ANEXO III

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Seguridad informática

Código: IFCT0109

Familia Profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC153_3 Seguridad informática (RD 1087/05 de 16 de septiembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

UC0486_3: Asegurar equipos informáticos.
UC0487_3: Auditar redes de comunicación y sistemas informáticos.
UC0488_3: Detectar y responder ante incidentes de seguridad.
UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

Entorno Profesional:

Ámbito Profesional:

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

Sectores Productivos:

Está presente en múltiples sectores productivos, sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. También está presente en los siguientes tipos de empresas:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (outsourcing) de servicios.

cve: BOE-A-2011-10055

Ocupaciones o puestos de trabajo relacionados:

3820.1017 Programador de Aplicaciones Informáticas
3812.1014 Técnico en Informática de Gestión
Técnico en seguridad informática.
Técnico en auditoría informática.

Duración de la formación asociada: 500 horas

Relación de módulos formativos y de unidades formativas:

MF0486_3: Seguridad en equipos informáticos. (90 horas)
MF0487_3: Auditoría de seguridad informática. (90 horas)
MF0488_3: Gestión de incidentes de seguridad informática. (90 horas)
MF0489_3: Sistemas seguros de acceso y transmisión de datos. (60 horas)
MF0490_3: (Transversal) Gestión de servicios en el sistema informático. (90 horas)
MP0175: Modulo de prácticas profesionales no laborales de Seguridad informática. (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: ASEGURAR EQUIPOS INFORMÁTICOS

Nivel: 3

Código: UC0486_3

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.

CR1.1 El plan de implantación del sistema informático de la organización se analiza comprobando que incorpora la información necesaria referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones entre otros, así como referencias de posibilidades de utilización de los equipos y restricciones de los mismos y protecciones contra agresiones de virus y otros elementos no deseados.

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.

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.

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 y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.

CR1.5 La política de seguridad es transmitida a los usuarios, asegurándose de su correcta y completa comprensión.

CR1.6 Las tareas realizadas se documentan convenientemente según los procedimientos de la organización.

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 y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.

cve: BOE-A-2011-10055

RP2: Configurar servidores para protegerlos de accesos no deseados según las necesidades de uso y dentro de las directivas de la organización.

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.

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.

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.

CR2.4 Los mecanismos de registro de actividad e incidencias del sistema se activan y se habilitan los procedimientos de análisis de dichas informaciones.

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.

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.

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: 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.

CR3.1 La topología del cortafuegos es seleccionada en función del entorno de implantación.

CR3.2 Los elementos hardware y software del cortafuegos son elegidos teniendo en cuenta factores económicos y de rendimiento.

CR3.3 Los cortafuegos son instalados y configurados según el nivel definido en la política de seguridad.

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.

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.

CR3.6 La instalación y actualización del cortafuegos y los procedimientos de actuación con el mismo quedan documentados según las especificaciones de la organización.

CR3.7 Los sistemas de registro son definidos y configurados para la revisión y estudio de los posibles ataques, intrusiones y vulnerabilidades.

Contexto profesional

Medios de producción

Aplicaciones ofimáticas corporativas. Verificadores 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 y robustos: basados en dispositivos físicos y medidas biométricas. Programas de comunicación con capacidades criptográficas. Herramientas de administración remota segura.

cve: BOE-A-2011-10055

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. Mapa y diseño del sistema de copias de respaldo. Planificación de la realización de las copias de respaldo. Informe de realización de copias de respaldo. Normativa para la elaboración del diseño de cortafuegos. Elaboración de una operativa de seguridad acorde con la política de seguridad.

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 hardware. Registro de comprobación con las medidas de seguridad aplicadas a cada sistema informático. Topología del sistema informático a proteger.

Unidad de competencia 2

Denominación: AUDITAR REDES DE COMUNICACIÓN Y SISTEMAS INFORMÁTICOS

Nivel: 3

Código: UC0487_3

Realizaciones profesionales y criterios de realización

RP1: Realizar análisis de vulnerabilidades, mediante programas específicos para controlar posibles fallos en la seguridad de los sistemas según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Las herramientas y los tipos de pruebas de análisis de vulnerabilidades se seleccionan y adecuan al entorno a verificar según las especificaciones de seguridad de la organización.

CR1.2 Los programas y las pruebas se actualizan para realizar ensayos consistentes con los posibles fallos de seguridad de las versiones de hardware y software instaladas en el sistema informático.

CR1.3 Los resultados de las pruebas se analizan y documentan conforme se indica en la normativa de la organización.

CR1.4 Los sistemas de acceso por contraseña se comprueban mediante herramientas específicas según las especificaciones de la normativa de seguridad.

