CUALIFICACIÓN PROFESIONAL:
Operación de sistemas informáticos

Familia Profesional:	***Informática y Comunicaciones***
Nivel:	***2***
Código:	***IFC300_2***
Estado:	***BOE***
Publicación:	***Orden PRE/1636/2015***
Referencia Normativa:	***RD 545/2023, RD 1201/2007***

Competencia general

Aplicar procedimientos de administración y configuración del software y hardware del sistema informático, garantizando su seguridad, así como solucionar las incidencias que se puedan producir en el normal funcionamiento del mismo y monitorizar sus rendimientos y consumos, siguiendo especificaciones recibidas.

Unidades de competencia

UC0219_2: GESTIONAR EL 'SOFTWARE' DE BASE EN SISTEMAS MICROINFORMÁTICOS
UC0957_2: Mantener y regular el subsistema físico en sistemas informáticos
UC0958_2: Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de cliente
UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos

Entorno Profesional

Ámbito Profesional

Desarrolla su actividad profesional en el área de soporte y de CAU (Centro de Atención a Usuarios) dedicados a la informática en entidades de naturaleza pública o privada, empresas de cualquier tamaño, 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 los subsectores productivos dedicados a la comercialización de equipos y servicios informáticos, a la asistencia técnica informática, en redes de telecentros y en todos aquellos sectores productivos que utilicen 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 omnicomprensivo de mujeres y hombres.

- Técnicos de soporte informático
- Operadores de sistemas (orientados a la máquina)

Formación Asociada (570 horas)

Módulos Formativos

MF0219_2: GESTIÓN DEL 'SOFTWARE' DE BASE EN SISTEMAS MICROINFORMÁTICOS (150 horas)
MF0957_2: Mantenimiento del subsistema físico de sistemas informáticos (150 horas)
MF0958_2: Mantenimiento del subsistema lógico de sistemas informáticos (150 horas)
MF0959_2: Mantenimiento de la seguridad en sistemas informáticos (120 horas)

UNIDAD DE COMPETENCIA 1
GESTIONAR EL 'SOFTWARE' DE BASE EN SISTEMAS MICROINFORMÁTICOS

Nivel: *2*
Código: *UC0219_2*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Instalar sistemas operativos en sistemas microinformáticos, configurándolos según necesidades y objetivos, siguiendo especificaciones y criterios de calidad y seguridad de la entidad responsable de sistemas.

CR1.1 Los requisitos de instalación del sistema operativo, tales como suficiencia de recursos y compatibilidad en el equipo destino de la instalación, se verifican consultando los requisitos del sistema y versión a instalar en su documentación técnica, cotejándolos con el 'hardware' y siguiendo el procedimiento establecido por la entidad responsable.

CR1.2 El equipo destino de la instalación se prepara, habilitando, configurando y particionando los dispositivos de almacenamiento masivo, así como preparando las conectividades necesarias, de acuerdo con especificaciones de la entidad responsable y de la documentación técnica.

CR1.3 El sistema operativo se instala, siguiendo los pasos indicados en los manuales de instalación y/o asistentes del mismo, utilizando en su caso una imagen y siguiendo el procedimiento establecido por la entidad responsable, para obtener un equipo informático en estado funcional.

CR1.4 El sistema operativo se configura para su funcionamiento, asignando los parámetros especificados por la persona responsable de sistemas, tales como la creación de los usuarios, la configuración de los parámetros de red o la parametrización corporativa, siguiendo los procedimientos y especificaciones establecidos en la entidad responsable y lo indicado en la documentación técnica.

CR1.5 La instalación se verifica, mediante pruebas de arranque y parada y análisis del rendimiento, entre otras, siguiendo procedimientos establecidos por la entidad responsable para comprobar la funcionalidad del sistema operativo y las aplicaciones instaladas.

CR1.6 La documentación de los procesos realizados se elabora, indicando sistema instalado, versión, licencia, referencia del equipo o dispositivo e incidencias detectadas y solucionadas, entre otros, siguiendo los modelos establecidos por la entidad responsable de sistemas y archivándola para facilitar su posterior uso y consulta.

RP2: Actualizar el sistema operativo y herramientas preinstaladas, usando las herramientas y opciones proporcionadas por el fabricante, siguiendo procedimientos especificados en la documentación técnica para el mantenimiento de su funcionamiento en condiciones de seguridad y calidad.

CR2.1 Las versiones del 'software' de base, complementos del sistema y controladores de dispositivos se comprueban, siguiendo el procedimiento establecido por la entidad responsable para asegurar su idoneidad y vigencia, seleccionando aquellos que no se ajustan a los requerimientos establecidos por la entidad responsable, para proceder a su actualización.

CR2.2 Los complementos y actualizaciones para el funcionamiento del 'software' de base se instalan, previa comprobación de requisitos técnicos, siguiendo los pasos indicados por el fabricante, configurándolos de acuerdo con los procedimientos establecidos por la entidad responsable para mantener la seguridad y funcionalidad en el sistema.

CR2.3 La actualización se verifica, mediante pruebas de arranque y parada y análisis de rendimiento, entre otros y siguiendo los procedimientos establecidos por la entidad responsable, para comprobar la funcionalidad de sistema operativo y aplicaciones.

CR2.4 La documentación de los procesos realizados se elabora, indicando sistema operativo, aplicaciones y complementos actualizados y sus versiones, la referencia del equipo o dispositivo e incidencias detectadas y solucionadas, entre otros, según los procedimientos establecidos por la entidad responsable, archivándola para su consulta posterior.

RP3: Mantener el sistema operativo, el 'software' de base y aplicaciones estándar del sistema microinformático, mediante revisión, verificación y monitorización teniendo en cuenta las necesidades de uso, para detectar problemas y solucionarlos en su caso, siguiendo especificaciones y criterios de calidad y seguridad de la entidad responsable de sistemas.

CR3.1 El sistema de archivos se verifica, reconfigurando particiones en caso necesario y limpiando errores físicos, lógicos u otros, usando las utilidades, herramientas e interfaces que proporciona el sistema operativo, siguiendo especificaciones técnicas y según necesidades de operación.

CR3.2 El rendimiento y el uso de recursos 'hardware' dentro del equipo, tales como uso de CPU, uso de RAM, memoria de intercambio y datos SMART, entre otros, se monitorizan según necesidades de operación, generando alarmas y notificaciones mediante la utilización de herramientas para dicha función y siguiendo los criterios y parámetros de la entidad responsable.

CR3.3 Las políticas de seguridad de usuarios y grupos se revisan, cotejándolas con las políticas actuales de la entidad responsable, para garantizar su vigencia y, en su caso, para realizar las modificaciones correspondientes, aplicando los parámetros especificados por dicha entidad responsable.

CR3.4 Las medidas de seguridad preventivas tales como copias de seguridad periódicas de la información en un servidor de 'backup', la comprobación que el proceso de restauración desde esos servidores es funcional, el mantenimiento de sistemas de disponibilidad u otros se activan para mantener la integridad de la información y la continuidad en la explotación.

CR3.5 El uso y gestión, por parte de los usuarios, de los dispositivos conectados directamente o por red al sistema microinformático, se comprueba, verificando que se realiza según la documentación técnica y procedimientos estipulados para explotar sus funcionalidades y en condiciones de seguridad.

CR3.6 Los problemas se detectan, interpretando los mensajes resultantes de la ejecución del 'software' de base tales como los registros 'log' del sistema u otros, mediante la consulta de los manuales, la documentación proporcionada por el fabricante y las especificaciones dadas por la organización.

CR3.7 Los problemas detectados se corrigen, aplicando soluciones según las necesidades en cada caso, teniendo en cuenta las señales de problema detectadas y su diagnóstico, siguiendo procedimientos del fabricante y de la entidad responsable de sistemas.

