

CUALIFICACIÓN PROFESIONAL: Gestión de sistemas informáticos

<i>Familia Profesional:</i>	Informática y Comunicaciones
<i>Nivel:</i>	3
<i>Código:</i>	IFC152_3
<i>Estado:</i>	BOE
<i>Publicación:</i>	Orden PRE/1636/2015
<i>Referencia Normativa:</i>	RD 1087/2005

Competencia general

Configurar, administrar y mantener un sistema informático a nivel de hardware y software, garantizando la disponibilidad, óptimo rendimiento, funcionalidad e integridad de los servicios y recursos del sistema.

Unidades de competencia

- UC0484_3:** Administrar los dispositivos hardware del sistema
- UC0485_3:** Instalar, configurar y administrar el software de base y de aplicación del sistema
- UC0486_3:** Asegurar equipos informáticos

Entorno Profesional

Ámbito Profesional

Desarrolla su actividad profesional en el departamento de informática dedicado al área sistemas y telemática, en entidades de naturaleza pública o privada, empresas de cualquier tamaño, por cuenta propia o 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 en el sector servicios en los subsectores de la comercialización de equipos informáticos y la asistencia técnica informática, así como en cualquier sector productivo que utilice sistemas informáticos para su 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 omnicomprendivo de mujeres y hombres.

- Administradores de sistemas
- Responsables de informática
- Administradores de sistemas de redes
- Técnicos de sistemas

Formación Asociada (420 horas)

Módulos Formativos

- MF0484_3:** Administración hardware de un sistema informático (120 horas)
- MF0485_3:** Administración software de un sistema informático (210 horas)
- MF0486_3:** Seguridad en equipos informáticos (90 horas)

UNIDAD DE COMPETENCIA 1

Administrar los dispositivos hardware del sistema

Nivel: 3
Código: UC0484_3
Estado: BOE

Realizaciones profesionales y criterios de realización

RP1: Inventariar los componentes físicos del sistema, manteniéndolos actualizados para asegurar su localización y disponibilidad según las normas de la organización.

CR1.1 El hardware y los componentes físicos del sistema se identifican correctamente y enumeran exhaustivamente para conocer su disponibilidad actual.

CR1.2 El inventario hardware se describe detalladamente para informar de las características, configuración actual, situación exacta y estado de cada dispositivo según las normas de la organización.

CR1.3 Las nuevas adquisiciones, cambios producidos en el hardware o en su configuración se modifican en el inventario para mantenerlo actualizado interpretando la documentación técnica.

CR1.4 La instalación del hardware se detalla incluyendo las incidencias y se referencia en la documentación generada para su uso posterior.

RP2: Analizar y parametrizar los dispositivos hardware, monitorizando y evaluando su rendimiento para optimizar el funcionamiento del sistema y proponer, en su caso, modificaciones o mejoras según las necesidades funcionales existentes.

CR2.1 Las técnicas o herramientas de monitorización a utilizar se seleccionan en función de las características del sistema para optimizar su funcionamiento.

CR2.2 El sistema se monitoriza, de forma que se puedan obtener las estadísticas de rendimiento, programaciones de alertas y otros elementos, utilizando las técnicas o herramientas de monitorización seleccionadas.

CR2.3 Los criterios de rendimiento del sistema se establecen según las disposiciones generales establecidas por el fabricante, y los particulares establecidos por la organización para obtener una monitorización adecuada.

CR2.4 Los datos obtenidos de la monitorización se recogen y presentan de forma clara y concisa mediante la utilización de técnicas de representación.

CR2.5 La representación del rendimiento del sistema generada por la monitorización, se analiza para localizar posibles pérdidas o degradaciones de rendimiento y proponer las modificaciones necesarias.

CR2.6 Los parámetros de los dispositivos físicos se ajustan de forma que el rendimiento mejore y las anomalías de funcionamiento detectadas en el sistema se corrijan.

RP3: Implementar y optimizar soluciones hardware de alta disponibilidad para garantizar y asegurar la protección y recuperación del sistema ante situaciones imprevistas según el plan de contingencias previsto.

CR3.1 Las incidencias de instalación y configuración del hardware se resuelven consultando la documentación técnica y los servicios de asistencia técnica.

CR3.2 La verificación de la instalación y configuración de los dispositivos físicos y sus controladores para el almacenamiento masivo y copias de seguridad, se realiza de modo que se pueda comprobar según los estándares y las normas de calidad y seguridad establecidas por la organización.

CR3.3 La gestión de la reparación o sustitución de los componentes hardware averiados se efectúa de acuerdo con las especificaciones técnicas del sistema y siguiendo el procedimiento de instalación establecido en la documentación técnica facilitada por el fabricante y los planes de implantación de la organización.

CR3.4 Las verificaciones de los componentes sustituidos se realizan para asegurar su correcto funcionamiento según los estándares y las normas de calidad y seguridad establecidas por la organización.

CR3.5 Los problemas o desajustes se resuelven garantizando la integridad de la información y la continuidad en el funcionamiento del sistema, tomando las medidas preventivas de seguridad necesarias, activando los posibles procedimientos de explotación alternativos y cumpliendo la normativa aplicable.

CR3.6 La información original y copias de seguridad se restauran para que el sistema vuelva a entrar en explotación siguiendo el protocolo de seguridad establecido y cumpliendo la normativa aplicable de protección de datos.

CR3.7 El almacenamiento de las copias se supervisa, comprobando que se cumplen los estándares de seguridad establecidos por la organización y la normativa aplicable en materia de protección de datos.

CR3.8 Los servidores redundantes y otros sistemas de alta disponibilidad se implementan según especificaciones del fabricante y normas de la organización.

RP4: Planificar las ampliaciones y crecimiento del sistema proponiendo nuevas configuraciones para asumir incrementos futuros en la carga de trabajo o usuarios según las necesidades de explotación.

CR4.1 El hardware se analiza y valora para realizar informes de posibles necesidades futuras, así como la viabilidad de posibles mejoras y actualizaciones.

CR4.2 Los informes de la organización acerca de futuros incrementos en la carga de trabajo o número de usuarios se analizan adecuadamente utilizando técnicas ajustadas a la situación.