CR1.5 La documentación del análisis de vulnerabilidades contiene referencias exactas de las aplicaciones y servicios que se han detectado funcionando en el sistema, el nivel de los parches instalados, vulnerabilidades de negación de servicio, vulnerabilidades detectadas y mapa de la red.

RP2: Verificar el cumplimiento de la normativa y requisitos legales vigentes en materia de protección de datos personales para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización.

CR2.1 Los ficheros con datos de carácter personal son identificados y tienen asignado un responsable de seguridad según normativa legal.

CR2.2 El listado de personas autorizadas a acceder a cada fichero existe y se encuentra actualizado según normativa legal.

cve: BOE-A-2011-10055

CR2.3 El control de accesos a los ficheros se comprueba siguiendo el procedimiento establecido en la normativa de seguridad de la organización.
CR2.4 La gestión del almacenamiento de los ficheros y sus copias de seguridad se realiza siguiendo la normativa legal y de la organización.
CR2.5 El acceso telemático a los ficheros se realiza utilizando mecanismos que garanticen la confidencialidad e integridad cuando así lo requiera la normativa.
CR2.6 El informe de la auditoría recoge la relación de ficheros con datos de carácter personal y las medidas de seguridad aplicadas y aquellas pendientes de aplicación.

RP3: Comprobar el cumplimiento de la política de seguridad establecida para afirmar la integridad del sistema según las necesidades de uso y dentro de las directivas de la organización.
CR3.1 Los procedimientos de detección y gestión de incidentes de seguridad se desarrollan y se incluyen en la normativa de seguridad de la organización.
CR3.2 Los puntos de acceso de entrada y salida de la red son verificados para que su uso se circunscriba a lo descrito en la normativa de seguridad de la organización.
CR3.3 Los programas de seguridad y protección de sistemas se activan y actualizan según las especificaciones de los fabricantes.
CR3.4 Los puntos de entrada y salida de la red adicionales son autorizados y controlados en base a las especificaciones de seguridad y al plan de implantación de la organización.
CR3.5 Los procesos de auditoría informática son revisados, tanto los de carácter interno, como aquellos realizados por personal externo a la organización.
CR3.6 Los procedimientos de las políticas de seguridad se verifican en su cumplimiento por parte de los usuarios.

Contexto profesional

Medios de producción
Aplicaciones ofimáticas corporativas
Analizadores de vulnerabilidades.
Herramientas para garantizar la confidencialidad de la información.
Programas que garantizan la confidencialidad e integridad de las comunicaciones.
Aplicaciones para gestión de proyectos.
Programas de análisis de contraseñas.

Productos y resultados
Informes de análisis de vulnerabilidades
Relación de contraseñas débiles.
Registro de ficheros de datos de carácter personal, según normativa vigente
Informe de auditoría de servicios y puntos de acceso al sistema informático.

Información utilizada o generada
Normativa sobre protección de datos personales.
Política de seguridad de la empresa.
Metodologías de análisis de seguridad (OSSTM, BS7799/ISO17799).
Boletines de seguridad y avisos de vulnerabilidades disponibles en formato electrónico.
Topología del sistema informático a proteger.

Unidad de competencia 3

Denominación: DETECTAR Y RESPONDER ANTE INCIDENTES DE SEGURIDAD

cve: BOE-A-2011-10055

Nivel: 3

Código: UC0488_3

Realizaciones profesionales y criterios de realización

RP1: Implantar procedimientos para la respuesta ante incidentes e implantar mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.

CR1.1 Los procedimientos de detección y respuesta de incidentes están documentados, indican los roles y responsabilidades de seguridad e implementan los requerimientos de la política de seguridad de la organización.

CR1.2 Los sistemas se modelan para detectar signos de comportamiento sospechoso seleccionando los mecanismos de registro a activar, observando las alarmas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones.

CR1.3 Los mecanismos de registro del sistema se activan y se planifican los procedimientos de análisis de los mismos según las especificaciones de seguridad de la organización.

CR1.4 Los sistemas de detección de intrusos se instalan, actualizan y configuran en función de las especificaciones de seguridad de la organización.

CR1.5 Los procedimientos de restauración del sistema informático se verifican para la recuperación del mismo ante un incidente grave dentro de las necesidades de la organización.

RP2: Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.

CR2.1 Las herramientas utilizadas para detectar intrusiones son analizadas para determinar que no han sido comprometidas ni afectadas por programas maliciosos.

CR2.2 Los parámetros de funcionamiento sospechoso se analizan con herramientas específicas según la normativa de seguridad.

CR2.3 Los componentes software del sistema se verifican periódicamente en lo que respecta a su integridad usando programas específicos.

CR2.4 Las pruebas realizadas a los dispositivos de protección física del sistema informático verifican el correcto funcionamiento de los mismos según la normativa de seguridad de la organización.

