CUALIFICACIÓN PROFESIONAL:
Seguridad informática

Familia Profesional:	***Informática y Comunicaciones***
Nivel:	***3***
Código:	***IFC153_3***
Estado:	***BOE***
Publicación:	***Orden PRE/1636/2015***
Referencia Normativa:	***RD 616/2020, RD 1087/2005***

Competencia general

Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndolos 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.

Unidades de competencia

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

Entorno Profesional

Ámbito Profesional

Desarrolla su actividad profesional en el área de sistemas del departamento de informática dedicado a la seguridad informática, en entidades de naturaleza pública o privada, empresas de tamaño pequeño/mediano/grande o microempresas, tanto por cuenta propia como ajena, con independencia de su forma jurídica. Desarrolla su actividad dependiendo, en su caso, funcional y/o jerárquicamente de un superior. Puede tener personal a su cargo en ocasiones, por temporadas o de forma estable. En el desarrollo de la actividad profesional se aplican los principios de accesibilidad universal de acuerdo con la normativa aplicable.

Sectores Productivos

Se ubica principalmente en el sector servicios, en el subsector de los servicios de asistencia técnica informática, y en cualquier sector productivo que disponga de equipamiento informático en sus procesos de gestión.

Ocupaciones y puestos de trabajo relevantes

Los términos de la siguiente relación de ocupaciones y puestos de trabajo se utilizan con carácter genérico y omnicomprensivo de mujeres y hombres.

- Técnicos en seguridad informática
- Técnicos en auditoría informática

Formación Asociada (420 horas)

Módulos Formativos

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: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO (90 horas)

UNIDAD DE COMPETENCIA 1
ASEGURAR EQUIPOS INFORMÁTICOS

Nivel: *3*
Código: *UC0486_3*
Estado: *BOE*

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:
- Información referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones, entre otros.
- Referencias de posibilidades de utilización de los equipos y restricciones de los mismos.
- Protecciones contra agresiones de virus y otros elementos no deseados, entre otros.

CR1.2 Los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema se asignan (provisionan) por medio de las herramientas correspondientes según el Plan de Implantación y el de seguridad del sistema informático.

CR1.3 La confidencialidad e integridad de la conexión en el acceso a servidores se garantiza 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 se transmite a los usuarios, asegurándose de su correcta y completa comprensión.

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

CR1.7 Las informaciones afectadas por la normativa aplicable 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.

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

CR2.1 El servidor se ubica en la red en una zona protegida y aislada según las normas 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 aplicable 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 se configuran 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, de forma que permitan sacar conclusiones a posteriori.

CR2.5 La utilización de los módulos adicionales del servidor se decide en base a sus funcionalidades y riesgos de seguridad, 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 las normas de seguridad y el plan de explotación de la organización.

RP3: Instalar y configurar elementos de seguridad (cortafuegos, equipos trampa, Sistemas de Prevención de Intrusión o Firewalls, entre otros) 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 se selecciona en función del entorno de implantación.

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

CR3.3 Los cortafuegos se instalan y configuran 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 se verifican con juegos de pruebas, asegurando 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 se documentan según las especificaciones de la organización.

CR3.7 Los sistemas de registro se definen y configuran 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. IDS Sistemas de Detección de Intrusión (IDS), Sistemas de Prevención de Intrusión (IPS), equipos trampa ('Honeypots').

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. Operativa de seguridad elaborada. Servidores y equipos configurados en materia 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 aplicable, reglamentación y estándares. 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

Auditar redes de comunicación y sistemas informáticos

Nivel: *3*
Código: *UC0487_3*
Estado: *BOE*

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, adecuándolas al entorno a verificar según las especificaciones de seguridad de la organización y el sector al que pertenece la misma.

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, documentándolos conforme se indica en las normas 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 El análisis de vulnerabilidades se documenta, incluyendo referencias exactas a 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 las normativas, buenas prácticas y requisitos legales aplicables para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización.