CR4.3 El sistema se representa mediante herramientas matemáticas y de modelado analítico para analizar el rendimiento con las nuevas cargas añadidas.

CR4.4 Los datos obtenidos a través del modelado y simulación del sistema se analizan para determinar si las nuevas cargas son asumibles.

CR4.5 Los dispositivos físicos disponibles en el mercado se evalúan para proponer los más adecuados al sistema y que garanticen la absorción de la carga de trabajo planteada.

CR4.6 La implantación de nuevos dispositivos se desarrolla minimizando sus efectos sobre la explotación del sistema, optimizando los rendimientos del mismo y adecuando la tecnología según la evolución del mercado.

CR4.7 Las ampliaciones y cambios de configuración del sistema se detallan y referencian en la documentación generada y se guardan para su uso posterior según el procedimiento establecido.

RP5: Definir las condiciones ambientales y de seguridad apropiadas para evitar interrupciones en la prestación de servicios del sistema según especificaciones del fabricante y el plan de seguridad de la organización.

CR5.1 Los requerimientos ambientales de los dispositivos físicos se establecen según las especificaciones técnicas y el plan de seguridad de la organización.

CR5.2 Las condiciones de alimentación eléctrica de los dispositivos físicos se establecen según las especificaciones técnicas y el plan de seguridad de la organización.

CR5.3 Los requerimientos ambientales y condiciones de alimentación eléctrica de los dispositivos físicos se contrastan con las posibilidades de la instalación para evitar incidencias e interrupciones en el servicio.

CR5.4 Las condiciones de ergonomía, seguridad y aprovechamiento del espacio disponible se establecen para la correcta ubicación de los equipos y dispositivos físicos de acuerdo con las especificaciones técnicas.

CR5.5 Las condiciones de seguridad se establecen para evitar accesos indeseados e interrupciones en el servicio de acuerdo con el plan de seguridad de la organización.

CR5.6 Las condiciones ambientales y de seguridad se detallan y referencian en la documentación generada y se guardan para su uso posterior, según el procedimiento establecido.

Contexto profesional

Medios de producción

Equipos informáticos y periféricos. Sistemas operativos y parámetros de configuración. Herramientas software para control inventarios. Herramientas software de diagnóstico. Dispositivos físicos para almacenamiento masivo y copias de seguridad (como RAID, SAN y NAS). Soportes para copias de seguridad. Herramientas de gestión de archivos de registro (log). Software de diagnóstico, seguridad y restauración. Documentación técnica. Herramientas de 'backup'. Herramientas de gestión de cambios, incidencias y configuración. Monitores de rendimiento. Sistemas de alimentación ininterrumpidas. Herramientas de modelado analítico. Herramientas de análisis del rendimiento del sistema. Dispositivos móviles. 'Hosting'.

Productos y resultados

Inventario y registro descriptivo de los dispositivos físicos del sistema y de su configuración. Sistema informático en funcionamiento con un rendimiento óptimo y una utilización adecuada de sus recursos. Conexión adecuada del sistema a una red dentro de una organización. Informes de ampliaciones y crecimiento del sistema.

Información utilizada o generada

Inventario de hardware. Especificaciones técnicas para la instalación de los dispositivos. Información técnica de los equipos. Documentación o manuales de uso y funcionamiento del sistema. Documentación sobre la configuración normas de seguridad para la instalación. Recomendaciones de mantenimiento de los fabricantes. Plan de mantenimiento. Relación de incidencias. Recomendaciones de mantenimiento de los fabricantes y soportes técnicos de asistencia. Catálogos de productos hardware, proveedores, precios, normativa empresarial sobre confidencialidad de datos. Normativas de seguridad e higiene. Normativa aplicable sobre protección de datos y normas internas del trabajo sobre confidencialidad de datos y seguridad e higiene.

UNIDAD DE COMPETENCIA 2

Instalar, configurar y administrar el software de base y de aplicación del sistema

Nivel: 3
Código: UC0485_3
Estado: BOE

Realizaciones profesionales y criterios de realización

RP1: Instalar y configurar el sistema operativo de servidor para asegurar la funcionalidad del sistema según las necesidades de la organización.

CR1.1 El sistema operativo del servidor se instala siguiendo los procedimientos y lo indicado en la documentación técnica.

CR1.2 La verificación de los componentes del sistema operativo y controladores de dispositivos se realiza mediante pruebas de arranque y parada, y la utilización de herramientas software de verificación y diagnóstico, de modo que se pueda comprobar que los componentes son reconocidos y habilitados y no aparecen conflictos según lo dispuesto por la organización.

CR1.3 Los parámetros del sistema operativo se configuran para garantizar la integridad y fiabilidad del sistema según el plan de seguridad de la organización.

CR1.4 La configuración de los parámetros de red se establece para conectar el servidor según el diseño de red del sistema y los estándares y normas de seguridad y calidad de la organización.

CR1.5 Los diferentes grupos y usuarios se crean para permitir la utilización del sistema según las necesidades de la organización y el plan de seguridad del sistema.

CR1.6 Las actualizaciones necesarias del sistema operativo del servidor se llevan a cabo con eficacia, asegurando la integridad del sistema, la idoneidad de las mismas y siguiendo las normas de seguridad de la organización.

CR1.7 Los detalles relevantes de la instalación, así como las incidencias durante el proceso, se reflejan en la documentación, según el procedimiento establecido por la organización.

RP2: Inventariar el software del sistema, actualizando el inventario para garantizar su localización y disponibilidad según las normas de la organización.

CR2.1 El software y sus versiones se enumeran de forma exhaustiva para mantener un inventario de las aplicaciones y sistemas operativos disponibles en el sistema.

CR2.2 La configuración actual del software de base y aplicación se registra de forma clara y completa para facilitar las labores de recuperación en caso de fallos.

CR2.3 La información del software instalado se enumera en relación con cada usuario para permitir el control de instalaciones de aplicaciones no permitidas.

CR2.4 El número de instalaciones, su situación e identificación se controlan por cada producto software para llevar a cabo un control exhaustivo de licencias cumpliendo la normativa aplicable sobre propiedad intelectual.