CR2.5 Los sucesos y signos extraños que pudieran considerarse una alerta son recogidos en el informe diario de actividad.

RP3: Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la organización.

CR3.1 La detección de un incidente de seguridad produce la realización de los procedimientos recogidos en los protocolos de la normativa de seguridad de la organización.

CR3.2 El sistema vulnerado, se aísla y se procede a recoger la información para el análisis forense de la misma según los procedimientos de la normativa de seguridad de la organización.

CR3.3 El sistema atacado se analiza mediante herramientas de detección de intrusos según los procedimientos de seguridad de la organización.

CR3.4 La intrusión es contenida mediante la aplicación de las medidas establecidas en la normativa de seguridad de la organización.

CR3.5 La documentación del incidente se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido.

cve: BOE-A-2011-10055

CR3.6 Los daños causados se determinan y se planifican las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado según las normas de calidad y el plan de explotación de la organización.

Contexto profesional

Medios de producción
Aplicaciones ofimáticas corporativas. Analizadores de vulnerabilidades. Herramientas para garantizar la confidencialidad de la información. Programas que garantizan la confidencialidad e integridad de las comunicaciones. Aplicaciones para gestión de proyectos. Programas de análisis de contraseñas. Software de monitorización de redes. Software de flujo de trabajo para envío de alarmas e incidencias a responsables. IDS y sus consolas. Consola de SNMP.

Productos y resultados
Informes de análisis de vulnerabilidades. Relación de contraseñas débiles. Registro de ficheros de datos de carácter personal, según normativa vigente. Informe de auditoría de servicios y puntos de acceso al sistema informático. Registro de actividad. Documento de seguridad. Registro de alarmas.

Información utilizada o generada
Normativa sobre protección de datos personales. Política de seguridad de la empresa. Metodologías de análisis de seguridad (OSSTM, BS7799/ISO17799). Boletines de seguridad y avisos de vulnerabilidades, en su mayoría redactados en inglés, y disponibles en formato electrónico. Documento de trabajo en base a la política de seguridad. Normativa de detección de intrusos. Normativa de prevención de amenazas de seguridad.

Unidad de competencia 4

Denominación: DISEÑAR E IMPLEMENTAR SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Nivel: 3

Código: UC0489_3

Realizaciones profesionales y criterios de realización

RP1: Implantar políticas de seguridad y cifrado de información en operaciones de intercambio de datos para obtener conexiones seguras según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Las comunicaciones con otras compañías o a través de canales inseguros utilizan redes privadas virtuales para garantizar la confidencialidad e integridad de dichas conexiones durante el tránsito a través de redes públicas según las especificaciones de la normativa de seguridad y el diseño de redes de la organización.

CR1.2 Los requerimientos para implantar la solución de red privada virtual se seleccionan y comunican al operador de telefonía para lograr soluciones adecuadas al plan de seguridad.

CR1.3 Las técnicas de protección de conexiones inalámbricas disponibles en el mercado son evaluadas y se seleccionan aquellas más idóneas, teniendo en cuenta el principio de proporcionalidad y las normas de seguridad de la organización.

cve: BOE-A-2011-10055

CR1.4 Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones son implantados según parámetros de la normativa de seguridad de la organización.
CR1.5 Los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas para garantizar la seguridad de las comunicaciones utilizan servicios de encapsulación.
CR1.6 Los servicios que incorporan soporte para certificados digitales para identificación del servidor, se emplean para garantizar al usuario la identidad del servidor.

RP2: Implantar sistemas de firma digital para asegurar la autenticidad, integridad y confidencialidad de los datos que intervienen en una transferencia de información utilizando sistemas y protocolos criptográficos según las necesidades de uso y dentro de las directivas de la organización.
CR2.1 El acceso a servicios a través de la red telemática utiliza autenticación basada en certificados digitales de identidad personal.
CR2.2 El proceso de obtención y verificación de firmas se aplica en caso de ser necesario según los requerimientos del sistema informático y los procesos de negocio
CR2.3 La transmisión de mensajes de correo electrónico utilizan certificados digitales para firmar y cifrar su contenido.
CR2.4 Los sistemas de firma digital de documentos mediante certificados digitales se implantan según la normativa de seguridad de la organización.
CR2.5 Los sistemas de sellado digital de tiempo, para garantizar la existencia de un documento en una determinada fecha, se implantan según las normas de seguridad de la organización.
CR2.6 Los componentes web son firmados digitalmente para garantizar la integridad de dichos componentes.

