FORMACIÓN CERTIFICADO DE PROFESIONALIDAD

UC0486_3
ASEGURAR EQUIPOS INFORMÁTICOS

MF0486_3

Seguridad en equipos informáticos

90 horas

(1/2) 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
- C2. Analizar e implementar los **mecanismos de acceso físicos y lógicos** a los servidores según especificaciones de seguridad
- C3. Evaluar la función y necesidad de cada **servicio en ejecución en el servidor** según las especificaciones de seguridad
- C4. **Instalar, configurar y administrar** un **cortafuegos** de servidor con las características necesarias según especificaciones de seguridad

C1. Planes de implantación
CE Teóricos

- ***CE1.1*** Identificar la **estructura** de un **plan de implantación**, explicando los **contenidos** que figuran en cada sección
- ***CE 1.2*** 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

C1. Planes de implantación
CE Práctico

- ***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. Acceso físicos y lógicos a servidores
CE Teóricos

- ***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**
  - **Filtrados de puertos IP** entre otros

C2. Acceso físicos y lógicos a servidores
CE Teóricos

- ***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**
  - **Filtrados de puertos IP** entre otros

C2. Acceso físicos y lógicos a servidores
CE Práctico

- ***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, dado el contexto del servidor
  - Determinar los **permisos asignados a los usuarios y grupos** de usuarios para la utilización del sistema

C3. Función y necesidad de los servicios
CE Teórico

- ***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 **servidores** en ejecución, aplicando los permisos más restrictivos, que **garantizan su ejecución y minimizan el riesgo**

C3. Función y necesidad de los servicios
CE Práctico

- ***CE2.4*** 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 firewalls

CE Teórico

- ***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

C4. Instalar, configurar y administrar firewalls

CE Práctico

- ***CE3.1*** 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 un 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

(2/2) FORMACIÓN

1. Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos
2. Análisis de impacto de negocio
3. Gestión de riesgos
4. Plan de implantación de seguridad
5. Protección de datos de carácter personal
6. Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas
7. Identificación de servicios
8. Robustecimientos de sistemas
9. Implantación y configuración de cortafuegos