CR2.5 Los privilegios de acceso de los usuarios del sistema a recursos software, se registran para el control de acceso, según el plan de seguridad del sistema y las leyes de datos vigentes.

CR2.6 Las aplicaciones de inventariado automático se utilizan para mantener actualizada la información acerca del software del sistema, según las normas de la organización.

RP3: Instalar y configurar aplicaciones corporativas para atender funcionalidades de usuarios según el plan de implantación de la organización.

CR3.1 La instalación del software corporativo se lleva a cabo con eficacia asegurando la integridad del sistema, cumpliendo los requisitos establecidos por la organización y siguiendo lo indicado en la documentación técnica.

CR3.2 La verificación del funcionamiento del software en el conjunto del sistema se realiza según los procedimientos de seguridad y calidad establecidos por la organización y el propio fabricante.

CR3.3 El software corporativo se configura con parámetros adecuados según el plan de seguridad del sistema y las necesidades de la organización.

CR3.4 Las actualizaciones necesarias del software corporativo se llevan a cabo con eficacia, asegurando la integridad del sistema, la idoneidad de las mismas y siguiendo las normas de seguridad de la organización.

CR3.5 Los detalles relevantes de la instalación, así como las incidencias durante el proceso, se reflejan en la documentación, según el procedimiento establecido por la organización.

RP4: Elaborar el plan de soporte a los usuarios, coordinando al personal técnico de apoyo y mantenimiento para asegurar el uso de las funciones del sistema informático.

CR4.1 Las pautas para la instalación, configuración y mantenimiento de software de base y de aplicación en puestos de usuario se documentan de forma exhaustiva.

CR4.2 La resolución de problemas comunes referidos a dispositivos hardware y de red en puestos de usuario se documentan de forma exhaustiva.

CR4.3 La asistencia al usuario se planifica aplicando las técnicas de comunicación, los protocolos de actuación establecidos por la organización y siguiendo las políticas de seguridad y protección de datos vigentes y calidad del servicio.

CR4.4 El entrenamiento de los usuarios en las diferentes herramientas y equipos a manejar se planifica para ser realizado de forma asistida y gradual, asegurando su completa adaptación al entorno.

CR4.5 Los procedimientos de asistencia se organizan para asegurar su máxima disponibilidad al requerimiento de asesoramiento y atención por parte de los usuarios.

RP5: Configurar y administrar los recursos del sistema para optimizar el rendimiento según los parámetros de explotación de las aplicaciones.

CR5.1 Las métricas de rendimiento a utilizar se establecen para especificar los atributos de rendimiento a considerar.

CR5.2 Las técnicas de análisis del rendimiento a utilizar se establecen para la obtención de parámetros de funcionamiento del sistema.

CR5.3 Los programas de comprobación a utilizar se establecen para obtener parámetros del rendimiento del sistema, según las especificaciones del fabricante, y los requisitos establecidos por la organización para obtener un rendimiento adecuado.

CR5.4 Los modelos que representan al sistema se realizan para obtener parámetros del rendimiento del mismo según las especificaciones del fabricante, y los requisitos establecidos por la organización para obtener un rendimiento adecuado.

CR5.5 Los sistemas de simulación del sistema se configuran para obtener parámetros del rendimiento del mismo, según las especificaciones del fabricante, y los requisitos establecidos por la organización para obtener un rendimiento adecuado.

CR5.6 Los parámetros de rendimiento del sistema obtenidos se analizan para localizar posibles conflictos y determinar los dispositivos hardware susceptibles de ser reconfigurados, eliminados o añadidos.

RP6: Planificar la realización de copias de seguridad así como la recuperación de las mismas para mantener niveles adecuados de seguridad en los datos según las necesidades de uso y dentro de las directivas de la organización.

CR6.1 La arquitectura del sistema de copias de respaldo se diseña teniendo en cuenta los requisitos del sistema informático.

CR6.2 Los procedimientos de realización de copias de respaldo y los niveles de dichas copias se planifican en función de las necesidades del servidor, de los tiempos de realización de las copias, de los tiempos de recuperación, de los espacios de almacenamiento requeridos y de la validez del histórico de copias.

CR6.3 Las pruebas de verificación de las copias de respaldo se realizan y se verifica su funcionalidad atendiendo a las especificaciones de calidad de la organización y de la normativa aplicable de protección de datos.

CR6.4 La planificación del sistema de identificación y almacenamiento de los soportes se realiza en función de las especificaciones del plan de seguridad de la organización y de la normativa aplicable de protección de datos.

CR6.5 La documentación de los procedimientos de obtención y verificación de copias de respaldo así como la de los planes de contingencias y resolución de incidencias se confecciona según las normativas de la organización y de la normativa aplicable de protección de datos.

RP7: Auditar la utilización de recursos del sistema para asegurar un rendimiento óptimo según los parámetros del plan de explotación.

CR7.1 El plan de auditoría con las pruebas funcionales necesarias y periodos de realización se implementa, de forma que garanticen el óptimo rendimiento del sistema.

CR7.2 La comprobación de incidencias se realiza para verificar, precisar y minimizar efectos negativos sobre el sistema, según las necesidades de la organización y el plan de seguridad del sistema.

CR7.3 El diagnóstico y localización de funcionamientos indeseados se realiza utilizando los equipos y las herramientas necesarias, y se aplica el correspondiente procedimiento correctivo en un tiempo adecuado.

CR7.4 El informe de auditoría se realiza en el formato normalizado que permita recoger la información requerida para la actuación del repositorio de incidencias.

Contexto profesional

Medios de producción

Equipos informáticos y periféricos. Software del sistema operativo de servidor. Software de aplicación corporativo. Actualizaciones y parches de software de base y aplicación. Controladores de dispositivos. Herramientas de seguridad y antivirus. Monitores de rendimiento. Herramientas de modelado y simulación de sistemas. Herramientas de inventariado automático. Herramientas ofimáticas. Herramientas de gestión y realización de copias de seguridad.

