Espacio Formativo	Equipamiento
Aula de Informática	– PCs instalados en red y conexión a Internet. – Armario de cableado con paneles de parcheado, y dispositivos de conexión a red. – Software de base, de red y del servidor web. – Software de seguridad y antivirus. – Software ofimático. – Software de páginas web – Software para crear y modificar imágenes – Impresora y periféricos. – Herramientas de edición web. – Herramientas de edición de código de programación cliente y de servidor. – Herramientas de depuración y pruebas. – Herramientas de publicación de páginas. – Herramientas de transferencia. – Herramientas multimedia. – Herramientas de desarrollo rápido. – Navegadores actuales. – Navegadores tipo texto. – Lenguajes de marcas. Lenguajes de guión. – Servidores web. – Aplicaciones para la verificación de accesibilidad de sitios web. – Buscadores de Internet. – Componentes software ya desarrollados y/o distribuidos por empresas informáticas. – Cañón de proyección. – Rotafolios. – Pizarra. – Material de aula. – Mesa y silla para el formador. – Mesas y sillas para alumnos. – Mobiliario auxiliar para el equipamiento de aula.

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

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

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

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

ANEXO II

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: OPERACIÓN DE SISTEMAS INFORMÁTICOS.

Código: IFCT0210

Familia Profesional: Informática y Comunicaciones.

Área Profesional: Sistemas y telemática.

cve: BOE-A-2011-19503

Nivel de cualificación profesional: 2

Cualificación profesional de referencia:

IFC300_2 Operación de Sistemas Informáticos (Real Decreto 1201/2007, de 14 de septiembre).

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

UC0219_2: Instalar y configurar el software 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 de base y de aplicación de cliente.
UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.

Competencia general:

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

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional por cuenta ajena, en empresas o entidades públicas o privadas de cualquier tamaño, que dispongan de equipos informáticos para su gestión, en el área de sistemas del departamento de informática.

Sectores productivos:

Se ubica sobre todo en el sector servicios, y principalmente en los siguientes tipos de empresas: empresas o entidades que utilizan sistemas informáticos para su gestión; empresas dedicadas a la comercialización de equipos y servicios informáticos; empresas que prestan servicios de asistencia técnica informática; redes de telecentros; en las distintas administraciones públicas, como parte del soporte informático de la organización.

Ocupaciones y puestos de trabajo relevantes:

3812.1023 Técnico en sistemas microinformáticos.
Operador de sistemas.
Técnico de soporte informático.

Duración de la formación asociada: 600 horas.

Relación de módulos formativos y de unidades formativas.

MF0219_2: (Transversal) Instalación y configuración de sistemas operativos. (140 horas)

- UF0852: Instalación y actualización de sistemas operativos. (80 horas)
- UF0853: Explotación de las funcionalidades del sistema microinformático. (60 horas)

MF0957_2: Mantenimiento del subsistema físico de sistemas informáticos. (150 horas)

- UF1349: Mantenimiento e inventario del subsistema físico. (90 horas)
- UF1350: Monitorización y gestión de incidencias de los sistemas físicos. (60 horas)

cve: BOE-A-2011-19503

MF0958_2: Mantenimiento del subsistema lógico de sistemas informáticos. (150 horas)

- UF1351: Gestión y operativa del software de un sistema informático. (90 horas)
- UF1352: Monitorización y gestión de incidencias del software. (60 horas)

MF0959_2: Mantenimiento de la seguridad en sistemas informáticos. (120 horas)

- UF1353: Monitorización de los accesos al sistema informático. (90 horas)
- UF1354: Copia de seguridad y restauración de la información. (30 horas)

MP0286: Módulo de prácticas profesionales no laborales de Operación de Sistemas Informáticos (40 horas).

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: INSTALAR Y CONFIGURAR EL SOFTWARE DE BASE EN SISTEMAS MICROINFORMÁTICOS.

Nivel: 2

Código: UC0219_2

Realizaciones profesionales y criterios de realización

RP1: Realizar procesos de instalación de sistemas operativos para su utilización en sistemas microinformáticos, siguiendo especificaciones recibidas.

CR1.1 Las características de los sistemas operativos se clasifican, para decidir la versión a instalar y el tipo de instalación, en función de las especificaciones técnicas recibidas.
CR1.2 Los requisitos de instalación del sistema operativo se comprueban, para verificar que hay suficiencia de recursos y compatibilidad en el equipo destino de la instalación, siguiendo el procedimiento establecido.
CR1.3 El equipo destino de la instalación se prepara para ubicar el sistema operativo, habilitando la infraestructura en los dispositivos de almacenamiento masivo, de acuerdo a las especificaciones técnicas recibidas.
CR1.4 El sistema operativo se instala aplicando los procesos indicados en los manuales de instalación que acompañan al mismo, para obtener un equipo informático en estado funcional, siguiendo el procedimiento establecido.
CR1.5 El sistema operativo se configura para su funcionamiento, dentro de los parámetros especificados, siguiendo los procedimientos establecidos y lo indicado en la documentación técnica.
CR1.6 Los programas de utilidad incluidos en el sistema operativo se instalan para su uso, de acuerdo a las especificaciones técnicas recibidas.
CR1.7 La verificación de la instalación se realiza para comprobar la funcionalidad del sistema operativo, mediante pruebas de arranque y parada, y análisis del rendimiento, siguiendo procedimientos establecidos.
CR1.8 La documentación de los procesos realizados se confecciona y archiva para su uso posterior, siguiendo los modelos internos establecidos por la organización.
CR1.9 La documentación técnica específica asociada se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP2: Actualizar el sistema operativo para garantizar su funcionamiento, siguiendo especificaciones técnicas recibidas y procedimientos de la organización.

cve: BOE-A-2011-19503

CR2.1 Las versiones del software base, complementos del sistema y controladores de dispositivos se comprueban para asegurar su idoneidad, siguiendo el procedimiento establecido.
CR2.2 Las versiones obsoletas del software de base, complementos del sistema y controladores de dispositivos se identifican para proceder a su actualización y asegurar su funcionalidad, siguiendo especificaciones técnicas y procedimientos establecidos.
CR2.3 Los complementos y «parches» para el funcionamiento del software base se instalan y configuran, a indicación del administrador del sistema para mantener la seguridad en el mismo, de acuerdo a los procedimientos establecidos.
CR2.4 La verificación de la actualización se realiza, para probar la funcionalidad del sistema operativo mediante pruebas de arranque y parada, y análisis de rendimiento, según procedimientos establecidos.
CR2.5 La documentación de los procesos realizados se confecciona y archiva para su uso posterior, según las normas establecidas por la organización.

RP3: Explotar las funcionalidades del sistema microinformático mediante la utilización del software base y aplicaciones estándares, teniendo en cuenta las necesidades de uso.

CR3.1 Las funciones y aplicaciones proporcionadas por el software base se identifican para su utilización, de acuerdo a las instrucciones de la documentación técnica y las necesidades de uso.
CR3.2 Las operaciones con el sistema de archivos se realizan utilizando la interfaz que proporciona el sistema operativo, siguiendo especificaciones técnicas y según necesidades de uso.
CR3.3 Las herramientas de configuración que proporciona el sistema operativo se ejecutan para seleccionar opciones del entorno de trabajo, según especificaciones recibidas y necesidades de uso.
CR3.4 Los procesos de ejecución de aplicaciones se realizan, para explotar las funciones de cada una de ellas de acuerdo a las necesidades operacionales y funcionales.
CR3.5 Los mensajes proporcionados por el software base se interpretan, para controlar el funcionamiento del sistema microinformático mediante la consulta de manuales, documentación proporcionada por el fabricante y especificaciones dadas por la organización.
CR3.6 Los procedimientos de uso y gestión de los periféricos conectados al sistema microinformático, por parte de los usuarios, se realizan para explotar sus funcionalidades, siguiendo la documentación técnica y procedimientos estipulados por la organización.

Contexto profesional

Medios de producción
Equipos informáticos. Periféricos. Sistemas operativos. Utilidades y aplicaciones incorporadas a los sistemas operativos. Versiones de actualización de sistemas operativos. Documentación técnica asociado a los sistemas operativos. Software libre.

Productos y resultados
Equipos informáticos con sistemas operativos instalados y configurados. Sistemas operativos configurados y en explotación. Equipo informático organizado lógicamente. Sistemas operativos actualizados.

