PERFIL PROFESIONAL

UC0486_3
ASEGURAR EQUIPOS INFORMÁTICOS

MF0486_3

Seguridad en equipos informáticos

90 horas

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*
- RP2: **Configurar servidores** para **protegerlos de accesos no deseados** *según las necesidades de uso y dentro de las directivas de la organización*
- RP3: **Instalar y configurar cortafuegos** en **equipos** y **servidores** para garantizar la seguridad ante los **ataques externos** *según las necesidades de uso y dentro de las directivas de la organización.*

RP1. Políticas de seguridad CR1.1

- El **plan de implantación** del sistema informático de la organización se analiza comprobando qué incorpora la **información necesaria referida** a:
  - **Procedimientos** de **instalación y actualización** de equipos
  - **Copias de respaldo**
  - **Detección de intrusiones**
- Así como referencias:
  - Posibilidades de **utilización de los equipos** y **restricciones** de los mismos
  - **Protección** contra **agresiones de virus** y otros **elementos no deseados**

RP1. Políticas de seguridad 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**

RP1. Políticas de seguridad 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

RP1. Políticas de seguridad 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**
  - **ámbitos de responsabilidades** debidas a la **utilización de los equipos informáticos**

RP1. Políticas de seguridad CR1.5

- La política de seguridad es **transmitida a los usuarios**, asegurándose de su **correcta** y **completa comprensión**

RP1. Políticas de seguridad CR1.6

- Las **tareas** realizadas se **documentan convenientemente** según los procedimientos de la organización

RP1. Políticas de seguridad 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**
  - los **cauces de distribución de dicha información** están **documentados y autorizados** según el **plan de seguridad**

RP2. Configuración segura contra accesos no deseados

CR2.1

- La **ubicación del servidor** en la red se realiza en una **zona protegida y aislada** *según la normativa de seguridad y el plan de implantación de la organización*

RP2. Configuración segura contra accesos no deseados

CR2.2

- Los **servicios que ofrece el servidor** se **activan** y **configuran desactivando los innecesarios** según la normativa de seguridad y plan de implantación de la organización

RP2. Configuración segura contra accesos no deseados

CR2.3

- Los **accesos y permisos a los recursos del servidor** por parte de los usuarios son **configurados** en función del **propósito del propio servidor** y *de la normativa de seguridad de la organización*.

RP2. Configuración segura contra accesos no deseados

CR2.4

- Los **mecanismos de registro de actividad** e **incidencias** del sistema se activan, y se habilitan los **procedimientos de análisis** de dichas informaciones

RP2. Configuración segura contra accesos no deseados

CR2.5

- Los **módulos adicionales del servidor** son **analizados en base a sus funcionalidades** y **riesgos de seguridad** que implican su utilización, llegando a una **solución de compromiso**

RP2. Configuración segura contra accesos no deseados

CR2.6

- Los **mecanismos de autenticación** se configuran para que ofrezcan **niveles de seguridad** e **integridad** en la conexión de usuarios de acuerdo con *la normativa de seguridad de la organización*

RP2. Configuración segura contra accesos no deseados

CR2.7

- Los **roles y privilegios de los usuarios** se definen y asignan siguiendo las instrucciones que figuren en la normativa de seguridad y el plan de explotación de la organización

RP3. Firewalls contra ataques externos CR3.1

- La **topología del cortafuegos** es seleccionada en función del entorno de implantación

RP3. Firewalls contra ataques externos CR3.2

- Los elementos **hardware y software del cortafuegos** son elegidos teniendo en cuenta **factores económicos y de rendimiento**

RP3. Firewalls contra ataques externos CR3.3

- Los **cortafuegos son instalados y configurados** según el **nivel** definido en la **política de seguridad**

RP3. Firewalls contra ataques externos CR3.4

- Las **reglas de filtrado** y los **niveles de registro** y **alarmas** se determinan, configuran y administran según las necesidades dictaminadas *por la normativa de seguridad de la organización*

RP3. Firewalls contra ataques externos CR3.5

- Los **cortafuegos son verificados** con juegos de **pruebas** y se comprueba que superan las especificaciones de la *normativa de seguridad de la organización*

RP3. Firewalls contra ataques externos CR3.6

- **La instalación y actualización del cortafuegos** y los **procedimientos de actuación** con el mismo, quedan *documentados según las especificaciones de la organización*

RP3. Firewalls contra ataques externos CR3.7

- Los **sistemas de registro** son **definidos y configurados** para la **revisión y estudio** de los posibles **ataques, intrusiones y vulnerabilidades**

CONTEXTO PROFESIONAL (1/3)Medios de Producción

- **Aplicaciones ofimáticas corporativas**
- Verificación de **fortaleza de contraseñas**
- **Analizadores de puertos**
- Analizadores de **ficheros de registro del sistema**
- **Cortafuegos**
  - Equipos específicos y/o de propósito general
  - Cortafuegos personales o de servidor
- **Sistemas de autenticación**
  - **Débiles**: basados en usuario y contraseña
  - **Robustos**: basados en dispositivos físicos y medidas biométricas
- **Programas de comunicación** con capacidades **criptográficas**
- **Herramientas** de **administración remota segura**

CONTEXTO PROFESIONAL (2/3)Productos y resultados

- **Planes de implantación** revisados según directivas de la organización
- **Informes de auditoría** de **servicios de red** de sistemas informáticos
- **Mapa y diseño de la topología** de **cortafuegos corporativo**
  - **Guía de instalación y configuración** de cortafuegos
  - **Informe de actividad** detectada en el cortafuegos
  - **Normativa** para la elaboración del **diseño de cortafuegos**
- **Mapa y diseño** del **sistema de respaldo**
  - **Informe de realización** de copias de respaldo
- Elaboración de una **operativa de seguridad** de acorde con la **política de seguridad**

CONTEXTO PROFESIONAL (3/3)Información utilizada o generada

- **Política de seguridad** de infraestructuras telemáticas
- **Manuales** de instalación, referencia y uso de **cortafuegos**
- **Información sobre redes locales** y de área extensa y sistemas de comunicación públicos y privados
- Información sobre **equipos** y **software de comunicaciones**
- **Normativa, reglamentación y estándares (ISO, EIA, UIT-T, RFC-IETF)**
- **Registro** inventariado del **HW**
- **Registro** de comprobación con las **medidas de seguridad** aplicadas a cada **sistema informático**
- **Topología** del **sistema informático a proteger**