CUALIFICACIÓN PROFESIONAL:
Gestión de sistemas informáticos

Familia Profesional:	***Informática y Comunicaciones***
Nivel:	***3***
Código:	***IFC152_3***
Estado:	***BOE***
Publicación:	***RD 917/2024***
Referencia Normativa:	***Orden PRE/1636/2015, RD 1087/2005***

Competencia general

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

Unidades de competencia

UC0484_3: Administrar los dispositivos "hardware" de un sistema informático
UC0485_3: Gestionar el "software" de un sistema informático
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 omnicomprensivo de mujeres y hombres.

- Técnicos en administración de equipos informáticos
- Administradores de equipos informáticos

Formación Asociada (420 horas)

Módulos Formativos

MF0484_3: Administración de los dispositivos "hardware" de un sistema informático (150 horas)

MF0485_3: Gestión del "software" de un sistema informático (150 horas)
MF0486_3: SEGURIDAD EN EQUIPOS INFORMÁTICOS (120 horas)

UNIDAD DE COMPETENCIA 1

Administrar los dispositivos "hardware" de un sistema informático

Nivel: *3*
Código: *UC0484_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Inventariar los dispositivos "hardware" y dispositivos externos conectados al sistema informático, incorporando información tal como, características técnicas (modelo, marca, entre otros), ubicación, estado, entre otras, siguiendo el procedimiento establecido en la organización para asegurar su localización física y disponibilidad.

CR1.1 Los dispositivos "hardware" (procesador, memoria, entre otros) y los dispositivos externos (impresora, monitor, entre otros) se identifican, describiendo sus características técnicas específicas, estado, disponibilidad, entre otros.

CR1.2 El alta de los dispositivos "hardware" y externos al sistema se registra en el inventario, cumplimentando información tal como, marca, modelo, ubicación, estado, entre otros y haciendo uso de las herramientas específicas (formularios, aplicaciones "software", entre otros) indicadas por la organización.

CR1.3 Los detalles técnicos y específicos de funcionamiento de los dispositivos "hardware" del sistema se incorporan, completando el inventario con la documentación técnica del fabricante, como manuales de configuración y de uso, entre otros.

CR1.4 El inventario se revisa, comprobando que las modificaciones realizadas en los dispositivos "hardware" del sistema (internos y externos), están reflejadas en la ficha de inventario del dispositivo correspondiente.

RP2: Gestionar los dispositivos "hardware" (procesador, memoria, entre otros), monitorizando y analizando sus parámetros de funcionamiento, haciendo uso de herramientas "software" de monitorización para garantizar el funcionamiento del sistema informático.

CR2.1 Las herramientas de monitorización a utilizar se seleccionan, teniendo en cuenta el dispositivo "hardware" (procesador, memoria, entre otros) a monitorizar y el sistema informático en el que se encuentran instalados.

CR2.2 La herramienta de gestión y monitorización se configura, añadiendo los dispositivos "hardware" a monitorizar y comprobando la recepción de valores en los parámetros específicos de funcionamiento.

CR2.3 Los dispositivos se monitorizan, comprobando que los valores de funcionamiento obtenidos en las herramientas de monitorización no muestran alertas de fallo o bajo rendimiento.

CR2.4 Las alertas de funcionamiento inadecuado se registran, clasificándolas por prioridades y asignándolas a la persona o equipo responsable de la reparación.

RP3: Planificar actualizaciones de "firmware", comprobando las versiones actuales instaladas en el sistema informático, obteniendo las nuevas e instalándolas, siguiendo los procedimientos establecidos por la organización, para garantizar la seguridad y funcionamiento de los dispositivos "hardware" del sistema.

CR3.1 Los dispositivos "hardware" ("firewall", "router", entre otros) se revisan, comprobando la versión de "firmware" instalada.

CR3.2 Las actualizaciones de "firmware" a realizar se clasifican, estableciendo prioridades para su ejecución, atendiendo a la urgencia en el impacto del rendimiento, errores o seguridad, entre otros.

CR3.3 La nueva versión de "firmware" se comprueba en un entorno de pruebas, configurando un dispositivo "hardware" de las mismas características técnicas al dispositivo a actualizar, instalando la nueva versión de "firmware", comprobando que el dispositivo queda operativo y estableciendo el procedimiento técnico de vuelta atrás.

CR3.4 El procedimiento técnico de vuelta atrás se comprueba, aplicando los pasos establecidos en el mismo (desinstalar "software", reconfigurar parámetros, entre otros), comprobando que el dispositivo queda operativo y con la configuración previa a la instalación del nuevo "firmware".

CR3.5 La configuración de los dispositivos de "hardware" se respalda, realizando el proceso de copia de seguridad específico para el dispositivo, conservando y documentando el historial de versiones implementadas.

CR3.6 La actualización del "firmware" del dispositivo se realiza, instalando la nueva versión y documentando el proceso e incidencias producidas.

CR3.7 El sistema informático con las actualizaciones de "firmware" instaladas se comprueba, verificando que los servicios (conexiones VPN, escritorio remoto, entre otros) están operativos y registrando en el inventario las nuevas versiones.

RP4: Implementar soluciones "hardware" de alta disponibilidad, configurando sistemas "cluster", sistemas RAID, entre otros, para disponer de un entorno tolerante a fallos y garantizar la protección y recuperación del sistema ante situaciones imprevistas.

CR4.1 Los dispositivos "hardware" del sistema de alta disponibilidad a instalar se comprueban, verificando que sus características técnicas son compatibles con el entorno "hardware" del sistema informático.

CR4.2 Los dispositivos "hardware" del sistema de alta disponibilidad se instalan, configurándolos y verificando que son reconocidos por el sistema informático.

CR4.3 Las simulaciones del plan de contingencias se ejecutan, comprobando que el sistema de alta disponibilidad está operativo y documentando el proceso, siguiendo el procedimiento establecido por la organización (formularios, herramientas "software", entre otros).

CR4.4 El sistema de alta disponibilidad se monitoriza, comprobando la ausencia de alertas y reportando las incidencias detectadas.

CR4.5 Los dispositivos "hardware" del sistema de alta disponibilidad con incidencias se reparan, sustituyéndolos por otros de las mismas características técnicas.

CR4.6 Las incidencias del sistema de alta disponibilidad y las soluciones aportadas se documentan, generando informes para uso posterior, siguiendo el procedimiento establecido por la organización (formularios, herramientas "software", entre otros).

RP5: Implementar mejoras del sistema informático, analizando sus necesidades de crecimiento y las características técnicas del "hardware" disponible en el mercado, para asegurar el funcionamiento y rendimiento del sistema ante futuros incrementos en la carga de trabajo.