Información utilizada o generada
Manuales y documentación técnica de sistemas operativos. Manuales de actualización de sistemas operativos. Manuales de las aplicaciones incluidas en el sistema operativo. Informes de instalación, configuración y actualización del sistema operativo. Plan de seguridad y calidad de la organización.

cve: BOE-A-2011-19503

Unidad de competencia 2

Denominación: MANTENER Y REGULAR EL SUBSISTEMA FÍSICO EN SISTEMAS INFORMÁTICOS.

Nivel: 2

Código: UC0957_2

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 El funcionamiento de los dispositivos físicos se comprueba utilizando las herramientas y técnicas adecuadas bajo condiciones de seguridad suficientes y según procedimientos establecidos.

CR1.2 Los dispositivos físicos averiados, con mal funcionamiento o bajo rendimiento son actualizados o sustituidos 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 tareas de comprobación y verificación para asegurar la conexión de los dispositivos físicos son realizadas según procedimientos establecidos o según indicación del administrador del sistema y siempre bajo condiciones de seguridad suficientes.

CR1.4 Las incidencias detectadas se comprueban si están registradas, en caso contrario se documentan y se registran para su uso posterior, según procedimientos establecidos.

CR1.5 La documentación técnica específica asociada a los dispositivos se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

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 suficientes.

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 comprueban si están registradas, en caso contrario se documentan y se registran para su uso posterior según procedimientos establecidos.

CR2.6 La documentación técnica específica asociada a los dispositivos se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

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 Las herramientas de monitorización se utilizan para detectar posibles anomalías en el funcionamiento de los dispositivos físicos del sistema, siguiendo procedimientos establecidos por la organización.

cve: BOE-A-2011-19503

CR3.3 Las alarmas y eventos monitorizados se documentan y su registro se archiva, para su uso posterior, según procedimientos establecidos.
CR3.4 Los programas de medición se ejecutan, para comprobar el rendimiento de los dispositivos físicos, según procedimientos establecidos y necesidades de uso.
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 comprueban si están registradas, en otro caso se documentan y se registran para su uso posterior, 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.

Productos y resultados
Inventarios revisados y actualizados del subsistema físico. Sistema informático con subsistema físico en funcionamiento óptimo y una utilización adecuada de sus recursos.

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. Normas y recomendaciones ambientales de seguridad. Normas 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

Denominación: EJECUTAR PROCEDIMIENTOS DE ADMINISTRACIÓN Y MANTENIMIENTO EN EL SOFTWARE DE BASE Y DE APLICACIÓN DE CLIENTE.

Nivel: 2

Código: UC0958_2

cve: BOE-A-2011-19503

Realizaciones profesionales y criterios de realización

RP1: Mantener y comprobar la actualización de 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 El software de aplicación no utilizado se desinstala para evitar un mal aprovechamiento del espacio de almacenamiento, según procedimientos establecidos.

CR1.3 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.

CR1.4 Las incidencias detectadas se comprueban si están registradas, caso contrario se documentan y se registran para su uso posterior, según procedimientos establecidos.

CR1.5 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.

CR1.6 La documentación técnica específica asociada se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

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 comprueban para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior, según procedimientos establecidos.

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

CR2.9 La documentación técnica específica asociada se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

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.

cve: BOE-A-2011-19503

CR3.2 Las herramientas de monitorización se utilizan para detectar posibles anomalías en el funcionamiento del software de base y de aplicación del sistema, siguiendo procedimientos establecidos por la organización.
CR3.3 Las alarmas y eventos monitorizados se documentan y su registro se archiva para su uso posterior, según procedimientos establecidos.
CR3.4 Los programas de medición del software se ejecutan, para comprobar el rendimiento de los procesos, 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 comprueban, para establecer si están registradas, en caso contrario se documentan y se registran para su uso posterior, 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 legislación vigente.
CR4.4 Las incidencias detectadas sobre mal funcionamiento 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: discos, cintas, CD-ROM, DVD, entre otros. 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.

Productos y resultados
Inventarios revisados y actualizados del subsistema lógico. Sistema informático con subsistema lógico en funcionamiento.

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. Legislación vigente acerca 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

Denominación: MANTENER LA SEGURIDAD DE LOS SUBSISTEMAS FÍSICOS Y LÓGICOS EN SISTEMAS INFORMÁTICOS.

cve: BOE-A-2011-19503

Nivel: 2

Código: UC0959_2

Realizaciones profesionales y criterios de realización

RP1: Revisar los accesos al sistema informático, para asegurar la aplicación de los procedimientos establecidos y el plan de seguridad, informando de las anomalías detectadas.

CR1.1 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.

CR1.2 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.

CR1.3 Las incidencias detectadas en el acceso al sistema son comprobadas para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior según procedimientos establecidos.

CR1.4 Los cambios detectados en la configuración de control de acceso de usuarios al sistema se documentan, para mantener el inventario actualizado, según procedimientos establecidos.

RP2: Comprobar el funcionamiento de los mecanismos de seguridad establecidos informando de las anomalías detectadas a personas de responsabilidad superior.

CR2.1 Los permisos de acceso de los usuarios al sistema se comprueban, para asegurar su validez, según el plan de seguridad del sistema.

CR2.2 Las políticas de seguridad de usuario se comprueban, para cerciorar su validez, según el plan de seguridad del sistema.

CR2.3 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.

CR2.4 Las incidencias detectadas son comprobadas para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior, siguiendo procedimientos establecidos e informando al inmediato superior.

CR2.5 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.

RP3: Realizar la copia de seguridad, para garantizar la integridad de los datos, según los procedimientos establecidos y el plan de seguridad.

CR3.1 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.

CR3.2 Las copias de seguridad se verifican, para asegurar la utilización de las mismas, según los procedimientos establecidos en el plan de seguridad del sistema.

CR3.3 El almacenaje 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.

CR3.4 Las incidencias detectadas son comprobadas, para establecer si están registradas, de otro modo se documentan y registran para su uso posterior, según procedimientos establecidos.

cve: BOE-A-2011-19503

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 son comprobadas para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior siguiendo procedimientos establecidos e informando al inmediato superior.
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. Legislación vigente acerca 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.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS.

Código: MF0219_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0219_2 Instalar y configurar el software base en sistemas microinformáticos.

Duración: 140 horas.

cve: BOE-A-2011-19503

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y ACTUALIZACIÓN DE SISTEMAS OPERATIVOS

Código: UF0852

Duración: 80 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP2.

Capacidades y criterios de evaluación

C1: Clasificar las funciones y características del software base para el funcionamiento de un sistema microinformático.

CE1.1 Describir las principales arquitecturas de sistemas microinformáticos detallando la misión de cada uno de los bloques funcionales que las componen.

CE1.2 Explicar el concepto de sistema operativo e identificar las funciones que desempeña en el sistema microinformático.

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

CE1.4 Clasificar los sistemas operativos y versiones que se utilizan en equipos informáticos detallando sus principales características y diferencias, según unas especificaciones técnicas.

CE1.5 Identificar las fases que intervienen en la instalación del sistema operativo comprobando los requisitos del equipo informático para garantizar la posibilidad de la instalación.

C2: Aplicar procesos de instalación y configuración de sistemas operativos para activar las funcionalidades del equipo informático, de acuerdo a unas especificaciones recibidas.

CE2.1 En supuestos prácticos, debidamente caracterizados, realizar la instalación de un sistema operativo en un equipo informático para su puesta en funcionamiento:

- Comprobar que el equipo informático cumple con los requisitos y cuenta con los recursos necesarios para la instalación del software base.
- Preparar el equipo destino de la instalación formateando y creando las particiones indicadas en las especificaciones.
- Instalar el sistema operativo siguiendo los pasos de la documentación técnica.
- Configurar el sistema con los parámetros indicados.
- Instalar los programas de utilidad indicados en las especificaciones.
- Verificar la instalación mediante pruebas de arranque y parada.
- Documentar el trabajo realizado.

CE2.2 Identificar los procedimientos que se utilizan para automatizar la instalación de sistemas operativos en equipos informáticos de las mismas características mediante el uso de herramientas software de clonación y otras herramientas de instalación desasistida.

CE2.3 En supuestos prácticos, debidamente caracterizados, realizar la instalación de un sistema operativo en equipos informáticos con las mismas características, de acuerdo a unas especificaciones recibidas:

- Preparar uno de los equipos para instalar el sistema operativo y las utilidades indicadas.
- Instalar y configurar el sistema operativo siguiendo los pasos de la documentación técnica.
- Instalar los programas de utilidad indicados en las especificaciones.
- Seleccionar la herramienta software para realizar el clonado de equipos.
- Proceder a la obtención de las imágenes del sistema instalado para su posterior distribución.

cve: BOE-A-2011-19503

– Implantar, mediante herramientas de gestión de imágenes de disco, aquellas obtenidas en varios equipos de iguales características al original para conseguir activar sus recursos funcionales.
– Realizar pruebas de arranque y parada para verificar las instalaciones.
– Documentar el trabajo realizado.

