I. DISPOSICIONES GENERALES

MINISTERIO DE TRABAJO E INMIGRACIÓN

10055 *Real Decreto 686/2011, de 13 de mayo, por el que se establecen seis certificados de profesionalidad de la familia profesional Informática y comunicaciones que se incluyen en el Repertorio Nacional de certificados de profesionalidad.*

La Ley 56/2003, de 16 de diciembre, de Empleo, establece, en su artículo 3, que corresponde al Gobierno, a propuesta del actual Ministerio de Trabajo e Inmigración, y previo informe de este Ministerio a la Conferencia Sectorial de Empleo y Asuntos Laborales, la elaboración y aprobación de las disposiciones reglamentarias en relación con, entre otras, la formación profesional ocupacional y continua en el ámbito estatal, así como el desarrollo de dicha ordenación.

El artículo 26.1 de la citada Ley 56/2003, de 16 de diciembre, tras la modificación llevada a cabo por el Real Decreto-ley 3/2011, de 18 de febrero, de medidas urgentes para la mejora de la empleabilidad y la reforma de las políticas activas de empleo, se ocupa del subsistema de formación profesional para el empleo, en el que, desde la entrada en vigor del Real Decreto 395/2007, de 23 de marzo, que lo regula, han quedado integradas las modalidades de formación profesional en el ámbito laboral –la formación ocupacional y la continua. Dicho subsistema, según el reseñado precepto legal y de acuerdo con lo previsto en la Ley Orgánica 5/2002, de las Cualificaciones y la Formación Profesional, se desarrollará en el marco del Sistema Nacional de Cualificaciones y Formación Profesional y del Sistema Nacional de Empleo.

Por su parte, la Ley Orgánica 5/2002, de 19 de junio, entiende el Sistema Nacional de Cualificaciones y Formación Profesional como el conjunto de instrumentos y acciones necesarios para promover y desarrollar la integración de las ofertas de formación profesional y la evaluación y acreditación de las competencias profesionales. Instrumentos principales de ese Sistema son el Catálogo Nacional de las Cualificaciones Profesionales y el procedimiento de reconocimiento, evaluación, acreditación y registro de las mismas. En su artículo 8, la Ley Orgánica 5/2002, de 19 de junio, establece que los certificados de profesionalidad acreditan las cualificaciones profesionales de quienes los han obtenido y que serán expedidos por la Administración competente, con carácter oficial y validez en todo el territorio nacional. Además, en su artículo 10.1, indica que la Administración General del Estado, de conformidad con lo que se establece en el artículo 149.1.30.ª y 7.ª de la Constitución y previa consulta al Consejo General de la Formación Profesional, determinará los títulos y los certificados de profesionalidad, que constituirán las ofertas de formación profesional referidas al Catálogo Nacional de Cualificaciones Profesionales.

El Catálogo Nacional de las Cualificaciones Profesionales, según el artículo 3.3 del Real Decreto 1128/2003, de 5 de septiembre, por el que se regula el Catálogo Nacional de las Cualificaciones Profesionales, en la redacción dada al mismo por el Real Decreto 1416/2005, de 25 de noviembre, constituye la base para elaborar la oferta formativa conducente a la obtención de los títulos de formación profesional y de los certificados de profesionalidad y la oferta formativa modular y acumulable asociada a una unidad de competencia, así como de otras ofertas formativas adaptadas a colectivos con necesidades específicas. De acuerdo con lo establecido en el artículo 8.5 del mismo real decreto, la oferta formativa de los certificados de profesionalidad se ajustará a los indicadores y requisitos mínimos de calidad que garanticen los aspectos fundamentales de un sistema integrado de formación, que se establezcan de mutuo acuerdo entre las Administraciones educativa y laboral, previa consulta al Consejo General de Formación Profesional.

El Real Decreto 34/2008, de 18 de enero, por el que se regulan los certificados de profesionalidad, modificado por el Real Decreto 1675/2010, de 10 de diciembre, ha actualizado, en consonancia con la normativa mencionada, la regulación de los certificados que se

cve: BOE-A-2011-10055

establecían en el anterior Real Decreto 1506/2003, de 28 de noviembre, por el que se establecen las directrices de los certificados de profesionalidad, que han sido derogados.

En dicho Real Decreto 34/2008, modificado por Real Decreto 1675/2010, se define la estructura y contenido de los certificados de profesionalidad, a partir del Catálogo Nacional de las Cualificaciones Profesionales y de las directrices fijadas por la Unión Europea, y se establece que el Servicio Público de Empleo Estatal, con la colaboración de los Centros de Referencia Nacional, elaborará y actualizará los certificados de profesionalidad, que serán aprobados por real decreto.

En este marco regulador procede que el Gobierno establezca seis certificados de profesionalidad de la familia profesional Informática y comunicaciones del área profesional de Sistemas y telemática, que se incorporarán al Repertorio Nacional de certificados de profesionalidad por niveles de cualificación profesional atendiendo a la competencia profesional requerida por las actividades productivas, tal y como se recoge en el artículo 4.4 y en el anexo II del Real Decreto 1128/2003, anteriormente citado.

Con la entrada en vigor de este real decreto, dos de los nuevos certificados de profesionalidad que ahora se establecen, el de Sistemas microinformáticos y el de Montaje y reparación de Sistemas microinformáticos, sustituyen a su antecedente, el certificado de profesionalidad de la ocupación de Técnico de Sistemas Microinformáticos, establecido por el Real Decreto 1598/1997 de 17 de octubre, que en consecuencia, queda derogado.

En el proceso de elaboración de este real decreto ha emitido informe el Consejo General de la Formación Profesional, el Consejo General del Sistema Nacional de Empleo y ha sido informada la Conferencia Sectorial de Empleo y Asuntos Laborales.

En su virtud, a propuesta del Ministro de Trabajo e Inmigración y previa deliberación del Consejo de Ministros en su reunión del día 13 de mayo de 2011,

DISPONGO:

Artículo 1. *Objeto y ámbito de aplicación.*

Este real decreto tiene por objeto establecer tres certificados de profesionalidad de la familia profesional Informática y comunicaciones que se incluyen en el Repertorio Nacional de certificados de profesionalidad, regulado por el Real Decreto 34/2008, de 18 de enero, por el que se regulan los certificados de profesionalidad, modificado por el Real Decreto 1675/2010, de 10 de diciembre.

Dichos certificados de profesionalidad tienen carácter oficial y validez en todo el territorio nacional y no constituyen una regulación del ejercicio profesional.

Artículo 2. *Certificados de profesionalidad que se establecen.*

Los certificados de profesionalidad que se establecen corresponden a la familia profesional Informática y comunicaciones y son los que a continuación se relacionan, cuyas especificaciones se describen en los anexos que se indican:

Familia profesional: INFORMÁTICA Y COMUNICACIONES

– Anexo I. Seguridad informática – Nivel 3.
– Anexo II. Sistemas microinformáticos – Nivel 2.
– Anexo III. Montaje y reparación de sistemas microinformáticos - Nivel 2.
– Anexo IV. Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia – Nivel 3.
– Anexo V. Administración de servicios de Internet – Nivel 3.
– Anexo VI. Programación de sistemas informáticos – Nivel 3.

Artículo 3. *Estructura y contenido.*

El contenido de cada certificado de profesionalidad responde a la estructura establecida en los apartados siguientes:

cve: BOE-A-2011-10055

a) En el apartado I: Identificación del certificado de profesionalidad.
b) En el apartado II: Perfil profesional del certificado de profesionalidad.
c) En el apartado III: Formación del certificado de profesionalidad.
d) En el apartado IV: Prescripciones de los formadores.
e) En el apartado V: Requisitos mínimos de espacios, instalaciones y equipamientos.

Artículo 4. *Requisitos de acceso a la formación de los certificados de profesionalidad.*

1. Corresponderá a la Administración laboral competente la comprobación de que los alumnos poseen los requisitos formativos y profesionales para cursar con aprovechamiento la formación en los términos previstos en los apartados siguientes.

2. Para acceder a la formación de los módulos formativos de los certificados de profesionalidad de los niveles de cualificación profesional 2 y 3 los alumnos deberán cumplir alguno de los requisitos siguientes:

a) Estar en posesión del Título de Graduado en Educación Secundaria Obligatoria para el nivel 2 o título de Bachiller para nivel 3.
b) Estar en posesión de un certificado de profesionalidad del mismo nivel del módulo o módulos formativos y/o del certificado de profesionalidad al que desea acceder.
c) Estar en posesión de un certificado de profesionalidad de nivel 1 de la misma familia y área profesional para el nivel 2 o de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional para el nivel 3.
d) Cumplir el requisito académico de acceso a los ciclos formativos de grado medio para el nivel 2 o de grado superior para el nivel 3, o bien haber superado las correspondientes pruebas de acceso reguladas por las administraciones educativas.
e) Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
f) Tener los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

Artículo 5. *Formadores.*

1. Las prescripciones sobre formación y experiencia profesional para la impartición de los certificados de profesionalidad son las recogidas en el apartado IV de cada certificado de profesionalidad y se deben cumplir tanto en la modalidad presencial como a distancia.