CR3.8 El trabajo realizado se documenta, indicando las incidencias surgidas y las soluciones aplicadas, utilizando un modelo de documento o una aplicación informática indicados por la entidad responsable de sistemas, para su archivo y posterior consulta.

Contexto profesional

Medios de producción

Equipos microinformáticos. Dispositivos asociados al sistema microinformático. Sistemas operativos. Utilidades y aplicaciones incluidas en los sistemas operativos. Herramientas de clonación de discos. 'Software' para elaboración y registro de informes y documentación. Utilidades no incluidas en el sistema operativo. Dispositivos de almacenamiento masivo. Dispositivos de almacenamiento en red. Aplicaciones de gestión de incidencias.

Productos y resultados

Sistema operativos instalados y configurados. Sistemas operativos y herramientas preinstaladas actualizados y en explotación. Sistema operativo, 'software' de base y aplicaciones estándar mantenidas.

Información utilizada o generada

Normativa aplicable de protección de datos, propiedad intelectual e industrial y planificación de la acción preventiva. Informes de instalación, configuración y actualización del sistema operativo. Registro histórico de actualizaciones de sistema operativo y aplicaciones. Plan de seguridad y calidad de la organización. Especificaciones de procedimientos de instalación y mantenimiento de sistemas y aplicaciones. Manuales y documentación técnica de sistemas operativos. Manuales de actualización de sistemas operativos. Manuales de las aplicaciones incluidas en el sistema operativo. Manuales de las aplicaciones externas al sistema operativo.

UNIDAD DE COMPETENCIA 2

Mantener y regular el subsistema físico en sistemas informáticos

Nivel: *2*
Código: *UC0957_2*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Comprobar el estado y mantener las conexiones de los dispositivos físicos para su utilización, siguiendo los procedimientos establecidos.

CR1.1 Las tareas de comprobación y verificación para asegurar la conexión de los dispositivos físicos y a la red se realizan según procedimientos establecidos o según indicación del administrador del sistema y siempre bajo condiciones de seguridad.

CR1.2 Los dispositivos físicos averiados, con mal funcionamiento o bajo rendimiento se actualizan o sustituyen por componentes iguales o similares que cumplan su misma función y aseguren su compatibilidad en el sistema para mantener operativo el mismo, según procedimientos establecidos.

CR1.3 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

RP2: Revisar y asegurar los elementos fungibles para el funcionamiento del sistema informático según las especificaciones establecidas y las necesidades de uso.

CR2.1 Los elementos fungibles se comprueban, para garantizar su compatibilidad y funcionalidad utilizando herramientas y técnicas, según procedimientos establecidos y bajo condiciones de seguridad suficientes.

CR2.2 Los elementos fungibles agotados, deteriorados o inservibles se sustituyen por otros iguales o similares que cumplan su misma función y aseguren su compatibilidad con los dispositivos del sistema siguiendo el procedimiento establecido, normas del fabricante y bajo condiciones de seguridad en la manipulación del material fungible.

CR2.3 El funcionamiento del sistema informático, con los elementos fungibles instalados, se comprueba para asegurar su operatividad, según el procedimiento establecido.

CR2.4 Los procedimientos de reciclaje y reutilización de materiales fungibles se aplican, para la consecución de objetivos tanto medioambientales como económicos, según normativa de la organización y especificaciones medioambientales.

CR2.5 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

RP3: Monitorizar el rendimiento del subsistema físico informando de las incidencias detectadas según especificaciones establecidas.

CR3.1 Las herramientas de monitorización se comprueban, para verificar su funcionamiento, según los procedimientos establecidos por la organización.

CR3.2 El funcionamiento de los dispositivos físicos del sistema se comprueba para detectar posibles anomalías, utilizando las herramientas de monitorización y siguiendo los procedimientos establecidos por la organización.

CR3.3 Los programas de medición se ejecutan, para comprobar el rendimiento de los dispositivos físicos, según procedimientos establecidos y necesidades de uso.

CR3.4 Las alarmas y eventos monitorizados se documentan y su registro se archiva, para su uso posterior, según procedimientos establecidos.

CR3.5 Las acciones correctivas establecidas para responder a determinadas alarmas e incidencias se llevan a cabo según procedimientos establecidos.

CR3.6 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

RP4: Controlar y revisar los inventarios del subsistema físico para asegurar su validez según los procedimientos establecidos.

CR4.1 Los inventarios de los componentes físicos del sistema se comprueban, para asegurar su validez, según las normas de la organización.

CR4.2 Los cambios detectados en las características, configuración o situación de componentes físicos se documentan según procedimientos establecidos, para mantener el inventario actualizado.

CR4.3 Las incidencias detectadas sobre componentes averiados, cambios no autorizados de configuración, instalación no autorizada de componentes, o usos indebidos de los mismos se documentan y se archivan para su uso posterior según procedimientos establecidos.

Contexto profesional

Medios de producción

Equipamiento informático: componentes, periféricos, cableado y equipamiento para equipos portátiles, entre otros. Equipos de gama media ('minis') y grande ('mainframes'). Equipamiento de ensamblaje y medida: herramientas de ensamblaje y desensamblaje, medidores de tensión, herramientas para la confección de cableado. Material fungible para el funcionamiento del sistema. Sistemas operativos. Software de inventariado automático. Herramientas ofimáticas. Software de monitorización. Software de diagnóstico. Herramientas de administración. Conexión a la red.

Productos y resultados

Inventarios revisados y actualizados del subsistema físico. Conexiones del subsistema físico comprobadas. Elementos fungibles comprobados. Rendimiento del sistema controlado. Sistema informático configurado para tener conexión con la red y en óptimo rendimiento físico.

Información utilizada o generada

Inventario del sistema informático. Documentación técnica de los dispositivos físicos del sistema. Documentación técnica del software de base del sistema. Manuales de operación del software de monitorización. Manuales de operación del software de inventariado. Documentación técnica de los fabricantes de elementos fungibles. Documentación técnica de diagnóstico del sistema y de los dispositivos periféricos. Guías de conexión a la red. Normas y recomendaciones ambientales de seguridad. Normativa aplicable de seguridad e higiene en el trabajo. Informes de incidencias de mantenimiento de dispositivos físicos. Informes de incidencias de mantenimiento de elementos fungibles. Informes de incidencias del rendimiento del subsistema físico.

UNIDAD DE COMPETENCIA 3

Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de cliente

Nivel: *2*
Código: *UC0958_2*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Mantener actualizadas las aplicaciones de usuario para garantizar su funcionamiento, según especificaciones técnicas y procedimientos de la organización.

CR1.1 El software de aplicación se instala para soportar las necesidades funcionales de los usuarios a indicación del administrador del sistema y según procedimientos establecidos.

CR1.2 Las actualizaciones del software de aplicación se realizan para mantener y renovar las funcionalidades del sistema, según especificaciones técnicas del fabricante y normas de la organización.

CR1.3 El software de aplicación no utilizado se desinstala para evitar un mal aprovechamiento del espacio de almacenamiento, según procedimientos establecidos.

CR1.4 Las incidencias detectadas se documentan y registran, en el caso en que no lo estén, según procedimientos establecidos.

CR1.5 El software de aplicación publicado en los servicios centrales se actualiza según la periodicidad establecida, se mantiene la gestión de usuarios y permisos y se desinstala cuando la organización decide prescindir de él.

CR1.6 Los procesos de diagnóstico se realizan en los equipos en los que se han detectado incidencias utilizando herramientas específicas y de gestión remota con el fin de solucionarlas o escalarlas siguiendo los procedimientos establecidos.

RP2: Realizar tareas de administración del software de base para mantener el sistema informático en funcionamiento, según procedimientos establecidos.

CR2.1 El mantenimiento físico y lógico y la limpieza de soportes de información se llevan a cabo periódicamente, con las herramientas específicas, para asegurar su integridad y funcionamiento, según procedimientos establecidos.