CE2.4 Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda en la instalación del sistema operativo.

C3: Actualizar el sistema operativo de un equipo informático para incluir nuevas funcionalidades y solucionar problemas de seguridad, atendiendo a unas especificaciones técnicas.

CE3.1 Identificar los componentes software de un sistema operativo susceptibles de reajuste para realizar su actualización, teniendo en cuenta sus especificaciones técnicas.

CE3.2 Identificar y clasificar las fuentes de obtención de elementos de actualización para realizar los procesos de implantación de parches y actualizaciones del sistema operativo.

CE3.3 Describir los procedimientos para la actualización del sistema operativo teniendo en cuenta la seguridad y la integridad de la información en el equipo informático.

CE3.4 En supuestos prácticos, debidamente caracterizados, realizar la actualización de un sistema operativo para la incorporación de nuevas funcionalidades, de acuerdo a unas especificaciones recibidas:

– Identificar los componentes a actualizar del sistema operativo.
– Comprobar los requisitos de actualización del software.
– Actualizar los componentes especificados.
– Verificar los procesos realizados y la ausencia de interferencias con el resto de componentes del sistema.
– Documentar los procesos de actualización.

Contenidos

1. Arquitecturas de un sistema microinformático.

– Esquema funcional de un ordenador.
  – Subsistemas.
– La unidad central de proceso y sus elementos.
  – Memoria interna, tipos y características.
  – Unidades de entrada y salida.
  – Dispositivos de almacenamiento, tipos y características.
– Buses.
  – Tipos.
  – Características.
– Correspondencia entre los Subsistemas físicos y lógicos.

2. Funciones del sistema operativo informático.

– Conceptos básicos.
  – Los procesos.
  – Los archivos.
  – Las llamadas al sistema.
  – El núcleo del sistema operativo.
  – El interprete de comandos.
– Funciones.
  – Interfaz de usuario.
  – Gestión de recursos.
  – Administración de archivos.
  – Administración de tareas.
  – Servicio de soporte.

cve: BOE-A-2011-19503

3. Elementos de un sistema operativo informático.
- Gestión de procesos.
- Gestión de memoria.
- El sistema de Entrada y Salida.
- Sistema de archivos.
- Sistema de protección.
- Sistema de comunicaciones.
- Sistema de interpretación de órdenes.
  - Línea de comando.
  - Interfaz gráfica.
- Programas del sistema.

4. Sistemas operativos informáticos actuales.
- Clasificación de los sistemas operativos.
- Software libre.
- Características y utilización.
- Diferencias.
- Versiones y distribuciones.

5. Instalación y configuración de sistemas operativos informáticos.
- Requisitos para la instalación. Compatibilidad hardware y software.
- Fases de instalación.
  - Configuración del dispositivo de arranque en la BIOS.
  - Formateado de discos.
  - Particionado de discos.
  - Creación del sistema de ficheros.
  - Configuración del sistema operativo y de los dispositivos.
  - Instalación y configuración de utilidades y aplicaciones.
- Tipos de instalación.
  - Instalaciones mínimas.
  - Instalaciones estándares.
  - Instalaciones personalizadas.
  - Instalaciones atendidas o desatendidas.
  - Instalaciones en red.
  - Restauración de una imagen.
- Verificación de la instalación. Pruebas de arranque y parada.
- Documentación de la instalación y configuración.

6. Replicación física de particiones y discos duros.
- Programas de copia de seguridad.
- Clonación.
- Funcionalidad y objetivos del proceso de replicación.
- Seguridad y prevención en el proceso de replicación.
- Particiones de discos.
  - Tipos de particiones.
  - Herramientas de gestión.
- Herramientas de creación e implantación de imágenes y réplicas de sistemas:
  - Orígenes de información.
  - Procedimientos de implantación de imágenes y réplicas de sistemas.

7. Actualización del sistema operativo informático.
- Clasificación de las fuentes de actualización.
- Actualización automática.
- Los centros de soporte y ayuda.
- Procedimientos de actualización.
- Actualización de sistemas operativos.

cve: BOE-A-2011-19503

- Actualización de componentes software.
  - Componentes críticos.
  - Componentes de seguridad.
  - Controladores.
  - Otros componentes.
- Verificación de la actualización.
- Documentación de la actualización.

UNIDAD FORMATIVA 2

Denominación: EXPLOTACIÓN DE LAS FUNCIONALIDADES DEL SISTEMA MICROINFORMÁTICO

Código: UF0853

Duración: 60 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP3

Capacidades y criterios de evaluación

C1: Utilizar las aplicaciones que proporcionan los sistemas operativos, para la explotación del mismo de acuerdo a unas especificaciones técnicas.

CE1.1 Utilizar las aplicaciones proporcionadas por el sistema operativo describiendo sus características para el uso y explotación del mismo, teniendo en cuenta sus especificaciones técnicas y necesidades funcionales.

CE1.2 Utilizar las aplicaciones proporcionadas por el sistema operativo para la organización del disco y el sistema de archivos, de acuerdo a unas especificaciones técnicas recibidas.

CE1.3 Utilizar las opciones de accesibilidad que tienen los sistemas operativos actuales, para configurar entornos accesibles para personas con discapacidades, de acuerdo a unas especificaciones técnicas y funcionales.

CE1.4 Configurar las opciones del entorno de trabajo utilizando las herramientas y aplicaciones que proporciona el sistema operativo, siguiendo especificaciones recibidas y necesidades de uso.

CE1.5 Describir las aplicaciones proporcionadas por el sistema operativo para la explotación de las funcionalidades de los periféricos conectados al sistema, de acuerdo a las necesidades de uso.

CE1.6 Clasificar los mensajes y avisos proporcionados por el sistema microinformático para discriminar su importancia y criticidad, y aplicar procedimientos de respuesta de acuerdo a unas instrucciones dadas.

CE1.7 Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda en el manejo del sistema operativo.

Contenidos

1. **Utilidades del sistema operativo.**
   - Características y funciones.
   - Configuración del entorno de trabajo.
   - Administración y gestión de los sistemas de archivo.
   - Gestión de procesos y recursos.
   - Gestión y edición de archivos.

2. **Organización del disco y sistema de archivos.**
   - El sistema de archivos.
     - FAT.
     - NTFS.

cve: BOE-A-2011-19503

- Unidades lógicas de almacenamiento.
- Estructuración de los datos.
  - Carpetas o directorios.
  - Ficheros.
- Tipos de ficheros.
- Carpetas y archivos del sistema.
- Estructura y configuración del explorador de archivos.
- Operaciones con archivos.
  - Creación.
  - Copiar y mover.
  - Eliminación y recuperación.
- Búsqueda de archivos.

3. Configuración de las opciones de accesibilidad.
- Opciones para facilitar la visualización de pantalla.
- Uso de narradores.
- Opciones para hacer más fácil el uso del teclado o del ratón.
- Reconocimiento de voz
- Uso de alternativas visuales y de texto para personas con dificultades auditivas

4. Configuración del sistema informático.
- Configuración del entorno de trabajo.
  - Personalización del entorno visual.
  - Configuración regional del equipo.
  - Personalización de los periféricos básicos.
  - Otros.
- Administrador de impresión.
- Administrador de dispositivos.
- Protección del sistema.
- Configuración avanzada del sistema

5. Utilización de las herramientas del sistema.
- Desfragmentado de disco.
- Copias de seguridad.
- Liberación de espacio.
- Programación de tareas.
- Restauración del sistema.

6. Gestión de procesos y recursos.
- Mensajes y avisos del sistema.
- Eventos del sistema.
- Rendimiento del sistema.
- Administrador de tareas.
- Editor del registro del sistema.

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Duración total en horas de las unidades formativas	N.º de horas máximas susceptibles de formación a distancia
Unidad formativa 1– UF0852	80	40
Unidad formativa 2– UF0853	60	30

Secuencia:

Para acceder a la unidad formativa 2 debe haberse superado la unidad formativa 1.

cve: BOE-A-2011-19503

Criterios de acceso para los alumnos

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

MÓDULO FORMATIVO 2

Denominación: MANTENIMIENTO DEL SUBSISTEMA FÍSICO DE SISTEMAS INFORMÁTICOS.

Código: MF0957_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0957_2: Mantener y regular el subsistema físico en sistemas informáticos.

Duración: 150 horas

UNIDAD FORMATIVA 1

Denominación: MANTENIMIENTO E INVENTARIO DEL SUBSISTEMA FÍSICO.