Productos y resultados

Sistema operativo y aplicaciones configurados y parametrizados de acuerdo a las necesidades. Inventarios software y de configuración de aplicaciones del sistema. Registro de incidencias del software

de base del sistema. Registro de incidencias del software de aplicación corporativo. Plan de asistencia y entrenamiento de usuarios. Copias de seguridad realizadas, archivadas y documentadas. Plan de realización, almacenamiento y recuperación de copias de respaldo. Plan de auditoría de los recursos del sistema. Informe de auditoría de los recursos del sistema.

Información utilizada o generada

Manuales de instalación del sistema operativo. Manual de operación del sistema operativo. Manuales de instalación de aplicaciones. Manuales de operación de aplicaciones. Manuales de operación de realización de copias de seguridad. Normas de seguridad (plan de seguridad) y calidad de la organización. Manuales de herramientas administrativas. Manuales de ayuda en línea. Asistencia técnica en línea. Planes de explotación e implantación de la organización. Normativa aplicable sobre protección de datos y propiedad intelectual, normativa empresarial sobre confidencialidad de datos. Documentación de instalación y configuración. Fichas específicas de identificación y configuración de equipos.

UNIDAD DE COMPETENCIA 3

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.

MÓDULO FORMATIVO 1

Administración hardware de un sistema informático

Nivel:	3
Código:	MF0484_3
Asociado a la UC:	UC0484_3 - Administrar los dispositivos hardware del sistema
Duración (horas):	120
Estado:	BOE

Capacidades y criterios de evaluación

- C1:** Identificar los componentes hardware del sistema distinguiendo sus características y detallando parámetros y procedimientos de instalación.
- CE1.1** Analizar y explicar los fundamentos de la arquitectura física de un sistema informático precisando las distintas partes que lo componen.
 - CE1.2** Enumerar y definir las funciones que realizan cada uno de los componentes hardware de un sistema informático explicando sus características.
 - CE1.3** Clasificar según su tipología cada uno de los componentes hardware de un sistema informático atendiendo a sus características, utilidad y propósitos.
 - CE1.4** Detallar las características técnicas y procedimientos de instalación y configuración de los componentes hardware de un sistema informático según especificaciones de funcionalidades dadas.
 - CE1.5** Distinguir y explicar los tipos de dispositivos físicos y técnicas de comunicación posibles entre los diferentes componentes hardware de un sistema informático, describiendo sus principales características y tipología.
 - CE1.6** Definir y clasificar los diferentes tipos de dispositivos periféricos atendiendo a su propósito, describiendo las diferentes técnicas utilizadas para realizar la comunicación con los mismos y las tecnologías disponibles en controladores de entrada/salida.
 - CE1.7** Identificar y clasificar los diferentes dispositivos físicos disponibles para conectar el sistema a través de una red de comunicaciones.
 - CE1.8** En un supuesto práctico de identificación y registro de dispositivos hardware:
 - Clasificar una colección de dispositivos hardware atendiendo a diferentes criterios: propósito, idoneidad para un sistema y compatibilidad, entre otros.
 - Operar con herramientas de inventariado registrando de forma exhaustiva las características de los dispositivos hardware en estudio.
 - Documentar la instalación de los dispositivos físicos detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.
- C2:** Seleccionar y aplicar los procedimientos y técnicas de monitorización del rendimiento de los dispositivos para ajustar los parámetros de configuración y asegurar la ausencia de conflictos.
- CE2.1** Enumerar y definir las métricas de rendimiento comúnmente utilizadas para medir el rendimiento de un sistema.
 - CE2.2** Caracterizar y analizar los principales procedimientos y técnicas de monitorización utilizados para medir las prestaciones de un sistema.

CE2.3 Aplicar las técnicas y herramientas seleccionadas para conseguir un rendimiento óptimo y determinar el estado del sistema analizando los resultados de las mediciones del rendimiento e indicando si éste se encuentra saturado, equilibrado o infrautilizado.

CE2.4 Representar gráficamente el rendimiento del sistema según los datos obtenidos en la monitorización.

CE2.5 Analizar las alarmas obtenidas en la monitorización y describir los principales problemas de configuración relativos a dispositivos hardware conocidos explicando las soluciones más comunes.

CE2.6 En un supuesto práctico, debidamente caracterizado, de monitorización y ajuste de sistemas:

- Seleccionar las métricas del rendimiento a utilizar según las necesidades del sistema.
- Obtener mediciones del rendimiento del sistema utilizando con destreza las herramientas necesarias para llevarlo a cabo.
- Analizar las mediciones obtenidas, documentándolas y presentándolas para facilitar la toma de decisiones acerca del sistema.
- Configurar los parámetros del sistema necesarios para que se cumplan los requisitos de rendimiento.
- Reconfigurar el sistema dependiendo de las alarmas obtenidas por las mediciones.
- Indicar y documentar las limitaciones que existen en el intento de mejorar las prestaciones de un sistema.

C3: Integrar e implantar en el sistema informático dispositivos hardware que garanticen la continuidad en la prestación de servicios y la seguridad de los datos.

CE3.1 Identificar las diferentes soluciones hardware disponibles para asegurar la continuidad del funcionamiento del sistema, describiendo sus principales características y configuraciones.

CE3.2 Definir las diferentes soluciones hardware disponibles para asegurar la recuperación del sistema ante situaciones imprevistas, describiendo sus principales características y configuraciones.

CE3.3 Identificar las políticas de seguridad y protección de datos y su relación en la recuperación y continuidad de servicios y aplicaciones según normativa de seguridad informática.

CE3.4 En un supuesto práctico, debidamente caracterizado, de implementación y configuración de soluciones para asegurar la continuidad del funcionamiento del sistema:

- Analizar el sistema para determinar las necesidades y disposición de sistemas de alimentación ininterrumpida.
- Instalar adecuadamente las unidades de alimentación y los estabilizadores de tensión respetando las características técnicas de los aparatos y cumpliendo las normas relativas a seguridad en el puesto de trabajo.
- Parametrizar y monitorizar los dispositivos instalados, adecuándolos al sistema para garantizar su total compatibilidad, óptimo funcionamiento, control y gestión de los mismos.
- Realizar un plan de intervención y activación de mecanismos alternativos.
- Documentar la instalación de los dispositivos físicos detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.