CR5.1 Los dispositivos "hardware" del entorno de producción se analizan, comprobando sus características técnicas y comparándolas con las requeridas por la organización para asumir incrementos futuros de carga de trabajo o número de usuarios.

CR5.2 Las necesidades de actualización y ampliación del sistema informático se recopilan, mediante informes de su rendimiento, informes sobre futuros incrementos en la carga de trabajo y número de usuarios, entre otros, analizándolas y realizando propuestas de actualización del "hardware".

CR5.3 El "hardware" disponible en el mercado se evalúa, analizando sus características técnicas, proponiendo el que satisface las necesidades de actualización y escalabilidad del sistema informático de la organización.

CR5.4 La actualización del "hardware" del sistema informático se implementa, planificando su instalación, configuración y documentando el proceso e incidencias.

CR5.5 El sistema informático actualizado y ampliado se revisa, monitorizando sus parámetros de funcionamiento, comprobando que no muestran alertas de fallo o bajo rendimiento.

CR5.6 Los cambios en el sistema informático se registran documentando las características técnicas del nuevo "hardware", su configuración, entre otros, según el procedimiento establecido por la organización (formularios, herramientas "software", entre otros).

CR5.7 Los residuos generados tras la implementación de mejoras en el sistema informático se gestionan, separando los residuos según su tipología, disponiéndolos en sus contenedores y clasificando los RAEE (Residuos de Aparatos Eléctricos y Electrónicos) para su reparación, reutilización de sus componentes y materiales o su recogida por gestores autorizados.

Contexto profesional

Medios de producción

Equipos informáticos y dispositivos externos conectados. 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 actualizado del "hardware" del sistema y su configuración. Sistema informático operativo, monitorizado y verificado. Sistema informático con "firmware" actualizado. Soluciones de alta disponibilidad implantadas. Soluciones de actualización y crecimiento del sistema informático implantadas.

Información utilizada o generada

Inventario de "hardware". Manuales técnicos de instalación y configuración de dispositivos "hardware". Información técnica del "hardware" de equipos informáticos. Documentación o manuales de uso y funcionamiento del sistema informático. Plan de mantenimiento. Relación de incidencias. Recomendaciones de mantenimiento de los fabricantes y soportes técnicos de asistencia. Catálogos de

productos "hardware", proveedores, precios. Normativa sobre protección de datos. Normativa sobre servicios de la sociedad de información. Normativa sobre prevención de riesgos laborales. Normativa medioambiental. Normativa aplicable sobre residuos de aparatos eléctricos y electrónicos.

UNIDAD DE COMPETENCIA 2

Gestionar el "software" de un sistema informático

Nivel: *3*
Código: *UC0485_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Instalar el sistema operativo en un sistema informático, estableciendo valores a sus parámetros de configuración, para asegurar su funcionalidad.

CR1.1 La máquina física o virtual, donde se instalará el sistema operativo se prepara, configurando el "hardware" (espacio libre en disco, memoria RAM, entre otros) requerido según las necesidades de uso.

CR1.2 El sistema operativo se instala, configurando parámetros de red, controladores de dispositivos "hardware" del equipo informático, entre otros, siguiendo los procedimientos estándar de la organización (plantillas, herramientas "software", entre otros) y la documentación técnica de referencia.

CR1.3 Los dispositivos "hardware" del sistema (procesador, memoria, entre otros) y sus controladores se verifican, realizando pruebas de arranque y parada, utilizando herramientas "software" de diagnóstico y verificación, comprobando la no existencia de incidencias en su funcionamiento.

CR1.4 El sistema operativo se configura, asignando valores a parámetros tales como dominio, nombre de equipo o grupo de trabajo, entre otros y haciendo uso de las herramientas que ofrece el sistema operativo.

CR1.5 Las tareas realizadas e incidencias detectadas durante el proceso de instalación y configuración del sistema operativo se registran, siguiendo procedimiento interno de la organización (plantillas, herramientas "software", entre otros).

RP2: Instalar "software" corporativo y paquetes informáticos de propósito general, estableciendo valores a sus parámetros de configuración y verificando su funcionamiento, siguiendo el plan de explotación de la organización para atender las necesidades de uso del sistema y su seguridad.

CR2.1 Los paquetes de propósito general, tales como, herramientas ofimáticas, navegadores, entre otros, se instalan, comprobando que los requisitos "hardware" y "software" disponibles en el equipo informático son compatibles y suficientes para su instalación y ejecutando el programa de instalación del "software" a instalar.

CR2.2 El "software" corporativo se instala, comprobando que los requisitos "hardware" y "software" disponibles en el equipo informático son compatibles y suficientes, configurando parámetros previos a su instalación.

CR2.3 El "software" corporativo, tal como "software" ERP (Planificación de Recursos Empresariales), bases de datos, entre otros, se configura, estableciendo valores en sus parámetros de configuración.

CR2.4 El acceso a los datos y aplicaciones se configura creando grupos de usuarios y cuentas, entre otros, con privilegios específicos de acceso a los recursos del sistema (datos, aplicaciones, entre otros).

CR2.5 El conjunto del "software" instalado se verifica, realizando pruebas de funcionamiento y compatibilidad, usando las herramientas proporcionadas por el sistema o de terceros.

CR2.6 Los pasos e incidencias del proceso de instalación y configuración se registran, siguiendo las normas establecidas por la organización (plantillas, herramientas "software", entre otros).

RP3: Comprobar el rendimiento del "software" instalado en el equipo informático, estableciendo métricas de rendimiento (estabilidad del sistema, tiempos de respuesta, entre otros), analizando los valores obtenidos y configurando los recursos del sistema para detectar posibles áreas de funcionamiento inapropiado y mejorarlas.

CR3.1 Las métricas de rendimiento del "software" instalado (estabilidad, capacidad de respuesta, velocidad, entre otras) se establecen, especificando parámetros a evaluar, herramientas "software" utilizar, entre otros.

CR3.2 Los datos de rendimiento del sistema se obtienen, utilizando herramientas de diagnóstico y técnicas de análisis de rendimiento, previamente establecidas.

CR3.3 Los datos de rendimiento del sistema informático se analizan, comprobando los valores obtenidos al aplicar las técnicas de análisis, detectando posibles anomalías de funcionamiento (uso elevado de procesador, falta de memoria, entre otros).

CR3.4 La corrección de las anomalías detectadas se programa, estableciendo un plan con las medidas correctivas a realizar (actualizaciones de "software", sustitución de "hardware", entre otros), definiendo prioridades para su ejecución, minimizando el impacto en el servicio a los usuarios.