Código: UF1349

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1, RP2 y RP4.

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 Identificar 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.
- Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.
- 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.

cve: BOE-A-2011-19503

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 Realizar la manipulación de material fungible para sustituirlo o reponerlo, según unas especificaciones dadas:

- Relacionar el material fungible con los dispositivos físicos correspondientes, según especificaciones técnicas del dispositivo.
- Elegir el material fungible para el dispositivo según criterios de funcionalidad y economía.
- Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, para utilizarla como ayuda.
- Interpretar las señales del dispositivo acerca del material fungible según indicaciones de la documentación técnica.
- Instalar el material fungible en el dispositivo siguiendo especificaciones técnicas.
- Hacer pruebas de funcionamiento del dispositivo con el nuevo material fungible.
- 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.

Contenidos

1. Componentes de un sistema informático.

- Los sistemas informáticos.
  - Definición.
  - Componentes.
  - Clasificación.
  - Estructura de un sistema informático.
- El sistema central.
  - La unidad central de proceso.
    - Funciones y tipos.
    - Propósito y esquema de funcionamiento.
    - Estructura interna.
    - Microprocesadores actuales. Características principales.
    - Arquitecturas de procesadores: CISC Y RISC.
  - El sistema de memoria principal.
    - Funciones y tipos.
    - Jerarquía de memorias.
    - Características de la memoria principal.
    - Espacios de direccionamiento y mapas de memoria.
- El sistema de E/S.
  - Funciones y tipos.
  - Procesadores de E/S.
  - Subsistema de E/S.
    - Controladores de periféricos.
    - Dispositivos periféricos.

cve: BOE-A-2011-19503

- Clasificación y tipos.
- Características técnicas y funcionales.

- Subsistema de comunicaciones.
  - Procesadores de comunicaciones.
  - Elementos físicos de la red de comunicaciones.
- Conexión entre componentes.
  - Jerarquía de buses. Clasificación.
  - Direccionamiento. Tipos de transferencia.
  - Temporización (síncrono, asíncrono, ciclo partido).
- Puertos y conectores.
- Arquitecturas multiprocesador.
  - Características de funcionamiento.
  - Tipología: MPP (Procesamiento Paralelo Masivo) vs SMP (Multiprocesamiento simétrico).
- Arquitecturas escalables y distribuidas.
  - Características.
  - Ventajas e inconvenientes.
  - Conceptos de Clusters, multiclusters y GRID.
- Herramientas de diagnóstico.
  - Tipos de herramientas. Detección de dispositivos.

2. Los dispositivos de almacenamiento masivo.

- Conceptos sobre dispositivos de almacenamiento masivo.
  - Tiempo de acceso.
  - Capacidad.
  - Velocidad de transferencia, etc.
- Tipos de dispositivos.
- Interfaces de almacenamiento/ tecnologías de conexión.
  - Integrated device Electronics (IDE).
  - Fibre Channel (FC)
  - Small Computer System Interface (SCSI)
  - Serial-Attached SCSI (SAS)
  - Internet SCSI (iSCSI)
- Arquitecturas / Tecnologías avanzadas de almacenamiento.
  - Protección discos RAID.
  - Redes de almacenamiento.
    - Storage Area Networks (SAN)
    - Network Attached Storage (NAS).
  - Gestor de volúmenes lógicos (LVM).

3. Dispositivos de disco.

- Componentes de un subsistema de almacenamiento en disco.
  - Controladora.
  - Unidades de disco duro.
  - Fuente de alimentación.
  - Cables.
  - LEDs, controles y tipos de conectores.
- Procedimientos de diagnóstico.
  - Los Indicadores de diagnóstico
  - Herramientas software de diagnóstico.
  - Herramientas hardware de diagnóstico.
- Actualización o sustitución de componentes.
  - Precauciones en el manejo de componentes sensibles a la estática.
  - Sustitución de unidades de disco.
  - Sustitución de otros componentes.
  - Comprobación o verificación del funcionamiento.

cve: BOE-A-2011-19503

- Cableado del subsistema de almacenamiento en disco.
- Configuraciones básicas del Hardware.
- Gestores de almacenamiento.
- Conceptos generales sobre Instalación de armarios de montaje.
  - Identificación de componentes y descripción de indicadores.
  - Procedimiento de sustitución o extracción de unidades de disco.
  - Interconexión de componentes.
  - Simbología.
  - Manejo ESD.

4. Dispositivos de almacenamiento en cinta.

- Tareas básicas de un operador.
  - Encendido y apagado de las unidades montadas en rack.
  - Protección o habilitación de escritura de los cartuchos.
  - Precaución en el manejo de cartuchos.
  - Inserción y extracción manual de cartuchos de cinta.
  - Identificación de cartuchos defectuosos.
  - Limpieza de las unidades de cinta.
  - Carga del programa inicial.
  - Tareas con el menú del sistema.
    - Conectar o desconectar unidades en línea.
    - Ver la configuración.
- Unidades de cinta.
  - Características y especificaciones.
  - Componentes de una unidad de cinta.
  - Procedimiento de instalación de una unidad de cinta.
  - Tipos de mensajes de la unidad de cinta e interpretación.
    - Identificación de problemas.
    - Procedimientos de intervención del operador.
    - El Estándar TapeAlert.
  - Panel de control e indicadores.
  - Cartuchos de cinta.
    - Tipos de cartuchos de cinta y características.
    - Formatos.
    - Componentes externos y memoria de un cartucho.
    - Cartuchos WORM (Write Only Read Many).
    - Información, manejo y cuidado.
    - Procedimientos de limpieza.
- Sistema de cintas.
- Librería de cintas.
  - Precauciones de seguridad y medio ambiente.
  - Componentes principales de una librería de cintas.
  - El panel de operador.
  - Funcionamiento de una librería de cintas.
    - Modo automatizado.
    - Modo manual. Tareas de un operador.
  - Componentes funcionales de un bastidor de una biblioteca de cintas.
  - Soportes de almacenamientos de cinta.
  - Modalidades y estados operativos de una librería de cintas.
  - Descripción de los controles e indicadores de una librería de cintas.
  - Procedimientos operativos básicos a realizar desde el panel de operador.
  - Procedimientos operativos avanzados a realizar desde el gestor de biblioteca.
  - Procedimientos operativos en modo manual.
  - Acciones del operador ante anomalías en la biblioteca.
- Virtualización en cinta.

cve: BOE-A-2011-19503

5. Material fungible de dispositivos físicos en un sistema informático.
- Tipos de dispositivos que utilizan material fungible.
- Clasificación del material fungible.
- Reciclaje.
  - Real Decreto 833/88 de 20 de julio, por el que se aprueba el reglamento para la ejecución de la Ley 20/1986, básica de residuos tóxicos y peligrosos.
  - Definiciones.
  - Etiquetado y envasado. Pictogramas.
  - Almacenamiento.
  - Catálogo Europeo de Residuos. Clasificación de material fungible.
- Las Fichas de Datos de Seguridad.
  - Identificación de peligros.
  - Primeros auxilios.
  - Manipulación y almacenamiento.
  - Otros datos.
- Reutilización del material fungible.

6. Impresoras matriciales de puntos y de líneas.
- Seguridad en el manejo de impresoras matriciales.
  - Advertencias y precauciones. Simbología.
  - Instrucciones de seguridad en la instalación, mantenimiento, manipulación del papel y en el manejo de la impresora.
- Componentes principales y su localización.
- Tipos de interfaces.
- El panel de control.
- Cintas de impresora.
- Colocación y/o sustitución de cartuchos de cinta.
- Alimentación de papel manual y continuo.
- Sistemas de gestión de las impresoras.
- Realización de pruebas de impresión.
- Configuración de la impresora.
- Búsqueda de errores y diagnósticos.

7. Impresoras láser.
- Seguridad en el manejo de impresoras láser.
  - Advertencias y precauciones. Simbología.
  - Instrucciones de seguridad en la instalación, mantenimiento, manipulación de los cartuchos de tóner, manejo de la impresora, radiación láser y seguridad de ozono.
- Componentes principales y su localización.
- Áreas funcionales.
- Tipos de interfaces.
- El panel de control.
- Tipos de material fungible y su duración.
- Alimentación de papel manual y continuo. Almacenamiento.
- Reemplazo del material fungible.
- Responsabilidades y tareas del operador.
- Limpieza de la impresora.