CR2.1 La asignación de responsable de seguridad a todos los ficheros con datos de carácter personal se comprueba según la normativa aplicable.

CR2.2 El estado del listado de personas autorizadas a acceder a cada fichero se verifica, comprobando que está actualizado según la normativa aplicable.

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 audita, comprobando que se realiza siguiendo la normativa aplicable y las normas de la organización.

CR2.5 El acceso telemático a los ficheros se audita, comprobando que se realiza utilizando mecanismos que garanticen la confidencialidad e integridad cuando así lo requiera la normativa.

CR2.6 El informe de la auditoría se elabora, incluyendo la relación de ficheros con datos de carácter personal, las medidas de seguridad aplicadas y aquellas pendientes de aplicación (no conformidades) así como puntos fuertes y puntos de mejora.

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 y teniendo en cuenta la normativa aplicable nacional e internacional.

CR3.1 Los procedimientos de detección y gestión de incidentes de seguridad se desarrollan y se revisan, comprobando que están incluidos en la normativa de seguridad de la organización y que incluyen todo lo necesario para administrar de forma eficiente las posibles incidencias que pueden afectar a la organización.

CR3.2 Los puntos de acceso de entrada y salida de la red se testean comprobando que su uso se circunscribe a lo descrito en la normativa de seguridad de la organización.

CR3.3 La activación y actualización de los programas de seguridad y protección de sistemas se comprueba, viendo que corresponden a las especificaciones de los fabricantes.

CR3.4 Los puntos de entrada y salida de la red adicionales se validan, verificando que se autorizan y controlan en base a las especificaciones de seguridad y al plan de implantación de la organización.

CR3.5 Los procesos de auditoría informática se revisan, tanto los de carácter interno, como aquellos realizados por personal externo a la organización, comprobando que se encuentran activados, actualizados y con los parámetros especificados en las normas de la organización.

CR3.6 El cumplimiento de los procedimientos de las políticas de seguridad por parte de los usuarios se verifica de forma que se detecte su correcta aplicación y adecuación a las necesidades de la organización en materia de seguridad.

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. Herramientas de control de cumplimiento de metodologías de análisis de seguridad. Programa de auditorías.

Productos y resultados

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

Información utilizada o generada

Normativa aplicable sobre protección de datos personales. Política de seguridad de la empresa. Metodologías de análisis de seguridad. Boletines de seguridad y avisos de vulnerabilidades disponibles en formato electrónico. Topología del sistema informático a proteger.

UNIDAD DE COMPETENCIA 3

Detectar y responder ante incidentes de seguridad

Nivel: *3*
Código: *UC0488_3*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Implantar procedimientos para la respuesta ante incidentes y 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 se localizan, verificando que están documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la organización.

CR1.2 La modelización de los sistemas se realiza 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 y signos de comportamiento sospechoso.

CR1.3 La activación de los mecanismos de registro del sistema se verifica, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

CR1.4 La planificación de los mecanismos de análisis de registros se verifica, de forma que se garantice la detección de los comportamientos no habituales mediante un sistema de indicadores y métricas.

CR1.5 La instalación, configuración y actualización de los sistemas de detección de intrusos se verifica en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

CR1.6 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 se analizan 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 El funcionamiento de los dispositivos de protección física se verifica por medio de pruebas según las normas de la organización y/o normativa aplicable de seguridad.

CR2.5 Los sucesos y signos extraños que pudieran considerarse una alerta se recogen en el informe para su posterior análisis en función de la gravedad de los mismos y la política de la organización.

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 Los procedimientos recogidos en los protocolos de la normativa de seguridad de la organización se activan ante la detección de un incidente de seguridad.

CR3.2 La información para el análisis forense del sistema vulnerado se recoge una vez aislado el sistema según los procedimientos de las normas de seguridad de la organización y/o normativa aplicable.

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 se contiene mediante la aplicación de las medidas establecidas en las normas de seguridad de la organización y aquellas extraordinarias necesarias aunque no estén previamente planificadas.