RP4: Realizar la actualización y reconfiguración de "software" de base y corporativo, instalando paquetes o nuevas versiones, siguiendo el plan de implantación de la organización para minimizar el impacto en el servicio a los usuarios y mantener el funcionamiento del sistema.

CR4.1 La documentación para casos de resolución de contingencias se revisa, comprobando que están actualizados datos como teléfono, correo electrónico, persona de contacto, entre otros, haciéndose público y accesible para los usuarios de la organización.

CR4.2 Las actualizaciones del "software" de base o corporativo se programan, estableciendo la franja horaria para su realización, la persona responsable de llevarla a cabo, servicios que quedarán inactivos, entre otros.

CR4.3 Las paradas de servicio por mantenimiento del sistema se publican, reflejándolas en los medios digitales y físicos, siguiendo los protocolos definidos por la organización (correos electrónicos, anuncios en la intranet, entre otros) para informar a los usuarios afectados.

CR4.4 El "software" de base o corporativo se actualiza, realizando una copia de seguridad de los datos del sistema informático, instalando la nueva actualización, verificando que el sistema queda operativo, así como aplicando procedimientos de vuelta atrás en caso de contingencia.

CR4.5 El proceso de actualización de "software" llevado a cabo, se documenta, registrando los pasos realizados, las incidencias detectadas, siguiendo el procedimiento establecido por la organización (herramientas "software", formularios, entre otros).

RP5: Planificar la realización de copias de seguridad, estableciendo la información o sistemas a respaldar y la frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.

CR5.1 La información de la organización se inventaría, clasificándola en función de su criticidad y de su tipo (datos de sistema o datos de la organización), determinando si necesita ser incorporada en las copias de seguridad y la frecuencia con la que debe salvaguardarse.

CR5.2 El plan de copias de seguridad se establece, teniendo en cuenta el volumen de datos a guardar, su criticidad, el impacto sobre el rendimiento del servidor y la duración de realización de las copias.

CR5.3 Las copias de seguridad se verifican, instalando una de ellas y comprobando que se puede recuperar la información contenida en la misma.

CR5.4 Los dispositivos de almacenamiento (cintas, discos externos, entre otros) se identifican, registrando en el plan de copias de seguridad qué información (fecha de la copia, información respaldada, entre otros) contiene cada dispositivo.

CR5.5 La documentación de los procedimientos de obtención y verificación de copias de seguridad, así como la de los planes de contingencias y resolución de incidencias se confecciona, siguiendo las normas establecidas por la organización (plantillas, herramientas "software", entre otros).

RP6: Inventariar el catálogo "software", incorporando información tal como, número de instalaciones de "software", fechas de instalación, el tipo de "software", siguiendo el procedimiento establecido en la organización para asegurar su localización física y disponibilidad.

CR6.1 El "software" de base y aplicaciones corporativas de la organización se catalogan, registrando información, tal como, número de instalaciones de "software", fechas de instalación, el tipo de "software" instalado, expiración y fechas de renovación de las licencias, entre otros.

CR6.2 El alta en el inventario "software" se realiza, cumplimentando información tal como, número de licencias, tipo "software", ubicación, entre otros y haciendo uso de las herramientas (formularios, herramientas "software" de inventario, entre otros) indicadas por la organización.

CR6.3 El inventario se revisa, comprobando que las modificaciones realizadas en el "software" de los equipos informáticos están reflejadas en la ficha de inventario del "software".

CR6.4 La información de contacto de proveedores y/o compañías de "software" se mantiene, actualizando los datos de persona de contacto, email, entre otros.

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 en un equipo informático instalado, configurado y operativo. "Software" corporativo instalado, configurado y operativo en un sistema informático. Medidas de rendimiento del sistema establecidas, valores de rendimiento obtenidos y analizados y posibles medidas correctivas planificadas

para solventar problemas de rendimiento del sistema informático. "Software" de base y corporativo del sistema informático actualizado y reconfigurado. Copias de seguridad planificadas, verificadas y documentadas. Inventario de "software" revisado y actualizado.

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. Normativa sobre riesgos laborales. Normativa medioambiental.

UNIDAD DE COMPETENCIA 3
ASEGURAR EQUIPOS INFORMÁTICOS

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

Realizaciones profesionales y criterios de realización

RP1: Configurar equipos informáticos siguiendo los procedimientos establecidos en el plan de seguridad de la organización para protegerlos de la pérdida, manipulación y sustracción de información no autorizada.

CR1.1 Los tipos de usuarios se definen, estableciendo los privilegios de acceso a los recursos (aplicaciones "software", carpetas, entre otros), según las funciones desempeñadas dentro de la organización.

CR1.2 Las cuentas de usuario se crean, utilizando las herramientas específicas del sistema operativo, dándoles un nombre de usuario, una contraseña y asignándolas a los tipos de usuarios definidos en el sistema informático.

CR1.3 La política de contraseñas se configura, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.

CR1.4 El control de acceso al equipo informático se establece, configurando parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.

CR1.5 La seguridad del equipo informático ante ataques externos se refuerza, configurando un cortafuegos según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.

CR1.6 La seguridad de la información del equipo informático (integridad, accesos, entre otros) frente a riesgos de ataque malicioso se revisa, comprobando la instalación y configuración del "software" de protección adecuado (EDP -"EndPoint Detection and Response"-, "anti-ransomware", "anti-malware", entre otros).

CR1.7 La recopilación, tratamiento y eliminación de la información por parte de los usuarios se revisa, documentando detalladamente los protocolos a seguir según el grado de confidencialidad de la información.

CR1.8 La política de seguridad de la organización se transmite a los usuarios, publicando informaciones tales como restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos.

RP2: Configurar equipos servidores, aplicando los mecanismos de protección establecidos en el plan de seguridad de la organización para protegerlos de accesos indebidos.

CR2.1 Los servicios que ofrece el servidor (correo, web, servicio de impresión, entre otros) se configuran, haciendo uso de los entornos específicos de cada servicio, estableciendo valores a sus parámetros de configuración, conforme a las medidas de bastionado establecidas por la organización, si procede.

CR2.2 Los servicios del sistema operativo preinstalados no necesarios (NFS, DNS, entre otros) en el servidor se desactivan, borrándolos del sistema, garantizando así que no pueden ser activados.

CR2.3 La comunicación con el servidor (autentificación de usuarios, intercambio de información) se asegura, activando y configurando protocolos de seguridad tales como TLS (TLS, SSH, entre otros).

CR2.4 Los mecanismos de registro de actividad e incidencias del servidor se activan, configurando el registro de eventos del sistema y parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).

