ANEXO III

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Seguridad informática

Código: IFCT0109

Familia Profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC153_3 Seguridad informática (RD 1087/05 de 16 de septiembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

UC0486_3: Asegurar equipos informáticos.
UC0487_3: Auditar redes de comunicación y sistemas informáticos.
UC0488_3: Detectar y responder ante incidentes de seguridad.
UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

Entorno Profesional:

Ámbito Profesional:

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

Sectores Productivos:

Está presente en múltiples sectores productivos, sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. También está presente en los siguientes tipos de empresas:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (outsourcing) de servicios.

cve: BOE-A-2011-10055

Ocupaciones o puestos de trabajo relacionados:

3820.1017 Programador de Aplicaciones Informáticas
3812.1014 Técnico en Informática de Gestión
Técnico en seguridad informática.
Técnico en auditoría informática.

Duración de la formación asociada: 500 horas

Relación de módulos formativos y de unidades formativas:

MF0486_3: Seguridad en equipos informáticos. (90 horas)
MF0487_3: Auditoría de seguridad informática. (90 horas)
MF0488_3: Gestión de incidentes de seguridad informática. (90 horas)
MF0489_3: Sistemas seguros de acceso y transmisión de datos. (60 horas)
MF0490_3: (Transversal) Gestión de servicios en el sistema informático. (90 horas)
MP0175: Modulo de prácticas profesionales no laborales de Seguridad informática. (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: ASEGURAR EQUIPOS INFORMÁTICOS

Nivel: 3

Código: UC0486_3

Realizaciones profesionales y criterios de realización

RP1: Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.

CR1.1 El plan de implantación del sistema informático de la organización se analiza comprobando que incorpora la información necesaria referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones entre otros, así como referencias de posibilidades de utilización de los equipos y restricciones de los mismos y protecciones contra agresiones de virus y otros elementos no deseados.

CR1.2 Los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema son determinados por medio de las herramientas correspondientes según el Plan de Implantación y el de seguridad del sistema informático.

CR1.3 EL acceso a los servidores se realiza garantizando la confidencialidad e integridad de la conexión según las normas de seguridad de la organización.

CR1.4 Las políticas de usuario se analizan verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.

CR1.5 La política de seguridad es transmitida a los usuarios, asegurándose de su correcta y completa comprensión.

CR1.6 Las tareas realizadas se documentan convenientemente según los procedimientos de la organización.

CR1.7 Las informaciones afectadas por la legislación de protección de datos se tratan verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.

cve: BOE-A-2011-10055

- Actualización de parches de seguridad de los sistemas informáticos
- Protección de los sistemas de información frente a código malicioso
- Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
- Monitorización de la seguridad y el uso adecuado de los sistemas de información

9. Implantación y configuración de cortafuegos

- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
- Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
- Definición de reglas de corte en los cortafuegos
- Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas del cortafuegos

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0486_3	90	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 2

Denominación: AUDITORÍA DE SEGURIDAD INFORMÁTICA

Código: MF0487_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0487_3: Auditar redes de comunicación y sistemas informáticos

Duración: 90 horas

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.

cve: BOE-A-2011-10055

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

cve: BOE-A-2011-10055

- 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

cve: BOE-A-2011-10055

- 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

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0487_3	90	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 3

Denominación: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Código: MF0488_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0488_3: Detectar y responder ante incidentes de seguridad

cve: BOE-A-2011-10055