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

CR3.6 Las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado se planifican a partir de la determinación de los daños causados, cumpliendo los criterios de calidad de servicio 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. Herramientas de análisis forense (creación de líneas de tiempo, recuperación de ficheros borrados, clonado de discos, entre otros).

Productos y resultados

Informes de análisis de vulnerabilidades. Relación de contraseñas débiles. Informe de auditoría de servicios y puntos de acceso al sistema informático. Registro de actividad. Documento de seguridad. Registro de alarmas. Planes de acción. Documento seguridad. Registro de alarmas. Registro de incidencias. Informe de auditoría. Informe de auditoría. Evaluación de impacto. Comunicación de incidentes de datos personales.

Información utilizada o generada

Normativa aplicable sobre protección de datos personales. Política de seguridad de la empresa. Metodologías de análisis de seguridad. 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. Normas internas de detección de intrusos y de prevención de amenazas de seguridad.

UNIDAD DE COMPETENCIA 4

Diseñar e implementar sistemas seguros de acceso y transmisión de datos

Nivel: *3*
Código: *UC0489_3*
Estado: *BOE*

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 se realizan haciendo uso de 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 aplicable 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 se evalúan y se seleccionan aquellas más idóneas, teniendo en cuenta el principio de proporcionalidad y las normas de seguridad de la organización.

CR1.4 Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones se implantan según parámetros de la normativa de seguridad de la organización.

CR1.5 La encapsulación, o encriptación extremo a extremo se activa para aquellos servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas para garantizar la seguridad de las comunicaciones.

CR1.6 Los servicios que incorporan soporte para certificados digitales para identificación del servidor, se emplean para garantizar al usuario la identidad del servidor.

CR1.7 Las políticas de seguridad y cifrado de información en operaciones de intercambio de datos implantadas se documentan en el formato establecido en la organización.

CR1.8 Los servicios que incorporan una autenticación de doble o triple factor, validación con certificados de usuario, DNI electrónico, "token", biométricos u otros dispositivos.

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 se implanta de forma que utilice la 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 utilización de certificados digitales para firmar y cifrar su contenido se asegura en la transmisión de mensajes de correo electrónico.

CR2.4 El perfil de firma digital de documentos estándar se emplea asegurando que es el más adecuado al uso que se va a realizar.

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 se firman digitalmente de forma que se pueda garantizar la integridad de dichos componentes.

CR2.7 Los sistemas de firma digital implantados se documentan en el formato establecido en la organización.

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 digital de la autoridad de certificación y su política asociada se ponen a disposición de 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.

CR3.8 Las infraestructuras de clave pública implantadas se documentan en el formato establecido en la organización.

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. Infraestructuras de Clave Pública (PKI) y dispositivos seguros de creación de firma (DNI electrónico, módulos PKCS y CSP).

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 instalación de infraestructuras de clave pública (PKI), Entidades de certificación (CA), DNI electrónico, certificados digitales, 'token'.

UNIDAD DE COMPETENCIA 5
GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: *3*
Código: *UC0490_3*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso, considerando despliegues en arquitecturas dedicadas o distribuidas, con y sin virtualización y cumpliendo las directivas de la organización.

CR1.1 Los procesos que intervienen en el sistema se identifican de forma que permitan evaluar parámetros de rendimiento, diferenciando los procesos que se encuentran repartidos en diferentes nodos, (si la arquitectura es distribuida) y/o si están asociados al software de gestión de la virtualización, al hipervisor de los host físicos o a los propios servicios virtualizados (si se trata de un modelo virtualizado).

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

CR1.3 Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización (tipo de proceso, usuario, perfil, entre otros).

CR1.4 Las herramientas de monitorización se implantan, configurándolas y determinando los niveles de las alarmas.

CR1.5 La conectividad y el ancho de banda que se necesita en arquitecturas distribuidas, se proporcionan según las especificaciones y/o manuales de fabricantes y de la organización.