RP3: Implementar infraestructuras de clave pública para garantizar la seguridad según los estándares del sistema y dentro de las directivas de la organización.
CR3.1 La jerarquía de certificación se diseña en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.
CR3.2 La declaración de prácticas de certificación y la política de certificación se redacta de forma que definen los procedimientos y derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.
CR3.3 El sistema de autoridad de certificación se instala siguiendo las indicaciones del fabricante.
CR3.4 El certificado de la autoridad de certificación y la política de certificación se disponen a los usuarios en la forma y modo necesario, siguiendo las directrices contenidas en la declaración de prácticas de certificación.
CR3.5 La clave privada de la autoridad de certificación se mantiene segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.
CR3.6 La emisión de certificados digitales se realiza según los usos que va a recibir el certificado y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.
CR3.7 El servicio de revocación de certificados mantiene accesible la información sobre validez de los certificados emitidos por la autoridad de certificación según lo indicado en la declaración de prácticas de certificación.

cve: BOE-A-2011-10055

Contexto profesional

Medios de producción
Programas para conexión segura. Sistemas para implantar autoridades de certificación digital. Servidores y clientes de redes privadas virtuales (VPN). Soportes seguros para certificados digitales. Servidores web con soporte SSL/TLS. Encapsuladores de tráfico con soporte criptográfico (HW y SW). Programas de conexión segura a servicios telemáticos. Interfaces de correo electrónico con soporte para correo seguro.

Productos y resultados
Política de certificación. Declaración de prácticas de certificación. Listado de certificados emitidos y certificados revocados. Guías y recomendaciones de implantación de sistemas de comunicación seguros. Guías de utilización de certificados digitales.

Información utilizada o generada
Normativa legal sobre firma digital. Estándares y recomendaciones, generalmente redactadas en inglés. Manuales de instalación de infraestructuras de clave pública (PKI).

Unidad de competencia 5

Denominación: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Los procesos que intervienen en el sistema son identificados para evaluar parámetros de rendimiento.

CR1.2 Los parámetros que afectan a los componentes del sistema: memoria, procesador y periféricos, entre otros, se ajustan a las necesidades de uso.

CR1.3 Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización.

CR1.4 Las herramientas de monitorización se implantan y configuran determinando los niveles de las alarmas en función del plan de explotación de la organización.

RP2: Administrar los dispositivos de almacenamiento según las necesidades de uso y dentro de las directivas de la organización.

CR2.1 Los dispositivos de almacenamiento se configuran para ser usados en los distintos sistemas operativos utilizados en el sistema informático.

CR2.2 La estructura de almacenamiento se define y se implanta atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de uso de la organización.

CR2.3 Los requerimientos de nomenclatura de objetos y restricciones de uso de cada dispositivo de almacenamiento se documentan adecuadamente.

CR2.4 Los dispositivos de almacenamiento se integran para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

cve: BOE-A-2011-10055

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.

CR3.1 El acceso de los usuarios al sistema informático se configura para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.

CR3.2 El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.

CR3.3 Los recursos disponibles para los usuarios se limitan con las herramientas adecuadas en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.

CR4.1 Los dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.

CR4.2 Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.

CR4.3 Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización.

Contexto profesional

Medios de producción

Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

Productos y resultados

Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada

Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: SEGURIDAD EN EQUIPOS INFORMÁTICOS

Código: MF0486_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

cve: BOE-A-2011-10055

UC0486_3: Asegurar equipos informáticos

Duración: 90 horas

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.

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

CE1.2 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.

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: Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.

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, filtrado de puertos IP entre otros).

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

C3: Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.

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 servicios en ejecución, aplicando los permisos más restrictivos, que garantizan su ejecución y minimizan el riesgo.

CE3.4 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.

cve: BOE-A-2011-10055

- 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 un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.

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.

CE4.4 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 el 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.

Contenidos

1. **Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos**
   - Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
   - Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
   - Salvaguardas y tecnologías de seguridad más habituales
   - La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

2. **Análisis de impacto de negocio**
   - Identificación de procesos de negocio soportados por sistemas de información
   - Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
   - Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

3. **Gestión de riesgos**
   - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
   - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
   - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

4. **Plan de implantación de seguridad**
   - 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.
   - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
   - Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

cve: BOE-A-2011-10055

5. Protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- 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

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

7. Identificación de servicios

- Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
- Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
- 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. Robustecimiento de sistemas

- Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
- Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
- Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
- Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

cve: BOE-A-2011-10055

- Actualización de parches de seguridad de los sistemas informáticos
- Protección de los sistemas de información frente a código malicioso
- Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
- Monitorización de la seguridad y el uso adecuado de los sistemas de información

9. Implantación y configuración de cortafuegos

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

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0486_3	90	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 2

Denominación: AUDITORÍA DE SEGURIDAD INFORMÁTICA

Código: MF0487_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0487_3: Auditar redes de comunicación y sistemas informáticos

Duración: 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.

CE1.1 Explicar las diferencias entre vulnerabilidades y amenazas.