CR2.2 Las tareas de administración para el mantenimiento de la configuración del software de base y de aplicación en los equipos cliente se realizan según procedimientos establecidos y necesidades de uso.

CR2.3 Los periféricos conectados a los equipos cliente se configuran lógicamente en el software de aplicación, para su explotación, según procedimientos establecidos y especificaciones técnicas.

CR2.4 La ejecución de tareas de administración se realiza utilizando herramientas software específicas que faciliten su ejecución, según especificaciones técnicas y necesidades de uso.

CR2.5 La ejecución de tareas de administración programadas se comprueba, para asegurar su funcionamiento y periodicidad, según procedimientos establecidos y necesidades de uso.

CR2.6 La ejecución de programas o guiones se realiza, a indicación del administrador, y según procedimientos establecidos, para llevar a cabo tareas administrativas, documentándose el resultado obtenido.

CR2.7 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

CR2.8 Las incidencias detectadas se resuelven o escalan, para proceder a su solución, según procedimientos establecidos.

RP3: Monitorizar el rendimiento del software de base y de aplicación, informando de los resultados obtenidos, según procedimientos establecidos.

CR3.1 Las herramientas de monitorización se comprueban, para verificar su funcionamiento, según los procedimientos establecidos por la organización.

CR3.2 Las herramientas de monitorización se utilizan para detectar posibles anomalías en el funcionamiento del software de base y de aplicación del sistema, así como del sistema origen para las aplicaciones publicadas, siguiendo procedimientos establecidos por la organización.

CR3.3 Los programas de medición del software se ejecutan tanto en los puestos como en los servidores donde se ejecutan las aplicaciones publicadas, para comprobar el rendimiento de los procesos, según procedimientos establecidos.

CR3.4 Las alarmas y eventos monitorizados se documentan y su registro se archiva para su uso posterior, según procedimientos establecidos.

CR3.5 Las acciones correctivas establecidas, para responder a determinadas alarmas e incidencias se llevan a cabo, según procedimientos establecidos.

CR3.6 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

RP4: Controlar y revisar los inventarios de software para asegurar su validez y actualización, según especificaciones recibidas.

CR4.1 Los inventarios de los componentes lógicos del sistema se comprueban, para asegurar su validez, según las normas de la organización.

CR4.2 Los cambios detectados en la versión, configuración o situación de componentes lógicos, se documentan para mantener el inventario actualizado, según procedimientos establecidos.

CR4.3 Los identificadores de los componentes lógicos sujetos a derechos de autor se comprueban, para mantener control sobre las licencias instaladas, según la normativa aplicable.

CR4.4 Las incidencias detectadas sobre malfuncionamiento de software, cambios no autorizados de configuración, instalación no autorizada de componentes, o usos indebidos de los mismos se documentan para su uso posterior, según procedimientos establecidos.

Contexto profesional

Medios de producción

Equipamiento informático y de periféricos. Soportes de información. Software de base. Aplicaciones ofimáticas. Software de aplicación. Software de monitorización. Parches y actualizaciones. Software de compresión de ficheros. Gestores de discos. Gestores de arranque. Herramientas administrativas. Software de inventariado automático. Herramientas de gestión remota. Herramientas de 'workflow' para la gestión colaborativa de los seguimientos y la documentación. Conexión a internet (activaciones y actualizaciones) y/o a la red departamental.

Productos y resultados

Inventarios revisados y actualizados del subsistema lógico. Aplicaciones de usuario en funcionamiento y actualizadas. Sistema informático con subsistema lógico en funcionamiento. Rendimiento del software base monitorizado.

Información utilizada o generada

Documentación técnica de los dispositivos físicos del sistema. Documentación técnica del software de base del sistema. Inventarios del subsistema lógico. Manuales de operación del software de monitorización. Manuales de operación del software de inventariado. Organigrama de la organización. Plan de seguridad y calidad de la organización. Normas y recomendaciones ambientales de seguridad. Normativa aplicable en materia de protección de datos y confidencialidad de la información. Manuales de herramientas administrativas. Informes de incidencias de mantenimiento de software de base y aplicación. Informes de incidencias del rendimiento del subsistema lógico.

UNIDAD DE COMPETENCIA 4

Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos

Nivel: *2*
Código: *UC0959_2*
Estado: *BOE*

Realizaciones profesionales y criterios de realización

RP1: Realizar la copia de seguridad, para garantizar la integridad de los datos, según los procedimientos establecidos y el plan de seguridad.

CR1.1 Las copias de seguridad se realizan, para proteger los datos del sistema, según la periodicidad, soporte y procedimiento establecidos en el plan de seguridad del sistema.

CR1.2 Las copias de seguridad se verifican, para asegurar la utilización de las mismas, según los procedimientos establecidos en el plan de seguridad del sistema.

CR1.3 El almacenamiento de las copias de seguridad, para evitar pérdidas de la información, se realiza en las condiciones y según el procedimiento indicado en el plan de seguridad del sistema y las recomendaciones del fabricante del soporte.

CR1.4 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

RP2: Revisar los accesos al sistema informático, para asegurar la aplicación de los procedimientos establecidos y el plan de seguridad, informando de las anomalías detectadas.

CR2.1 Las herramientas de monitorización, para trazar los accesos y la actividad del sistema se comprueban para asegurar su funcionamiento, según el plan de seguridad del sistema.

CR2.2 Los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema se recopilan para localizar la existencia de accesos o actividades no deseados.

CR2.3 Las incidencias de acceso al sistema detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

CR2.4 Los cambios detectados en la configuración del acceso de usuarios al sistema se documentan, para mantener el inventario actualizado, según procedimientos establecidos.

RP3: Comprobar el funcionamiento de los mecanismos de seguridad establecidos informando de las anomalías detectadas a personas de responsabilidad superior.

CR3.1 Los permisos de acceso de los usuarios al sistema se comprueban, para asegurar su validez, según el plan de seguridad del sistema.

CR3.2 Las políticas de seguridad de usuario se comprueban, para cerciorar su validez, según el plan de seguridad del sistema.

CR3.3 Los sistemas de protección antivirus y de programas maliciosos se revisan, en lo que respecta a su actualización y configuración funcional, para garantizar la seguridad del equipo, según los procedimientos establecidos por la organización.

CR3.4 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

CR3.5 Los procesos de diagnóstico se realizan en los equipos en los que se han detectado incidencias utilizando herramientas específicas y de gestión remota con el fin de solucionarlas o escalarlas siguiendo los procedimientos establecidos.

RP4: Verificar que las condiciones ambientales y de seguridad se mantienen según los planes establecidos, informando de posibles anomalías.

CR4.1 Las especificaciones técnicas de los dispositivos se comprueban para asegurar que se cumplen las recomendaciones de los fabricantes en cuanto a condiciones ambientales y de seguridad.

CR4.2 La ubicación de los equipos y dispositivos físicos se revisa para asegurar que se cumplen los requisitos en cuanto a seguridad, espacio y ergonomía establecidos por la organización.

CR4.3 Las incidencias detectadas se documentan y registran, en el caso en que no estén ya registradas, según procedimientos establecidos.

CR4.4 Las acciones correctivas establecidas para solucionar determinadas incidencias detectadas se realizan según procedimientos establecidos.

Contexto profesional

Medios de producción

Equipos informáticos y periféricos. Soportes de información. Software de base. Aplicaciones ofimáticas. Software de monitorización. Software para la realización de copias de seguridad. Software antivirus. Parches y actualizaciones. Software de compresión de ficheros. Gestores de discos. Gestores de arranque. Herramientas administrativas. Herramientas y dispositivos de seguridad.

Productos y resultados

Copias de seguridad del sistema para evitar pérdidas de información. Sistema informático con subsistema lógico en funcionamiento. Sistema informático asegurado frente accesos y acciones no deseadas. Sistema informático organizado en condiciones de seguridad ambientales.