CR1.6 La distribución de la información en arquitecturas distribuidas se gestiona, siguiendo las especificaciones y/o manuales de fabricantes y de la organización, para maximizar el rendimiento del sistema.

CR1.7 El software de gestión de virtualización y el hipervisor, de los hosts físicos y los propios servicios virtualizados, en el caso de despliegues virtualizados, se gestiona, revisando la configuración y monitorizando el rendimiento, siguiendo las especificaciones y/o manuales de fabricantes y de la organización, y maximizando el rendimiento del sistema.

RP2: Administrar el almacenamiento según las necesidades de uso, considerando despliegues en arquitecturas dedicadas o distribuidas, con y sin virtualización y cumpliendo las directivas de la organización.

CR2.1 Los dispositivos de almacenamiento se configuran para ser usados, asignando los parámetros propios del sistema operativo utilizado en el sistema informático.

CR2.2 El almacenamiento se configura, teniendo en cuenta la posible necesidad de arquitecturas distribuidas que requieran distribución de la información, así como la necesidad de entornos virtualizados que requieren software de gestión de virtualización, hipervisores y los propios servicios virtualizados.

CR2.3 La estructura de almacenamiento se define, implantándose, atendiendo a las necesidades de los sistemas de archivos y a las especificaciones de uso de la organización.

CR2.4 Los requerimientos de nomenclatura de objetos y restricciones de uso del almacenamiento se documentan, siguiendo el formato (tipo de documento, tamaño, maquetación, tipografía, entre otros) y otras indicaciones establecidas por la organización.

CR2.5 El almacenamiento se integra para ofrecer un sistema funcional al usuario, siguiendo las especificaciones de la organización, con independencia del tipo de arquitectura (distribuida o dedicada) y de la existencia o no de capa de virtualización.

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, asignando métodos de autenticación y perfiles, entre otros, para garantizar la seguridad e integridad del sistema.

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 (dispositivos, espacio, número de conexiones, caudal/ancho de banda, entre otros) para los usuarios se limitan, usando las herramientas instaladas en el sistema, 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 servicios de comunicación se establecen con un sistema de calidad de servicio, garantizándose las comunicaciones de los mismos.

CR4.2 Los dispositivos de comunicaciones se verifican en lo que respecta a su configuración y rendimiento, siguiendo las especificaciones de la organización.

CR4.3 Los consumos de recursos de los servicios de comunicaciones se analizan, verificando que se encuentran dentro de los límites permitidos por las especificaciones.

CR4.4 Las incidencias detectadas en los servicios de comunicaciones se documentan para informar a los responsables de la explotación del sistema y de la gestión de las mismas según los protocolos de la organización indicando, entre otros, el momento, la descripción y la solución aplicadas al problema.

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

Dispositivos de almacenamiento configurados y estructurados. Sistema configurado y operando. Rendimiento del sistema según los parámetros de explotación. Usuarios gestionados. Sistema seguro e íntegro en el acceso y utilización de servicios y recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de protección de datos y publicación de la información). Normas internas de trabajo (plan de explotación de la organización; gráficas y análisis de rendimiento; listados de acceso y restricciones de usuarios; informe de incidencias; protocolo de actuación ante incidencias). Documentaciones técnicas (manuales de explotación del sistema operativo y de los dispositivos; manuales de las herramientas de monitorización utilizadas).

MÓDULO FORMATIVO 1
SEGURIDAD EN EQUIPOS INFORMÁTICOS

Nivel: *3*
Código: *MF0486_3*
Asociado a la UC: *UC0486_3 - ASEGURAR EQUIPOS INFORMÁTICOS*
Duración (horas): *90*
Estado: *BOE*

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 de análisis de un plan de implantación de seguridad 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 implementación de mecanismos de acceso físico y lógico en la implantación de un servidor según unas 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 evaluación de la función y necesidad de servicios en ejecución, a partir de un servidor en implantación 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.
- 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 En 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.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.4; C2 respecto a CE2.4; C3 respecto a CE3.4; C4 respecto a CE4.4.