8. Impresoras de inyección de tinta.
- Seguridad en el manejo de impresoras de inyección de tinta.
  - Advertencias y precauciones. Simbología.
  - Instrucciones de seguridad en la instalación, mantenimiento, manipulación de los cartuchos de tinta y en el manejo de la impresora.
- Piezas de una impresora de inyección de tinta.
- Limpieza de la impresora.
- Lubricación.

cve: BOE-A-2011-19503

- Consumibles.
- Sustitución de consumibles.
  - Comprobación del estado del cartucho de tinta a través del panel de control, de indicadores luminosos o a través del controlador de la impresora.
  - Sustitución de cartuchos de tinta.
  - Sustitución de la caja de mantenimiento.

9. Técnicas de inventario en sistemas informáticos.

- Registros de inventario de dispositivos físicos.
  - Ciclo de Vida de un inventario.
  - Información relevante para un inventario.
  - Técnicas de inventariado (escaneo pasivo, activo).
  - Metodología ITIL.
- Herramientas software de inventario del sistema informático.
  - Funciones básicas.
  - Componentes.
    - Agente remoto de monitorización.
    - Agente de gestión remota
    - Interfaz de usuario de administración.
    - Escáner de dispositivos
    - Módulo de generación de informes
  - Configuración.
    - Configuración de los agentes
    - Configuración del escaneo de dispositivos
  - Interpretación de los informes.
  - Utilización básica de un software de inventario.

UNIDAD FORMATIVA 2

Denominación: MONITORIZACIÓN Y GESTIÓN DE INCIDENCIAS DE LOS SISTEMAS FÍSICOS.

Código: UF1350

Duración: 60 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP3.

Capacidades y criterios de evaluación

C1: Regular el rendimiento de los dispositivos físicos utilizando herramientas de monitorización, siguiendo unas especificaciones dadas.

CE1.1 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.

CE1.2 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.

CE1.3 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.

CE1.4 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.

CE1.5 Aplicar procedimientos de medida del rendimiento físico utilizando las herramientas indicadas para comprobar que la funcionalidad del sistema

cve: BOE-A-2011-19503

informático está dentro de parámetros prefijados, según unas especificaciones técnicas dadas.

CE1.6 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.

CE1.7 Realizar la 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, actuando según procedimientos establecidos ante situaciones anómalas.
- Realizar cambios de configuración en los dispositivos físicos indicados de acuerdo a especificaciones recibidas.
- Registrar en el inventario los cambios de configuración realizados.
- Documentar el trabajo realizado detallando las situaciones anómalas detectadas.

C2: Interpretar las incidencias y alarmas detectadas en el subsistema físico y realizar acciones correctivas para su solución siguiendo unas especificaciones dadas.

CE2.1 Identificar incidencias de funcionamiento producidas por los dispositivos físicos que forman el subsistema para clasificar las acciones correctivas a aplicar según las especificaciones recibidas.

CE2.2 Explicar las estrategias para detectar situaciones anómalas en el funcionamiento del subsistema.

CE2.3 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.

CE2.4 Aplicar procedimientos establecidos de respuesta para la resolución de incidencias detectadas en el funcionamiento y rendimiento de los dispositivos físicos según unas especificaciones dadas.

CE2.5 Realizar acciones correctivas para solucionar el mal funcionamiento de dispositivos físicos del sistema, dados unos procedimientos a aplicar:

- Ejecutar 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.
- Documentar el trabajo realizado detallando las situaciones de incidencia producidas.

Contenidos

1. **Introducción a la evaluación y a las métricas de rendimiento.**
   - Definiciones y conceptos básicos de la evaluación del rendimiento.
     - Sistema de procesamiento de información.
     - Prestaciones.
     - Rendimiento.
   - Recursos y componentes críticos de los sistemas informáticos.

cve: BOE-A-2011-19503

- Técnicas de evaluación del rendimiento.
  - Medición. Índices.
  - Simulación. Carga de trabajo.
  - Modelado analítico.
- Sistemas de referencia.
- Métricas de rendimiento
  - Métricas de rendimiento de red.
  - Métricas de rendimiento de sistema.
  - Métricas de rendimiento de servicios.

2. Técnicas de monitorización y medida de rendimiento de los dispositivos físicos.

- Representación y análisis de los resultados de las mediciones.
- Rendimiento de los dispositivos físicos.
- Parámetros de configuración y rendimiento.

3. Herramientas de monitorización.

- Procedimiento de instalación de una plataforma de monitorización.
- Requisitos técnicos.
- Conceptos generales relacionados con la monitorización.
  - Protocolos de gestión de red (ICMP, SNMP).
  - Repositorios de información:
  - CMDB (Base de Datos de la Gestión de Configuración).
  - MIB (Base de Información Gestionada).
  - Elementos o instancias a monitorizar.
  - Tipos de instancias.
  - Tipos de eventos.
  - Los Servicios.
  - La supervisión.
    - Perfiles de usuario.
    - Responsabilidades.
- Arquitectura de una plataforma de monitorización.
  - Consola de gestión.
  - Componentes de una plataforma de monitorización.
    - Servidor central.
    - Repositorio de componentes.
    - Agentes de monitorización.
    - Proxies, gestión remota.
- La consola de monitorización.
  - Descripción.
  - Gestión de eventos, tipos y acciones.
  - Otros tipos de gestión.
  - Funcionalidades para gestionar y supervisar la infraestructura.
  - Sistema de notificaciones.

4. Monitorización de dispositivos físicos.

- El estándar IPMI.
- Herramientas de monitorización en distintas plataformas.
  - Monitorización de recursos.
    - Carga de procesador.
    - Espacio libre en filesystems.
    - Uso de la memoria física.
    - Número de operaciones de entrada/salida.
    - Número de ficheros abiertos.
    - Monitorización de impresoras.
    - Monitorización de otros recursos.

cve: BOE-A-2011-19503

- Monitorización del uso de servicios de red.
  - Correo electrónico (SMTP, POP3).
  - Conexiones HTTP abiertas.
  - Conexiones remotas seguras (SSH).
  - Otros servicios.
- Parámetros de configuración y rendimiento de los dispositivos físicos.
  - Optimización de la memoria caché.
  - Tamaño del fichero de paginación.
  - Tamaño de memoria dedicada a la Maquina Virtual Java.
  - Otros parámetros.
- Definición de alarmas activas, pasivas, eventos y alertas.

5. Modelos de gestión y monitorización: Gestión de Servicios según ITIL

- Estructura de procesos en ITIL y la relación entre ellos.
- Responsabilidades, funciones, niveles de personal, etc., del Centro de Servicio al Usuario.
- Procesos y procedimientos del Centro de Servicio al Usuario.

6. Técnicas de diagnóstico de incidencias y alarmas del subsistema físico.

- Clasificación de incidencias y alarmas de los dispositivos físicos.
  - Caídas del sistema.
  - Servicios no disponibles.
  - Alertas automáticas de fallos de periféricos.
  - Umbral de uso de espacio en disco excedido.
  - Otras incidencias y alarmas.
- Estrategias para detectar situaciones anómalas en el funcionamiento del subsistema.
- Herramientas de diagnóstico de incidencias y alarmas de los dispositivos físicos.
- Métodos establecidos para solución incidencias.
  - Herramientas de gestión remota de dispositivos (consolas virtuales, terminales remotos, etc.)
  - Herramientas de gestión de incidencias
    - Registro de incidentes y su valoración.
    - Cierre temporal y cierre definitivo.
    - Rechazar / reclamar incidencias.
    - Registro tiempo actuación y Control de tiempos máximos.
    - Elaboración de informes.

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Duración total en horas de las unidades formativas	N.º de horas máximas susceptibles de formación a distancia
Unidad formativa 1– UF1349	90	50
Unidad formativa 2– UF1350	60	40

Secuencia:

Para acceder a la unidad formativa 2 debe haberse superado la unidad formativa 1.

Criterios de acceso para los alumnos

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

cve: BOE-A-2011-19503

MÓDULO FORMATIVO 3

Denominación: MANTENIMIENTO DEL SUBSISTEMA LÓGICO DE SISTEMAS INFORMÁTICOS.

Código: MF0958_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0958_2: Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de cliente.

Duración: 150 horas

UNIDAD FORMATIVA 1

Denominación: GESTIÓN Y OPERATIVA DEL SOFTWARE DE UN SISTEMA INFORMÁTICO

Código: UF1351

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1, RP2 y RP4.

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 Realizar la identificación de componentes software del sistema para su utilización, según unas especificaciones dadas:

- Operar con el 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 legislación vigente.