CR2.5 Los mecanismos de registro de actividad e incidencias de los servicios ofrecidos por el servidor se activan, configurando y parametrizando, según el servicio, valores tales como tamaño de los ficheros logs, rotación, nivel de detalle (dirección IP, fecha, usuario, entre otros).

CR2.6 Las configuraciones realizadas e incidencias producidas se documentan, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas "software", entre otros).

RP3: Eliminar información en soportes y sistemas de almacenamiento de equipos informáticos, de forma segura, aplicando procedimientos de borrado seguro y destrucción física de información, siguiendo los procedimientos establecidos en la política de seguridad de la organización para prevenir la fuga de información confidencial.

CR3.1 Los métodos de destrucción física (trituración, desintegración, incineración, entre otros) se revisan, comprobando que el método utilizado se corresponde con el tipo de soporte de información.

CR3.2 El protocolo de retención de datos se interpreta, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.

CR3.3 La información almacenada en los equipos informáticos y en los soportes de información se borran, utilizando herramientas "software" de borrado seguro de datos.

CR3.4 El procedimiento realizado se registra, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del "hardware", entre otras.

RP4: Aplicar medidas de seguridad física a equipos servidores, comprobando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras, siguiendo el plan de seguridad de la organización para evitar interrupciones en la prestación de servicios del sistema.

CR4.1 La ubicación física de los servidores se revisa, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.

CR4.2 Las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores se comprueban, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.

CR4.3 El Sistema de Alimentación Ininterrumpida (SAI) se revisa, comprobando que está operativo a través de su sistema de alertas y reportando su estado en caso de anomalías de funcionamiento.

RP5: Verificar la realización de copias de seguridad, comprobando la información a respaldar, la frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.

CR5.1 La información del equipo informático se comprueba, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde al plan de copias de seguridad.

CR5.2 El plan de copias de seguridad se verifica, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.

CR5.3 Los dispositivos de almacenamiento de copias de seguridad (cintas, discos externos, entre otros) se comprueban, verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en el plan de copias de seguridad.

CR5.4 Los procedimientos de obtención y verificación de copias de seguridad se verifican, realizando pruebas de funcionamiento de los mismos.

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"). Herramientas de borrado seguro de información.

Productos y resultados

Equipos informáticos con control de acceso seguro, cortafuegos y "software" de protección configurado. Equipos servidores con mecanismos de protección establecidos. Documentos de configuración e incidencias producidas. Equipos informáticos reutilizables. Equipos servidores en ubicaciones protegidas y seguras.

Información utilizada o generada

Política de seguridad de infraestructuras telemáticas. 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. Normativa sobre protección de datos. Normativa sobre servicios de la sociedad de información. Normativa sobre prevención de riesgos laborales. Normativa medioambiental, en especial sobre producción y gestión de residuos y suelos contaminados.

MÓDULO FORMATIVO 1

Administración de los dispositivos "hardware" de un sistema informático

Nivel:	*3*
Código:	*MF0484_3*
Asociado a la UC:	*UC0484_3 - Administrar los dispositivos "hardware" de un sistema informático*
Duración (horas):	*150*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Inventariar dispositivos "hardware" y dispositivos externos conectados a un sistema informático, incorporando información tal como, características técnicas (modelo, marca, entre otros), ubicación, estado, entre otras.

CE1.1 Explicar la arquitectura física de un sistema informático, diferenciando las partes que lo componen.

CE1.2 Definir funciones de dispositivos "hardware" de un sistema informático (procesador, memoria, entre otros), explicando sus características técnicas específicas.

CE1.3 Describir procedimientos de instalación y configuración de componentes "hardware" de un sistema informático detallando pasos a seguir, herramientas de instalación a utilizar, medidas de seguridad a considerar, entre otros.

CE1.4 Distinguir tipos de dispositivos "hardware" conectados en un sistema informático, describiendo su función y características técnicas.

CE1.5 Identificar dispositivos "hardware" para conectar en un sistema informático a través de una red de comunicaciones, clasificándolos según su función y describiendo sus características técnicas, procesos de instalación, entre otros.

CE1.6 En un supuesto práctico de identificación y registro de dispositivos "hardware", haciendo uso de una herramienta de inventariado y de dispositivos "hardware" dados:

- Clasificar una colección de dispositivos "hardware", atendiendo a diferentes criterios tales como propósito, idoneidad para un sistema y compatibilidad, entre otros.
- Operar con herramientas de inventariado, registrando las características técnicas de los dispositivos "hardware", modelo.
- Documentar la instalación de los dispositivos físicos, detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.

C2: Aplicar técnicas de monitorización del rendimiento de dispositivos "hardware" (procesador, memoria, entre otros), comprobando parámetros de funcionamiento y haciendo uso de herramientas "software".

CE2.1 Seleccionar herramientas de monitorización, teniendo en cuenta dispositivo "hardware" a analizar y configuración del sistema informático en el que se encuentra.

CE2.2 Configurar herramientas de monitorización, añadiendo dispositivos "hardware" a monitorizar y comprobando la recepción de valores en los parámetros específicos de funcionamiento.

CE2.3 Determinar el estado de un sistema informático, representando gráficamente su rendimiento, tomando como muestras los valores obtenidos en su monitorización.

CE2.4 Analizar alarmas obtenidas en la monitorización, describiendo problemas de configuración asociados a ellas y explicando soluciones.

CE2.5 En un supuesto práctico de monitorización de un sistema informático, según una configuración y condiciones de uso dadas:

- Seleccionar herramientas de monitorización del rendimiento a utilizar, definiendo parámetros a medir y configurándolas para la obtención de esos valores.
- Obtener mediciones del rendimiento del sistema informático, haciendo uso de los parámetros configurados en las herramientas de monitorización.
- Analizar las mediciones obtenidas, documentándolas y presentándolas para facilitar la toma de decisiones acerca del sistema.
- Resolver problemas de rendimiento bajo, configurando parámetros del sistema.
- Solventar alarmas detectadas en la monitorización, reconfigurando el sistema informático.
- Documentar soluciones, indicando limitaciones existentes en el sistema para mejorar su rendimiento.

C3: Aplicar procedimientos de actualización de "firmware", planificándolas, comprobando versiones actuales instaladas en el sistema informático, obteniendo nuevas e instalándolas.

CE3.1 Identificar la versión de "firmware" instalada en dispositivos "hardware" ("firewall", "router", entre otros) del sistema informático, comprobando cuales no la tienen actualizada.

CE3.2 Implementar un plan de actualizaciones "firmware", estableciendo dispositivos "hardware" afectados, medidas de contingencia aplicables, prioridades para su ejecución según la urgencia en el impacto del rendimiento, errores o seguridad, entre otros.