Otras Capacidades:

Mantener el área de trabajo con el grado apropiado de orden y limpieza.
Demostrar creatividad en el desarrollo del trabajo que realiza.
Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.
Interpretar y ejecutar instrucciones de trabajo.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.

Contenidos

1 Gestión de la seguridad y riesgos

Seguridad: objetivo de la seguridad; amenazas; atacante externo e interno; tipos de ataque; mecanismos de protección.
Riesgos: proceso de gestión de riesgos; métodos de identificación y análisis de riesgos; reducción del riesgo.

2 Seguridad Física

Protección del sistema informático.
Protección de los datos.

3 Seguridad lógica del sistema

Sistemas de ficheros.
Permisos de archivos.
Listas de control de acceso (ACLs) a ficheros.
Registros de actividad del sistema.
Autenticación de usuarios: sistemas de autenticación débiles; sistemas de autenticación fuertes; sistemas de autenticación biométricos.
Introducción a la Criptografía y Establecimiento de Políticas de Contraseñas.

4 Acceso remoto al sistema

Mecanismos del sistema operativo para control de accesos.
Cortafuegos de servidor: filtrado de paquetes; cortafuegos de nivel de aplicación; registros de actividad del cortafuegos.

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con el aseguramiento de equipos informáticos, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 2

Auditoría de seguridad informática

Nivel: *3*
Código: *MF0487_3*
Asociado a la UC: *UC0487_3 - Auditar redes de comunicación y sistemas informáticos*
Duración (horas): *90*
Estado: *BOE*

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 los diferencias entre vulnerabilidades y amenazas.

CE1.2 Enunciar las características de los 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.

CE1.4 Seleccionar la herramienta de auditoría de seguridad más adecuada en función del servidor o red y los requisitos de seguridad.

CE1.5 En un supuesto práctico, de análisis de vulnerabilidades a partir de un sistema informático en unas 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 aplicable.

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 aplicable asociándolos a los requisitos exigidos.

CE2.4 En un supuesto práctico, de verificación del cumplimiento de la normativa 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 auditoria de cumplimiento de normativa 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.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.5; C2 respecto a CE2.4.

Otras Capacidades:

Demostrar un buen hacer profesional.
Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Mantener una actitud asertiva, empática y conciliadora con los demás demostrando cordialidad y amabilidad en el trato.
Adaptarse a situaciones o contextos nuevos.
Respetar los procedimientos y normas internas de la organización.

Contenidos

1 Vulnerabilidades

Fallos de programa.
Programas maliciosos.
Programación segura.

2 Análisis de vulnerabilidades

Análisis local.
Análisis remoto: análisis de caja blanca; análisis de caja negra.
Optimización del proceso de auditoría.
Contraste de vulnerabilidades e informe de auditoría.

3 Normativa aplicable

Normativa europea.
Normativa nacional: Código penal; normativa de protección de datos. Normativa para el Tratamiento Automatizado de Datos.
Trámites para la aplicación de la normativa de protección de datos en la empresa.

4 Cortafuegos de red

Componentes de un cortafuegos de red.
Tipos de cortafuegos de red: filtrado de paquetes; cortafuegos de red de aplicación.

Arquitecturas de cortafuegos de red: cortafuegos de red con dos interfaces; zona desmilitarizada. Otras arquitecturas de cortafuegos de red.

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la auditoría de redes de comunicación y sistemas informáticos, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 3

Gestión de incidentes de seguridad informática

Nivel: 3
Código: MF0488_3
Asociado a la UC: UC0488_3 - Detectar y responder ante incidentes de seguridad
Duración (horas): 90
Estado: BOE

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 debidamente caracterizado de instalación de alarmas 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 varios supuestos prácticos de implantación de sistemas de detección 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 En un supuesto práctico, de aplicación de procedimientos de análisis, 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, de coordinación de respuesta ante 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.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.6 y CE1.7; C2 respecto a CE2.4; C3 respecto a CE3.5.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Tratar al cliente con cortesía, respeto y discreción.
Proponerse objetivos retadores que supongan un nivel de rendimiento y eficacia superior al alcanzado previamente.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
Interpretar y ejecutar instrucciones de trabajo.
Actuar con rapidez en situaciones problemáticas y no limitarse a esperar.
Demostrar flexibilidad para entender los cambios.