CE1.2 Enunciar las características de los principales tipos de vulnerabilidades y programas maliciosos existentes, describiendo sus particularidades.

cve: BOE-A-2011-10055

CE1.3 Describir el funcionamiento de una herramienta de análisis de vulnerabilidades, indicando las principales técnicas empleadas y la fiabilidad de las mismas.
CE1.4 Seleccionar la herramienta de auditoría de seguridad más adecuada en función del servidor o red y los requisitos de seguridad.
CE1.5 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 para 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: Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.
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.
CE2.3 Describir los niveles de seguridad establecidos en la normativa legal vigente asociándolos a los requisitos exigidos.
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 deficiencias encontradas y las correcciones pertinentes.

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.
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 generales comúnmente aceptados sobre auditoría informática
- Código deontológico de la función de auditoría
- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- Criterios a seguir para la composición del equipo auditor

cve: BOE-A-2011-10055

- Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- Tipos de muestreo a aplicar durante el proceso de auditoría
- Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

2. Aplicación de la normativa de protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Normativa europea recogida en la directiva 95/46/CE
- Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
- Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

3. Análisis de riesgos de los sistemas de información

- Introducción al análisis de riesgos
- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- Particularidades de los distintos tipos de código malicioso
- Principales elementos del análisis de riesgos y sus modelos de relaciones
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Identificación de los activos involucrados en el análisis de riesgos y su valoración
- Identificación de las amenazas que pueden afectar a los activos identificados previamente
- Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
- Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
- Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
- Determinación de la probabilidad e impacto de materialización de los escenarios
- Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
- Relación de las distintas alternativas de gestión de riesgos

cve: BOE-A-2011-10055

- Guía para la elaboración del plan de gestión de riesgos
- Exposición de la metodología NIST SP 800-30
- Exposición de la metodología Magerit versión 2

4. **Uso de herramientas para la auditoría de sistemas**
   - Herramientas del sistema operativo tipo Ping, Traceroute, etc.
   - Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
   - Herramientas de análisis de vulnerabilidades tipo Nessus
   - Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
   - Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
   - Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

5. **Descripción de los aspectos sobre cortafuegos en auditorías de Sistemas Informáticos.**
   - Principios generales de cortafuegos
   - Componentes de un cortafuegos de red
   - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
   - Arquitecturas de cortafuegos de red
   - Otras arquitecturas de cortafuegos de red

6. **Guías para la ejecución de las distintas fases de la auditoría de sistemas de información**
   - Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
   - Guía para la elaboración del plan de auditoría
   - Guía para las pruebas de auditoría
   - Guía para la elaboración del informe de auditoría

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0487_3	90	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 3

Denominación: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Código: MF0488_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0488_3: Detectar y responder ante incidentes de seguridad

cve: BOE-A-2011-10055

Duración: 90 horas

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.

cve: BOE-A-2011-10055

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

cve: BOE-A-2011-10055

- 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

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0488_3	90	40

cve: BOE-A-2011-10055

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 4

Denominación: SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Código: MF0489_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos

Duración: 60 horas

Capacidades y criterios de evaluación

C1: Evaluar las técnicas de cifrado existentes para escoger la necesaria en función de los requisitos de seguridad exigidos.

CE1.1 Describir las diferencias entre los algoritmos de cifrado de clave privada y los de clave pública, indicando sus diferentes usos.
CE1.2 Identificar los diferentes modos de cifrado, describiendo las características principales.
CE1.3 Clasificar los diferentes algoritmos de clave privada, describiendo sus fases de ejecución.
CE1.4 Clasificar los diferentes algoritmos de clave pública, describiendo sus fases de ejecución.
CE1.5 Identificar los diferentes protocolos de intercambio de claves, describiendo su funcionamiento.

C2: Implantar servicios y técnicas criptográficas en aquellos servicios que lo requieran según especificaciones de seguridad informática.

CE2.1 Justificar la necesidad de utilizar técnicas criptográficas en las comunicaciones entre sistemas informáticos en función de los canales utilizados.
CE2.2 Definir las técnicas de cifrado para conectar de forma segura dos redes describiendo las funcionalidades y requisitos necesarios.
CE2.3 Definir las técnicas empleadas para conectar de forma segura dos equipos (túneles SSL y SSH), describiendo las funcionalidades y requisitos necesarios.
CE2.4 En un caso práctico, en el que se desea establecer una comunicación segura entre dos sistemas informáticos:

- Analizar los requisitos de seguridad de la arquitectura de comunicaciones propuesta.
- Indicar la solución más indicada, justificando la selección.
- Instalar los servicios de VPN e IPSec para conectar redes.
- Instalar los servicios de túneles SSL o SSH para conectar equipos distantes.