2. De acuerdo con lo establecido en el artículo 13.3 del Real Decreto 34/2008, de 18 de enero, podrán ser contratados como expertos para impartir determinados módulos formativos que se especifican en el apartado IV de cada uno de los anexos de los certificados de profesionalidad, los profesionales cualificados con experiencia profesional en el ámbito de la unidad de competencia a la que está asociado el módulo.

3. Para acreditar la competencia docente requerida, el formador/a o persona experta deberá estar en posesión del certificado de profesionalidad de Formador ocupacional o formación equivalente en metodología didáctica de formación profesional para adultos.

Del requisito establecido en el párrafo anterior estarán exentos:

a) Quienes estén en posesión de las titulaciones universitarias oficiales de licenciado en Pedagogía, Psicopedagogía o de Maestro en cualquiera de sus especialidades, de un título universitario de graduado en el ámbito de la Psicología o de la Pedagogía, o de un título universitario oficial de posgrado en los citados ámbitos.
b) Quienes posean una titulación universitaria oficial distinta de las indicadas en el apartado anterior y además se encuentren en posesión del Certificado de Aptitud Pedagógica o de los títulos profesionales de Especialización Didáctica y el Certificado de Cualificación Pedagógica. Asimismo estarán exentos quienes acrediten la posesión del Máster Universitario habilitante para el ejercicio de las Profesiones reguladas de Profesor de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Escuelas Oficiales de Idiomas.

cve: BOE-A-2011-10055

c) Quienes acrediten una experiencia docente contrastada de al menos 600 horas en los últimos siete años en formación profesional para el empleo o del sistema educativo.

4. Los formadores que impartan formación a distancia deberán contar con formación y experiencia en esta modalidad, en el uso de las tecnologías de la información y la comunicación, así como reunir los requisitos específicos que se establecen para cada certificado de profesionalidad. A tal fin, las autoridades competentes desarrollarán programas y actuaciones específicas para la formación de estos formadores.

Artículo 6. *Contratos para la formación.*

1. La formación teórica de los contratos para la formación podrá realizarse a distancia hasta el máximo de horas susceptibles de desarrollarse en esta modalidad que se establece, para cada módulo formativo, en el certificado de profesionalidad.
2. La formación de los módulos formativos que no se desarrolle a distancia podrá realizarse en el puesto de trabajo o en procesos formativos presenciales.

Artículo 7. *Formación a distancia.*

1. Cuando el módulo formativo incluya formación a distancia, ésta deberá realizarse con soportes didácticos autorizados por la administración laboral competente que permitan un proceso de aprendizaje sistematizado para el participante que deberá cumplir los requisitos de accesibilidad y diseño para todos y necesariamente será complementado con asistencia tutorial.
2. La formación de los módulos formativos impartidos mediante la modalidad a distancia se organizará en grupos de 25 participantes como máximo.
3. Los módulos formativos que, en su totalidad, se desarrollen a distancia requerirán la realización de, al menos, una prueba final de carácter presencial.

Artículo 8. *Centros autorizados para su impartición.*

1. Los centros y entidades de formación que impartan formación conducente a la obtención de un certificado de profesionalidad deberán cumplir con las prescripciones de los formadores y los requisitos mínimos de espacios, instalaciones y equipamiento establecidos en cada uno de los módulos formativos que constituyen el certificado de profesionalidad.
2. Los centros que impartan exclusivamente la formación teórica de los contratos para la formación estarán exentos de cumplir los requisitos sobre espacios, instalaciones y equipamiento, establecidos en el apartado anterior, garantizando en todo caso a las personas con discapacidad los apoyos tecnológicos necesarios y la eliminación de las posibles barreras físicas y de comunicación.

Articulo 9. *Correspondencia con los títulos de formación profesional.*

La acreditación de unidades de competencia obtenidas a través de la superación de los módulos profesionales de los títulos de formación profesional surtirán los efectos de exención del módulo o módulos formativos de los certificados de profesionalidad asociados a dichas unidades de competencia establecidos en el presente real decreto.

Disposición adicional primera. *Nivel de los certificados de profesionalidad en el marco europeo de cualificaciones.*

Una vez que se establezca la relación entre el marco nacional de cualificaciones y el marco europeo de cualificaciones, se determinará el nivel correspondiente de los certificados de profesionalidad establecidos en este real decreto dentro del marco europeo de cualificaciones.

cve: BOE-A-2011-10055

Disposición adicional segunda. *Equivalencias con certificados de profesionalidad anteriores.*

Se declara la equivalencia a todos los efectos de los siguientes certificados de profesionalidad:

Certificado de profesionalidad que se deroga	Certificados de profesionalidad equivalentes
Real Decreto 1598/97 de 17 de octubre, por el que se establece el certificado de profesionalidad de la ocupación de Técnico de Sistemas microinformáticos.	Sistemas microinformáticos. Montaje y reparación de Sistemas microinformáticos.

Disposición transitoria primera. *Modificación de planes de formación y acciones formativas.*

En los planes de formación y en las acciones formativas que ya estén aprobados, en virtud de la Orden TAS, 718/2008, de 7 de marzo, por la que se desarrolla el Real Decreto 395/2007, de 23 de marzo, por el que se regula el subsistema de formación para el empleo, en materia de formación de oferta y se establecen las bases reguladoras para la concesión de subvenciones públicas destinadas a su financiación, en la fecha de entrada en vigor de este real decreto, que incluyan formación asociada al certificado de profesionalidad que ahora se deroga, se podrá sustituir dicha formación por la que esté asociada a los nuevos certificados de profesionalidad declarados equivalentes en la disposición adicional segunda, previa autorización de la Administración que lo aprobó y siempre que se cumplan las prescripciones de los formadores y los requisitos mínimos de espacios, instalaciones y equipamientos establecidos en el certificado.

Disposición transitoria segunda. *Baja en el Fichero de Especialidades.*

La especialidad correspondiente al certificado de profesionalidad derogado causará baja en el fichero de especialidades a partir de los nueve meses posteriores a la entrada en vigor de este real decreto. Durante este periodo dicho certificado mantendrá su vigencia, a los efectos previstos en este real decreto. En todo caso, las acciones formativas vinculadas a este certificado deberán iniciarse antes de transcurrido dicho periodo de nueve meses.

Disposición transitoria tercera. *Solicitud de expedición de los certificados de profesionalidad derogados.*

1. Las personas que, según lo dispuesto en la disposición transitoria primera del Real Decreto 34/2008, de 18 de enero, hayan completado con evaluación positiva la formación asociada al certificado de profesionalidad que aquí se deroga, durante la vigencia del mismo, dispondrán de un plazo de cinco años para solicitar su expedición, a contar desde la entrada en vigor del presente real decreto.
2. También podrán solicitar la expedición, en el plazo de cinco años desde la finalización con evaluación positiva de la formación de dicho certificado de profesionalidad:

a) Las personas que, habiendo realizado parte de aquella formación durante la vigencia del real decreto que ahora se deroga, completen la misma después de su derogación.
b) Las personas que realicen la formación de este certificado de profesionalidad bajo los planes de formación y las acciones formativas que ya estén aprobados en la fecha de entrada en vigor de este real decreto, en virtud de la Orden TAS 718/2008, de 7 de marzo.

Disposición transitoria cuarta. *Acreditación provisional de centros.*

Los centros de formación que a la entrada en vigor de este real decreto estuvieran incluidos en los registros de las Administraciones competentes y homologados para impartir

cve: BOE-A-2011-10055

formación en las especialidades formativas correspondientes al certificado de profesionalidad que ahora se deroga, se considerarán acreditados de forma provisional a efectos de la impartición de acciones formativas vinculadas a los certificados de profesionalidad establecidos en este real decreto y declarados equivalentes en la disposición adicional segunda, previa autorización de la Administración competente. Esta acreditación tendrá efectos durante un año desde la entrada en vigor de este real decreto y hasta la finalización, en su caso, de las acciones formativas aprobadas. Transcurrido este periodo, para poder impartir formación dirigida a la obtención de los certificados de profesionalidad establecidos en este real decreto, los centros de formación deberán solicitar a las Administraciones competentes su acreditación, para lo que deberán cumplir los requisitos establecidos en los certificados.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 1598/97 de 17 de octubre, por el que se establece el certificado de profesionalidad de la ocupación Técnico de Sistemas microinformáticos.