Información utilizada o generada

Documentación técnica de los dispositivos físicos del sistema. Documentación técnica del software de base del sistema. Manuales de operación del software de monitorización. Manuales de operación de los dispositivos y herramientas de seguridad. Organigrama de la organización. Plan de seguridad y calidad de la organización. Normas y recomendaciones ambientales de seguridad. Normativa aplicable en materia de protección de datos y confidencialidad de la información. Manuales de herramientas administrativas. Informes de incidencias de accesos al sistema. Informes de incidencias de los mecanismos de seguridad del sistema. Informes de incidencias de copias de seguridad.

MÓDULO FORMATIVO 1

GESTIÓN DEL 'SOFTWARE' DE BASE EN SISTEMAS MICROINFORMÁTICOS

Nivel:	*2*
Código:	*MF0219_2*
Asociado a la UC:	*UC0219_2 - GESTIONAR EL 'SOFTWARE' DE BASE EN SISTEMAS MICROINFORMÁTICOS*
Duración (horas):	*150*
Estado:	*BOE*

Capacidades y criterios de evaluación

C1: Aplicar procesos de instalación y configuración de sistemas operativos, comprobando requisitos y según objetivos de uso y de acuerdo con unas especificaciones, para obtener un equipo microinformático en estado funcional.

CE1.1 Describir arquitecturas de sistemas microinformáticos, detallando la misión de cada uno de sus bloques funcionales.

CE1.2 Identificar las funciones que desempeña un sistema operativo en el sistema microinformático, explicando sus características, subsistemas y objetivos.

CE1.3 Distinguir elementos de un sistema operativo, identificando las funciones de cada uno de ellos, teniendo en cuenta sus especificaciones técnicas.

CE1.4 Clasificar sistemas operativos y versiones que se utilizan en un equipo informático detallando sus características y diferencias, según unas especificaciones técnicas.

CE1.5 Describir el proceso de instalación de un sistema operativo, identificando los requisitos del equipo informático.

CE1.6 En un supuesto práctico de instalación y configuración de un sistema operativo en un equipo microinformático, comprobando requisitos y según objetivos de uso y de acuerdo con unas especificaciones:

- Verificar los requisitos de instalación de un sistema operativo tales como suficiencia de recursos y compatibilidad en el equipo destino de la instalación, consultando los requisitos del sistema y versión a instalar en su documentación técnica, cotejándolos con el 'hardware'.
- Preparar un equipo destino de la instalación, habilitando, configurando y particionando los dispositivos de almacenamiento masivo, así como preparando las conectividades necesarias, de acuerdo con la documentación técnica.
- Instalar el sistema operativo, siguiendo los pasos indicados en los manuales de instalación y/o asistentes del mismo, utilizando en su caso una imagen, para obtener un equipo informático en estado funcional.
- Configurar el sistema operativo para su funcionamiento, asignando unos parámetros especificados, tales como la creación de unos usuarios, la configuración de unos parámetros de red, siguiendo lo indicado en la documentación técnica.
- Verificar la instalación, mediante pruebas de arranque y parada, y análisis del rendimiento, para comprobar la funcionalidad del sistema operativo y aplicaciones instaladas.
- Elaborar la documentación de los procesos realizados, indicando sistemas instalados, versión, referencia del equipo o dispositivo e incidencias detectadas y solucionadas, entre otros, siguiendo un modelo de documento o usando una aplicación informática.

CE1.7 Identificar procedimientos a utilizar para automatizar la instalación de sistemas operativos en varios equipos informáticos de las mismas características mediante el uso de herramientas 'software' de clonación y otras herramientas de instalación desasistida.

CE1.8 En un supuesto práctico de instalación y configuración de un sistema operativo en varios equipos microinformáticos con las mismas características, comprobando requisitos y según objetivos de uso y de acuerdo con unas especificaciones:

- Preparar uno de los equipos para instalar el sistema operativo y las utilidades, verificando el 'hardware' requerido.
- Instalar el sistema operativo y los programas de utilidad indicados, configurándolos.
- Seleccionar la herramienta 'software' para realizar el clonado de equipos, procediendo a la obtención de las imágenes del sistema instalado para su posterior distribución.
- Implantar las imágenes obtenidas en varios equipos de iguales características al original, mediante herramientas de gestión de imágenes de disco, para conseguir activar sus recursos funcionales.
- Realizar pruebas de arranque y parada, verificando las instalaciones.
- Documentar el trabajo realizado, indicando sistema instalado, versión, licencia, referencia de equipos o dispositivos e incidencias detectadas y solucionadas, entre otros, siguiendo un modelo de documento o usando una aplicación informática.

C2: Aplicar procedimientos de actualización de un sistema operativo, 'software' de base y herramientas preinstaladas en un equipo informático, usando las herramientas y opciones proporcionadas por el fabricante, atendiendo a unas especificaciones técnicas, para incluir nuevas funcionalidades y solucionar problemas de seguridad.

CE2.1 Identificar componentes 'software' de un sistema operativo susceptibles de reajuste para realizar su actualización, teniendo en cuenta sus especificaciones técnicas.

CE2.2 Identificar las fuentes de obtención de elementos de actualización de un sistema operativo, clasificándolas para realizar los procesos de implantación de actualizaciones.

CE2.3 Describir procedimientos para la actualización de un sistema operativo, teniendo en cuenta la seguridad y la integridad de la información en el equipo informático.

CE2.4 Determinar servicios y herramientas de asistencia para la actualización tales como sistemas de alerta temprana o servicios de actualización, describiendo el procedimiento de configuración y uso.

CE2.5 En un supuesto práctico de actualización de un sistema operativo, 'software' de base y herramientas preinstaladas en un equipo informático, usando las herramientas y opciones proporcionadas por el fabricante, atendiendo a unas especificaciones técnicas:

- Comprobar las versiones del 'software' de base, complementos del sistema y controladores de dispositivos, utilizando las opciones y herramientas del propio sistema.
- Seleccionar el 'software' de base, complementos del sistema y controladores de dispositivos con versiones obsoletas, anotando aquellos que no se ajustan a los requerimientos, para proceder a su actualización.
- Instalar complementos y 'parches' para el funcionamiento del 'software' de base, previa comprobación de requisitos técnicos, siguiendo los pasos indicados por el fabricante, configurándolos, para mantener la seguridad y funcionalidad en el sistema.
- Verificar la actualización, mediante pruebas de arranque y parada y análisis de rendimiento, para comprobar la funcionalidad de sistema operativo y aplicaciones.
- Elaborar la documentación de los procesos realizados, indicando sistema operativo, aplicaciones y complementos actualizados y sus versiones, la referencia del equipo o dispositivo e incidencias detectadas y solucionadas, entre otros.

C3: Aplicar procesos de mantenimiento del sistema operativo, 'software' de base y aplicaciones estándar, mediante revisión, verificación y monitorización, teniendo en cuenta las necesidades de uso, para detectar problemas y solucionarlos en su caso, en condiciones de calidad y seguridad.

CE3.1 Describir el sistema de archivos, explicando sus características y objetivos y las herramientas de gestión del almacenamiento, tales como herramientas de particionado y de tratamiento de errores físicos y lógicos.

CE3.2 Explicar el sistema de gestión de usuarios y grupos, describiendo las políticas de seguridad aplicables.

CE3.3 Describir procedimientos de copia de seguridad, clasificando los tipos de copia, explicando los pasos a seguir en cada caso, para salvaguardar la integridad y disponibilidad de un sistema.

CE3.4 Describir herramientas de monitorización de los recursos 'hardware' del sistema microinformático, tales como memoria RAM, procesos activos, espacio en disco, CPU y Entrada/Salida, entre otros, explicando los procedimientos de uso.

CE3.5 Explicar el proceso de configuración de las opciones de accesibilidad de un sistema operativo, para facilitar el uso del equipo microinformático a personas con discapacidades, indicando los parámetros configurables y su funcionalidad.