C3: Utilizar sistemas de certificados digitales en aquellas comunicaciones que requieran integridad y confidencialidad según especificaciones de seguridad.

cve: BOE-A-2011-10055

CE3.1 Identificar los atributos empleados en los certificados digitales para servidor, describiendo sus valores y función.
CE3.2 Describir los modos de utilización de los certificados digitales, asociándolos a las especificaciones de seguridad: confidencialidad, integridad y accesibilidad.
CE3.3 Describir la estructura de un sistema de sellado digital, indicando las funciones de los elementos que la integran.

C4: Diseñar e implantar servicios de certificación digital según necesidades de explotación y de seguridad informática.
CE4.1 Describir la estructura de la infraestructura de clave pública, indicando las funciones de los elementos que la integran.
CE4.2 Describir los servicios y obligaciones de la autoridad de certificación, relacionándolos con la política de certificado y la declaración de prácticas de certificación.
CE4.3 Identificar los atributos obligatorios y opcionales de un certificado digital, describiendo el uso habitual de dichos atributos.
CE4.4 Describir la estructura de una infraestructura de gestión de privilegios, indicando las funciones de los elementos que la integran.
CE4.5 Determinar los campos de los certificados de atributos, describiendo su uso habitual y la relación existente con los certificados digitales.
CE4.6 En un caso práctico, en el que se desea establecer un sistema de certificación para un sistema informático:
- Diseñar una infraestructura de clave pública, en función de las especificaciones.
- Justificar la jerarquía de autoridades de certificación diseñada.
- Emitir los certificados siguiendo los procedimientos indicados en la Declaración de Prácticas de Certificación.

Contenidos

1. Criptografía
- Perspectiva histórica y objetivos de la criptografía
- Teoría de la información
- Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
- Elementos fundamentales de la criptografía de clave privada y de clave publica
- Características y atributos de los certificados digitales
- Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
- Algoritmos criptográficos mas frecuentemente utilizados
- Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
- Elementos fundamentales de las funciones resumen y los criterios para su utilización
- Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica
- Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
- Criterios para la utilización de técnicas de cifrado de flujo y de bloque
- Protocolos de intercambio de claves
- Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

cve: BOE-A-2011-10055

2. Aplicación de una infraestructura de clave pública (PKI)

- Identificación de los componentes de una PKI y su modelo de relaciones
- Autoridad de certificación y sus elementos
- Política de certificado y declaración de practicas de certificación (CPS)
- Lista de certificados revocados (CRL)
- Funcionamiento de las solicitudes de firma de certificados (CSR)
- Infraestructura de gestión de privilegios (PMI)
- Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
- Aplicaciones que se apoyan en la existencia de una PKI

3. Comunicaciones seguras

- Definición, finalidad y funcionalidad de redes privadas virtuales
- Protocolo IPSec
- Protocolos SSL y SSH
- Sistemas SSL VPN
- Túneles cifrados
- Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0489_3	60	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO FORMATIVO 5

Denominación: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

CE1.1 Identificar los procesos del sistema y los parámetros que los caracterizan (procesos padre, estado del proceso, consumo de recursos, prioridades y

cve: BOE-A-2011-10055

usuarios afectados entre otros) para determinar su influencia en el rendimiento del sistema.

CE1.2 Describir cada una de las herramientas provistas por el sistema para la gestión de procesos con objeto de permitir la intervención en el rendimiento general del sistema.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema.

CE1.4 En un supuesto práctico en el que se cuenta con un sistema informático con una carga de procesos debidamente caracterizada:

- Utilizar las herramientas del sistema para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar las operaciones de activación, desactivación y modificación de prioridad entre otras con un proceso utilizando las herramientas del sistema.
- Monitorizar el rendimiento del sistema mediante herramientas específicas y definir alarmas, que indiquen situaciones de riesgo.

C2: Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

CE2.1 Identificar los distintos sistemas de archivo utilizables en un dispositivo de almacenamiento dado para optimizar los procesos de registro y acceso a los mismos.

CE2.2 Explicar las características de los sistemas de archivo en función de los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento en el sistema informático asociando los dispositivos con los distintos sistemas de archivos existentes.

CE2.4 En un supuesto práctico en el que se dispone de un sistema de almacenamiento de la información con varios dispositivos:

- Realizar el particionamiento, en los casos que sea necesario, y la generación de la infraestructura de los sistemas de archivo a instalar en cada dispositivo.
- Implementar la estructura general de almacenamiento integrando todos los dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado.

C3: Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

CE3.1 Identificar las posibilidades de acceso al sistema distinguiendo los accesos remotos de los accesos locales.

CE3.2 Describir las herramientas que se utilizan en la gestión de permisos a usuarios para el uso de los recursos del sistema.