CE3.5 En un supuesto práctico, debidamente caracterizado, de implementación y configuración de soluciones para la recuperación del sistema ante situaciones imprevistas:

- Instalar y configurar un servidor local de respaldo que garantice la recuperación inmediata del funcionamiento en casos de caída del servidor principal.

- Instalar y configurar soluciones de 'arrays' de discos para aumentar la tolerancia a fallos del sistema y un sistema de 'clusters' atendiendo a su tipología para aumentar la fiabilidad y productividad del sistema.
- Realizar un plan de intervención y activación de posibles mecanismos alternativos y localizar los dispositivos de hardware responsables de una posible avería y establecer los procedimientos necesarios para su reparación o sustitución.
- Configurar adecuadamente los dispositivos sustituidos siguiendo los pasos establecidos en el plan de intervención establecido.
- Documentar la instalación de los dispositivos físicos detallando los procedimientos, incidencias más frecuentes y parámetros utilizados y los pasos a seguir para la recuperación del sistema una vez que se ha producido una situación imprevista.
- Planificar y realizar pruebas para verificar la idoneidad de las soluciones implementadas, realizando las mejoras y ajustes necesarios hasta conseguir un óptimo funcionamiento.

C4: Analizar y evaluar los dispositivos disponibles en el mercado para proponer implantaciones hardware que mejoren el rendimiento y las prestaciones del sistema informático.

CE4.1 Identificar, evaluar y clasificar los dispositivos hardware existentes en el mercado, según evolución y tipología, utilizando para ello catálogos comerciales, documentación técnica, revistas especializadas u cualquier otro método y soporte.

CE4.2 Identificar las partes de un sistema informático, típicamente susceptibles de provocar cuellos de botella y degradaciones de la productividad.

CE4.3 Explicar las tendencias de evolución tecnológica en los dispositivos físicos comunes de un sistema informático con objeto de proponer mejoras en el mismo.

CE4.4 En un supuesto práctico, debidamente caracterizado, de planificación de crecimiento de un sistema, dadas unas estimaciones de posibles aumentos de la carga de trabajo o de usuarios:

- Analizar las cargas de trabajo esperadas y futuras, caracterizando las mismas de forma adecuada.
- Implementar las nuevas cargas de trabajo, integrándolas en el sistema para observar posibles efectos en el rendimiento del mismo.
- Analizar los parámetros de rendimiento obtenidos tras someter al sistema a las nuevas cargas de trabajo.
- Planificar y ejecutar la implantación de nuevos dispositivos hardware necesarios para soportar las nuevas cargas de trabajo y minimizando sus efectos sobre el sistema.
- Documentar los resultados de la evaluación del sistema sometido a nuevas cargas y proponer, de forma razonada, cambios en la configuración actual o nuevas implantaciones hardware.

C5: Aplicar procedimientos de seguridad y de acondicionamiento ambiental con el fin de garantizar la integridad del sistema y el entorno adecuado según especificaciones y requisitos de los sistemas a instalar.

CE5.1 Enumerar y describir los principales factores ambientales y del entorno a tener en cuenta en la instalación adecuada de equipos informáticos, para establecer las precauciones que puedan evitarlos o aminorar su efecto.

CE5.2 Enumerar y describir los principales factores ambientales y del entorno que pueden degradar el funcionamiento de una red de comunicaciones, para establecer las precauciones que puedan evitarlos o aminorar su efecto.

CE5.3 Interpretar las especificaciones técnicas de los dispositivos y el plan de seguridad para adecuar su instalación y ubicación física consiguiendo un óptimo rendimiento de los mismos.

CE5.4 Evaluar la instalación de la red eléctrica asegurándose que su capacidad y los equipos disponibles son los adecuados para conectar todos los dispositivos hardware y que el funcionamiento de estos sea óptimo.

CE5.5 En un supuesto práctico, debidamente caracterizado, de instalación de equipamiento informático:

- Ubicar los equipos informáticos respetando las condiciones ambientales de temperatura y humedad recomendadas por los fabricantes.
- Ubicar los equipos informáticos respetando las condiciones ergonómicas y de seguridad laboral recomendadas.
- Comprobar que el entorno de instalación de los equipos informáticos se encuentra libre de humo, polvo o cualquier otra perturbación ambiental.
- Documentar las características de ubicación de los equipos informáticos, detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.

CE5.6 En un supuesto práctico, debidamente caracterizado, de comprobación de la seguridad del sistema informático:

- Asegurar la manipulación de los equipos por parte de los usuarios para que no se varíen las condiciones iniciales de temperatura y humedad.
- Asegurar la manipulación de los equipos por parte de los usuarios comprobando que se respeta la normativa en cuanto a seguridad.
- Comprobar la realización de las copias de respaldo, asegurando la idoneidad de la frecuencia, el soporte y la información salvaguardada.
- Documentar las incidencias de seguridad encontradas para su posterior corrección.
- Interpretar el plan de seguridad del sistema, extrayendo los procedimientos de seguridad a aplicar.

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

C1 respecto a CE1.8; C2 respecto a CE2.6; C3 respecto a CE3.4 y CE3.5; C4 respecto a CE4.4; C5 respecto a CE5.5 y CE5.6.

Otras Capacidades:

Adaptarse a la organización específica de la empresa integrándose en el sistema de relaciones técnico-laborales.

Interpretar y ejecutar las instrucciones que recibe y responsabilizarse de la labor que desarrolla, comunicándose de forma eficaz con la persona adecuada en cada momento.

Organizar y ejecutar la intervención de acuerdo a las instrucciones recibidas, con criterios de calidad y seguridad, aplicando los procedimientos específicos de la empresa.

Habituar al ritmo de trabajo de la empresa cumpliendo los objetivos de rendimiento diario definidos en la organización.

Mostrar en todo momento una actitud de respeto hacia los compañeros, procedimientos y normas internas de la empresa.

Tomar en consideración las propuestas recibidas.