CE3.6 Describir la configuración de un entorno de trabajo, tal como selección de fuentes, ajuste de la resolución del monitor, inclusión de accesos directos, aplicaciones de inicio y aspecto en general, indicando las opciones disponibles y su objetivo.

CE3.7 Enumerar las aplicaciones proporcionadas por un sistema operativo para la explotación de las funcionalidades de los dispositivos asociados al sistema, señalando sus características.

CE3.8 Clasificar mensajes y avisos proporcionados por el sistema microinformático para discriminar su importancia y criticidad, y explicar el proceso de respuesta según el tipo de alarma.

CE3.9 En un supuesto práctico de mantenimiento de un sistema operativo, 'software' de base y aplicaciones estándar en un equipo microinformático mediante revisión, verificación y monitorización, teniendo en cuenta las necesidades de uso:

- Verificar el sistema de archivos, reconfigurando particiones en caso necesario y limpiando errores físicos, lógicos u otros, utilizando las utilidades, herramientas e interfaces que proporciona el sistema operativo, siguiendo unas especificaciones técnicas y según necesidades de operación.
- Monitorizar el rendimiento y el uso de recursos 'hardware' dentro del equipo, tales como uso de CPU, uso de RAM, memoria de intercambio y datos SMART, entre otros, según necesidades de operación, generando alarmas y notificaciones mediante la utilización de herramientas para dicha función.
- Revisar las políticas de seguridad de usuarios y grupos, cotejándolas con unas políticas dadas, para garantizar su vigencia y, en su caso, para realizar las modificaciones correspondientes.
- Activar medidas de seguridad preventivas tales como copias de seguridad periódicas de la información en un servidor de 'backup', comprobando que el proceso de restauración desde esos servidores es funcional, para mantener la integridad de la información y la continuidad en la explotación.- Comprobar el uso y gestión, por parte de los usuarios, de los dispositivos conectados directamente o por red al sistema microinformático, verificando que se realiza según la documentación técnica y procedimientos estipulados para explotar sus funcionalidades y en condiciones de seguridad.

- Detectar problemas, interpretando los mensajes resultantes de la ejecución del 'software' de base tales como los registros 'log' del sistema u otros, mediante la consulta de los manuales o la documentación proporcionada por el fabricante, entre otros.
- Corregir los problemas detectados, aplicando soluciones según las necesidades en cada caso, teniendo en cuenta las señales de problema detectadas y su diagnóstico, siguiendo procedimientos del fabricante.
- Documentar el trabajo realizado, indicando las incidencias surgidas y las soluciones aplicadas, utilizando un modelo de documento, para su archivo y posterior consulta.

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

C1 respecto a CE1.6 y CE1.8; C2 respecto a CE2.5; C3 respecto a CE3.9

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.
Finalizar el trabajo atendiendo a criterios de idoneidad, economía y eficacia.
Adaptarse a situaciones o contextos nuevos.
Respetar los procedimientos y normas internas de la organización.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Arquitectura del ordenador para la gestión del 'software' de base

Esquema funcional de un ordenador: componentes.
Unidad central de proceso (CPU) y elementos que la componen: tipos y características.
Memoria RAM: tipos y características.
Dispositivos de entrada y salida.
Dispositivos de almacenamiento masivo: tipos y características.
Buses internos: características y tipos.
Buses externos: características y tipos.
Correspondencia entre los subsistemas físicos y lógicos de un equipo informático.

2 Sistemas operativos en equipos microinformáticos

Clasificación de los sistemas operativos. Tipos de licencia.
Funciones de un sistema operativo.
Sistemas operativos para equipos microinformáticos: características y utilización.
Modo comando.
Modo gráfico.

3 Instalación de sistemas operativos en equipos microinformáticos

Procedimientos para la instalación de sistemas operativos.
Preparación del soporte: particionado y formateado.
Instalación de sistemas operativos. Procedimientos.
Instalación de drivers y configuraciones de dispositivos.
Creación de usuarios y grupos. Permisos.
Herramientas para la clonación de discos.
Configuración y mantenimiento de copias de seguridad.

Actualización de sistemas operativos. Servidores y herramientas de actualización, servicios y herramientas de alerta temprana.

4 Utilidades del sistema operativo

Características y funciones.

Utilidades del 'software' de base: configuración del entorno de trabajo; administración y gestión de los sistemas de archivos; gestión de procesos y recursos; gestión y edición de archivos; monitorización de recursos; gestión de la seguridad de sistemas operativos y aplicaciones preinstaladas.

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 laborales, accesibilidad universal, igualdad de género 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 del 'software' de base en sistemas microinformáticos, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) 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

Mantenimiento del subsistema físico de sistemas informáticos

Nivel: *2*
Código: *MF0957_2*
Asociado a la UC: *UC0957_2 - Mantener y regular el subsistema físico en sistemas informáticos*
Duración (horas): *150*
Estado: *BOE*

Capacidades y criterios de evaluación

C1: Identificar los componentes físicos del sistema informático detallando sus conexiones y principales indicadores de funcionamiento y estado para obtener parámetros de explotación adecuados, según unas especificaciones establecidas.

CE1.1 Identificar los tipos de componentes físicos del sistema clasificándolos según diferentes criterios: funciones y tipos del dispositivo, entre otros.

CE1.2 Describir las tecnologías de conexión de dispositivos, ranuras de expansión y puertos detallando las características básicas para identificar las posibilidades de interconexión de componentes con el sistema, según especificaciones técnicas.

CE1.3 Describir las técnicas y herramientas de inventario utilizadas en el sistema para realizar el registro de componentes físicos así como los cambios en los mismos según las indicaciones técnicas especificadas.

CE1.4 En un supuesto práctico, debidamente caracterizado, de identificación de los dispositivos físicos que forman el sistema, para clasificarlos y describir su funcionalidad:
- Clasificar los dispositivos según su tipología y funcionalidad.
- Reconocer los indicadores y el estado de funcionamiento de los dispositivos según indicaciones del manual técnico.
- Comprobar el registro de los dispositivos en el inventario y registrar los cambios detectados.
- Relacionar dispositivos físicos con sus respectivos conectores.

C2: Manipular los tipos de material fungible asociando los mismos a los dispositivos físicos, para garantizar su funcionalidad, según especificaciones técnicas.

CE2.1 Describir los tipos de dispositivos que utilizan material fungible como parte de su operativa de funcionamiento para aplicar los procedimientos de control y sustitución del mismo según especificaciones técnicas.

CE2.2 Clasificar los tipos de material fungible atendiendo a criterios de fabricante, de función, de duración, de material, de grado de reutilización y posibilidad de reciclaje entre otros para identificar las características de los mismos.

CE2.3 Identificar las tareas y los problemas de mantenimiento para cada tipo de material fungible según especificaciones técnicas de la documentación asociada.

CE2.4 Explicar la forma de manipular los tipos de materiales fungibles para garantizar la seguridad e higiene en el trabajo según las especificaciones indicadas en la documentación técnica.

CE2.5 Describir los procedimientos de reciclado y tratamiento de residuos de materiales fungibles para cumplir la normativa medioambiental.

CE2.6 En un supuesto práctico, debidamente caracterizado, de manipulación de material fungible para sustituirlo o reponerlo:
- Relacionar el material fungible con los dispositivos físicos correspondientes, según sus especificaciones técnicas.
- Elegir el material fungible para el dispositivo según criterios de funcionalidad y economía.
- Interpretar las señales del dispositivo acerca del material fungible.
- Instalar el material fungible en el dispositivo y hacer pruebas de funcionamiento del dispositivo.
- Aplicar los procedimientos de manipulación del material fungible establecidos: inserción, extracción, manipulación para el reciclado y manipulación para la recarga de una unidad fungible, entre otros.
- Documentar los procesos realizados.

C3: Regular el rendimiento de los dispositivos físicos utilizando herramientas de monitorización, siguiendo unas especificaciones dadas.