Disposición final primera. *Título competencial.*

El presente Real Decreto se dicta en virtud de las competencias que se atribuyen al Estado en el artículo 149.1.1.ª, 7.ª y 30.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; la legislación laboral; y la regulación de las condiciones de obtención, expedición y homologación de títulos académicos y profesionales y normas básicas para el desarrollo del artículo 27 de la Constitución, a fin de garantizar el cumplimiento de las obligaciones de los poderes públicos en esta materia.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al Ministro de Trabajo e Inmigración para dictar cuantas disposiciones sean precisas para el desarrollo de este real decreto.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid, el 13 de mayo de 2011.

JUAN CARLOS R.

El Ministro de Trabajo e Inmigración,
VALERIANO GÓMEZ SÁNCHEZ

cve: BOE-A-2011-10055

ANEXO I

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: SISTEMAS MICROINFORMÁTICOS

Código: IFCT0209.

Familia Profesional: Informática y Comunicaciones.

Área Profesional: Sistemas y telemática.

Nivel de cualificación profesional: 2

Cualificación profesional de referencia:

IFC078_2 Sistemas Microinformáticos (Real Decreto 295/2004, de 20 de febrero, modificado por 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.
UC0220_2: Instalar, configurar y verificar los elementos de la red local según procedimientos establecidos.
UC0221_2: Instalar, configurar y mantener paquetes informáticos de propósito general y aplicaciones específicas.
UC0222_2: Facilitar al usuario la utilización de paquetes informáticos de propósito general y aplicaciones específicas.

Competencia general:

Instalar, configurar y mantener sistemas microinformáticos para su utilización además de apoyar al usuario en el manejo de aplicaciones sobre dichos sistemas como parte del servicio de soporte informático de una organización.

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional en los siguientes ámbitos:
- Empresas o entidades que utilizan sistemas informáticos para su gestión, dentro del departamento de microinformática.
- Pequeñas empresas que comercializan y/ o reparan equipos informáticos y software o como profesional autónomo.

Sectores productivos:

Está presente en los siguientes tipos de empresas:
- Empresas o entidades de cualquier tamaño que utilizan sistemas informáticos para su gestión y que pueden estar enmarcadas en cualquier sector productivo.
- Empresas proveedoras y distribuidoras de servicios de informática y comunicaciones.
- Empresas dedicadas a la comercialización de equipos microinformáticos.
- Empresas que prestan servicios de asistencia técnica microinformática.
- 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.

cve: BOE-A-2011-10055

Instalador de equipos microinformáticos.
Reparador de microordenadores.
Comercial de microinformática.
Personal de soporte técnico.
Operador de Teleasistencia.

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)

MF0220_2 (Transversal): Implantación de los elementos de la red local. (160 horas)
- UF0854: Instalación y configuración de los nodos de una red de área local. (90 horas)
- UF0855: Verificación y resolución de incidencias en una red de área local. (70 horas)

MF0221_2: Instalación y configuración de aplicaciones informáticas. (60 horas)
MF0222_2: Aplicaciones microinformáticas. (200 horas)
- UF0856: Asistencia de usuarios en el uso de aplicaciones ofimáticas y de correo electrónico. (40 horas)
- UF0857: Elaboración de documentos de texto. (50 horas)
- UF0858: Elaboración de hojas de cálculo. (50 horas)
- UF0859: Elaboración de presentaciones. (30 horas)
- UF0860: Elaboración y modificación de imágenes u otros elementos gráficos. (30 horas)

MP0177: Módulo de prácticas profesionales no laborales de Sistemas Microinformáticos. (40 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: INSTALAR Y CONFIGURAR 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.

cve: BOE-A-2011-10055

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.

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

cve: BOE-A-2011-10055

sus funcionalidades, siguiendo la documentación técnica y procedimientos estipulados por la organización.

Contexto profesional

Medios de producción y/o creación de servicios

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 o resultado del trabajo

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.

Unidad de competencia 2

Denominación: INSTALAR, CONFIGURAR Y VERIFICAR LOS ELEMENTOS DE LA RED LOCAL SEGÚN PROCEDIMIENTOS ESTABLECIDOS

Nivel: 2

Código: UC0220_2

Realizaciones profesionales y criterios de realización:

RP1: Instalar y configurar los nodos de la red local y el software para implementar servicios de comunicaciones internas, siguiendo procedimientos establecidos.

CR1.1 El mapa físico de la red se interpreta para identificar los elementos que componen la red local, atendiendo a las especificaciones recibidas.

CR1.2 Los módulos de los equipos de la red se instalan, para que ofrezcan las características de conectividad especificadas según la configuración física indicada y siguiendo los procedimientos establecidos.

CR1.3 Los elementos activos de la red (encaminadores y conmutadores) se configuran lógicamente, para implementar servicios usando técnicas y herramientas software de acuerdo a las especificaciones recibidas.

CR1.4 Los programas de gestión de protocolos y servicios se instalan y configuran, para implementar los servicios de comunicaciones internas siguiendo las especificaciones técnicas de los fabricantes y aplicando los procedimientos establecidos.

CR1.5 El software de los nodos de la red se instala y configura, para proporcionar conectividad entre dichos nodos según las especificaciones recibidas.

CR1.6 Los procesos de instalación y configuración de los dispositivos de la red local, se documentan para su registro utilizando los formatos indicados por la organización según el procedimiento establecido.

CR1.7 La documentación técnica específica asociada al software y a los dispositivos, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

cve: BOE-A-2011-10055

RP2: Verificar el funcionamiento y los parámetros operativos de los concentradores y otros dispositivos de interconexión de la red, para asegurar el servicio que prestan según procedimientos establecidos.

CR2.1 El funcionamiento de los dispositivos de interconexión de la red local se comprueba, para verificar la operatividad de la red utilizando las herramientas hardware y software específicas, según los procedimientos establecidos.

CR2.2 El estado de los dispositivos de interconexión se comprueba, para verificar que se encuentran activos y son accesibles accediendo a ellos por medio de las herramientas de gestión de red, según procedimientos establecidos.

CR2.3 Las opciones de conexión permitidas y prohibidas se comprueban para garantizar la seguridad en los servicios, utilizando herramientas específicas según las especificaciones recibidas.

CR2.4 El acceso a los recursos de la red se comprueba para asegurar el servicio, siguiendo los procedimientos establecidos para verificar que se accede a los recursos permitidos.

CR2.5 La configuración de los dispositivos de interconexión se verifica localmente y en remoto, para asegurar su funcionalidad según los procedimientos establecidos.

RP3: Configurar los protocolos de comunicaciones para la integración de los dispositivos la red, según indicaciones del administrador y especificaciones operativas de la organización.

CR3.1 Los valores de los parámetros configurables de los protocolos de comunicaciones se fijan, para integrar cada nodo de la red según los procedimientos establecidos y siguiendo las políticas de direccionamiento y seguridad de la organización.

CR3.2 Los protocolos asociados a las aplicaciones de red instaladas se configuran en los servidores, para soportar los servicios implementados de acuerdo con los manuales de instalación y siguiendo las especificaciones recibidas.

CR3.3 Los encaminadores y conmutadores se configuran, para que gestionen protocolos y servicios según especificaciones recibidas y procedimientos de trabajo predefinidos.

CR3.4 El software de cifrado se instala y configura en los nodos de la red que se determine, según las especificaciones recibidas y procedimientos establecidos para crear redes privadas virtuales.

CR3.5 Las pruebas funcionales de la configuración de los dispositivos de comunicaciones, se realizan para asegurar la conformidad de la misma con respecto a los requerimientos establecidos en la especificación operativa de la organización.

CR3.6 La configuración de protocolos se documenta para su registro, utilizando los formatos indicados por la organización según el procedimiento establecido.

RP4: Gestionar las incidencias detectadas en los dispositivos de la red para corregirlas o informar de ellas, según los protocolos establecidos y los procedimientos de actuación predefinidos.

CR4.1 Los sistemas de notificación de incidencias se observan, para atender posibles alarmas según los procedimientos operativos y de seguridad de la organización.

CR4.2 La localización del elemento en el que se ha producido la incidencia, se realiza mediante la interpretación de la información recibida y la documentación técnica, para aislar el problema físico y lógico, según la documentación técnica y los protocolos de actuación de la organización ante contingencias.