CE3.3 Implementar un entorno de pruebas, configurando un dispositivo "hardware" de las mismas características técnicas a un dispositivo a actualizar, instalando la nueva versión de "firmware" y comprobando que el dispositivo queda operativo.

CE3.4 Realizar copias de seguridad específicas para tipos de dispositivos "hardware" de un sistema informático, previas a una actualización del "firmware", salvaguardando la configuración de los mismos.

CE3.5 Aplicar procesos de actualización "firmware" de dispositivos "hardware" de un sistema informático, instalando nuevas versiones y documentando el proceso e incidencias producidas.

CE3.6 Comprobar el funcionamiento de un sistema informático con actualizaciones de "firmware" instaladas, verificando que los servicios (conexiones VPN, escritorio remoto, entre otros) están operativos y registrando en el inventario las nuevas versiones.

C4: Implementar soluciones "hardware" de alta disponibilidad, configurando sistemas "cluster", sistemas RAID, entre otros, garantizando la protección y recuperación del sistema ante situaciones imprevistas.

CE4.1 Identificar soluciones "hardware" para asegurar la continuidad del funcionamiento de un sistema informático, describiendo sus características y configuraciones.

CE4.2 Definir soluciones "hardware" para asegurar la recuperación del sistema ante situaciones imprevistas, describiendo sus características y configuraciones.

CE4.3 En un supuesto práctico, de implementación y configuración de "hardware" de alta disponibilidad, siguiendo unos requisitos dados:

- Instalar dispositivos "hardware" de alta disponibilidad, configurándolos y verificando que son reconocidos por el sistema informático.

- Probar el sistema de alta disponibilidad, ejecutando simulaciones de contingencias, comprobando que el sistema de alta disponibilidad está operativo y documentando el proceso mediante formularios, herramientas "software", entre otros.
- Monitorizar el sistema de alta disponibilidad, comprobando la ausencia de alertas y registrando incidencias detectadas.
- Reparar dispositivos "hardware" de alta disponibilidad con incidencias, sustituyéndolos por otros de las mismas características técnicas.
- Documentar incidencias del sistema de alta disponibilidad y soluciones aportadas, generando informes (formularios, herramientas "software", entre otros).

C5: Implementar soluciones que mejoren el rendimiento y las prestaciones de sistemas informáticos, analizando sus necesidades de crecimiento y evaluando las características técnicas del "hardware" disponible en el mercado.

CE5.1 Identificar dispositivos "hardware" existentes en el mercado, describiendo sus características técnicas, utilizando catálogos comerciales, documentación técnica, entre otros.

CE5.2 Identificar partes de un sistema informático, susceptibles de provocar cuellos de botella y bajo rendimiento, describiendo causas que los provocan.

CE5.3 En un supuesto de planificación de crecimiento de un sistema informático, según unos requisitos de aumento de la carga de trabajo o de usuarios dados:
- Analizar los dispositivos "hardware" del sistema informático, comprobando sus características técnicas y parámetros de rendimiento, comparándolos con los requeridos, según requisitos de aumento de carga de trabajo o de usuarios dados.
- Realizar propuestas de actualización de "hardware", considerando las necesidades del sistema informático, según los requisitos de aumento de carga de trabajo o de usuarios dados.
- Implementar la actualización del "hardware" del sistema informático, planificando su instalación, configuración y documentando el proceso e incidencias.
- Revisar el sistema informático actualizado y ampliado, monitorizando sus parámetros de funcionamiento, comprobando que no muestran alertas de fallo o bajo rendimiento.
- Documentar los cambios en el sistema informático, registrando las características técnicas del nuevo "hardware", su configuración, entre otros, según el procedimiento dado (formularios, herramientas "software", entre otros).

CE5.4 Aplicar procesos de tratamiento de residuos generados en la implementación de mejoras en un sistema informático, separando los residuos según su tipología, disponiéndolos en sus contenedores y clasificando los RAEE (Residuos de Aparatos Eléctricos y Electrónicos) para su reparación, reutilización de sus componentes y materiales o su recogida por gestores autorizados.

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

C1 respecto a CE1.6; C2 respecto a CE2.6; C4 respecto a CE4.3 y C5 respecto a CE5.3.

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.

Habituarse 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.
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 de ordenadores

Arquitectura Von-Neumann: 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" del sistema informático

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. Dispositivos "hardware" ("firewall", "router", entre otros): función, características. "Firmware": función.

4 Rendimiento del sistema informático

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 del sistema informático

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: 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. Normativa de protección medioambiental (CO2, producción y gestión de residuos, entre otros).

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:

- Taller de 4 m² por alumno o alumna.

- 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 administración de los dispositivos "hardware" de un sistema informático, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) 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

Gestión del "software" de un sistema informático

Nivel:	*3*
Código:	*MF0485_3*
Asociado a la UC:	*UC0485_3 - Gestionar el "software" de un sistema informático*
Duración (horas):	*150*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de instalación y configuración de sistemas operativos, estableciendo valores a sus parámetros de configuración.

CE1.1 Analizar la idoneidad de los tipos de sistemas operativos aplicables a sistemas informáticos, según el propósito de estos, enumerando y describiendo las características que les hacen adecuados para cada caso, según unas necesidades de uso.

CE1.2 Identificar parámetros de configuración del sistema operativo, describiendo su función e importancia en el funcionamiento del sistema informático.

CE1.3 En un supuesto práctico, de instalación de un sistema operativo en un equipo informático, configurándolo según unos requisitos de uso dados:

- Comprobar que se dispone de la configuración "hardware" requerida para la instalación del sistema operativo, verificando parámetros, tales como cantidad de memoria, tipo de procesador, entre otros.
- Preparar el equipo informático, configurando el "hardware" requerido (espacio libre en disco, memoria RAM, procesador, entre otros) para instalar el sistema operativo.
- Establecer los sistemas de ficheros (NTFS, ext4, entre otros), teniendo en cuenta los dispositivos de almacenamiento existentes y las necesidades de uso del equipo informático.
- Instalar el "software" del sistema operativo, configurando parámetros solicitados durante el proceso de instalación.
- Configurar el sistema operativo, atendiendo a los requisitos de uso dados, creando usuarios, impresoras, entre otros.
- Verificar el funcionamiento del equipo informático, haciendo uso de una lista de comprobación que incorporará todos los elementos "hardware" y "software" (acceso a red, impresoras, cuentas de usuarios, entre otros) a comprobar.
- Documentar el trabajo realizado, indicando la configuración "hardware" del equipo informático, la versión del sistema operativo instalado y las incidencias ocurridas durante la instalación.