CE3.1 Detallar los componentes críticos que afectan al rendimiento del sistema informático, para identificar las causas de posibles deficiencias en el funcionamiento del equipo, según especificaciones técnicas.

CE3.2 Explicar los tipos de métricas utilizadas para la realización de pruebas y determinación del rendimiento de dispositivos físicos, según especificaciones técnicas de los propios dispositivos.

CE3.3 Identificar los parámetros de configuración y rendimiento de los dispositivos físicos del sistema para optimizar la funcionalidad y calidad en los servicios desempeñados por el equipo informático teniendo en cuenta parámetros de calidad y rendimiento.

CE3.4 Describir las herramientas de medida del rendimiento físico y monitorización del sistema, clasificando las métricas disponibles en cada caso, para aplicar los procedimientos de evaluación en los elementos del sistema informático, según especificaciones técnicas recibidas.

CE3.5 Aplicar procedimientos de medida del rendimiento físico utilizando las herramientas indicadas para comprobar que la funcionalidad del sistema informático está dentro de parámetros prefijados, según unas especificaciones técnicas dadas.

CE3.6 Aplicar procedimientos de verificación y detección de anomalías en los registros de eventos y alarmas de rendimiento en los dispositivos físicos para su notificación al administrador del sistema, siguiendo unas especificaciones técnicas dadas.

CE3.7 En un supuesto práctico, debidamente caracterizado, de evaluación del rendimiento de los dispositivos físicos del sistema para comprobar su funcionalidad y operatividad, según especificaciones de rendimiento dadas:
- Seleccionar la herramienta de medición según especificaciones dadas o indicaciones del administrador.
- Ejecutar procedimientos de medida utilizando la herramienta seleccionada.
- Revisar los resultados obtenidos para comprobar que las medidas están dentro de los parámetros normales, y actuar según procedimientos establecidos ante situaciones anómalas.
- Realizar cambios de configuración en los dispositivos físicos indicados de acuerdo con especificaciones recibidas.
- Registrar en el inventario los cambios de configuración realizados.
- Documentar el trabajo realizado detallando las situaciones anómalas detectadas.

C4: Interpretar las incidencias y alarmas detectadas en el subsistema físico y realizar acciones correctivas para su solución siguiendo unas especificaciones dadas.

CE4.1 Identificar incidencias de funcionamiento producidas por los dispositivos físicos que forman el subsistema para clasificar las acciones correctivas a aplicar según las especificaciones recibidas.

CE4.2 Explicar las estrategias para detectar situaciones anómalas en el funcionamiento del subsistema.

CE4.3 Aplicar procedimientos para la detección de incidencias mediante el uso de herramientas específicas y el control de los indicadores de actividad de los dispositivos físicos del sistema teniendo en cuenta las especificaciones técnicas de funcionamiento.

CE4.4 Aplicar procedimientos establecidos de respuesta para la resolución de incidencias detectadas en el funcionamiento y rendimiento de los dispositivos físicos según unas especificaciones dadas.

CE4.5 En un supuesto práctico, debidamente caracterizado, de ejecución de acciones correctivas para solucionar el mal funcionamiento de dispositivos físicos del sistema, dados unos procedimientos a aplicar:

- Llevar a cabo procedimientos de medida utilizando la herramienta seleccionada.
- Comprobar las conexiones de los dispositivos.
- Comparar los resultados de las medidas con los resultados esperados para comprobar si se ha producido o no una incidencia.
- Sustituir o actualizar el componente o dispositivo causante de la avería asegurando su compatibilidad con el sistema.
- Ejecutar procedimientos establecidos de respuesta ante las incidencias producidas.
- Registrar en el inventario las acciones correctivas y documentar el trabajo realizado detallando las situaciones de incidencia producidas.

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

C1 respecto a CE1.4; C2 respecto a CE2.3 y CE2.6; C3 respecto a CE3.7; C4 respecto a CE4.5.

Otras Capacidades:

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.
Respetar los procedimientos y normas internas de la organización.

Contenidos

1 Componentes de un sistema informático

La unidad central de proceso: funciones y tipos, propósito y esquema de funcionamiento y estructura interna.

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

El sistema de E/S: funciones y tipos, controladores de E/S, dispositivos periféricos, dispositivos de almacenamiento y dispositivos de impresión, entre otros.

Conexión entre componentes.

Puertos y conectores.

2 Técnicas de inventario en sistemas informáticos

Registros de inventario de dispositivos físicos.
Herramientas software de inventario del sistema informático.

3 Material fungible de dispositivos físicos en un sistema informático

Dispositivos con material fungible.
Clasificación del material fungible.
Mantenimiento de material fungible.
Reciclaje y reutilización.

4 Técnicas de monitorización y medida de rendimiento de los dispositivos físicos

Métricas de rendimiento.
Representación y análisis de los resultados de las mediciones.
Rendimiento de los dispositivos físicos.
Parámetros de configuración y rendimiento.
Herramientas de monitorización de dispositivos físicos.

5 Técnicas de diagnóstico de incidencias y alarmas del subsistema físico

Clasificación de incidencias y alarmas de los dispositivos físicos.
Herramientas de diagnóstico de incidencias y alarmas de los dispositivos físicos.
Métodos establecidos para solución incidencias.

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 mantenimiento y la regulación del subsistema físico en 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

Mantenimiento del subsistema lógico de sistemas informáticos

Nivel:	*2*
Código:	*MF0958_2*
Asociado a la UC:	*UC0958_2 - Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de cliente*
Duración (horas):	*150*
Estado:	*BOE*

Capacidades y criterios de evaluación

C1: Identificar los componentes software de un sistema informático detallando sus características y los parámetros de configuración, según unas especificaciones funcionales dadas.

CE1.1 Citar los tipos de software para realizar su clasificación según el propósito, las funciones y los modos de ejecución entre otros, según las especificaciones técnicas de fabricantes de software.

CE1.2 Describir las características de los componentes software del sistema, distinguiendo sus funcionalidades, teniendo en cuenta las especificaciones técnicas.

CE1.3 Explicar y describir los tipos de interfaces de usuario discriminando las principales características de cada uno de ellos, según especificaciones técnicas de los sistemas utilizados.

CE1.4 Identificar los elementos de configuración de los componentes software para garantizar el funcionamiento del sistema, según especificaciones recibidas.

CE1.5 En un supuesto práctico, debidamente caracterizado, de identificación de componentes software del sistema para su utilización, según unas especificaciones dadas:

- Operar con la interfaz de usuario del componente software utilizando los mecanismos habituales para cada tipo.
- Operar con las opciones funcionales de cada componente software según indicaciones de la documentación técnica.
- Identificar la configuración de un componente software según indicaciones de procedimientos establecidos.
- Comprobar el registro de un componente software en el inventario y registrar los cambios detectados.
- Comprobar las licencias de utilización del software teniendo en cuenta los derechos de autor y la normativa aplicable.

C2: Instalar y actualizar programas del software de aplicación para ofrecer funcionalidades a los usuarios, siguiendo unas especificaciones dadas.

CE2.1 En un supuesto práctico, debidamente caracterizados, realizar la instalación de componentes software de aplicación para añadir funcionalidad al sistema:

- Comprobar los requisitos de instalación del software a implantar en el sistema.
- Verificar que las licencias de utilización de los componentes software cumplen la normativa aplicable.
- Realizar los procedimientos de instalación de componentes.

- Configurar los componentes software instalados para utilizar los periféricos y dispositivos del sistema informático.
- Realizar los procedimientos de desinstalación de componentes software, si fuera necesario.
- Verificar los procesos realizados y la ausencia de interferencias con el resto de componentes del sistema.
- Documentar los procesos de instalación y desinstalación realizados detallando las actividades realizadas.
- Mantener el inventario de software actualizado registrando los cambios realizados.

