DATOS IDENTIFICATIVOS DEL MÓDULO FORMATIVO

MÓDULO FORMATIVO	GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA	Duración	90
Código	MF0488_3		
Familia profesional	INFORMÁTICA Y COMUNICACIONES		
Área profesional	Sistemas y telemática		
Certificado de profesionalidad	Seguridad informática	Nivel	3
Resto de formación para completar el certificado de profesionalidad	Seguridad en equipos informáticos	Duración	90
	Auditoría de seguridad informática		90
	Sistemas seguros de acceso y tratamiento de datos		60
	Gestión de servicios en el sistema informático (Transversal)		90
	Prácticas profesionales no laborales en seguridad informática		80

Apartado A: **REFERENTE DE COMPETENCIA**

Este módulo formativo se corresponde con la unidad de competencia UC0488_3: DETECTAR Y RESPONDER ANTE INCIDENTES DE SEGURIDAD

Apartado B: **ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS**

Capacidades y criterios de evaluación

C1: Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.

CE1.1 Describir las técnicas de detección y prevención de intrusos, exponiendo los principales parámetros que pueden emplearse como criterios de detección.

CE1.2 Determinar el número, tipo y ubicación de los sistemas de detección de intrusos, garantizando la monitorización del tráfico indicado en el plan de implantación.

CE1.3 Seleccionar las reglas del sistema de detección de intrusos, en función del sistema informático a monitorizar.

CE1.4 Determinar los umbrales de alarma del sistema, teniendo en cuenta los parámetros de uso del sistema.

CE1.5 Elaborar reglas de detección, partiendo de la caracterización de las técnicas de intrusión.

CE1.6 A partir de un supuesto práctico convenientemente caracterizado en el que se ubican servidores con posibilidad de accesos locales y remotos:

- Instalar y configurar software de recolección de alarmas.
- Configurar diferentes niveles de recolección de alarmas.

CE1.7 En una colección de supuestos prácticos en un entorno controlado de servidores en varias zonas de una red departamental con conexión a Internet:

- Decidir áreas a proteger.
- Instalar un sistema de detección de intrusos.
- Definir y aplicar normas de detección.
- Verificar funcionamiento del sistema atacando áreas protegidas.
- Elaborar un informe detallando conclusiones.

C2: Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.

CE2.1 Analizar la información de los sistemas de detección de intrusos, extrayendo aquellos eventos relevantes para la seguridad.

CE2.2 Analizar los indicios de intrusión, indicando los condicionantes necesarios para que la amenaza pueda materializarse.

CE2.3 Clasificar los elementos de las alertas del sistema de detección de intrusiones, estableciendo las posibles correlaciones existentes entre ellos, distinguiendo las alertas por tiempos y niveles de seguridad.

CE2.4 A partir de un supuesto práctico, en el que realizan intentos de intrusión al sistema informático:

- Recopilar las alertas de los sistemas de detección de intrusiones.
- Relacionar los eventos recogidos por los sistemas de detección de intrusiones.
- Determinar aquellas alertas significativas.
- Elaborar el informe correspondiente indicando las posibles intrusiones y el riesgo asociado para la seguridad del sistema informático de la organización.

CE2.5 Establecer procesos de actualización de las herramientas de detección de intrusos para asegurar su funcionalidad según especificaciones de los fabricantes.

C3: Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

CE3.1 Describir las fases del plan de actuación frente a incidentes de seguridad, describiendo los objetivos de cada fase.

CE3.2 Indicar las fases del análisis forense de equipos informáticos, describiendo los objetivos de cada fase.
CE3.3 Clasificar los tipos de evidencias del análisis forense de sistemas, indicando sus características, métodos de recolección y análisis.
CE3.4 Describir las distintas técnicas para análisis de programas maliciosos, indicando casos de uso.
CE3.5 En un supuesto práctico, en el que se ha producido una intrusión en un sistema informático:
- Realizar la recogida de evidencias volátiles.
- Realizar la recogida de evidencias no volátiles.
- Análisis preliminar de las evidencias.
- Análisis temporal de actividad del sistema de ficheros.
- Elaborar el informe final, recogiendo las evidencias encontradas, las posibles vulnerabilidades utilizadas para la intrusión y la actividad realizada por el intruso que ha sido detectada en el sistema.

CE3.6 Estandarizar métodos de recuperación de desastres de equipos informáticos ante la detección de intrusiones.

Contenidos

1. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- Identificación y caracterización de los datos de funcionamiento del sistema
- Arquitecturas más frecuentes de los sistemas de detección de intrusos
- Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

2. Implantación y puesta en producción de sistemas IDS/IPS
- Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
- Definición de políticas de corte de intentos de intrusión en los IDS/IPS
- Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
- Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
- Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

3. Control de código malicioso
- Sistemas de detección y contención de código malicioso
- Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
- Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
- Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
- Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
- Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

4. Respuesta ante incidentes de seguridad
- Procedimiento de recolección de información relacionada con incidentes de seguridad
- Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
- Proceso de verificación de la intrusión
- Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

5. Proceso de notificación y gestión de intentos de intrusión
- Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
- Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
- Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
- Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
- Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
- Establecimiento del nivel de intervención requerido en función del impacto previsible
- Guía para la investigación y diagnostico del incidente de intento de intrusión o infecciones
- Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
- Proceso para la comunicación del incidente a terceros, si procede
- Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

6. Análisis forense informático
- Conceptos generales y objetivos del análisis forense
- Exposición del Principio de Lockard

- Guía para la recogida de evidencias electrónicas:
    - Evidencias volátiles y no volátiles
    - Etiquetado de evidencias
    - Cadena de custodia
    - Ficheros y directorios ocultos
    - Información oculta del sistema
    - Recuperación de ficheros borrados
- Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
- Guía para la selección de las herramientas de análisis forense

Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

– Estar en posesión del título de Bachiller
– Estar en posesión de algún certificado de profesionalidad de nivel 3.
– Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional
– Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior
– Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años
– Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad: Seguridad informática.