CE1.4 Verificar dispositivos "hardware" del sistema (memoria, tarjeta de red, entre otros) y sus controladores realizando pruebas de arranque y parada, utilizando herramientas "software" de diagnóstico y verificación, comprobando la no existencia de incidencias en su funcionamiento.

CE1.5 Automatizar tareas en el sistema informático, elaborando "scripts" y planificando su ejecución.

C2: Aplicar procedimientos de instalación y configuración de "software" corporativo y paquetes informáticos de propósito general, estableciendo valores a sus parámetros y verificando su funcionamiento.

CE2.1 Instalar paquetes de propósito general, (herramientas ofimáticas, navegadores, entre otros), comprobando que los requisitos "hardware" y "software" disponibles en el equipo informático son compatibles y suficientes para su instalación.

CE2.2 Instalar "software" corporativo (ERP (Planificación de Recursos Empresariales), bases de datos, entre otros), comprobando que los requisitos "hardware" y "software" disponibles en el equipo informático son compatibles y suficientes para su instalación, configurando parámetros previos a su instalación.

CE2.3 Configurar "software" corporativo (ERP, bases de datos, entre otros), estableciendo valores en sus parámetros de configuración, según requisitos de uso dados.

CE2.4 Configurar el acceso a datos y aplicaciones, creando grupos y cuentas de usuarios, entre otros, estableciendo privilegios específicos de acceso a los recursos del sistema (datos, aplicaciones, entre otros).

CE2.5 Verificar el conjunto del "software" instalado, realizando pruebas de funcionamiento y compatibilidad, usando herramientas del sistema operativo o de terceros.

CE2.6 Registrar incidencias de procesos de instalación y configuración de "software", siguiendo un procedimiento dado (plantillas, herramientas "software", entre otros).

CE2.7 En un supuesto práctico de instalación de un gestor de base de datos, atendiendo a unos requisitos dados (sistema operativo, número de registros en la base de datos, número de usuarios simultáneos, entre otros):

- Seleccionar un gestor de base de datos, describiendo las características que le hacen idóneo para los requisitos dados.
- Comprobar que se dispone de la configuración "hardware" en el equipo informático, verificando que cumple los requisitos necesarios para la instalación del gestor de base de datos seleccionado.
- Seleccionar el formato de sistema de ficheros (NTFS, ext4, entre otros) donde se ubicará la base de datos, indicando las características que le hacen idóneo para el gestor de base de datos y requisitos dados.
- Instalar el gestor de base de datos, configurando sus parámetros, según unos requisitos dados.
- Crear usuarios en el gestor de base de datos (administrador, prueba, entre otros), comprobando que tienen acceso a los datos del gestor.
- Comprobar la conectividad externa al gestor de base de datos, realizando pruebas de acceso desde equipos clientes.

C3: Implementar procedimientos de monitorización del rendimiento del "software" instalado en el equipo informático, estableciendo métricas de rendimiento (estabilidad del sistema, tiempos de respuesta, entre otros), analizando los valores obtenidos.

CE3.1 Enumerar medidas de rendimiento "software", describiendo el impacto en el comportamiento del sistema.

CE3.2 Establecer métricas de rendimiento del "software" instalado (estabilidad, capacidad de respuesta, velocidad, entre otras), especificando parámetros a evaluar, herramientas "software" utilizar, entre otros.

CE3.3 Obtener datos de rendimiento de un sistema informático, utilizando herramientas de diagnóstico y técnicas de análisis de rendimiento previamente establecidas.

CE3.4 Analizar datos de rendimiento del sistema informático, comprobando los valores obtenidos al aplicar las técnicas de análisis, detectando posibles anomalías de funcionamiento (uso elevado de procesador, falta de memoria, entre otros).

CE3.5 Programar correcciones de anomalías de rendimiento, estableciendo planes con medidas correctivas a realizar (actualizaciones de "software", sustitución de "hardware", entre otros), definiendo prioridades para su ejecución, minimizando el impacto en el servicio a los usuarios.

CE3.6 En un supuesto práctico de comprobación del rendimiento de un equipo informático, teniendo instalado un paquete "software" de aplicación:

- Deshabilitar el "software" haciendo uso de herramientas del sistema operativo o directivas específicas del "software" de aplicación.
- Medir los parámetros del rendimiento del equipo (memoria ocupada, uso de CPU, latencia en la conexión de datos, entre otros), utilizando herramientas del sistema operativo.
- Habilitar el "software" haciendo uso de herramientas del sistema operativo o directivas específicas del "software" de aplicación.
- Medir los parámetros del rendimiento del equipo (memoria ocupada, uso de CPU, latencia en la conexión de datos, entre otros) con el "software" de aplicación sometido a una sesión de trabajo, utilizando las herramientas del sistema operativo.
- Analizar los datos obtenidos, comparando y describiendo el impacto en el rendimiento.
- Documentar el proceso realizado, describiendo los pasos seguidos, resultados obtenidos, entre otros.

C4: Aplicar procedimientos de actualización y configuración de "software" de base y corporativo, instalando paquetes o nuevas versiones.

CE4.1 Crear listas con datos sobre personas y/o instituciones relacionadas con la organización (responsable sistemas, operadora telecomunicaciones, entre otros), definiendo su rol en caso de contingencia e indicando cómo y dónde se publicaría dicha lista.

CE4.2 Describir la función de un plan de mantenimiento "software", detallando tipos de mantenimiento, procedimientos, recursos, planificación de tareas, entre otros.

CE4.3 Establecer planes de actualización de "software", definiendo franjas horarias para su ejecución, persona responsable para llevarla a cabo, servicios que quedarán inactivos, equipos afectados, entre otros.

CE4.4 Actualizar "software" de base o corporativo, haciendo una copia de seguridad previa de los datos del equipo informático, instalando la nueva actualización, verificando que el sistema queda operativo y aplicando procedimientos técnicos de vuelta atrás, en caso de contingencia.

CE4.5 Documentar procesos de actualización de "software", registrando pasos realizados, incidencias detectadas, siguiendo procedimiento establecido por la organización (herramientas "software", formularios, entre otros).

C5: Implementar planes para la realización de copias de seguridad, estableciendo información o sistemas a respaldar y frecuencia de respaldo, entre otros, para mantener la seguridad y disponibilidad de la información.

CE5.1 Identificar tipos de copias de seguridad, describiendo características, ventajas e inconvenientes de cada tipo.

CE5.2 Clasificar la información de la organización, inventariándola en función de su criticidad y de su tipo (datos de sistema o datos de la organización), determinando si necesita ser respaldada y la frecuencia con la que debe ser salvaguardada.