Contenidos

1 Introducción a la arquitectura de ordenadores

Fundamentos de la arquitectura Von-Neumann: principios de funcionamiento, esquema y estructura, elementos funcionales y subsistemas.

Otras arquitecturas de procesadores.

Periféricos.
Arquitecturas de buses.
Unidades de control de entrada y salida.
Arquitecturas de ordenadores personales, sistemas departamentales y grandes ordenadores.

2 Componentes de un sistema informático

La unidad central de proceso: funciones; propósito y esquema de funcionamiento; estructura interna: unidad de control, unidad aritmético-lógica y registros.

El sistema de memoria: funciones, espacios de direccionamiento y mapas de memoria, jerarquías de memoria.

El sistema de E/S: funciones y tipos de E/S (programada, interrupciones, DMA), controladores de E/S, funciones de un sistema de bus, tipos de arquitecturas de bus, organización y arbitraje de un sistema de bus, dispositivos periféricos.

El subsistema de almacenamiento: dispositivos de almacenamiento, interfaces.

Placas base.

Fuentes de alimentación y cajas.

Disipadores de calor.

3 Dispositivos hardware

Evolución actual y tendencias futuras en dispositivos hardware. Procesadores múltiples y memoria distribuida entre otros.

Clasificación y tipología: unidades centrales, memorias, dispositivos de almacenamiento, periféricos.

Instalación y configuración de dispositivos: herramientas y aparatos de medida, normas de seguridad, procedimiento de ensamblado de dispositivos, comprobación de las conexiones, verificación del sistema.

Dispositivos y técnicas de conexión: técnicas de conexión y comunicación; comunicaciones entre sistemas informáticos; conexión a redes: topologías de red, protocolos de comunicación, dispositivos de cableado y conexión en redes locales; herramientas de diagnóstico y medición.

4 Rendimiento de sistemas

Evaluación del rendimiento de sistemas informáticos: métricas del rendimiento, representación y análisis de los resultados de las mediciones.

Técnicas de configuración y ajuste de sistemas: rendimiento de los sistemas, caracterización de cargas de trabajo (cargas reales, cargas sintéticas como 'benchmarks', núcleos, programas sintéticos y conjuntos de instrucciones, entre otros).

Técnicas de medición de parámetros del sistema: herramientas de monitorización.

Consumo y competencia de recursos.

Modelos predictivos y análisis de tendencias.

Planes de pruebas preproducción.

Técnicas de diagnóstico y solución de problemas: diagnóstico mediante utilidades del sistema operativo, diagnóstico mediante software específico, diagnóstico mediante herramientas.

Técnicas de actuación: puesta en marcha de mecanismos alternativos, métodos establecidos para solución del problema, verificación.

Alta disponibilidad: definición y objetivos: funcionamiento ininterrumpido, instalación y configuración de soluciones; sistemas de archivo: nomenclatura y codificación, jerarquías de almacenamiento, migraciones y archivado de datos; volúmenes lógicos y físicos: particionamiento, sistemas NAS y SAN, gestión de volúmenes lógicos, acceso paralelo, protección RAID.

5 Políticas de seguridad y de salvaguarda

Acceso restringido por cuentas de usuario.

Propiedad de la información.

Identificador único de acceso.

Entorno físico de un sistema informático: los equipos y el entorno: adecuación del espacio físico, agentes externos y su influencia en el sistema, efectos negativos sobre el sistema, factores que afectan al funcionamiento de una red de comunicaciones.

Creación del entorno adecuado: control de las condiciones ambientales: humedad y temperatura, factores industriales: polvo, humo, interferencias, ruidos y vibraciones, factores humanos: funcionalidad, ergonomía y calidad de la instalación, otros factores.

Evaluación de los factores de riesgo: conceptos básicos en seguridad eléctrica, requisitos eléctricos de la instalación, perturbaciones eléctricas y electromagnéticas, electricidad estática, otros factores de riesgo, introducción a los aparatos de medición.

Salvaguarda física y lógica.

'Cluster' y balanceo de carga.

Integridad de datos y recuperación de servicio.

Custodia de ficheros de seguridad.

Normativas sobre seguridad e higiene en el trabajo.

Reglamentos eléctricos y electrotécnicos.

Normativas de calidad y normalización (ISO, AENOR).

Normativas sobre protección de la información.

La protección jurídica de los programas de ordenador.

Organizaciones nacionales e internacionales de normalización.

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 administración de los dispositivos hardware del sistema, 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

Administración software de un sistema informático

Nivel:	3
Código:	MF0485_3
Asociado a la UC:	UC0485_3 - Instalar, configurar y administrar el software de base y de aplicación del sistema
Duración (horas):	210
Estado:	BOE

Capacidades y criterios de evaluación

C1: Especificar y aplicar procedimientos de instalación y configuración del software base y de aplicación según necesidades de explotación del sistema informático.

CE1.1 Analizar la idoneidad de los diferentes tipos de sistemas operativos para diferentes tipos de sistemas y propósitos.

CE1.2 Identificar y describir las distintas fases a seguir en la instalación de software en un sistema informático.

CE1.3 Identificar y explicar los principales parámetros de configuración del sistema operativo para la administración de dispositivos, memoria, procesos y de sistemas de ficheros.

CE1.4 Reconocer y describir los principales parámetros de configuración del software de aplicación para la correcta utilización de los recursos del sistema.

CE1.5 Automatizar y planificar tareas en el sistema mediante la elaboración de 'scripts'.

CE1.6 En un supuesto práctico, debidamente caracterizado, de instalación y configuración de un sistema operativo en un sistema informático:

- Instalar el software del sistema operativo documentando el proceso, las incidencias ocurridas y los parámetros utilizados.

- Configurar los parámetros del sistema operativo referidos al sistema de memoria, indicando la organización a seguir y la utilización de técnicas avanzadas de gestión.

- Configurar los parámetros del sistema operativo relativos a la ejecución de tareas: planificación de trabajos, mecanismos de sincronización y asignación de recursos.

- Parametrizar el sistema de entrada salida comprobando el funcionamiento óptimo de los dispositivos periféricos.