Contenidos

1 Gestión de incidentes de seguridad

Justificación de la necesidad de gestionar incidentes de seguridad.

Identificación y caracterización de los datos de funcionamiento del sistema.
Sistemas de detección de intrusos: sistemas basados en equipo (HIDS); sistemas basados en red (NIDS); sistemas de prevención de intrusiones (IPS); señuelos.

2 Respuesta ante incidentes de seguridad

Recolección de información.
Análisis y correlación de eventos.
Verificación de la intrusión.
Organismos de gestión de incidentes: nacionales (IRIS-CERT, esCERT); Internacionales (CERT, FIRST).

3 Análisis forense informático

Objetivos del análisis forense.
Principio de Lockard.
Recogida de evidencias.
Principio de indeterminación: evidencias volátiles; evidencias no volátiles; etiquetado de evidencias; cadena de custodia.
Análisis de evidencias: ficheros y directorios ocultos; información oculta en el sistema de ficheros, Slack-space; recuperación de ficheros borrados; herramientas de análisis forense.
Análisis de programas maliciosos: desensambladores; entornos de ejecución controlada.

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la detección y respuesta ante incidentes de seguridad, en lengua propia y extranjera, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 4

Sistemas seguros de acceso y transmisión de datos

Nivel:	*3*
Código:	*MF0489_3*
Asociado a la UC:	*UC0489_3 - Diseñar e implementar sistemas seguros de acceso y transmisión de datos*
Duración (horas):	*60*
Estado:	*BOE*

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 supuesto 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.

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 supuesto práctico, de establecimiento de 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.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C2 respecto a CE2.4; C4 respecto a CE4.6.

Otras Capacidades:

Demostrar interés por el conocimiento amplio de la organización y sus procesos.
Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
Adaptarse a la organización, a sus cambios organizativos y tecnológicos así como a situaciones o contextos nuevos.
Demostrar flexibilidad para entender los cambios.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
Habituarse al ritmo de trabajo de la organización.

Contenidos

1 Criptografía

Seguridad de la información y criptografía.
Conceptos básicos.
Cifrado de clave simétrica.
Firma digital.
Cifrado de clave pública.
Funciones resumen.
Cifrado de flujo y de bloque.
Protocolos de intercambio de clave.

2 Comunicaciones Seguras

Redes privadas virtuales.

IP Security Protocol.
Túneles cifrados.

3 Autoridades de Certificación

Infraestructura de clave pública (PKI).
Política de certificado y declaración de prácticas de certificación.
Jerarquías de autoridades de certificación.
Infraestructuras de gestión de privilegios (PMI).

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con el diseño e implementación de sistemas seguros de acceso y transmisión de datos, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 5

GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel:	*3*
Código:	*MF0490_3*
Asociado a la UC:	*UC0490_3 - GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO*
Duración (horas):	*90*
Estado:	*BOE*

Capacidades y criterios de evaluación

C1: Analizar procesos del sistema, asegurando un rendimiento acorde a los parámetros especificados en el plan de explotación considerando despliegues en arquitecturas dedicadas o distribuidas, con y sin capa de virtualización.

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

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema, indicando qué parámetros se miden y qué funciones se controlan.

CE1.4 En un supuesto práctico de análisis del rendimiento de un sistema informático con una carga de procesos concreta:

- Utilizar herramientas del sistema, monitorizando sus parámetros para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar 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 del almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, confidencial y disponible.