CE2.2 Enumerar los principales procedimientos para mantener el software actualizado, según las especificaciones técnicas del tipo de software y del fabricante.

CE2.3 Describir los procedimientos, para aplicar una actualización, detallando los problemas de seguridad en la instalación y actualización de software para mantener los parámetros funcionales del equipo.

CE2.4 En un supuesto práctico, debidamente caracterizado, de actualización de software de aplicación en un sistema para reajustarlo a las nuevas necesidades:
- Identificar la versión del componente software a actualizar y los condicionantes de compatibilidad a tener en cuenta para la actualización.
- Localizar las actualizaciones, puesta a disposición por el fabricante, aún no implantadas e identificar los "parches" y otros módulos de código disponibles para aumentar la funcionalidad del componente o para corregir un comportamiento no adecuado, comprobando que las licencias de utilización de los componentes software cumplen la normativa aplicable.
- Desinstalar los componentes implicados antes de aplicar alguna actualización, según indicaciones de la documentación técnica, procedimientos establecidos e indicaciones del administrador.
- Aplicar las actualizaciones anteriormente identificadas al componente software según indicaciones de la documentación técnica, procedimientos establecidos e indicaciones del administrador, configurando el componente software de acuerdo con las especificaciones dadas después de la actualización.
- Verificar que el componente software tiene la funcionalidad deseada realizando pruebas de funcionamiento.
- Documentar el proceso de actualización detallando las incidencias producidas y mantener el inventario de software actualizado registrando los cambios.

C3: Aplicar procedimientos de administración y mantener el funcionamiento del sistema dentro de unos parámetros especificados, según unas especificaciones técnicas dadas y necesidades de uso.

CE3.1 Identificar las herramientas administrativas disponibles en el sistema detallando sus características y usos, para realizar los procedimientos de administración.

CE3.2 Explicar los tipos de soportes físicos para el almacenamiento de información detallando las tareas para el mantenimiento de sus estructuras de datos.

CE3.3 Describir los tipos de tareas de administración de sistemas informáticos detallando sus características, modos de ejecución y mecanismos disponibles, para su ejecución automática teniendo en cuenta las especificaciones técnicas.

CE3.4 Citar las técnicas de mantenimiento de la configuración del software de base y de aplicación que se necesitan para mantener la operatividad del sistema.

CE3.5 En un supuesto práctico, debidamente caracterizado, de mantenimiento de los componentes del sistema, siguiendo unas especificaciones dadas:
- Seleccionar la herramienta administrativa apropiada.

- Aplicar procedimientos establecidos para el mantenimiento de los soportes de información y para el mantenimiento de la configuración del software de base y de aplicación.
- Configurar y verificar el funcionamiento de los dispositivos instalados desde el software de aplicación.
- Ejecutar y comprobar la programación de las tareas administrativas automáticas.
- Ejecutar programas y guiones administrativos según indicaciones del administrador.
- Documentar todos los procedimientos aplicados detallando las incidencias detectadas y mantener el inventario de software actualizado registrando los cambios.

C4: Identificar los parámetros de rendimiento del software base y de aplicación utilizando técnicas y herramientas específicas de monitorización y medida para verificar la calidad y funcionalidad de los servicios prestados por el sistema informático.

CE4.1 Explicar los fundamentos de la medida del rendimiento de software detallando las técnicas utilizadas para la evaluación de la funcionalidad del sistema.

CE4.2 Identificar los parámetros de configuración y rendimiento de los elementos del software base y de aplicación, para monitorizar el sistema.

CE4.3 Describir las herramientas de medida del rendimiento del software, clasificando las métricas disponibles en cada caso, teniendo en cuenta las especificaciones técnicas asociadas.

CE4.4 Explicar las técnicas de monitorización y medida efectuadas por las herramientas, para mejorar el rendimiento del software base y de aplicación, teniendo en cuenta las especificaciones técnicas asociadas.

CE4.5 Aplicar procedimientos de verificación y detección de anomalías en los registros de eventos y alarmas de rendimiento en el software, para su notificación al administrador del sistema, siguiendo unas especificaciones dadas.

CE4.6 En un supuesto práctico, debidamente caracterizado, de medición del rendimiento del software base y aplicación para detectar situaciones anómalas:
- Seleccionar la herramienta de medición según indicaciones del administrador.
- Ejecutar procedimientos de medida utilizando la herramienta seleccionada.
- Revisar los resultados obtenidos para comprobar que las medidas están dentro de los parámetros normales.
- Documentar el trabajo realizado.

C5: Identificar las incidencias y alarmas detectadas en el subsistema lógico para realizar acciones correctivas según unas especificaciones dadas.

CE5.1 Clasificar las incidencias y alarmas de funcionamiento y acceso producidas en los elementos software del sistema para detectar problemas de funcionamiento en el software.

CE5.2 Clasificar las herramientas de diagnóstico a utilizar para aislar la causa que produce la alerta o incidencia, teniendo en cuenta los procedimientos de resolución de incidencias dados.

CE5.3 Aplicar procedimientos especificados de respuesta para atender incidencias detectadas en el funcionamiento del software base y aplicación, siguiendo las instrucciones dadas.

CE5.4 En un supuesto práctico, debidamente caracterizado, de aplicación de acciones correctivas para solventar el mal funcionamiento del software base y aplicación:
- Identificar las incidencias detectadas en el funcionamiento del software base o de aplicación.
- Utilizar herramientas de diagnóstico en caso de mal funcionamiento del software.
- Ejecutar procedimientos establecidos de respuesta ante las incidencias producidas.
- Utilizar herramientas de gestión local o remota del sistema para resolver la incidencia.
- Documentar el trabajo realizado detallando las situaciones de incidencia producidas.

- Mantener el inventario de software actualizado registrando las incidencias y los cambios realizados.

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

C1 respecto a CE1.5; C2 respecto a CE2.1 y CE2.4; C3 respecto a CE3.5; C4 respecto a CE4.6; C5 respecto a CE5.4.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Mantener una actitud proactiva orientada a la mejora de procesos.
Demostrar resistencia al estrés, estabilidad de ánimo y control de impulsos.
Actuar con rapidez en situaciones problemáticas y no limitarse a esperar.

Contenidos

1 El software en el sistema informático

Tipos de software.
Software de sistema y software de usuario.
Funciones y características.

2 Procedimientos para la instalación de componentes software

Requisitos del sistema.
Licencias de propiedad, uso y distribución del software.
El inventario de software.
Parámetros y configuración del sistema en el proceso de instalación.
Registros y bases de datos del software instalado.
Configuración de aplicaciones para el acceso a periféricos.

3 Procedimientos de mantenimiento de software

Objetivos de un plan de mantenimiento.
Actualización del software de aplicación, verificación de requisitos y procesos de actualización.

4 Procedimientos de administración

Tipos de tareas administrativas.
Herramientas administrativas.
Mantenimiento del sistema de archivos y soportes de información.
Tareas programadas.

5 Técnicas de monitorización y medida del rendimiento de los elementos de software

Parámetros de configuración y rendimiento de los componentes software.
Herramientas de monitorización de software.
Procedimientos de medida del rendimiento.

6 Incidencias y alarmas del software del sistema informático

Clasificación de incidencias y alarmas del software.
Herramientas de diagnóstico de incidencias y alarmas de software.
Métodos establecidos para la solución de problemas de software.

Mantenimiento remoto: herramientas y configuración.

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 ejecución de procedimientos de administración y mantenimiento en el software base y de aplicación de cliente, 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

Mantenimiento de la seguridad en sistemas informáticos

Nivel: *2*
Código: *MF0959_2*
Asociado a la UC: *UC0959_2 - Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos*
Duración (horas): *120*
Estado: *BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de copia de seguridad y restauración, verificar su realización y manipular los medios de almacenamiento para garantizar la integridad de la información del sistema informático, siguiendo unas especificaciones dadas.