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

CE2.1 Realizar la instalación de componentes software de aplicación para añadir funcionalidad al sistema:

cve: BOE-A-2011-19503

- Comprobar los requisitos de instalación del software a implantar en el sistema.
- Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector utilizándola de ayuda.
- Verificar que las licencias de utilización de los componentes software cumplen la legislación vigente.
- 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 Realizar la 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.
- Identificar los «parches» y otros módulos de código disponibles para aumentar la funcionalidad del componente o para corregir un comportamiento no adecuado.
- Verificar y comprobar que las licencias de utilización de los componentes software cumplen la legislación vigente.
- 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.
- Configurar el componente software de acuerdo a 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.
- Mantener el inventario de software actualizado registrando los cambios realizados.

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.

cve: BOE-A-2011-19503

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 Realizar tareas de administración para el mantenimiento de los componentes del sistema, siguiendo unas especificaciones dadas:

- Seleccionar la herramienta administrativa.
- Interpretar la documentación técnica asociada, incluso si está editada en la lengua extranjera de uso más frecuente en el sector utilizándola de ayuda.
- Aplicar procedimientos establecidos para el mantenimiento de los soportes de información.
- Aplicar procedimientos establecidos 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.
- Mantener el inventario de software actualizado registrando los cambios realizados.

Contenidos

1. **El Software en el sistema informático.**
   - Definición de «Software».
   - Clasificación del software.
     - Según el propósito.
     - Según las funciones,
     - Según el modo de ejecución.
   - Software de sistema y software de usuario.
     - Funciones y características.
   - Interfaces de usuario.
     - Definiciones de interfaz.
     - Características de una interfaz.
     - Tipos de interfaces.
   - Elementos de configuración de los componentes software.

2. **Procedimientos para la instalación de componentes software.**
   - El software de gestión y mantenimiento de activos informáticos.
   - Funciones básicas de un software de gestión y mantenimiento de activos informáticos.
     - Gestión de usuarios.
     - Inventario de Hardware y Software.
     - Avisos.
     - Medición de aplicaciones.
     - Gestión de licencias.
     - Distribución de software.
     - Otras funciones.

cve: BOE-A-2011-19503

- Requisitos de un sistema gestión y mantenimiento de activos informáticos.
  - Componentes y requisitos del sistema.
  - Instalación de componentes: parámetros y configuración.
  - Servidor de Base de Datos.
  - Cliente. Herramientas de despliegue remoto.
  - La consola del sistema.
  - El Gateway del servidor.
  - El Gateway de cliente.
  - Instalación y configuración de la base de datos.
- Aplicación de configuraciones específicas a clientes, grupos y/o departamentos.
- Gestión de usuarios.

3. El inventario de software.

- Registros y bases de datos del software instalado.
- Herramientas software de inventario.
  - Funciones básicas.
  - El Inventario de Software.
    - Obtención de aplicaciones instaladas.
    - Realización de consultas a la base de datos.
    - Generación de informes.
    - Administración de licencias.
    - Otras operaciones.

4. Procedimientos para la instalación de componentes software.

- Licencias del software.
  - Definiciones.
  - Tipos de licencia: propiedad, uso y distribución del software.
  - Licencias más importantes de software no propietario: GPL, BSD, MPL, EUPL.
  - Derechos de autor y normativa vigente.
- Instalación y prueba de componentes software de aplicación.
  - Identificación de los requisitos del sistema.
  - Documentación del fabricante.
  - Parámetros y configuración del sistema en el proceso de instalación.
  - El Proceso de instalación.
  - Instalaciones programadas e instalaciones remotas.
  - Configuración de aplicaciones para el acceso a periféricos.
  - Realización de pruebas.
  - Registros y bases de datos del software instalado.
- Herramientas para la distribución del software.
  - Obtención de información de la distribución del software.
  - Realización de consultas a la base de datos.
  - Generación de informes.
  - Administración de paquetes software.
    - Creación y distribución de paquetes.
    - Programación del despliegue.
    - Publicación de paquetes.
    - Instalaciones no automatizadas.
      - Creación de instaladores y archivos de comando.
    - Otras funciones.

5. Procedimientos de mantenimiento de software.

- Tipos de mantenimiento del software.
  - Correctivo.
  - Evolutivo.
- Objetivos de un plan de mantenimiento.
- Procedimientos de gestión del mantenimiento.

cve: BOE-A-2011-19503

- Control de cambios.
- Gestión de peticiones de cambio y responsables de las mismas.

- Proceso de actualización del software de aplicación.
  - Similitudes con el proceso de instalación.
  - Verificación de requisitos de actualización.
  - Proceso de desinstalación del software no utilizado.
  - Proceso de actualización del software.
  - Restauración del software previo a la actualización.
  - Realización de pruebas.
- Mantenimiento de la base de datos.
  - Eliminación de datos, equipos y usuarios.
  - Eliminación de aplicaciones y programas.
  - Exportación e importación de datos.
  - Copias de seguridad.

6. Procedimientos de administración.

- Conceptos básicos sobre administración de sistemas en red.
  - El sistema operativo de red.
  - Tareas básicas de administración.
  - Entornos de sistema, perfiles y propiedades.
    - Administración de aplicaciones y procesos.
  - Controladores y dispositivos hardware.
  - Administración de procesos, servicios y eventos.
  - Automatizar tareas administrativas, directiva y procedimientos.
- Tipos de tareas administrativas más comunes, características y modos de ejecución.
- Herramientas administrativas.
  - Mantenimiento del sistema de archivos y soportes de información.
    - Tipos de soportes físicos para el almacenamiento de información.
    - Mantenimiento de medios de almacenamiento extraíbles.
    - Desfragmentación de discos.
    - Compresión de unidades, carpetas y archivos.
    - Liberación de espacio de disco.
    - Realización de copias de seguridad y recuperación de datos.
  - Mantenimiento de la configuración del software de base y de aplicación.
  - Administración de impresoras de red y servicios de impresión.
    - Instalación y configuración de impresoras locales y de red.
    - Gestión de los trabajos.
  - Ejecución de tareas administrativas automáticas.
    - Asistentes y utilidades en línea de comandos.
    - Administración de tareas programadas.
    - Programación de tareas.
  - Ejecución de programas y guiones administrativos.
    - Tipos de archivos de comando.
    - Contenido de los archivos de comando.
    - Asignación de archivos de comandos.
- Herramientas de gestión remota.

UNIDAD FORMATIVA 2

Denominación: MONITORIZACIÓN Y GESTIÓN DE INCIDENCIAS DEL SOFTWARE.

Código: UF1352

Duración: 60 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP3.

cve: BOE-A-2011-19503

Capacidades y criterios de evaluación

C1: 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.

CE1.1 Explicar los fundamentos de la medida del rendimiento de software detallando las técnicas utilizadas para la evaluación de la funcionalidad del sistema.

CE1.2 Identificar los parámetros de configuración y rendimiento de los elementos del software base y de aplicación, para monitorizar el sistema.

CE1.3 Describir las herramientas de medida del rendimiento del software, clasificando las métricas disponibles en cada caso, teniendo en cuenta las especificaciones técnicas asociadas.

CE1.4 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.

CE1.5 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.

CE1.6 Realizar la medición del rendimiento del software base y aplicación para detectar situaciones anómalas, siguiendo unas especificaciones dadas:

- 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, actuando según indicaciones recibidas.
- Documentar el trabajo realizado.

C2: Identificar las incidencias y alarmas detectadas en el subsistema lógico para realizar acciones correctivas según unas especificaciones dadas.

CE2.1 Clasificar las incidencias y alarmas de funcionamiento y acceso producidas en los elementos software del sistema para detectar problemas de funcionamiento en el software.

CE2.2 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.

CE2.3 Aplicar procedimientos especificados de respuesta para atender incidencias detectadas en el funcionamiento del software base y aplicación, siguiendo las instrucciones dadas.

CE2.4 Aplicar las acciones correctivas para solventar el mal funcionamiento del software base y aplicación siguiendo unas especificaciones dadas:

- 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.

Contenidos

1. **Técnicas de monitorización y medida del rendimiento de los elementos de software.**
   - Conceptos básicos sobre evaluación y métricas del rendimiento.
   - Parámetros de configuración y rendimiento de los componentes software.

cve: BOE-A-2011-19503

- Parámetros de configuración y rendimiento del software base.
- Parámetros de configuración y rendimiento del software de aplicación.

