si estás interesad@ en participar debes cumplimentar la solicitud que se adjunta y enviarla a cursos@aemta.es , junto a la siguiente documentación:

TRABAJADORES y DEMANDANTES DE EMPLEO
○ Solicitud de participación (ANEXO III) ○ Fotocopia DNI ○ Fotocopia Tarjeta de la seguridad Social ○ Fotocopia Cabecera de la última Nomina o último recibo de autónomo o tarjeta de demandante de empleo ○ CV actualizado ○ Fotocopia de titulación académica

*Debes cumplir alguno de los **requisitos de acceso** según artículo 20 del RD 189/2013, de 15 de marzo, que modifica el RD 34/2008, de 18 de enero:*

a) Graduado en ESO para el nivel 2 o título de Bachiller para nivel 3.
b) Certificado de profesionalidad del mismo nivel del módulo o módulos formativos y/o del certificado de profesionalidad al que desea acceder.
c) Certificado de profesionalidad de nivel 1 de la misma familia y área profesional para el nivel 2 o de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional para el nivel 3.
d) Cumplir el requisito académico de acceso a los ciclos formativos de grado medio para el nivel 2 o de grado superior para el nivel 3, o bien haber superado las correspondientes pruebas de acceso reguladas por las administraciones educativas.
e) Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
f) Tener las competencias clave necesarias, de acuerdo con lo recogido en el anexo IV de este real decreto, para cursar con aprovechamiento la formación correspondiente al certificado de profesionalidad.

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