CE5.3 Establecer planes de copias de seguridad, teniendo en cuenta volumen de datos a guardar y su criticidad, impacto sobre el rendimiento del servidor y duración en la realización de las copias.

CE5.4 Realizar pruebas de verificación de copias de seguridad, instalando una copia de seguridad y comprobando que se puede recuperar información contenida en ella.

CE5.5 Identificar dispositivos de almacenamiento (cintas, discos externos, entre otros), registrando en el plan de copias de seguridad qué información (fecha de la copia, información respaldada, entre otros) contiene cada dispositivo.

CE5.6 Confeccionar documentación de procedimientos de obtención y verificación de copias de seguridad, así como la de planes de contingencias y resolución de incidencias, siguiendo las normas establecidas por la organización (plantillas, herramientas "software", entre otros).

CE5.7 En un supuesto práctico de realización de copias de seguridad, utilizando herramientas de "backup" y requisitos de salvaguarda dados:

- Identificar qué datos se van a respaldar, calculando el espacio de almacenamiento requerido para la salvaguarda.
- Determinar el tipo de "backup" (incremental, diferencial, entre otros) a realizar, teniendo en cuenta el espacio de almacenamiento disponible.
- Realizar la copia de seguridad, haciendo uso de la herramienta dada.
- Clasificar los dispositivos de respaldo (cintas, discos, entre otros), etiquetándolos con información relevante tal como fecha, datos guardados, entre otros.
- Verificar que la copia de seguridad realizada es funcional, recuperando los datos de ella y comprobando que son iguales a los originales.
- Documentar el proceso realizado, describiendo los pasos seguidos, resultados obtenidos, entre otros.

C6: Inventariar "software", registrando información tal como número de instalaciones de "software", fechas de instalación, el tipo de "software", haciendo uso de herramientas de inventariado.

CE6.1 Describir un inventario "software", explicando su función y ventajas de su gestión.

CE6.2 Enumerar herramientas de gestión de inventario "software", describiendo sus características.

CE6.3 Dar de alta en un inventario "software", registrando información tal como número de licencias, tipo "software", ubicación, entre otros y haciendo uso de las herramientas (formularios, herramientas "software" de inventario, entre otros) indicadas por la organización.

CE6.4 En un supuesto práctico de registro e identificación del "software" instalado en equipos informáticos, comprobando que los términos de licencia se cumplen y actualizando la información en el inventario "software":

- Clasificar el "software" instalado, atendiendo a criterios tales como propósito, sistema operativo, entre otros.
- Revisar el número y ubicación de copias de "software" instalado, comprobando que se cumplen las condiciones de la licencia.
- Revisar los paquetes "software" instalados en los equipos informáticos, comprobando que todos tienen licencia y ésta se cumple.
- Registrar la información del "software" instalado en los equipos informáticos haciendo uso de una herramienta "software" de inventario, incorporando información tal como número de licencia, fecha de instalación, entre otros.

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

C1 respecto a CE1.3; C2 respecto a CE2.7; C3 respecto a CE3.6; C5 respecto a CE5.7 y 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 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.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Clasificación del "software" de un sistema informático

Sistemas operativos: concepto de "software" de base o sistema operativo; evolución de los sistemas operativos: generaciones y características. Tipos: monousuario/multiusuario, monoprocesador/multiprocesador, monolítico/microkernel. Funciones de un sistema operativo, estructura de un sistema operativo: características y funciones; gestión de procesos; gestión y organización de memoria; gestión de dispositivos; gestión y sistemas de ficheros; "firmware"; gestión de usuarios y grupos; 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; gestión de logs; alarmas; tareas programadas; hipervisores; virtualización. Lenguajes de programación: propósito de los lenguajes de programación, clasificación según el grado de independencia de la máquina, compiladores e intérpretes, librerías, clasificación por generaciones. Programas de aplicación: procesadores de lenguaje, aplicaciones de propósito general, aplicaciones ofimáticas, gestores de bases de datos, ventajas e inconvenientes de las aplicaciones a medida; tipos de licencias de uso de "software". Normativa de protección medioambiental (CO2, producción y gestión de residuos, entre otros).

2 Procedimientos de implantación de "software" de un sistema informático

El ciclo de implantación de "software": instalación, configuración, verificación y ajuste. La necesidad de la planificación en los procesos de instalación. Parámetros del sistema informático 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.

3 Procedimientos de mantenimiento del "software" de un sistema informático

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. Inventario "software". Herramientas de gestión de inventario "software".

4 Copias de respaldo de un sistema informático

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.

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:

- Taller de 4 m² por alumno o alumna.

- 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 un sistema informático, que se acreditará mediante una de las dos formas siguientes:
- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior), 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):	*120*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de configuración de seguridad de equipos informáticos instalando "software", configurando opciones del sistema operativo, entre otros, para protegerlos ante el riesgo de pérdida, manipulación y/o sustracción de información no autorizada.

CE1.1 Definir tipos de usuario o roles, estableciendo los privilegios de acceso a los recursos (aplicaciones "software", carpetas, entre otros), según las funciones desempeñadas dentro de la organización.

CE1.2 Crear cuentas de usuario, asignándolas a los tipos de usuarios definidos en el sistema informático.

CE1.3 Configurar la política de contraseñas, estableciendo parámetros tales como complejidad, caducidad, revocación, bloqueo, reutilización, entre otros.

CE1.4 Configurar el control de acceso al equipo informático, estableciendo parámetros tales como el número de intentos fallidos permitidos, tiempo permitido entre fallos de acceso consecutivos, entre otros.

CE1.5 Configurar un cortafuegos en el equipo informático, según las necesidades de uso del equipo, estableciendo reglas de filtrado de las conexiones entrantes y salientes.

CE1.6 Aplicar medidas de seguridad a la información del equipo informático (integridad, accesos, entre otros), frente a riesgos de ataque malicioso, revisando la instalación y configuración del "software" de protección adecuado (EDP -"Endpoint Detection and Response"-, "anti-ransomware", "anti-malware", entre otros).

CE1.7 Contrastar los procesos de recopilación, tratamiento y eliminación de la información por parte de los usuarios, comprobando que cumplen protocolos a seguir según el grado de confidencialidad de la información.

CE1.8 Crear documentación informativa sobre la política de seguridad de la organización tal como, restricciones asignadas a equipos y usuarios, ámbitos de responsabilidades relativos a la utilización de los equipos informáticos, entre otros.

C2: Aplicar procedimientos de configuración de seguridad a equipos servidores, estableciendo mecanismos de registro de la actividad del servidor, deshabilitando los servicios no prestados, haciendo uso de protocolos de seguridad, entre otros.