CR4.3 Los síntomas reportados por el usuario o por los sistemas de gestión de incidencias, se verifican para obtener un diagnóstico del problema según la documentación técnica.

cve: BOE-A-2011-10055

CR4.4 La incidencia detectada y aislada se diagnostica y se plantea su solución, para rehabilitar los servicios interrumpidos o deteriorados, según la normativa de calidad y los planes de contingencia.
CR4.5 La incidencia que no se ha conseguido aislar se reporta al nivel de responsabilidad superior para su gestión según los protocolos y procedimientos de actuación ante contingencias de la organización.
CR4.6 La reparación de la incidencia se realiza con las herramientas adecuadas y respetando las normas de seguridad establecidas por la organización.
CR4.7 La documentación de la detección, diagnóstico y solución de la incidencia se confecciona para realizar el registro de la misma según los protocolos de la organización.
CR4.8 La información del estado de la incidencia se transmite al usuario final para cumplimentar el proceso de su gestión según la normativa de la organización.

Contexto profesional

Medios de producción y/o creación de servicios
Analizadores de red. Certificadores de cableado. Herramientas manuales para trabajos eléctricos y mecánicos. Herramientas software para pruebas de conectividad. Herramientas software para control de inventario de elementos de red. Ordenadores, impresoras y periféricos. Sistemas operativos. Concentradores, conmutadores, encaminadores. Tarjetas de red. Cables y conectores. Software de clientes de red. Software de gestión de red. Software propietario de los dispositivos de red. Herramientas ofimáticas. Mapa de la red.

Productos o resultado del trabajo
Equipo de comunicaciones conectado a las líneas de datos. Red local instalada y configurada según especificaciones. Inventario y registro descriptivo de los dispositivos físicos de comunicaciones de la red y de su configuración.

Información utilizada o generada
Mapa de la red. Inventario del hardware de la organización. Órdenes de trabajo. Documentación de red. Manuales de instalación de los dispositivos. Manuales de configuración de los dispositivos. Especificaciones operativas de la organización. Manual de calidad. Normas y criterios de calidad de la organización. Plan de seguridad. Plan de mantenimiento. Normativa medioambiental. Normativa de seguridad e higiene en el trabajo. Documentación de red fiable y actualizada.

Unidad de competencia 3

Denominación: INSTALAR, CONFIGURAR Y MANTENER PAQUETES INFORMÁTICOS DE PROPÓSITO GENERAL Y APLICACIONES ESPECÍFICAS.

Nivel: 2

Código: UC0221_2

Realizaciones profesionales y criterios de realización

RP1: Instalar, configurar y actualizar paquetes informáticos de propósito general, utilidades y aplicaciones específicas para su explotación posterior por parte de los usuarios y según las directrices recibidas.

CR1.1 La configuración de parámetros y definiciones en los equipos de la infraestructura de red de datos se realiza de manera individual con los valores fijados en el diseño. La comprobación del paquete informático dispuesto para la instalación o actualización y la documentación asociada asegura su compatibilidad

cve: BOE-A-2011-10055

con las características de la máquina y el sistema operativo sobre el que será instalado y las especificaciones establecidas.
CR1.2 La aplicación o utilidad se instala y configura siguiendo el procedimiento establecido y utilizando las herramientas de la propia aplicación o del sistema operativo.
CR1.3 Las incidencias que aparezcan se resuelven mediante la consulta de la documentación técnica o recurriendo al administrador de la red
CR1.4 La documentación técnica se interpreta con corrección tanto si se encuentra editada en castellano, en la lengua propia de la Comunidad Autónoma o en el idioma técnico de uso habitual.
CR1.5 La realización de las pruebas establecidas asegura que se han instalado todos los paquetes y que la aplicación funciona correctamente en todos sus aspectos (accesos a periféricos, accesos a red, etc.)
CR1.6 Si la aplicación o utilidad lo requiere, las pruebas establecidas verifican también se verificará la conexión de la aplicación cliente con el servidor.
CR1.7 La realización de las pruebas asegura también que la instalación de la aplicación o utilidad no ha perjudicado el funcionamiento de otras aplicaciones previamente instaladas
CR1.8 La actualización del software se lleva a cabo con eficiencia asegurando la integridad del equipo y la disponibilidad de la información
CR1.9 Las incidencias en la instalación se documentan en los formatos establecidos para ese efecto.
CR1.10 Los detalles relevantes de la instalación o configuración se reflejan en la documentación del equipo, según el procedimiento establecido, para su consulta posterior
CR1.11 La documentación y soportes para la instalación del software se detallan y referencian en la documentación generada y se guardan convenientemente para su uso posterior

RP2: Asistir al usuario resolviendo los problemas que se presenten en la explotación de las aplicaciones identificando su naturaleza y solventando la incidencia en el tiempo adecuado y con el nivel de calidad esperado.

CR2.1 La asistencia al usuario tiene en cuenta las técnicas de comunicación interpersonal establecidas, para identificar la actuación requerida, satisfaciendo las exigencias y demandas del usuario y garantizando el resultado de la actuación.
CR2.2 Los componentes software afectados se reinstalan, actualizan o configuran con los parámetros adecuados de acuerdo con las especificaciones establecidas en la documentación técnica y las necesidades de uso.
CR2.3 La documentación técnica se interpreta con corrección tanto si se encuentra editada en castellano, en la lengua propia de la Comunidad Autónoma o en el idioma técnico de uso habitual.
CR2.4 La integridad de la información y la continuidad en la explotación quedan garantizadas durante la resolución del problema, tomando las medidas preventivas de seguridad y activando los posibles procedimientos de explotación alternativos.
CR2.5 La información original se restaura y actualiza, siguiendo el protocolo establecido, para que el sistema vuelva a estar en explotación.
CR2.6 El funcionamiento del sistema restaurado se verifica mediante la realización de las pruebas establecidas.
CR2.7 Las actuaciones realizadas se documentan en los formatos establecidos a tal efecto para facilitar su seguimiento, actualizando el repositorio de incidencias y la documentación técnica de la instalación y de la configuración del sistema.

cve: BOE-A-2011-10055

Contexto profesional

Medios de producción y/o creación de servicios

Ordenadores, impresoras, escáneres, y otros periféricos. Software de las aplicaciones. Software de seguridad y antivirus. Software de actualización. Parches. Herramientas software de diagnóstico. Software para la detección, diagnóstico y reparación de errores por medios telemáticos. Herramientas software de instalación y actualización. Programas de ayuda. Software para copias de seguridad y recuperación. Soportes para copias de seguridad.

Productos o resultado del trabajo

Paquetes informáticos instalados y correctamente configurados. Procedimientos de instalación operativos y actualizados. Asistencia a los usuarios ante los problemas de funcionamiento de las aplicaciones. Elementos para la instalación (programas, manuales, licencias) almacenados y controlados. Informes de incidencias almacenados y controlados. Adaptación de la aplicación ofimática o corporativa a nuevas configuraciones del sistema.

Información utilizada o generada

Manuales de instalación del software de aplicación o de la aplicación específica. Guía de explotación de la aplicación. Partes de incidencias e histórico de incidencias. Documentación de la instalación. Petición de asistencia de usuarios. Normas de la empresa sobre atención al cliente. Legislación sobre protección de datos y propiedad intelectual, normativa empresarial sobre confidencialidad de datos, etc.

Unidad de competencia 4

Denominación: FACILITAR AL USUARIO LA UTILIZACIÓN DE PAQUETES INFORMÁTICOS DE PROPÓSITO GENERAL Y APLICACIONES ESPECÍFICAS.

Nivel: 2

Código: UC0222_2

Realizaciones profesionales y criterios de realización

RP1: Facilitar a los usuarios la explotación de los paquetes informáticos mediante la capacitación para su utilización.

CR1.1 Los usuarios son iniciados en el uso de nuevas aplicaciones o versiones tras su instalación con el objeto de garantizar una transición eficaz.

CR1.2 La instalación de una aplicación o nueva versión se completa con la elaboración de unas instrucciones de explotación.

CR1.3 Los usuarios son asesorados en el manejo de utilidades (antivirus, programas de compresión, etc.)

CR1.4 Los usuarios son asesorados en la aplicación de políticas de seguridad (realización de copias de seguridad, protección de carpetas, uso de carpetas compartidas, etc.)

RP2: Facilitar a los usuarios la explotación de los paquetes informáticos mediante la elaboración directa de trabajos.

CR2.1 Las plantillas de documentos, hojas de cálculo y presentaciones se realizan según las instrucciones recibidas y son puestas a disposición de los usuarios

CR2.2 Las plantillas de documentos, hojas de cálculo y presentaciones realizadas son conocidas por los usuarios y son ubicadas de forma que su acceso sea fácil y cómodo.

CR2.3 Las operaciones de importación/ exportación de datos entre aplicaciones se realizan asegurando su integridad.

cve: BOE-A-2011-10055

CR2.4 Las imágenes y gráficos que se necesitan en la elaboración de documentos se obtienen mediante programas sencillos de elaboración y/ o retoque de imágenes.
CR2.5 Los documentos, hojas de cálculo y presentaciones elaborados por los usuarios son adaptadas, si es necesario, a los modelos corporativos.
CR2.6 Los modelos corporativos generados se codifican y archivan (en formato digital) para su posterior uso o consulta, según lo establecido en el sistema de gestión de configuración para conservar archivos históricos de documentación.