– Herramientas de monitorización del software.
  – Herramientas de medida del rendimiento del software.
    – El Monitor del sistema.
      – Conceptos básicos.
      – La interfaz del monitor.
      – La configuración del monitor.
    – Registros y alertas de rendimiento.
    – Utilidades de supervisión del rendimiento desde la línea de comandos.
– Procedimiento de medida del rendimiento.
  – Configuración de la supervisión del rendimiento.
    – Método y frecuencia de la supervisión.
    – Componentes y aspectos de supervisión.
    – Registro de los datos del rendimiento.
  – Selección de contadores adecuados de supervisión.
  – Descripción de problemas de rendimiento típicos.
  – Estrategias de optimización, prueba de equipos y resolución de problemas.
    – Supervisión del uso de la memoria.
    – Supervisión de la actividad del procesador.
    – Supervisión de la actividad del disco.
    – Supervisión la actividad de la red.
    – Supervisión de los servicios disponibles en el Sistema operativo.
– Mantenimiento remoto: herramientas y configuración.

2. La plataforma de gestión de operaciones.

– Conceptos de seguridad de una plataforma de gestión de operaciones.
  – Terminología.
  – Perfiles, descripción y ámbito.
– Componentes básicos de una plataforma de gestión de operaciones.
– La consola de operaciones.
  – Descripción de la consola de Operaciones.
    – Características y funciones.
    – Acceso a la consola.
– Descripción de los módulos de los módulos de administración.
– Los monitores.
– Las reglas para la obtención de datos y sus tipos.
– Incidencias y alarmas
  – Identificación de las incidencias y alarmas.
  – Clasificación de la gravedad.
  – Resolución de incidencias y alarmas mediante la ejecución de tareas.
  – Configuración de notificaciones.
– Creación de informes.

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Duración total en horas de las unidades formativas	N.º de horas máximas susceptibles de formación a distancia
Unidad formativa 1– UF1351	90	50
Unidad formativa 1– UF1352	60	40

Secuencia:

Para acceder a la unidad formativa 2 debe haberse superado la unidad formativa 1.

cve: BOE-A-2011-19503

Criterios de acceso para los alumnos

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

MÓDULO FORMATIVO 4

Denominación: MANTENIMIENTO DE LA SEGURIDAD EN SISTEMAS INFORMÁTICOS.

Código: MF0959_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.

Duración: 120 horas

UNIDAD FORMATIVA 1

Denominación: MONITORIZACIÓN DE LOS ACCESOS AL SISTEMA INFORMÁTICO.

Código: UF1353

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP2.

Capacidades y criterios de evaluación

C1: 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.

CE1.1 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.

CE1.2 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.

CE1.3 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.

CE1.4 Identificar los mecanismos de protección del sistema contra virus y programas maliciosos para asegurar su actualización.

CE1.5 Identificar los mecanismos de seguridad del sistema para mantener la protección del mismo, según unos procedimientos de operación especificados:

– Identificar los usuarios y grupos definidos en el sistema operando con 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.

cve: BOE-A-2011-19503

– Comprobar el registro de los usuarios y grupos en el inventario, registrando los cambios detectados.

C2: Interpretar las trazas de monitorización de los accesos y actividad del sistema identificando situaciones anómalas, siguiendo unas especificaciones dadas.

CE2.1 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.

CE2.2 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.

CE2.3 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.

CE2.4 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.

CE2.5 En supuestos prácticos, donde se cuenta con ficheros de traza de conexión de usuarios y ficheros de actividad del sistema, realizar el análisis y la evaluación de los mismos para detectar posibles accesos y actividades no deseadas, según unas especificaciones dadas:

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

CE2.6 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.

Contenidos

1. Gestión de la seguridad informática

– Objetivo de la seguridad.
– Términos relacionados con la seguridad informática.
– Procesos de gestión de la seguridad.
  – Objetivos de la gestión de la seguridad.
  – Beneficios y dificultades.
  – Política de seguridad. La Ley Orgánica de Protección de Datos de carácter personal.
  – Análisis de riesgo.
    – Identificación de recursos.
    – Identificación de vulnerabilidades y amenazas: atacante externo e interno.
    – Medidas de protección.
  – Plan de seguridad.
– Interrelación con otros procesos de las tecnologías de la información.
– Seguridad física y seguridad lógica.

2. Seguridad lógica del sistema

– Acceso al sistema y al software de aplicación.
  – Concepto de usuario, cuenta, grupo de usuario, permisos, lista de control de accesos (ACL).
  – Políticas de seguridad respecto de los usuarios.

cve: BOE-A-2011-19503

- Autenticación de usuarios:
  - Definición y conceptos básicos.
  - Sistemas de autenticación débiles y fuertes.
  - Sistemas de autenticación biométricos y otros sistemas.
  - Acceso local, remote y Single Sing-On.
- Herramientas para la gestión de usuarios.
  - El servicio de directorio: conceptos básicos, protocolos e implementaciones.
  - Directorios: LDAP, X500, Active Directory.
  - Herramientas de administración de usuarios y equipos.
  - Administración básica del servicio de directorio.
- Confidencialidad y Disponibilidad de la información en el puesto de usuario final.
  - Sistemas de ficheros y control de acceso a los mismos.
  - Permisos y derechos sobre los ficheros.
- Seguridad en el puesto de usuario.
  - Tipología de software malicioso.
  - Software de detección de virus y programas maliciosos.
    - Antivirus, antispyware, firewall, filtros antispam, etc.
  - Técnicas de recuperación y desinfección de datos afectados.
- Herramientas de gestión remota de incidencias.

3. Procedimientos de monitorización de los accesos y la actividad del sistema

- Objetivos de la monitorización y de la gestión de incidentes de seguridad.
- Procedimientos de monitorización de trazas.
  - Identificación y caracterización de aspectos monitorizables o auditables.
  - Clasificación de eventos e incidencias: de sistema, de aplicación, de seguridad
  - Mecanismos de monitorización de trazas: logs del sistema, consolas de monitorización de usuarios
  - Información de los registros de trazas.
- Técnicas y herramientas de monitorización.
  - Técnicas: correlación de logs, de eventos.
  - Herramientas de monitorización.
    - Herramientas propias del sistema operativo.
    - Sistemas basados en equipo (HIDS).
    - Sistemas basados en red (NIDS).
    - Sistemas de prevención de intrusiones (IPS).
- Informes de monitorización.
  - Recolección de información.
  - Análisis y correlación de eventos.
  - Verificación de la intrusión.
  - Alarmas y acciones correctivas
- Organismos de gestión de incidentes:
  - Nacionales. IRIS-CERT, esCERT.
  - Internacionales. CERT, FIRST.

UNIDAD FORMATIVA 2

Denominación: COPIA DE SEGURIDAD Y RESTAURACIÓN DE LA INFORMACIÓN.

Código: UF1354

Duración: 30 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP3 y RP4.

cve: BOE-A-2011-19503

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 de copias de seguridad y almacenamiento de datos del sistema informático para garantizar la integridad de la información del sistema.

CE1.3 Explicar los procedimientos y herramientas para la restauración de datos de un sistema informático para la recuperación de la información del sistema, según las especificaciones dadas.

CE1.4 Explicar los procedimientos y herramientas para la verificación de la copia de seguridad y de la restauración de datos para asegurar la fiabilidad del proceso según las especificaciones dadas.

CE1.5 En un sistema de almacenamiento de datos con varios dispositivos, realizar copias de seguridad para garantizar la integridad de datos, dados unos procedimientos a seguir:

- Seleccionar el dispositivo de almacenamiento y 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 almacenaje según las condiciones ambientales, de ubicación y de seguridad especificadas.
- Comprobar y registrar las incidencias detectadas.
- Documentar los procesos realizados.

CE1.6 Realizar la restauración de copias de seguridad para recuperar la información almacenada, dados unos procedimientos a seguir:

- Seleccionar la herramienta para realizar la restauración de acuerdo al tipo y soporte de copia de seguridad realizada.
- Realizar el proceso de restauración según las indicaciones recibidas.
- Verificar el proceso de restauración comprobando el destino de la misma.
- Comprobar y registrar las incidencias detectadas.
- Documentar los procesos realizados.

C2: Describir las condiciones ambientales y de seguridad para el funcionamiento de los equipos y dispositivos físicos que garanticen los parámetros de explotación dados.

CE2.1 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.

CE2.2 Identificar los factores de seguridad y ergonomía a tener en cuenta en la ubicación de equipos y dispositivos físicos para garantizar los condicionantes de implantación de los dispositivos, según las especificaciones técnicas de los mismos.

CE2.3 Comprobar las condiciones ambientales para asegurar la situación de equipos y dispositivos físicos, de acuerdo a las normas especificadas:

- 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.

cve: BOE-A-2011-19503

- Identificar las condiciones de seguridad y ambientales adecuadas y no adecuadas.
- Proponer acciones correctivas para asegurar los requisitos de seguridad y de condiciones ambientales.