CE1.1 Clasificar los distintos medios de almacenamiento y seguridad de datos del sistema informático para utilizarlos en los procesos de copia en función de especificaciones técnicas establecidas.

CE1.2 Explicar los procedimientos y herramientas para la realización, restauración y verificación de copias de seguridad y almacenamiento de datos del sistema informático para garantizar la integridad de la información del sistema, según unas especificaciones dadas.

CE1.3 En un supuesto práctico, debidamente caracterizado, en el que se dispone de un sistema de almacenamiento de datos con varios dispositivos, de realización de copias de seguridad para garantizar la integridad de los datos, dados unos procedimientos a seguir:
- Seleccionar el dispositivo de almacenamiento y la herramienta para realizar la copia.
- Realizar la copia de seguridad según la periodicidad y el procedimiento especificado, o bien a indicación del administrador.
- Verificar la realización de la copia.
- Etiquetar la copia realizada y proceder a su almacenamiento según las condiciones ambientales, de ubicación y de seguridad especificadas.
- Comprobar y registrar las incidencias detectadas.
- Documentar los procesos realizados.

CE1.4 En un supuesto práctico, debidamente caracterizado, de restauración de copias de seguridad para recuperar la información almacenada, dados unos procedimientos a seguir:
- Seleccionar la herramienta para realizar la restauración de acuerdo con el tipo y soporte de copia de seguridad realizada.
- Realizar el proceso de restauración según las indicaciones recibidas.
- Verificar el proceso de restauración comprobando el su destino de la misma.
- Comprobar y registrar las incidencias detectadas.
- Documentar los procesos realizados.

C2: Identificar los tipos de acceso al sistema informático, así como los mecanismos de seguridad del mismo, describiendo sus características principales y

herramientas asociadas más comunes para garantizar el uso de los recursos del sistema.

CE2.1 Describir los mecanismos del sistema de control de acceso detallando la organización de usuarios y grupos para garantizar la seguridad de la información y funcionalidades soportadas por el equipo informático, según las especificaciones técnicas.

CE2.2 Explicar los procedimientos de los sistemas para establecer permisos y derechos de usuarios, detallando su organización y herramientas administrativas asociadas para organizar políticas de seguridad, según los procedimientos establecidos en el software base.

CE2.3 Clasificar los mecanismos de seguridad comunes en sistemas detallando sus objetivos, características y herramientas asociadas para garantizar la seguridad de la información y funcionalidades soportadas por el equipo informático.

CE2.4 Identificar los mecanismos de protección del sistema contra virus y programas maliciosos para asegurar su actualización.

CE2.5 En un supuesto práctico, debidamente caracterizado, de identificación de mecanismos de seguridad del sistema para mantener la protección del mismo:

- Identificar los usuarios y grupos definidos en el sistema mediante las herramientas administrativas indicadas en los procedimientos dados.
- Localizar, para cada usuario, los permisos de acceso y las políticas de seguridad asociadas, operando con las herramientas administrativas indicadas en los procedimientos dados.
- Verificar que las aplicaciones antivirus y de protección contra programas maliciosos están actualizadas.
- Comprobar el registro de los usuarios y grupos en el inventario, registrando los cambios detectados.

C3: Interpretar las trazas de monitorización de los accesos y actividad del sistema identificando situaciones anómalas, siguiendo unas especificaciones dadas.

CE3.1 Enumerar los mecanismos del sistema de trazas de acceso y de actividad para su monitorización detallando su ámbito de acción, características principales y herramientas asociadas.

CE3.2 Describir las incidencias producidas en el acceso de usuarios y de actividad del sistema clasificándolas por niveles de seguridad para detectar situaciones anómalas en dichos procesos.

CE3.3 Identificar las herramientas para extraer los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para facilitar su consulta y manipulación, de acuerdo a sus especificaciones técnicas.

CE3.4 Interpretar el contenido de ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para localizar accesos y actividades no deseadas siguiendo el procedimiento indicado por el administrador.

CE3.5 En un supuesto práctico, debidamente caracterizado, de análisis y la evaluación de ficheros de traza de conexión de usuarios y ficheros de actividad del sistema para detectar posibles accesos y actividades no deseadas, según unas especificaciones dadas:

- Identificar las características de un conjunto de registros de usuarios.
- Localizar un registro de un usuario dado y explicar sus características.
- Extraer y registrar las situaciones anómalas relativas a un usuario.
- Documentar las acciones realizadas.

CE3.6 Distinguir las herramientas utilizadas para el diagnóstico y detección de incidencias tanto en aplicación local como remota, para su gestión, solución o escalado de las mismas, según unas especificaciones dadas.

C4: Describir las condiciones ambientales y de seguridad para el funcionamiento de los equipos y dispositivos físicos que garanticen los parámetros de explotación dados.

CE4.1 Describir los factores ambientales que influyen en la ubicación y acondicionamiento de espacios de dispositivos físicos, material fungible y soportes de información para cumplimentar los requisitos de instalación de dispositivos, según las especificaciones técnicas de los mismos.

CE4.2 Identificar los factores de seguridad y ergonomía a tener en cuenta en la ubicación de equipos y dispositivos físicos para garantizar sus condicionantes de implantación, según sus especificaciones técnicas.

CE4.3 En un supuesto práctico, debidamente caracterizado, de comprobación de las condiciones ambientales para asegurar la situación de equipos y dispositivos físicos:

- Comprobar que la ubicación de los dispositivos físicos, material fungible y soportes de información cumplen las normas establecidas y las especificaciones técnicas.
- Comprobar el registro de ubicación de dispositivos físicos y material fungible en el inventario, registrando los cambios detectados.
- Identificar las condiciones de seguridad y ambientales adecuadas y no adecuadas.
- Proponer acciones correctivas para asegurar los requisitos de seguridad y de condiciones ambientales.

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

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

Otras Capacidades:

Actuar con rapidez en situaciones problemáticas y no limitarse a esperar.
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.
Mantener una actitud proactiva orientada a la mejora de procesos.

Contenidos

1 Gestión de la seguridad informática

Objetivo de la seguridad.
Procesos de gestión de la seguridad.
Métodos de identificación de amenazas: atacante externo e interno.

2 Seguridad lógica del sistema

Sistemas de ficheros y control de acceso.
Permisos y derechos de usuarios.
Registros de usuarios: sistemas de autenticación débiles; sistemas de autenticación fuertes; sistemas de autenticación biométricos y otros sistemas.
Herramientas para la gestión de usuarios.
Software de detección de virus y programas maliciosos, técnicas de recuperación y desinfección de datos afectados.

Herramientas de gestión remota de incidencias.

3 Copias de seguridad

Tipos de copias.
Arquitectura del servicio de copias de respaldo.
Medios de almacenamiento para copias de seguridad.
Herramientas para la realización de copias de seguridad.
Restauración de copias y verificación de la integridad de la información.

4 Procedimientos de monitorización de los accesos y la actividad del sistema

Objetivos de la monitorización.
Procedimientos de monitorización de trazas: aspectos monitorizables o auditables; clasificación de eventos e incidencias: de sistema, de aplicación, de seguridad; mecanismos de monitorización de trazas: alarmas y acciones correctivas; información de los registros de trazas.
Técnicas y herramientas de monitorización.
Informes de monitorización.

5 Entorno físico de un sistema informático

Los equipos y el entorno: adecuación del espacio físico.
Reglamentos y normativas aplicables.
Agentes externos y su influencia en el sistema.
Efectos negativos sobre el sistema.
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.
Factores de riesgo: conceptos de seguridad eléctrica; requisitos eléctricos de la instalación; perturbaciones eléctricas y electromagnéticas; electricidad estática; otros factores de riesgo.
Los aparatos de medición.
Acciones correctivas para asegurar requisitos de seguridad y ambientales.

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 mantenimiento de la seguridad de los subsistemas físicos y lógicos en 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.