CE2.1 Identificar 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 un sistema de archivo, en función de la arquitectura hardware (dedicada o distribuida), los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento asociando, para cada nodo o sistema informático final, los dispositivos con los sistemas de archivos existentes.

CE2.4 Describir la distribución del almacenamiento en nodos, dispositivos y sistemas de archivo, comprobando que se garantice la funcionalidad y el rendimiento del conjunto.

CE2.5 En un supuesto práctico de aplicación de procedimientos de administración de almacenamiento de la información con varios dispositivos:

- Particionar los dispositivos, en los casos que se requiera distribuir la información de manera separada, generando la infraestructura de los sistemas de archivo a instalar.
- Distribuir la información en diferentes nodos, integrándolos en un sistema de almacenamiento común, garantizando las comunicaciones y el rendimiento cuando la distribución del almacenamiento sea un requisito de implementación.
- Implementar la estructura general de almacenamiento, integrando todos los nodos, dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado, indicando la restricción o el requerimiento y el tipo de dispositivo afectado.
- Aplicar los puntos anteriores sobre sistemas virtualizados.

C3: Administrar accesos al sistema y a los recursos para asegurarlos, restringiendo su uso en función del perfil de acceso.

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

CE3.2 Describir 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 de administración del acceso al sistema en el que se cuenta con derecho de administración de usuarios:
- Identificar los posibles accesos de un usuario al sistema, monitorizando mediante visionado de log o usando herramienta software.
- Modificar los permisos de utilización de un recurso del sistema a un usuario, estableciendo otros que se hayan solicitado.
- Definir limitaciones de uso de un recurso del sistema a los usuarios, verificando dicha limitación simulando el acceso.

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

CE4.1 Explicar parámetros de configuración y funcionamiento de los dispositivos de comunicaciones, indicando los servicios afectados por cada uno para asegurar su funcionalidad dentro del sistema.

CE4.2 Relacionar servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos, analizando y evaluando el rendimiento.

CE4.3 En un supuesto práctico de evaluación de uso y rendimiento de un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:
- Identificar los dispositivos de comunicaciones, describiendo sus características.
- Verificar el estado de los servicios de comunicaciones, comprobando su funcionalidad.
- Evaluar el rendimiento de los servicios de comunicaciones, midiendo los parámetros de conectividad y caudal.
- Detectar las incidencias producidas en el sistema, documentando las que se produzcan.

Capacidades cuya adquisición debe ser completada en un entorno real de trabajo

C1 respecto a CE1.4; C2 respecto a CE2.5; C3 respecto a CE3.3; C4 respecto a CE4.3.

Otras Capacidades:

Mantener el área de trabajo con el grado apropiado de orden y limpieza.
Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.

Demostrar creatividad en el desarrollo del trabajo que realiza.
Interpretar y ejecutar instrucciones de trabajo.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
Valorar el talento y el rendimiento profesional con independencia del sexo.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Cumplir las medidas que favorezcan el principio de igualdad de trato y de oportunidades entre hombres y mujeres.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Procesos en el sistema informático

Estados de un proceso.
Manejo de señales entre procesos.
Administración de procesos.
Cambio de prioridades.
Monitorización de procesos.
Gestión del consumo de recursos.

2 Almacenamiento de información en la gestión de servicios

Dispositivos de almacenamiento.
Sistemas de archivo.
Estructura general de almacenamiento.
Herramientas del sistema para gestión del almacenamiento.

3 Gestión de usuarios en la gestión de servicios

Acceso al sistema.
Permisos y acceso a los recursos.
Limitaciones de uso de recursos.

4 Servicios de comunicaciones en la gestión de servicios

Dispositivos de comunicaciones.
Protocolos de comunicaciones.
Servicios de comunicaciones.
Rendimientos de los servicios de comunicaciones.

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la gestión de servicios en el sistema informático, que se acreditará mediante una de las dos formas siguientes:

- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), Ingeniero Técnico, Diplomado o de otras de superior nivel relacionadas con el campo profesional.
- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.

2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.