Contexto profesional

Medios de producción y/o creación de servicios

Ordenadores, impresoras, escáneres, y otros periféricos. Software de las aplicaciones. Software de seguridad y antivirus. Software de actualización. Parches. Herramientas software de diagnóstico. Herramientas de generación de plantillas de las aplicaciones. Asistentes de creación de plantillas y programas de ayuda. Software para copias de seguridad y recuperación. Soportes para copias de seguridad.

Productos o resultado del trabajo

Asistencia a los usuarios ante los problemas de utilización de las aplicaciones. Instrucciones de utilización para el usuario de una nueva aplicación o versión. Informes de incidencias almacenados y controlados. Plantillas y documentos creados en función del manual de normalización de la empresa, y documentación realizada para los usuarios. Formularios de entrada/ salida creados y operativos, y documentación de uso realizada.

Información utilizada o generada

Manuales de instalación del software de aplicación o de la aplicación específica. Guía de explotación de la aplicación. Partes de incidencias e histórico de incidencias. Documentación de la instalación. Petición de asistencia de usuarios. Reglas de normalización de documentos. Normas de la empresa sobre atención al cliente. Legislación sobre protección de datos y propiedad intelectual, normativa empresarial sobre confidencialidad de datos, etc.

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.

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y ACTUALIZACIÓN DE SISTEMAS OPERATIVOS

Código: UF0852

Duración: 80 horas

cve: BOE-A-2011-10055

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.
- 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.

cve: BOE-A-2011-10055

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.

3. Elementos de un sistema operativo informático.

- Gestión de procesos.
- Gestión de memoria.
- El sistema de Entrada y Salida.

cve: BOE-A-2011-10055

- 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.
- Actualización de componentes software.
  - Componentes críticos.
  - Componentes de seguridad.
  - Controladores.
  - Otros componentes.

cve: BOE-A-2011-10055

- Verificación de la actualización.
- Documentación de la actualización.

UNIDAD FORMATIVA 2

Denominación: EXPLOTACIÓN DE LAS FUNCIONALIDADES DEL SISTEMA MICROINFORMATICO.

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.
   - Unidades lógicas de almacenamiento.
   - Estructuración de los datos.
     - Carpetas o directorios.
     - Ficheros.

cve: BOE-A-2011-10055

- 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-2011-10055

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: IMPLANTACIÓN DE LOS ELEMENTOS DE LA RED LOCAL.

Código: MF0220_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0220_2: Instalar, configurar y verificar los elementos de la red local según procedimientos establecidos

Duración: 160 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y CONFIGURACIÓN DE LOS NODOS DE UNA RED DE AREA LOCAL.

Código: UF0854

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1, RP3.

Capacidades y criterios de evaluación

C1: Clasificar los elementos de comunicaciones que conforman una red local, para identificar los componentes que constituyen el mapa físico.

CE1.1 Explicar las topologías de una red local teniendo en cuenta las arquitecturas y tecnologías existentes.

CE1.2 Enumerar los elementos que pueden encontrarse en el mapa físico de una red local en función del ámbito de aplicación y las infraestructuras de red utilizadas.

CE1.3 escribir cada uno de los elementos integrantes de una red local teniendo en cuenta sus características y funcionalidades asociadas.

CE1.4 En un caso práctico de una red local ya instalada elaborar su mapa físico y lógico según unas especificaciones recibidas.

CE1.5 Identificar la normativa legal y técnica que afecta a la implantación de las redes locales en función de los procedimientos dados.

CE1.6 Interpretar la documentación técnica asociada a los elementos de comunicación, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.

C2: Aplicar los procedimientos de instalación y configuración de los nodos de la red local, así como los gestores de protocolos y otros programas que soportan servicios de comunicaciones.

CE2.1 Enumerar y explicar las características de los protocolos que se configuran en una red local teniendo en cuenta la tecnología y estándares utilizados

CE2.2 Explicar el sistema de direccionamiento de los nodos que se utiliza en la red local en función de las tecnologías de red usadas.

cve: BOE-A-2011-10055

CE2.3 En un caso práctico de instalación y configuración de los nodos de una red para implementar servicios de comunicaciones internas, según unas especificaciones recibidas:
- Interpretar la documentación técnica identificando los elementos que conforman la instalación.
- Identificar las diferentes tomas de red de los nodos y su representación en el armario de conexiones.
- Seleccionar las herramientas adecuadas para realizar la instalación.
- Instalar los adaptadores de red junto con sus correspondientes controladores.
- Instalar y configurar los protocolos de red a utilizar según las especificaciones recibidas.
- Instalar y configurar los diferentes servicios de red según las especificaciones recibidas.
- Documentar las actividades realizadas.

CE2.4 Aplicar la configuración especificada a los elementos activos (conmutadores y encaminadores), haciendo uso de unos procedimientos especificados.
CE2.5 Identificar la normativa legal y técnica que afecta a la implantación de las redes locales en función de unas especificaciones dadas.

C3: Establecer la configuración de los parámetros de los protocolos de comunicaciones en los nodos de la red, para su integración en la propia red, siguiendo unos procedimientos dados.
CE3.1 Identificar los parámetros de los protocolos de comunicaciones a configurar, su función y su rango de valores permitido.
CE3.2 Interpretar las especificaciones de una configuración de protocolos de comunicaciones determinada, teniendo en cuenta las necesidades de integración del nodo en la red y la implementación de los servicios correspondientes.
CE3.3 Enumerar el procedimiento a seguir para aplicar una configuración predeterminada a un nodo de red.
CE3.4 Configurar los diferentes protocolos de comunicaciones según unas especificaciones técnicas dadas.
CE3.5 Identificar los parámetros de configuración de los protocolos con características de seguridad de transmisión y cifrado, para su integración en redes seguras teniendo en cuenta los criterios de seguridad dados.
CE3.6 Documentar los procesos a realizar en la configuración de los protocolos en los nodos de la red local de acuerdo a unas especificaciones dadas.

Contenidos

1. **Arquitectura de redes de área local.**
   - Clasificación de las redes en función del territorio que abarcan.
   - Características de una red local.
   - Arquitectura de redes de área local.
     - Topologías básicas.
     - Topología lógica y física.
     - Método de acceso al cable.
     - Protocolos de comunicaciones.
     - Arquitecturas de redes de área local más usadas.
   - Normativa.
     - Comités de estandarización.
     - Estándares de redes de área local.
     - Infraestructuras Comunes de Telecomunicación.
2. **Elementos de una red de área local.**
   - Características y funciones
   - Estaciones de trabajo.
   - Servidores.

cve: BOE-A-2011-10055

- Tarjetas de red.
- Equipos de conectividad.
    - Repetidores.
    - Concentradores (Hubs).
    - Conmutadores (Switches).
    - Encaminadores (Routers).
    - Pasarelas (Gateways).
    - Puentes (Bridges).
    - Dispositivos inalámbricos.
- Sistemas operativos de red.
- Medios de transmisión.
    - Medios de cobre: Cables de para trenzado y coaxial.
    - Medios ópticos: Cables de fibra óptica.
    - Comunicaciones inalámbricas.
- El cableado estructurado.
    - Subsistemas de cableado estructurado.
    - Estándares TIA/EIA sobre cableado estructurado.
    - Estándares de Cable UTP/STP.
- El mapa físico y lógico de una red de área local.

3. Protocolos de una red de área local.

- Introducción a los protocolos.
- Modelo de Interconexión de Sistemas Abiertos (OSI).
- El nivel físico.
- Protocolos del nivel de enlace.
    - Protocolos de control de enlace lógico (LLC).
    - Protocolos de control de acceso al medio (MAC).
        - Protocolos de contienda.
        - Protocolos de paso de testigo.
        - Otros.
- Ethernet.
    - Introducción a Ethernet.
    - Ethernet y el modelo OSI.
    - Direccionamiento MAC.
    - Trama Ethernet.
    - Tecnologías Ethernet.
- Otros protocolos de nivel de enlace: Token Ring, FDDI, etc.
- Protocolos de nivel de red.
    - Protocolo de Internet (IP).
        - Introducción a IP
        - Dirección IP.
        - Asignación de direcciones.
        - Enrutamiento
    - Otros Protocolos de nivel de red (IPX, etc)
- Direcciones físicas y lógicas.

4. Instalación y configuración de los nodos de la red de área local.

- El armario de comunicaciones.
    - Elementos del armario de comunicaciones.
    - Representación en el armario de la tomas de red de los nodos.
- Instalación de adaptadores de red y controladores.