CE3.3 En un supuesto práctico en el que se cuenta con derecho de administración de usuarios:

- Identificar los posibles accesos de un usuario al sistema.
- Modificar los permisos de utilización de un recurso del sistema a un usuario.
- Definir limitaciones de uso de un recurso del sistema a los usuarios.

C4: Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados.

CE4.1 Explicar los parámetros de configuración y funcionamiento de los dispositivos de comunicaciones para asegurar su funcionalidad dentro del sistema.

cve: BOE-A-2011-10055

CE4.2 Relacionar los servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos con objeto de analizar y evaluar el rendimiento.
CE4.3 En un supuesto práctico en el que tomamos un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:
- Identificar los dispositivos de comunicaciones y describir sus características.
- Verificar el estado de los servicios de comunicaciones.
- Evaluar el rendimiento de los servicios de comunicaciones.
- Detectar y documentar las incidencias producidas en el sistema.

Contenidos

1. **Gestión de la seguridad y normativas**
   - Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
   - Metodología ITIL Librería de infraestructuras de las tecnologías de la información
   - Ley orgánica de protección de datos de carácter personal.
   - Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

2. **Análisis de los procesos de sistemas**
   - Identificación de procesos de negocio soportados por sistemas de información
   - Características fundamentales de los procesos electrónicos
     - Estados de un proceso,
     - Manejo de señales, su administración y los cambios en las prioridades
   - Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
   - Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
   - Técnicas utilizadas para la gestión del consumo de recursos

3. **Demostración de sistemas de almacenamiento**
   - Tipos de dispositivos de almacenamiento más frecuentes
   - Características de los sistemas de archivo disponibles
   - Organización y estructura general de almacenamiento
   - Herramientas del sistema para gestión de dispositivos de almacenamiento

4. **Utilización de métricas e indicadores de monitorización de rendimiento de sistemas**
   - Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
   - Identificación de los objetos para los cuales es necesario obtener indicadores
   - Aspectos a definir para la selección y definición de indicadores
   - Establecimiento de los umbrales de rendimiento de los sistemas de información
   - Recolección y análisis de los datos aportados por los indicadores
   - Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

5. **Confección del proceso de monitorización de sistemas y comunicaciones**
   - Identificación de los dispositivos de comunicaciones
   - Análisis de los protocolos y servicios de comunicaciones

cve: BOE-A-2011-10055

- Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
- Procesos de monitorización y respuesta
- Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
- Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
- Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
- Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

6. Selección del sistema de registro de en función de los requerimientos de la organización

- Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
- Análisis de los requerimientos legales en referencia al registro
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
- Asignación de responsabilidades para la gestión del registro
- Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
- Guía para la selección del sistema de almacenamiento y custodia de registros

7. Administración del control de accesos adecuados de los sistemas de información

- Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
- Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
- Requerimientos legales en referencia al control de accesos y asignación de privilegios
- Perfiles de de acceso en relación con los roles funcionales del personal de la organización
- Herramientas de directorio activo y servidores LDAP en general
- Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
- Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0490_3	90	40

Criterios de acceso para los alumnos

Serán los establecidos en el artículo 4 del Real Decreto que regula el certificado de profesionalidad de la familia profesional al que acompaña este anexo.

cve: BOE-A-2011-10055

MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES DE SEGURIDAD INFORMÁTICA

Código: MP0175

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Proporcionar soporte técnico en materia de seguridad.

CE1.1. Proporcionar asistencia técnica en el diseño y configuración de soluciones de seguridad.

CE1.2. Dar soporte a otras áreas en las tareas de diseño y reingeniería de procesos para aportar la visión de seguridad.

CE1.3. Actuar como enlace entre las distintas áreas de la compañía para coordinar medidas de seguridad multidepartamentales.

CE1.4. Analizar las reglas específicas desarrolladas por las áreas técnicas específicas para las herramientas de seguridad corporativas.

CE1.5. Coordinar el uso de las herramientas de cifrado y la gestión de las claves

CE1.6. Dar soporte técnico a los comités de dirección que proceda.

CE1.7. Evaluar y mantenerse permanentemente informado de los errores, informes, noticias, boletines, etc. de seguridad recibidos y dar el primer nivel de soporte y distribución.

CE1.8. Desarrollar las políticas y procedimientos operativos en materia de seguridad de la información y dar soporte a las distintas áreas de la organización para su puesta en producción.

C2: Verificar la correcta aplicación de las medidas de seguridad.

CE2.1. Realizar las verificaciones necesarias para determinar el grado de vulnerabilidad de las distintas plataformas tecnológicas, así como el resto de revisiones periódicas de seguridad de los sistemas de información.

CE2.2. Mantener actualizado el análisis de riesgos de la organización

CE2.3. Coordinar las auditorías técnicas de seguridad.