- Organizar los sistemas de ficheros creando las estructuras necesarias para el correcto funcionamiento del sistema.

- Configurar los parámetros del sistema operativo de forma que se cumplan las especificaciones del plan de seguridad del sistema.

CE1.7 En un supuesto práctico, debidamente caracterizado, de verificación y configuración de la instalación de un sistema operativo en un sistema informático:

- Verificar el funcionamiento del sistema operativo y dispositivos intervinientes en el sistema, asegurando configuración de sus controladores y la ausencia de conflictos, utilizando el software de diagnóstico que fuese necesario.

- Establecer y configurar los parámetros de red del sistema operativo de forma que se aseguren y garanticen la integridad de los datos y fiabilidad del sistema siguiendo en todo momento el plan de seguridad y calidad de la organización.

- Habilitar la organización y configuración de usuarios según las necesidades y plan de seguridad de la organización.
- Actualizar el sistema operativo del servidor asegurando la integridad del sistema, de los datos y según el plan de seguridad de la organización.
- Documentar la configuración del sistema operativo detallando los parámetros utilizados.
- Interpretar el plan de seguridad de la organización para implementar las medidas especificadas en el mismo según normativa de seguridad informática.

CE1.8 En un supuesto práctico, debidamente caracterizado, de instalación y configuración de software de aplicación en un sistema informático:

- Instalar el software de aplicación documentando el proceso, las incidencias ocurridas y los parámetros utilizados.
- Configurar los parámetros del software de aplicación referidos a la utilización de recursos del sistema de forma que se minimice el impacto sobre su rendimiento.
- Configurar los parámetros del software de aplicación de forma que se cumplan las especificaciones del plan de seguridad del sistema.
- Verificar el funcionamiento del software de aplicación y dispositivos que componen el sistema, asegurando la configuración de sus controladores y la ausencia de conflictos utilizando el software de diagnóstico necesario.
- Actualizar el software de aplicación asegurando la integridad del sistema, y de los datos según el plan de seguridad de la organización.
- Documentar la configuración del software de aplicación detallando los parámetros utilizados.
- Interpretar el plan de seguridad de la organización para implementar las medidas especificadas según la normativa de seguridad informática.

C2: Identificar los componentes software del sistema distinguiendo sus características y detallando parámetros.

CE2.1 Analizar y enumerar los diferentes tipos de sistemas operativos precisando sus características más importantes.

CE2.2 Clasificar y describir los diferentes tipos de aplicaciones y componentes software explicando sus principales características, funciones y propósito.

CE2.3 Identificar las funciones que realiza un sistema operativo instalado en un sistema informático.

CE2.4 Explicar los requisitos legales relativos a propiedad intelectual a tener en cuenta en la instalación de software en el sistema.

CE2.5 En un supuesto práctico, debidamente caracterizado, de identificación y registro de software de un sistema informático:

- Clasificar una colección de software instalado atendiendo a diferentes criterios: propósito, idoneidad para un sistema y compatibilidad, entre otros.
- Operar con herramientas de inventariado registrando de forma exhaustiva las características del software instalado.
- Comprobar el número y ubicación de licencias instaladas de aplicaciones protegidas por las leyes de propiedad intelectual para su correcto cumplimiento.
- Comprobar las aplicaciones instaladas para comprobar la no existencia de software no permitido.
- Registrar y controlar los privilegios de acceso a las aplicaciones de los usuarios según el plan de seguridad y las leyes de protección de datos vigentes.
- Documentar la instalación del software detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.

- C3:** Planificar el soporte a los usuarios asegurando la máxima disponibilidad y la documentación de las tareas correspondientes.
- CE3.1** Definir los objetivos de un plan de asistencia técnica y de soporte a usuarios.
 - CE3.2** Explicar las ventajas y características principales de las técnicas de asistencia remota a los usuarios a través de los servicios y herramientas disponibles en el sistema.
 - CE3.3** Enumerar y describir los problemas más comunes relativos a la implantación de software en puestos de usuario.
 - CE3.4** Enumerar y describir los problemas más comunes relativos a dispositivos hardware y de red en puestos de usuario.
 - CE3.5** Establecer procedimientos de instalación, configuración y mantenimiento de software de base y aplicación en puestos de usuario.
 - CE3.6** En un supuesto práctico, debidamente caracterizado, de planificación de soporte a los usuarios en un sistema informático:
 - Fijar procedimientos de asistencia basados en la anotación sistemática de los problemas detectados y consulta al personal de apoyo.
 - Documentar exhaustivamente los problemas más comunes relativos a los recursos software del sistema.
 - Documentar exhaustivamente los problemas más comunes relativos a los recursos hardware del sistema.
 - Planificar el entrenamiento para la adaptación del personal a las herramientas de trabajo.
 - Configurar y operar adecuadamente con herramientas de asistencia remota de usuarios.
- C4:** Analizar el sistema mediante técnicas de simulación y modelado para optimizar el rendimiento.
- CE4.1** Definir el concepto de simulación explicando las ventajas de utilización de esta técnica así como sus posibles aplicaciones en diferentes ámbitos.
 - CE4.2** Explicar la necesidad de representación de sistemas a través de modelos para su posterior estudio.
 - CE4.3** Identificar y caracterizar adecuadamente los pasos a seguir para realizar la simulación de un sistema.
 - CE4.4** En un supuesto práctico, debidamente caracterizado, de simulación de un sistema informático debidamente caracterizado:
 - Enumerar los objetivos a alcanzar a través de la simulación del sistema.
 - Analizar las características del sistema y construir un modelo del mismo utilizando herramientas de modelado disponibles.
 - Construir un modelo de simulación según los objetivos definidos y el modelo obtenido, utilizando las herramientas de simulación disponibles.
 - Ejecutar el modelo de simulación documentando exhaustivamente los datos obtenidos.
 - Analizar los resultados de la simulación identificando los puntos de mal funcionamiento o problemáticos del sistema.
 - Ajustar la configuración del sistema para solucionar los problemas detectados y optimizar el rendimiento y documentar los procesos de simulación detallando los objetivos, modelos y resultados obtenidos.
- C5:** Analizar y definir las políticas de realización de copias de respaldo y de recuperación de datos en función de las especificaciones de seguridad.