CE2.1 Identificar tipos de servicios (correo, web, entre otros) que puede ofrecer un servidor, describiendo su función y características.

CE2.2 Identificar las amenazas existentes para cada tipo de servicio, describiendo las configuraciones a realizar para minimizar/proteger dicho servicio.

CE2.3 Configurar un servicio (correo, web, entre otros) en un servidor, haciendo uso del entorno específico del servicio, estableciendo sus parámetros de configuración según unos valores dados.

CE2.4 En un supuesto práctico de aseguramiento de un tipo de servidor, configurando los servicios necesarios para prestar su función (web, correo, entre otros) y deshabilitando los innecesarios:

- Identificar qué servicios están activos en el servidor, haciendo uso de la directiva correspondiente de sistema operativo específico y verificando su estado.
- Identificar los servicios que están activos que no se van a utilizar, deshabilitándolos del sistema operativo.
- Eliminar el "software" de los servicios deshabilitados, borrándolos del sistema operativo.

CE2.5 Identificar los protocolos de seguridad (TLS -Transport Layer Security, Seguridad de la Capa de Transporte-, SSH -Secure Shell-, entre otros) utilizados en las comunicaciones con un tipo de servidor, describiendo sus características e indicando cómo se activan y configuran para un sistema operativo específico.

CE2.6 Activar mecanismos de auditoría de la actividad e incidencias del servidor, configurando el registro de eventos del sistema y parametrizando valores tales como periodicidad, nivel de detalle (fecha, usuario, entre otros).

CE2.7 Documentar las configuraciones realizadas e incidencias producidas, detallando el procedimiento llevado a cabo, las incidencias ocurridas (descripción, tipo, entre otros) y el correctivo aplicado para solventarlas, según procedimiento interno de la organización (plantillas, herramientas "software", entre otros).

C3: Aplicar procedimientos de borrado seguro y destrucción física de información en soportes y sistemas de almacenamiento de un equipo informático, haciendo uso de las técnicas de borrado y destrucción específicas al tipo de soporte de información.

CE3.1 Identificar las técnicas de borrado o destrucción apropiadas para cada tipo de soporte (lógico, óptico, magnético o memorias de estado sólido), describiendo sus características y función.

CE3.2 Redactar un protocolo de retención de datos, teniendo en cuenta la organización, búsqueda, acceso y eliminación de la información.

CE3.3 Revisar los métodos de borrado o destrucción física aplicado en soportes de información, comprobando que el método o técnica utilizados se corresponde con el tipo de soporte [magnético, óptico, electrónico (SSD -"Solid State Drive", Unidad de Estado Sólido-)].

CE3.4 En un supuesto práctico de borrado seguro de información de soporte de información de datos (IDE -"Integrated Drive Electronics"-, SATA -"Serial Advanced Technology Attachment"-, SCSI -"Small Computer System Interface"- y USB -"Universal Serial Bus"-), utilizando una herramienta "software" de borrado seguro:

- Comprobar que el equipo informático donde se va a instalar o utilizar la herramienta "software" de borrado seguro cumple los requisitos (tipo de procesador, tamaño de memoria, puerto USB, entre otros) para su instalación o uso y verificando que se encuentra aislado (sin conexión a red) y libre de "malware".
- Configurar el equipo informático para que permita el arranque desde USB, configurando la BIOS (Sistema básico de entrada/salida).

- Reinicia el equipo, introduciendo el dispositivo USB con la herramienta de borrado seguro antes de que comience el proceso de arranque.
- Hacer uso de la herramienta de borrado seguro, seleccionando los soportes con la información a borrar y el método de borrado a aplicar.
- Realizar el proceso de borrado seguro de los soportes de información seleccionados, obteniendo un informe de proceso terminado y guardándolo en el lugar indicado.
- Verificar que la información en los dispositivos de almacenamiento seleccionados ha sido borrada de forma segura, visualizando en el informe generado que el borrado se ha realizado sin ningún error.
- Documentar el trabajo realizado, indicando los dispositivos de almacenamiento, método de borrado y evidencias del proceso de borrado seguro.

CE3.5 Registrar un procedimiento realizado de borrado o destrucción, generando un documento de certificación que detalle informaciones tales como, evidencias lógicas o gráficas del proceso, cuándo y cómo se ha realizado el proceso de destrucción o reutilización, especificaciones técnicas del "hardware", entre otras.

C4: Comprobar medidas de seguridad física a equipos servidores, verificando que su ubicación dispone de protección de acceso y condiciones ambientales específicas, entre otras.

CE4.1 Revisar la ubicación física de servidores, comprobando que se encuentran situados en un espacio con acceso físico controlado y protegido.

CE4.2 Comprobar las condiciones ambientales (temperatura, humedad) de la ubicación física de equipos servidores, verificando que se encuentran dentro del rango de trabajo óptimo considerado entre 17 y 21 grados.

CE4.3 Revisar el sistema de alimentación ininterrumpida (SAI), comprobando que está operativo a través de su sistema de alertas.

C5: Aplicar técnicas de verificación de copias de seguridad, comprobando que la información a respaldar, la frecuencia de respaldo, entre otros, permite mantener la seguridad y disponibilidad de la información.

CE5.1 Comprobar la información de un equipo informático, verificando que su clasificación en función de su criticidad y de su tipo (datos de sistema o datos de la organización) es acorde a un plan de copias de seguridad.

CE5.2 Verificar un plan de copias de seguridad, comprobando que contempla los datos a guardar, su criticidad, tipo de salvaguarda, frecuencia de respaldo, entre otros.

CE5.3 Comprobar dispositivos de almacenamiento de copias de respaldo (cintas, discos externos, entre otros), verificando que la información (fecha de la copia, información respaldada, entre otros) contenida en ellos se encuentra registrada en un plan de copias de seguridad.

CE5.4 Verificar procedimientos de obtención y verificación de copias de seguridad, realizando pruebas de funcionamiento de los mismos.

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

C2 respecto a CE2.4 y C3 respecto a CE3.4.

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.
Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Gestión de la seguridad y riesgos de un sistema informático

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. Normativa de protección medioambiental (CO2, producción y gestión de residuos, entre otros).

2 Seguridad física en el sistema informático

Protección del sistema informático. Protección de los datos. Técnicas de borrado seguro y destrucción de información. Herramientas "software" de borrado seguro de información.

3 Seguridad lógica del sistema informático

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. 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.

4 Acceso remoto al sistema informático

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 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:

- Taller de 4 m² por alumno o alumna.

- Instalación de 2 m² por alumno o alumna.

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) 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.