

GESTIÓN DE LA SEGURIDAD EN EQUIPOS Y SISTEMAS INFORMATICOS (80 HORAS)

TEORÍA: (35 HORAS)

Todos los contenidos de la presente acción formativa están relacionados con los del modelo formativo MFO486_3: Seguridad en equipos informáticos del Certificado de Profesionalidad. ITCT0109: Seguridad Informática de la Familia Profesional de Informática y Comunicaciones: Sistemas y Telemática.

1. Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos(4 Horas)

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

2. Análisis de impacto de negocio (4 Horas)

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

3. Gestión de riesgos (5 Horas)

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

4. Plan de implantación de seguridad (5 Horas)

- 4.1 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.
- 4.2 Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
- 4.3 Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

5. Protección de datos de carácter personal (5 Horas)

- 5.1 Principios generales de protección de datos de carácter personal
- 5.2 Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- 5.3 Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- 5.4 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 (6 Horas)

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

7. Identificación de servicios (3 Horas)

- 7.1 Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
- 7.2 Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
- 7.3 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. Implantación y configuración de cortafuegos (3 Horas)

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

PRACTICAS: (45 HORAS)

- 1 Analizar los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar.
 - 1.1 Identificar la estructura de un plan de implantación, explicando los contenidos que figuran en cada sección.
 - 1.2 Distinguir los sistemas que pueden aparecer en el plan de implantación, describiendo las funcionalidades de seguridad que implementan.
 - 1.3 Describir los niveles de seguridad que figuran en el plan de implantación, asociándolos a los permisos de acceso para su implantación.
 - 1.4 En un supuesto práctico en el que se pide analizar el plan de implantación y sus repercusiones en el sistema:
 - 1.4.1 Determinar los sistemas implicados en el plan de implantación.
 - 1.4.2 Analizar los requisitos de seguridad de cada sistema.
 - 1.4.3 Describir las medidas de seguridad a aplicar a cada sistema.
 - 1.4.4 Cumplimentar los formularios para la declaración de ficheros de datos de carácter personal.
- 2. Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.
 - 2.1 Describir las características de los mecanismos de control de acceso físico, explicando sus principales funciones.
 - 2.2 Exponer los mecanismos de traza, asociándolos al sistema operativo del servidor.
 - 2.3 Identificar los mecanismos de control de acceso lógico, explicando sus principales características (contraseñas, filtrado de puertos IP entre otros).
 - 2.4 En un supuesto práctico de implantación de un servidor según especificaciones dadas:
 - 2.4.1 Determinar la ubicación física del servidor para asegurar su funcionalidad.
 - 2.4.2 Describir y justificar las medidas de seguridad física a implementar que garanticen la integridad del sistema.
 - 2.4.3 Identificar los módulos o aplicaciones adicionales para implementar el nivel de seguridad requerido por el servidor.
 - 2.4.4 Determinar las amenazas a las que se expone el servidor, evaluando el riesgo que suponen, dado el contexto del servidor.

- 2.4.5 Determinar los permisos asignados a los usuarios y grupos de usuarios para la utilización del sistema.
- 3 Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.
- 3.1 Identificar los servicios habituales en el sistema informático de una organización, describiendo su misión dentro de la infraestructura informática y de comunicaciones.
- 3.2 Identificar y describir los servicios necesarios para el funcionamiento de un servidor, en función de su misión dentro del sistema informático de la organización.
- 3.3 Describir las amenazas de los servicios en ejecución, aplicando los permisos más restrictivos, que garantizan su ejecución y minimizan el riesgo.
- 3.4 En un supuesto práctico de implantación de un servidor con un conjunto de servicios en ejecución con correspondencias a un plan de explotación dado:
- 3.4.1 Indicar las relaciones existentes entre dicho servidor y el resto del sistema informático de la organización.
- 3.4.2 Extraer del plan de implantación los requisitos de seguridad aplicables al servidor.
- 3.4.3 Determinar los servicios mínimos necesarios para el funcionamiento del sistema.
- 4 Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.
- 4.1 Clasificar los tipos de cortafuegos, de red y locales, hardware y software, de paquetes y aplicación, describiendo sus características y funcionalidades principales.
- 4.2 Describir las reglas de filtrado de un cortafuegos de servidor, explicando los parámetros principales.
- 4.3 Explicar el formato de traza de un cortafuegos de servidor, reflejando la información de seguridad relevante.
- 4.4 A partir de un supuesto práctico de instalación de un cortafuegos de servidor en un escenario de accesos locales y remotos:
- 4.4.1 Determinar los requisitos de seguridad del servidor.
- 4.4.2 Establecer las relaciones del servidor con el resto de equipos del sistema informático.
- 4.4.3 Elaborar el listado de reglas de acceso a implementar en el servidor.
- 4.4.4 Componer un plan de pruebas del cortafuegos implementado.
- 4.4.5 Ejecutar el plan de pruebas, redactando las correcciones necesarias para corregir las deficiencias detectadas.