

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.

CR3.1 El acceso de los usuarios al sistema informático se configura para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.

CR3.2 El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.

CR3.3 Los recursos disponibles para los usuarios se limitan con las herramientas adecuadas en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.

CR4.1 Los dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.

CR4.2 Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.

CR4.3 Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización.

## Contexto profesional

### Medios de producción

Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

### Productos y resultados

Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

### Información utilizada o generada

Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

## III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

### 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

### Capacidades y criterios de evaluación

C1: Analizar los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar.

CE1.1 Identificar la estructura de un plan de implantación, explicando los contenidos que figuran en cada sección.

CE1.2 Distinguir los sistemas que pueden aparecer en el plan de implantación, describiendo las funcionalidades de seguridad que implementan.

CE1.3 Describir los niveles de seguridad que figuran en el plan de implantación, asociándolos a los permisos de acceso para su implantación.

CE1.4 En un supuesto práctico en el que se pide analizar el plan de implantación y sus repercusiones en el sistema:

- Determinar los sistemas implicados en el plan de implantación.
- Analizar los requisitos de seguridad de cada sistema.
- Describir las medidas de seguridad a aplicar a cada sistema.
- Cumplimentar los formularios para la declaración de ficheros de datos de carácter personal.

C2: Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.

CE2.1 Describir las características de los mecanismos de control de acceso físico, explicando sus principales funciones.

CE2.2 Exponer los mecanismos de traza, asociándolos al sistema operativo del servidor.

CE2.3 Identificar los mecanismos de control de acceso lógico, explicando sus principales características (contraseñas, filtrado de puertos IP entre otros).

CE2.4 En un supuesto práctico de implantación de un servidor según especificaciones dadas:

- Determinar la ubicación física del servidor para asegurar su funcionalidad.
- Describir y justificar las medidas de seguridad física a implementar que garanticen la integridad del sistema.
- Identificar los módulos o aplicaciones adicionales para implementar el nivel de seguridad requerido por el servidor.
- Determinar las amenazas a las que se expone el servidor, evaluando el riesgo que suponen, dado el contexto del servidor.
- Determinar los permisos asignados a los usuarios y grupos de usuarios para la utilización del sistema.

C3: Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.

CE3.1 Identificar los servicios habituales en el sistema informático de una organización, describiendo su misión dentro de la infraestructura informática y de comunicaciones.

CE3.2 Identificar y describir los servicios necesarios para el funcionamiento de un servidor, en función de su misión dentro del sistema informático de la organización.

CE3.3 Describir las amenazas de los servicios en ejecución, aplicando los permisos más restrictivos, que garanticen su ejecución y minimizan el riesgo.

CE3.4 En un supuesto práctico de implantación de un servidor con un conjunto de servicios en ejecución con correspondencias a un plan de explotación dado:

- Indicar las relaciones existentes entre dicho servidor y el resto del sistema informático de la organización.

- Extraer del plan de implantación los requisitos de seguridad aplicables al servidor.
- Determinar los servicios mínimos necesarios para el funcionamiento del sistema.

C4: Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.

CE4.1 Clasificar los tipos de cortafuegos, de red y locales, hardware y software, de paquetes y aplicación, describiendo sus características y funcionalidades principales.

CE4.2 Describir las reglas de filtrado de un cortafuegos de servidor, explicando los parámetros principales.

CE4.3 Explicar el formato de traza de un cortafuegos de servidor, reflejando la información de seguridad relevante.

CE4.4 A partir de un supuesto práctico de instalación de un cortafuegos de servidor en un escenario de accesos locales y remotos:

- Determinar los requisitos de seguridad del servidor.
- Establecer las relaciones del servidor con el resto de equipos del sistema informático.
- Elaborar el listado de reglas de acceso a implementar en el servidor.
- Componer un plan de pruebas del cortafuegos implementado.
- Ejecutar el plan de pruebas, redactando las correcciones necesarias para corregir las deficiencias detectadas.

## 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

#### 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.