CE5.1 Clasificar los diferentes tipos de sistemas de copias de respaldo, basándose en el soporte empleado, en la topología o arquitectura y sistemas soportados (fichero, partición de disco y base de datos, entre otros).

CE5.2 Describir los niveles de copias de respaldo explicando las diferencias entre ellos.

CE5.3 Asociar la política de realización de copias a los sistemas implicados, justificando las decisiones y cumpliendo la normativa vigente en materia de protección de datos de carácter personal.

CE5.4 En un supuesto práctico, de sistemas de almacenamiento de información:

- Estimar el volumen de información a copiar por unidad de tiempo.
- Identificar áreas de almacenamiento de los soportes utilizados para las copias de respaldo.
- Planificar el acceso autorizado a los soportes.
- Mantener registro de información respecto al contenido, versiones y ubicación de los archivos de datos.
- Organizar el inventario de medios de almacenamiento y archivos almacenados.
- Verificar que las copias de respaldo reciben el mismo nivel de seguridad que los archivos originales.

C6: Aplicar procedimientos de auditoría utilizando técnicas y herramientas adecuadas para garantizar los parámetros de funcionamiento del sistema informático.

CE6.1 Enumerar y explicar los objetivos a cumplir con la habilitación de las auditorías del sistema.

CE6.2 Clasificar, según prioridad, los eventos del sistema y de las aplicaciones susceptibles de ser auditados para el mantenimiento del óptimo funcionamiento del sistema.

CE6.3 Determinar, para cada evento detectado, la necesidad de llevar a cabo acciones correctivas, implantándolas en caso afirmativo.

CE6.4 En un supuesto práctico, debidamente caracterizado, de aplicación de procedimientos de auditoría en un sistema:

- Establecer las políticas de auditoría de forma adecuada para no sobrecargar el funcionamiento del sistema y afectar a su rendimiento.
- Seleccionar una lista de eventos a auditar que proporcionen información útil: inicio y detención de servicios, accesos a recursos, conexión y desconexión de usuarios, eventos de aplicaciones y eventos de sistema.
- Fijar las acciones correctivas necesarias asociadas a los eventos detectados y aplicar e integrar las herramientas disponibles al sistema según el plan de auditoría establecido.
- Establecer alarmas para resaltar la detección de eventos prioritarios o críticos.
- Operar con las herramientas disponibles para la planificación, definición e implementación de auditorías y analizar los registros de las mismas extrayendo información acerca del funcionamiento y estado del sistema para la realización del informe de auditoría.
- Interpretar documentación técnica del sistema, aplicaciones y herramientas de auditoría.

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

C1 respecto a CE1.6 y CE1.7; C2 respecto a CE2.5; C3 respecto a CE3.6; C4 respecto a CE4.4; C5 respecto a CE5.4; C6 respecto a CE6.4.

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.

Demostrar un buen hacer profesional.
Ser capaz de proponer mejoras en los procesos y procedimientos de trabajo.
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 Representación de la información

Necesidad de la representación de la información.
Sistemas de representación de la información.

2 Clasificación del software

Sistemas operativos: concepto de software de base o sistema operativo; evolución de los sistemas operativos: generaciones y características; conceptos: monousuario/multiusuario, monotarea/multitarea, monoprocesador/multiprocesador; funciones de un sistema operativo, estructura de un sistema operativo: características y funciones; gestión de procesos; gestión y organización de memoria; gestión y sistemas de ficheros; gestión de usuarios y grupos; gestión de dispositivos, opciones de accesibilidad para personas con discapacidades; herramientas comunes del sistema operativo; conceptos de sistemas operativos en red y distribuidos; conceptos de sistemas operativos en tiempo real; tendencias de los sistemas operativos.

Lenguajes de programación: propósito de los lenguajes de programación, clasificación según el grado de independencia de la máquina, clasificación según la forma de sus instrucciones, clasificación por generaciones.

Programas de aplicación: procesadores de lenguaje, aplicaciones de propósito general, ventajas e inconvenientes de las aplicaciones a medida.

3 Procedimientos de implantación de software

El ciclo de implantación de software: instalación, configuración, verificación y ajuste.

La necesidad de la planificación en los procesos de instalación.

Parámetros del sistema a tener en cuenta en un proceso de instalación de software.

Procedimientos para la instalación de sistemas operativos: requisitos del sistema, controladores de dispositivos, software de clonación, configuración de interfaces de usuario, pruebas y optimización de la configuración, normativa aplicable sobre propiedad intelectual, licencias y tipos de licencias.

4 Procedimientos de mantenimiento de software

La necesidad de la planificación en los procesos de instalación.

Planificación y automatización de tareas mediante scripts.

Objetivos de un plan de mantenimiento.

El mantenimiento preventivo como estrategia.

Problemas comunes en las instalaciones software.

Problemas comunes en las instalaciones hardware.

Mantenimiento remoto: herramientas y configuración.

Adecuación de sistemas: parches y actualizaciones.

5 Copias de respaldo

Arquitectura del servicio de copias de respaldo: sistemas centralizados, sistemas distribuidos, copias locales.

Planificación del servicio de copias de respaldo: niveles de copia de respaldo, dimensionamiento del servicio de copias de respaldo.

Soportes para copias de respaldo: soportes tradicionales, jerarquías de almacenamiento.

6 Procedimientos de auditoría del sistema

Objetivos de la auditoría: estándares.

Políticas de auditoría: ámbito de la auditoría, aspectos auditables; clasificación de eventos: de sistema, de aplicación, de seguridad; mecanismos de auditoría: alarmas y acciones correctivas; información del registro de auditoría.

Técnicas y herramientas de auditoría.

Informes de auditoría.

7 Introducción al modelado y simulación

Concepto de simulación: finalidad y aplicaciones.

Representación de sistemas mediante modelos: conceptos principales.

El ciclo de vida de un proyecto de simulación.

Visión general de herramientas de simulación de sistemas informáticos.

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 instalación, configuración y administración del software base y de aplicación del sistema, 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

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.