

MF0486_3: SEGURIDAD EN EQUIPOS INFORMÁTICOS. 90 HORAS

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.

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)

Unidad de competencia 2

Denominación: AUDITAR REDES DE COMUNICACIÓN Y SISTEMAS INFORMÁTICOS

Nivel: 3

Código: UC0487_3

MÓDULO FORMATIVO 1

Denominación: SEGURIDAD EN EQUIPOS INFORMÁTICOS

Código: MF0486_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia: UC0486_3: Asegurar equipos informáticos

Duración: 90 horas

Contenidos

1. Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos

- Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
- Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
- Salvaguardas y tecnologías de seguridad más habituales
- La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

2. Análisis de impacto de negocio

- Identificación de procesos de negocio soportados por sistemas de información
- Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
- Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

3. Gestión de riesgos

- Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
- Metodologías comúnmente aceptadas de identificación y análisis de riesgos
- Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

4. Plan de implantación de seguridad

- Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
- Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

5. Protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

6. Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas

- Determinación de los perímetros de seguridad física
- Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
- Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
- Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
- Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
- Elaboración de la normativa de seguridad física e industrial para la organización
- Sistemas de ficheros más frecuentemente utilizados
- Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
- Configuración de políticas y directivas del directorio de usuarios
- Establecimiento de las listas de control de acceso (ACLs) a ficheros
- Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
- Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
- Sistemas de autenticación de usuarios débiles, fuertes y biométricos
- Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
- Elaboración de la normativa de control de accesos a los sistemas informáticos

7. Identificación de servicios

- Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

- Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
- Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

8. Robustecimiento de sistemas

- Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
- Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
- Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
- Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
- 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