- Instalación y configuración de protocolos de red más habituales.
    - Parámetros característicos.
    - Configuración del protocolo TCP/IP.
        - Elementos de configuración de TCP/IP.
        - Dirección IP.

cve: BOE-A-2011-10055

- Mascara de subred.
- Puerta de enlace.
- Servidor DNS.
- Servidor WINS.
- Configuración de NetBIOS.
- Asignación a un grupo de trabajo.

- Procedimiento de configuración de otros protocolos: SPX/IPX, etc.
- Configuración de la seguridad
  - Autenticación de identidad.
  - Cifrado de datos.
- Procedimientos sistemáticos de configuración.

- Instalación y configuración de servicios de red.
  - Servicios de acceso a la red.
  - Servicio de ficheros.
  - Servicios de impresión.
  - Servicio de correos.
  - Otros servicios.
- Procedimiento de aplicación de configuraciones a routers y switches.
  - Las aplicaciones de emulación de terminal.
  - Configuración de las aplicaciones de emulación de terminal.
  - Aplicación de configuraciones a routers y switches.

UNIDAD FORMATIVA 2

Denominación: VERIFICACION Y RESOLUCIÓN DE INCIDENCIAS EN UNA RED DE AREA LOCAL.

Código: UF0855

Duración: 70 horas

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

Capacidades y criterios de evaluación

C1: Aplicar los procedimientos de prueba y verificación de los elementos de conectividad de la red y las herramientas para estos procesos.

CE1.1 Explicar las etapas de un proceso de verificación de conectividad en una red local.

CE1.2 Enumerar las herramientas utilizadas para verificar la conectividad en una red local, según las tecnologías implementadas en las redes locales.

CE1.3 Explicar el funcionamiento operativo de las herramientas de gestión de red para comprobar el estado de los dispositivos de comunicaciones, teniendo en cuenta las especificaciones técnicas de las herramientas.

CE1.4 En un caso práctico de una red local ya instalada, verificar las opciones de conexión permitidas y prohibidas, así como el acceso a los recursos compartidos, siguiendo unos procedimientos dados.

CE1.5 En un caso práctico de una red local ya instalada: documentar los procesos de prueba y verificación realizados, de acuerdo a unas especificaciones técnicas.

C2: Atender las incidencias de los elementos de comunicaciones de la red local, y proceder a su solución siguiendo unas especificaciones dadas.

CE2.1 Describir las incidencias que se producen en los elementos de comunicaciones de las redes locales, según las tecnologías de comunicaciones empleadas y los elementos involucrados con ellas.

cve: BOE-A-2011-10055

CE2.2 Enumerar los procedimientos y herramientas utilizadas para la detección de incidencias de los elementos de comunicaciones de la red local, según especificaciones de un plan de contingencias definido.
CE2.3 Describir las técnicas y herramientas que se utilizan para aislar y diagnosticar las causas que han producido una incidencia reportada en la red, según se indica en el plan de contingencias.
CE2.4 Explicar los procedimientos sistemáticos de resolución de incidencias de los elementos de comunicaciones de la red local, en función de los dispositivos en los que se detectan las incidencias.
CE2.5 En casos prácticos, debidamente caracterizados, resolver averías simuladas dentro de una red local, para proceder a su solución según unas especificaciones recibidas y siguiendo unos procedimientos dados:
- Interpretar las alarmas generadas por el sistema de detección de incidencias.
- Localizar el elemento causante de la incidencia.
- Resolver la incidencia aplicando los procedimientos preestablecidos.
- Registrar la incidencia en el documento adecuado.

Contenidos

1. **Verificación y prueba de elementos de conectividad de redes de área local.**
   - Herramientas de verificación y prueba.
     - Herramientas de verificación y prueba de los sistemas operativos.
     - Comandos TCP/IP.
     - Obtención de la Configuración IP.
     - Realización de pruebas de conexión.
     - Interpretación de respuestas.
   - Procedimientos sistemáticos de verificación y prueba de elementos de conectividad de redes locales.
2. **Tipos de incidencias que se pueden producir en una red de área local.**
   - Incidencias a nivel de conectividad del enlace.
   - Incidencias a nivel de red.
3. **Detección y diagnóstico de incidencias en redes de área local.**
   - Herramientas de diagnóstico de dispositivos de comunicaciones en redes locales.
   - Procesos de gestión de incidencias en redes locales.
4. **Comprobación de cables de par trenzado y coaxial.**
   - Categorías de herramientas de comprobación de cableado.
   - Analizadores o comprobadores de cable.
     - Características.
     - Procedimiento de comprobación de cables de par trenzado.
       - Circuito abierto.
       - Cortocircuito.
       - Hilos cruzados.
       - Pares cruzados.
       - Par dividido.
       - Detección de voltajes telefónicos.
       - Derivación en puente.
       - Detección de puertos Ethernet.
     - Procedimiento de comprobación de cables coaxiales.
     - Procedimiento de detección de alimentación por Ethernet.
     - Procedimientos de localización de cables utilizando tonos.
5. **Comprobación y solución de incidencias a nivel de red.**
   - Herramientas de comprobación.

cve: BOE-A-2011-10055

- Detección de problemas relacionados con:
  - Tramas largas y cortas.
  - Tráfico excesivo.
  - Netware.
  - TCP/IP.
  - Configuración del Host.
  - Resolución de nombres.
  - NetBIOS.
  - Conexión al servidor http o proxy.
  - Conexión al servidor de correos.
  - Conexión al servidor de impresión.
  - Otros.

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 - UF0854	90	50
Unidad formativa 2 - UF0855	70	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.

MÓDULO FORMATIVO 3

Denominación: INSTALACIÓN Y CONFIGURACIÓN DE APLICACIONES INFORMÁTICAS.

Código: MF0221_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0221_2: Instalar, configurar y mantener paquetes informáticos de propósito general y aplicaciones específicas.

Duración: 60 horas

Capacidades y criterios de evaluación

C1: Interpretar la información relativa a la configuración de los equipos informáticos para determinar la adecuada instalación de las aplicaciones.

CE1.1 Describir los recursos y componentes de un sistema que deben tenerse en cuenta en la instalación de una aplicación.

CE1.2 Clasificar tipos de programas y aplicaciones según sus necesidades en recursos del equipo para su funcionamiento óptimo.

cve: BOE-A-2011-10055

CE1.3 Interpretar la documentación técnica con corrección tanto si se encuentra editada en castellano, en la lengua propia de la Comunidad Autónoma o en el idioma técnico de uso habitual.

CE1.4 En supuestos prácticos de instalación de aplicaciones en equipos informáticos:

- Identificar y localizar todos los elementos necesarios para la instalación de la aplicación (soportes magnéticos, llaves, licencias, mochilas, procedimientos y manuales)
- Interpretar desde la documentación de instalación de la aplicación, los requisitos mínimos y óptimos requeridos en función de los componentes que se desean instalar
- Determinar las características del equipo informático requeridas por la aplicación (velocidad de CPU, cantidad de memoria, espacio disponible en disco, hardware específico y otras) usando las herramientas del sistema operativo
- En función de las conclusiones anteriores, determinar qué tipo de instalación puede realizarse, qué partes no pueden ser instaladas y en ese caso, qué modificaciones (hardware o software) deben realizarse para realizar una instalación óptima
- Documentar las actividades realizadas y los resultados obtenidos

C2: Instalar, configurar y actualizar las aplicaciones ofimáticas y corporativas en un equipo informático.

CE2.1 Enumerar los tipos de virus, la forma de propagación de la infección y los efectos que pueden causar en un equipo informático.

CE2.2 Explicar el funcionamiento de las herramientas usadas para la prevención y reparación de los daños causados por los virus informáticos (antivirus).

CE2.3 Describir las precauciones básicas que deben tomar los usuarios en cuestiones de seguridad informática y de prevención de infecciones por virus informático.

CE2.4 Describir las actividades que se han de realizar en el proceso de instalación o actualización de una aplicación en un equipo informático.

CE2.5 En un supuesto práctico debidamente caracterizado de actualización del software antivirus disponible:

- Comprobar la versión de antivirus y de los patrones de virus.
- Descargar desde Internet la última versión de patrones de virus.
- Actualizar el soporte magnético de instalación / actualización del antivirus con la última base de datos de patrones disponibles.
- Documentar convenientemente los datos de configuración de la base de datos de patrones
- Documentar las actividades realizadas y los resultados obtenidos.

CE2.6 En un supuesto práctico de instalación o actualización de un programa antivirus:

- Instalar o actualizar correctamente el programa antivirus siguiendo el procedimiento establecido.
- Configurar el programa de acuerdo a los requisitos establecidos.
- Actualizar la versión del antivirus con los últimos patrones disponibles.
- Anotar la acción realizada en la hoja de registro del equipo.
- Documentar las actividades realizadas y los resultados obtenidos.