Contenidos

1. **Copias de seguridad**
   - Tipos de copias de seguridad (total, incremental, diferencial).
   - Arquitectura del servicio de copias de respaldo.
   - Medios de almacenamiento para copias de seguridad.
   - Herramientas para la realización de copias de seguridad.
     - Funciones básicas.
     - Configuración de opciones de restauración y copias de seguridad.
     - Realización de copias de seguridad.
     - Restauración de copias y verificación de la integridad de la información.
   - Realización de copias de seguridad y restauración en sistemas remotos.

2. **Entorno físico de un sistema informático.**
   - Los equipos y el entorno: adecuación del espacio físico.
     - Ubicación y acondicionamiento de espacios de dispositivos físicos.
       - Factores ambientales.
       - Factores de seguridad y ergonomía.
     - Ubicación y acondicionamiento de material fungible y soportes de información.
   - Agentes externos y su influencia en el sistema.
   - Efectos negativos sobre el sistema.
   - Creación del entorno adecuado.
     - Condiciones ambientales: humedad 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.
   - El Centro de Proceso de datos (CPD).
     - Requisitos y ubicación de un CPD.
     - Condiciones del medio ambiente externo.
     - Factores que afectan a la seguridad física de un CPD.
     - Acondicionamiento.
     - Sistemas de seguridad física.
   - Plan de Emergencia y Evacuación.

3. **Reglamentos y normativas**
     - El estándar ANSI/TIA-942-2005.
     - Medidas de seguridad en el tratamiento de datos de carácter personal (RD 1720/2007).
       - La guía de seguridad.

cve: BOE-A-2011-19503

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Duración total en horas de las unidades formativas	N.º de horas máximas susceptibles de formación a distancia
Unidad formativa 1– UF1353	90	50
Unidad formativa 1– UF1354	30	20

Secuencia:

Para acceder a la unidad formativa 2 debe haberse superado la unidad formativa 1.

Criterios de acceso para los alumnos

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

MÓDULOS DE PRÁCTICAS PROFESIONALES NO LABORALES DE OPERACIÓN DE SISTEMAS INFORMÁTICOS.

Código: MP0286

Duración: 40 horas

Capacidades y criterios de evaluación

C1: Instalar y configurar el software de base de acuerdo con los protocolos y procedimientos establecidos en la empresa.

CE1.1 Identificar las fases que intervienen en la instalación de sistema operativo comprobando los requisitos del equipo informático.

CE1.2 Realizar la instalación, configuración y/o actualización del sistema operativo, así como, de los programas de utilidades, de acuerdo con las unas especificaciones recibidas y las necesidades del cliente.

CE1.3 Verificar el funcionamiento del equipo una vez realizada la instalación.

CE1.4 Utilizar las aplicaciones que proporcionan los sistemas operativos para la explotación del mismo.

CE1.5 Documentar el trabajo realizado de acuerdo con los procedimientos de la empresa.

C2: Mantener y regular el sistema informático empresarial, así como la seguridad de los subsistemas, de acuerdo con los procedimientos establecidos y dependiendo del administrador del sistema o persona en quien delegue.

CE2.1 Realizar tareas de comprobación y verificación de las conexiones de los componentes físicos del sistema, así como de los propios equipos, procediendo a su sustitución o actualización, de acuerdo con los procedimientos de la empresa o del administrador del sistema.

CE2.2 Sustituir los elementos fungibles a petición de los usuarios o cuando así lo indique una alarma, de acuerdo con los procedimientos establecidos en la empresa, verificando posteriormente el funcionamiento del equipo.

CE2.3 Colaborar en la monitorización del rendimiento del subsistema físico y lógico, ejecutando los programas de medición, bajo la supervisión del administrador del sistema, informándole de los resultados obtenidos y colaborando, cuando sea necesario, en las medidas correctivas.

CE2.4 Realizar o revisar el inventario del sistema, de acuerdo con las normas de la organización, anotando las incidencias detectadas para su uso posterior, de acuerdo con los procedimientos establecidos.

cve: BOE-A-2011-19503

CE2.5 Realizar procesos de diagnósticos en los equipos clientes, así como, instalar y actualizar las aplicaciones de usuario de acuerdo con las indicaciones del administrador del sistema y de los procedimientos empresariales.
CE2.6 Colaborar en tareas de administración del software de base y de aplicación por indicación del administrador del sistema
CE2.7 Colaborar en la comprobación de los mecanismos de seguridad establecidos por la empresa, así como los accesos al sistema, así como, realizar las copias de seguridad, establecidas en los procedimientos, o por indicación del administrador del sistema.
CE2.8 Documentar el trabajo realizado de acuerdo con las prescripciones y procedimientos empresariales.

C3: Participar en los proceso de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.
CE3.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.
CE3.2 Respetar los procedimientos y normas del centro de trabajo.
CE3.3 Emprender con diligencia las tareas según las instrucciones recibidas tratando de que se adecuen al ritmo de trabajo de la empresa.
CE3.4 Integrarse en los procesos de producción del centro de trabajo.
CE3.5 Utilizar los canales de comunicación establecidos.
CE3.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. **Instalación, configuración y mantenimiento de sistemas microinformáticos de acuerdo con los procedimientos de la empresa.**
   - Instalación y configuración del software de base.
   - Participación en la instalación y configuración de redes de área local.
   - Colaboración en la instalación, configuración, mantenimiento y asistencia al usuario de paquetes informáticos de acuerdo con los procedimientos empresariales.

2. **Mantenimiento y políticas de seguridad del sistema informático empresarial.**
   - Arquitectura del sistema informático de la empresa.
   - Funciones del operador de sistemas informáticos.
   - El inventario del sistema y las aplicaciones corporativas.
   - Las plataformas de monitorización y el software de gestión y mantenimiento de activos informáticos empresariales.
   - Procedimientos de operación para el mantenimiento del subsistema físico.
   - Procedimientos de mantenimiento lógico de la organización.
   - Las políticas de seguridad de la organización.
   - Procedimientos de copias de seguridad y restauración.

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

cve: BOE-A-2011-19503

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	*Experiencia profesional requerida en el ámbito de la Unidad de competencia	
		Con acreditación	Sin acreditación
MF0219_2: Instalación y configuración de sistemas operativos.	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes • Técnico Superior en la familia de Informática y comunicaciones • Certificado de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones, área de Sistemas y telemática	1 año	3 años
MF0957_2: Mantenimiento del subsistema físico en sistemas informáticos.	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes • Técnico Superior en la familia de Informática y comunicaciones • Certificado de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones, área de Sistemas y telemática	2 años	4 años
MF0958_2: Mantenimiento del subsistema lógico en sistemas informáticos.	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes • Técnico Superior en la familia de Informática y comunicaciones • Certificado de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones, área de Sistemas y telemática	2 años	4 años
MF0959_2: Mantenimiento de la seguridad en sistemas informáticos.	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes • Técnico Superior en la familia de Informática y comunicaciones • Certificado de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones, área de Sistemas y telemática	2 años	4 años

* En los últimos cinco, excepto MF0219_2 que será en los últimos tres años.

cve: BOE-A-2011-19503

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m² 15 alumnos	Superficie m² 25 alumnos
Aula de Informática.	60	75

Espacio Formativo	M1	M2	M3	M4
Aula de Informática.	X	X	X	X

Espacio Formativo	Equipamiento
Aula de Informática	– PCs instalados en red y conexión a Internet. – Armario de cableado con paneles de parcheado, y dispositivos de conexión a red. – Software de base y de red. – Software de seguridad y antivirus. – Software para copias de seguridad y recuperación. – Software de gestión y mantenimiento de activos informáticos: software de inventariado automático, medición de aplicaciones, gestión de licencias, distribución del software, etc. – Software de monitorización. – Software de diagnóstico. – Herramientas de administración. – Software de compresión de ficheros. – Gestores de discos y de arranque. – Software de diagnóstico. – Software para pruebas de conectividad. – Herramientas de gestión remota. – Software ofimático. – Subsistema de almacenamiento en disco y/o en cinta. – Impresoras matriciales, láser y de inyección de tinta. – Equipamiento de ensamblaje y medida: herramientas de ensamblaje y desensamblaje, medidores de tensión, herramientas para la confección de cableado. – Cañón de proyección. – Rotafolios. – Pizarra. – Material de aula. – Mesa y silla para el formador. – Mesas y sillas para alumnos. – Mobiliario auxiliar para el equipamiento de aula. * El equipamiento y el software correspondiente deberán estar actualizados.

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

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

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

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

cve: BOE-A-2011-19503