C3: Participar en los procesos de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.

CE3.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.

CE3.2 Respetar los procedimientos y normas del centro de trabajo.

CE3.3 Emprender con diligencia las tareas según las instrucciones recibidas, tratando de que se adecuen al ritmo de trabajo de la empresa.

CE3.4 Integrarse en los procesos de producción del centro de trabajo.

CE3.5 Utilizar los canales de comunicación establecidos.

CE3.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. Revisión de la situación de la seguridad de la información

- Revisión de las normas internas de seguridad
- Revisión de la gestión de usuarios, privilegios y política de contraseñas
- Revisión de las copias de seguridad
- Revisión de las incidencias que se han producido

cve: BOE-A-2011-10055

- Revisión de la situación con respecto a la protección frente a código malicioso
- Revisión de la seguridad de las redes de datos
- Revisión de la seguridad de servidores y puestos de trabajo
- Revisión de la seguridad física, suministro eléctrico, climatización y protección de incendios según proceda

2. Configuración de reglas de relacionadas con la seguridad
- Configuración de la seguridad de el/los router
- Configuración de la seguridad de el/los switch
- Configuración de la seguridad de el/los cortafuegos
- Configuración de la seguridad de el/los sistema de detección de intrusos
- Configuración de la seguridad de el/los antivirus

3. Comunicación de los aspectos relacionados con la seguridad
- Establecimiento de canales para mantener a la organización actualizada en materia de seguridad
- Establecimiento de los canales internos para coordinar la seguridad entre los departamentos de la organización

4. Monitorización de la seguridad
- Monitorización de las comunicaciones
- Monitorización del rendimiento de sistemas

5. Aplicación de la normativa y metodología de seguridad
- Aplicación de códigos de buenas practicas de seguridad a la gestión diaria de los sistemas de información
- Integración de los requerimientos de seguridad en los procesos de negocio de la organización

6. Integración y comunicación en el centro de trabajo
- Comportamiento responsable en el centro de trabajo.
- Respeto a los procedimientos y normas del centro de trabajo.
- Interpretación y ejecución con diligencia las instrucciones recibidas.
- Reconocimiento del proceso productivo de la organización.
- Utilización de los canales de comunicación establecidos en el centro de trabajo.
- Adecuación al ritmo de trabajo de la empresa.
- Seguimiento de las normativas de prevención de riesgos, salud laboral y protección del medio ambiente.

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	*Experiencia profesional en el ámbito de la unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0486_3: Asegurar equipos informáticos	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	1 año	3 años

cve: BOE-A-2011-10055

Módulos Formativos	Acreditación requerida	*Experiencia profesional en el ámbito de la unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0487_3: Auditoría de seguridad informática	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	2 años	4 años
MF0488_3: Gestión de incidentes de seguridad informática	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	1 año	3 años
MF0489_3: Sistemas seguros de acceso y transmisión de datos	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	1 año	3 años
MF0490_3: Gestión de servicios en el sistema informático	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	2 años	4 años

* En los últimos tres años.

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTOS

Espacio Formativo	Superficie m^2 15 alumnos	Superficie m^2 25 alumnos
Aula de gestión	45	60

Espacio Formativo	M1	M2	M3	M4	M5
Aula de gestión	X	X	X	X	X

Espacio Formativo	Equipamiento
Aula de gestión	- Equipos audiovisuales - PCs instalados en red, cañón de proyección e internet - Software especifico de la especialidad - Pizarras para escribir con rotulador - Rotafolios - Material de aula - Mesa y sillas para formador - Mesas y sillas para alumnos

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

cve: BOE-A-2011-10055

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico-sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.

El número de unidades que se deben disponer de los utensilios, máquinas y herramientas que se especifican en el equipamiento de los espacios formativos, será el suficiente para un mínimo de 15 alumnos y deberá incrementarse, en su caso, para atender a número superior.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

ANEXO IV

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: IMPLANTACIÓN Y GESTIÓN DE ELEMENTOS INFORMÁTICOS EN SISTEMAS DOMÓTICOS/INMÓTICOS, DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Código: IFCT0409

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y Telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC365_3 Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia (RD 1701/2007, de 14 diciembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

UC0490_3: Gestionar servicios en el sistema informático
UC1219_3: Implantar y mantener sistemas domóticos-inmóticos
UC1220_3: Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia

Competencia general:

Integrar y mantener elementos informáticos y de comunicaciones en sistemas de automatización de edificios domóticos e inmóticos, de control de accesos y presencia y de videovigilancia a nivel de hardware y software, asegurando el funcionamiento de los distintos módulos que los componen, en condiciones de calidad y seguridad, cumpliendo la normativa y reglamentación vigentes.

cve: BOE-A-2011-10055