CE2.7 En un supuesto práctico debidamente caracterizado, en el que se pide instalar o actualizar una determinada aplicación en un equipo informático:

- Instalar o actualizar correctamente los componentes establecidos de la aplicación siguiendo el procedimiento establecido por el fabricante y/o las especificaciones recibidas.
- Configurar la aplicación en función de las características y recursos del equipo en el que se ha instalado.

cve: BOE-A-2011-10055

- Personalizar la aplicación para atender diferentes posibles preferencias del usuario.
- Configurar la aplicación para tener en cuenta posibles discapacidades del usuario, aprovechando para ello todas las capacidades que ofrezca la misma aplicación, el sistema operativo y el hardware instalado para ese fin.
- Configurar los directorios que usa la aplicación para facilitar el acceso a la documentación preexistente, plantillas u otra información relevante.
- Comprobar el funcionamiento de la aplicación mediante pruebas sistemáticas que aseguren el correcto funcionamiento de los componentes instalados y el acceso tanto a los recursos del propio del equipo como a los compartidos en la red.

CE2.8 En un supuesto práctico debidamente caracterizado, en el que el procedimiento de instalación no dé los resultados esperados:

- Consultar la documentación técnica para identificar el problema y encontrar su solución.
- Consultar Internet (páginas de servicio técnico, foros) para identificar el problema y encontrar su solución.
- Documentar la incidencia y la solución encontrada en un formato establecido para tal efecto.

C3: Facilitar el uso de las aplicaciones informáticas mediante la asistencia técnica ante el mal funcionamiento del programa.

CE3.1 Describir el proceso de gestión de una incidencia desde que se recibe un aviso hasta que se resuelve totalmente.

CE3.2 Enumerar el tipo de averías más comunes en un sistema microinformático y los síntomas asociados y asociar a cada una posibles soluciones y niveles de urgencia en la reparación.

CE3.3 Elaborar informes de incidencia a partir de supuestos errores descritos por un usuario.

CE3.4 En un supuesto práctico debidamente caracterizado, en el que se dispone de un equipo informático averiado y una descripción del error:

- Reproducir el problema en el equipo.
- Describir de forma clara la incidencia asociado a la avería del equipo.
- Establecer el tipo de causa probable (hardware, sistema operativo, aplicación, virus, correo, acceso a Internet, otros).
- Establecer el nivel de urgencia en la reparación.
- Describir posibles causas y soluciones al problema.
- Enumerar los elementos necesarios para su reparación.
- Enumerar las actividades prevista para la reparación.
- Estimar el tiempo necesario para la reparación del equipo informático.

CE3.5 Recuperar, en la medida de lo posible, la información dañada por la avería.

CE3.6 Aplicar los procedimientos establecidos para la salvaguarda de información y la recuperación de la misma después de una reparación.

CE3.7 En el supuesto de que el problema se haya clasificado como fallo de software (sistema operativo o aplicación):

- Identificar la causa del fallo con la ayuda de asistentes, programas de ayuda, manuales y consultas en Internet (FAQ, tutoriales, foros)
- Identificar y localizar los elementos necesarios para la reparación (firmware, drivers, soporte magnético de instalación, licencias, manuales, etc.) usando Internet en el caso de no tenerlos disponibles.
- Realizar la reparación siguiendo los procedimientos adecuados.
- Comprobar, una vez finalizada la reparación, que no se produce el mal funcionamiento que antes se producía.
- Documentar las actividades realizadas y los resultados obtenidos.

cve: BOE-A-2011-10055

CE3.8 En el supuesto de que el problema se haya clasificado como infección por un virus:
- Comprobar que el equipo informático tiene un programa antivirus y que éste está actualizado (consultando si es necesario Internet), y en caso contrario, y si es posible, instalar la última versión.
- Localizar los ficheros infectados mediante el programa antivirus.
- Eliminar el virus procurando salvar la mayor cantidad de datos.
- Documentar las actividades realizadas y los resultados obtenidos.

Contenidos

1. Recursos y componentes de un sistema informático.
- Herramientas del sistema operativo para la obtención de información.
- Recursos Hardware: Conflictos y recursos compartidos, DMA, E/S, Canales IRQ, Memoria, Hardware forzado.
- El administrador de dispositivos.
  - Información acerca de dispositivos y recursos.
  - Configurar valores y propiedades.
  - Instalación y desinstalación de dispositivos.
  - Actualizar y ver controladores de dispositivos.
  - Impresión de informes de dispositivos instalados y/o del sistema.

2. Requisitos del sistema exigidos por las aplicaciones informáticas.
- Fuentes de obtención.
- Requisitos de componentes hardware.
- Requisitos de sistema operativo.
- Otros requisitos.

3. Tipos de licencia de software.
- Tipos de programa.
  - Tipos de programas en cuanto a licencias.
  - Aplicaciones de libre uso.
  - Aplicaciones de uso temporal.
  - Aplicaciones en desarrollo (beta).
  - Aplicaciones necesarias de licencia.
  - Acuerdos corporativos de uso de aplicaciones.
  - Licencias mediante código.
  - Licencias mediante mochilas.
- Derechos de autor y normativa vigente.
  - Derechos de Autor.
  - Patentes, Marcas y Propiedad Industrial.
  - La Ley Orgánica de Protección de Datos y Seguridad Informática.
  - La Ley de la Propiedad Intelectual.

4. Instalación de aplicaciones informáticas.
- Componentes de una aplicación.
  - Formato.
  - Manual de instalación.
  - Manual de usuario.
- Procedimientos de copia de seguridad.
- Instalación y registro de aplicaciones.
  - Software legal e ilegal. La ley de propiedad intelectual.
    - Validación de software original.
    - Certificados de autenticidad.
  - Instalación o actualización de componentes y aplicaciones.
    - Ofimáticas.
      - Procesadores de texto.

cve: BOE-A-2011-10055

- Hojas de cálculo.
- Aplicaciones de presentación de diapositivas.
- Aplicaciones de tratamiento de gráficos.
- Otras aplicaciones y componentes.
- Instalación desde un CD.
- Instalación desde internet.
- Utilización de asistentes en la instalación.
- Archivos comprimidos.
- Activación y registro de aplicaciones.
- Desinstalación de aplicaciones.
- Configuración de aplicaciones ofimáticas más comunes.
- Procedimientos de prueba y verificación de:
  - Componentes instalados.
  - Acceso a recursos propios.
  - Acceso a recursos compartidos.

5. Diagnóstico y resolución de averías software.

- Metodología para la resolución de problemas.
  - Documentación.
  - Ayuda y soporte técnico en la web.
  - Foros, blogs, comunidades, etc
- Programas de diagnóstico.
- Configuración de informes de errores del sistema y de las aplicaciones.
- Identificación de los fallos.
  - Pérdida de datos y de archivos.
  - Inestabilidad del sistema.
  - Mal funcionamiento del sistema.
  - Mal funcionamiento del equipo por cambios en la configuración del sistema o de las aplicaciones.
  - Mal funcionamiento de una aplicación.
  - El sistema operativo no se inicia.
  - Otros.
- Procedimientos comunes de solución.
  - Copias de seguridad de archivos y carpetas.
  - Reinstalación de controladores.
  - Restauración del sistema y aplicaciones.
  - Deshabilitación de dispositivos hardware.
  - Agregar o quitar programas.
  - Restauración de la última configuración válida.
  - Inicio del equipo en modo a prueba de errores.
  - La consola de recuperación.
  - Copia de seguridad.
  - Restauración del sistema.
  - Reinstalación del sistema operativo.
  - Otros.

6. Instalación y configuración del software antivirus.

- Virus informáticos.
  - Software malicioso: Conceptos y definiciones.
    - Evolución.
    - Virus, gusanos, troyanos, otros.
    - Vulnerabilidades en programas y parches.
    - Tipos de ficheros que pueden infectarse.
    - Medios de propagación.
    - Virus en correos, en programas y en documentos.
    - Ocultación del software malicioso.

cve: BOE-A-2011-10055

- Páginas web.
- Correo electrónico.
- Memoria principal del ordenador.
- Sector de arranque.
- Ficheros con macros.
- Efectos y síntomas de la infección.
- Virus informáticos y sistemas operativos.
- Actualizaciones criticas de sistemas operativos.
- Precauciones para evitar infección.
- Definición de software antivirus.
- Componentes activos de los antivirus.
  - Vacuna.
  - Detector.
  - Eliminador.
- Características generales de los paquetes de software antivirus.
  - Protección anti-spyware.
  - Protección contra el software malicioso.
  - Protección firewall.
  - Protección contra vulnerabilidades.
  - Protección contra estafas.
  - Actualizaciones automáticas.
  - Copias de seguridad y optimización del rendimiento del ordenador.
- Instalación de software antivirus.
  - Requisitos del sistema.
  - Instalación, configuración y activación del software.
  - Creación de discos de rescate.
  - Desinstalación.
- La ventana principal.
  - Estado de las protecciones. Activación y desactivación.
  - Tipos de análisis e informes.
  - Actualización automática y manual.
    - Actualización de patrones de virus y/ o ficheros identificadores de malware.
  - Configuración de las protecciones. Activación y desactivación.
  - Análisis, eliminación de virus y recuperación de los datos.
  - Actualizaciones.
  - Acceso a servicios.
    - Soporte.
    - Obtención de información.
  - Otras opciones.

