FORMACIÓN

UC0487_3

AUDITORÍA REDES DE COMUNICACIÓN Y SISTEMAS INFORMÁTICOS

MF0487_3

AUDITORÍA DE SEGURIDAD INFORMÁTICA (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
- **C2.** Aplicar procedimientos relativos al cumplimiento de la **normativa legal** vigente
- **C3. Planificar** y **aplicar medidas de seguridad** para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental

C1. Herramientas de auditoría y análisis de vulnerabilidades
CE Teóricos

- CE1.1 Explicar las diferencias entre vulnerabilidades y amenazas
- CE1.2 Enunciar las características de las principales tipos de vulnerabilidades y programas maliciosos existentes, describiendo sus particularidades
- CE1.3 Describir el funcionamiento de una herramienta de análisis de vulnerabilidades, indicando las principales técnicas empleadas y la fiabilidad de las mismas
- CE 1.4 Seleccionar la herramienta de auditoría de seguridad más adecuada en función del servidor o red y los requisitos de seguridad

C1. Herramientas de auditoría y análisis de vulnerabilidades
CE Práctico

- CE 1.5 A partir de un supuesto práctico, ante un sistema informático dado en circunstancias de implantación concretas:
  - Establecer los requisitos de seguridad que debe cumplir cada sistema
  - Crear una prueba nueva la herramienta de auditoría, partiendo de las especificaciones de la vulnerabilidad
  - Elaborar el plan de pruebas teniendo en cuenta el tipo de servidor analizado
  - Utilizar varias herramientas para detectar posibles vulnerabilidades
  - Analizar el resultado de la herramienta de auditoría, descartando falsos positivos
  - Redactar el informe de auditoría, reflejando las irregularidades detectadas, y las sugerencias para su regularización

C2. Normativa Legal
CE Teóricos

- CE2.1 Explicar la normativa legal vigente (autonómica, nacional, europea e internacional) aplicable a datos de carácter personal
- CE2.2 Exponer los trámites legales que deben cumplir los ficheros con datos de carácter personal, teniendo en cuenta la calidad de los mismos
- CR2.3 Describir los niveles de seguridad establecidos en la normativa legal asociándolos a los requisitos exigidos

C2. Normativa Legal
CE Práctico

- CE2.4 A partir de un supuesto práctico, en el que se cuenta con una estructura de registro de información de una organización
  - Identificar los ficheros con datos de carácter personal, justificando el nivel de seguridad que le corresponde
  - Elaborar el plan de auditoría de cumplimiento de legislación en materia de protección de datos de carácter personal
  - Revisar la documentación asociada a los ficheros con datos de carácter personal, identificando las carencias existentes
  - Elaborar el informe correspondiente a los ficheros de carácter personal, indicando las definiciones encontradas y las correcciones pertinentes

C3. Medidas de seguridad
CE Teóricos

- CE3.1 Identificar las fases del análisis de riesgos, describiendo el objetivo de cada una de ellas
- CE3.2 Describir los términos asociados al análisis de riesgos (amenaza, vulnerabilidad, impacto y contramedidas), estableciendo la relación existente entre ellos
- CE3.3 Describir las técnicas de análisis de redes, explicando los criterios de selección
- CE3.4 Describir las topologías de cortafuegos de red comunes, indicando sus funcionalidades principales

CONTENIDOS

1. Criterios deontológico de la función de auditoría
2. Aplicación de la normativa de protección de datos de carácter personal
3. Análisis de riesgos de los sistemas de información
4. Uso de herramientas para la auditoría de sistemas
5. Descripción de los aspectos sobre cortafuegos en auditorías de Sistemas Informáticos
6. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información