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0221_2	60	30

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-2011-10055

MÓDULO FORMATIVO 4

Denominación: APLICACIONES MICROINFORMÁTICAS.

Código: MF0222_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0222_2 Facilitar al usuario la utilización de paquetes informáticos de propósito general y aplicaciones específicas.

Duración: 200 horas

UNIDAD FORMATIVA 1

Denominación: ASISTENCIA DE USUARIOS EN EL USO DE APLICACIONES OFIMÁTICAS Y DE CORREO ELECTRÓNICO

Código: UF0856

Duración: 40 horas

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

Capacidades y criterios de evaluación

C1: Facilitar el uso de las aplicaciones informáticas asistiendo al usuario durante el período de utilización.

CE1.1 Aplicar las técnicas de comunicación personal adecuadas para conseguir una buena comunicación con el usuario.

CE1.2 laborar una guía visual con los conceptos básicos de uso de una aplicación, en la que se describen los procedimientos y las precauciones básicas.

CE1.3 En diferentes supuestos prácticos de asistencia simulada al usuario debidamente carácterizados:

- Interpretar adecuadamente la necesidad del usuario según las explicaciones del mismo.
- Definir el procedimiento de intervención.
- Elaborar la guía textual o visual adecuada al problema planteado.
- Adiestrar al usuario en la aplicación de la solución.

C2: Gestionar correo y agenda electrónica mediante aplicaciones ofimáticas.

CE2.1 Describir los elementos que componen un correo electrónico.

CE2.2 Enumerar y describir las necesidades básicas de gestión de correros y agendas electrónicas.

CE2.3 Enumerar las similitudes y diferencias entre correo electrónico, correo electrónico en Internet y foros de noticias «news».

CE2.4 Conectar y sincronizar agendas en equipos informáticos con agendas en dispositivos portátiles tipo «palm».

CE2.5 En un supuesto práctico de la gestión de la libreta de direcciones:

- Importar y exportar contactos.
- Organizar los contactos en carpetas y crear listas de distribución
- Disponer la libreta de direcciones a otros programas para envío de cartas o creación de etiquetas.
- Insertar nuevos contactos eliminar o modificar los ya existentes

CE2.6 En un supuesto práctico de gestión del correo electrónico:

- Importar y exportar correos de / a otras herramientas u otras versiones del programa de correo.
- Crear plantillas de correo y firmas corporativas.

cve: BOE-A-2011-10055

- Organizar el correo en carpetas siguiendo los criterios que se indiquen.
- Realizar salvaguardas, recuperación y eliminación de correos antiguos.
- Configurara la aplicación para redirección automática de correos, evitar correo no deseado «spam» y otras funciones de la aplicación

CE2.7 En un supuesto práctico de gestión de la agenda:
- Incluir entradas en la agenda.
- Organizar reuniones.
- Incluir tareas.
- Incluir avisos.

CE2.8 En un caso práctico, efectuar la suscripción a foros de noticias, sincronizar los correos y participar en él para comprobar su funcionamiento.

Contenidos

1. Técnicas de comunicación en la asistencia al usuario.
- Tipos de comunicación.
- Efectos de la comunicación.
- Obstáculos o barreras para la comunicación.
- La comunicación en la empresa.
- Formas de comunicación oral.
- Precisión y claridad en el lenguaje.
- Asistencia al usuario.
  - Formación a usuarios.
    - Asesoramiento en el manejo de utilidades y aplicaciones.
    - Políticas de seguridad.
  - Utilización del soporte técnico y sus procedimientos.
  - Elaboración de guías textuales o visuales para usuarios.
- Tipos de licencia de software.
  - Tipos de programa
  - Tipos de programas en cuanto a licencias.
    - Aplicaciones de libre uso.
    - Aplicaciones de uso temporal.
    - Aplicaciones en desarrollo (beta).
    - Aplicaciones necesarias de licencia.
    - Acuerdos corporativos de uso de aplicaciones.
    - Licencias mediante código.
    - Licencias mediante mochilas.
  - Derechos de autor y normativa vigente.
    - Derechos de Autor.
    - Patentes, Marcas y Propiedad Industrial.
    - La Ley Orgánica de Protección de Datos y Seguridad Informática.
    - La Ley de la Propiedad Intelectual.

2. Gestión del correo electrónico y de la agenda.
- Definiciones y términos.
- Funcionamiento.
- El formato de un correo electrónico.
  - Encabezado.
  - Cuerpo del mensaje
  - Archivos adjuntos.
- Configuración de cuentas de correo.
- Gestores de correo electrónico.
  - Ventanas.
  - Redacción y envío de un mensaje.
    - Remitente.
    - Destinatario (A:, CC:, CCC)

cve: BOE-A-2011-10055

- Asunto.
- Texto del mensaje.
- Datos adjuntos.
- Lectura del correo.
- Respuesta del correo.
- Organización de mensajes.
- Impresión de correos.
- Libreta de direcciones.
- Filtrado de mensajes.
- Correo Web.
- Plantillas y firmas corporativas.
- Gestión de la libreta de direcciones.
  - Importar.
  - Exportar.
  - Añadir contactos.
  - Crear listas de distribución.
  - Poner la lista a disposición de otras aplicaciones ofimáticas.
- Gestión de correo.
  - Organización de carpetas.
  - Importar.
  - Exportar.
  - Borrar mensajes antiguos guardando copias de seguridad.
  - Configuración del correo de entrada.
  - Protección de correos no deseados “spam”.
- Componentes fundamentales de una aplicación de gestión de correos y agendas electrónicas.
- Foros de noticias “news”:
  - Configuración.
  - Uso.
  - Sincronización de mensajes.
- Programas de agendas en sincronización con dispositivos portátiles tipo “palm”.
  - Instalación.
  - Uso.
  - Sincronización.
- Gestión de la agenda.
  - Citas.
  - Calendario.
  - Avisos.
  - Tareas.
  - Notas.
  - Organizar reuniones.
  - Disponibilidad del asistente.

3. Instalación de programas de cifrado de correos.

- Descarga e instalación.
- Generación de claves pública y privada.
- La gestión de claves.
- Configuración.
- Distribución y obtención de claves.
- Envío de correos cifrados/firmados.

4. Obtención de certificados de firma electrónica.

- Conceptos sobre seguridad en las comunicaciones.
- Certificados electrónicos.
- Firma electrónica.
- Prestador de servicios de certificación.

cve: BOE-A-2011-10055

- Obtención de un certificado por una persona física.
- El certificado y el correo electrónico.

UNIDAD FORMATIVA 2

Denominación: ELABORACIÓN DE DOCUMENTOS DE TEXTO.

Código: UF0857

Duración: 50 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2 en lo referido a procesadores de texto.

Capacidades y criterios de evaluación

C1: Elaborar documentos mediante aplicaciones ofimáticas de procesador de textos.

CE1.1 Describir las características fundamentales de un documento que puedan ser realizadas por un procesador de textos.

CE1.2 Describir la forma de elaborar distintos documentos tipo: cartas, oficios, certificados, reclamaciones, faxes, actas, convocatorias y otros documentos.

CE1.3 Explicar las características fundamentales que proporcionan los procesadores de textos para comentar y revisar documentos por muchas personas.

CE1.4 Organizar las carpetas y los documentos del ordenador para que tengan un acceso cómodo y eficaz desde el procesador de texto.

CE1.5 Realizar operaciones de localización, recuperación, nombrado y grabación de documentos desde un procesador de textos.

CE1.6 Incorporar al documento elementos de otras aplicaciones (tablas, gráficas, trozos de texto).

CE1.7 Importar documentos procedentes de otros procesadores de textos o de versiones anteriores usando las herramientas de la aplicación.

CE1.8 Imprimir documentos desde el procesador de textos, usando todas las posibilidades de la aplicación y de la impresora.

CE1.9 Elaborar plantillas, usando para ello las características proporcionadas por el procesador de textos. Elaborar sobres y etiquetas combinando plantillas con campos de una base de datos.

CE1.10 Elaborar macros sencillas y ponerlas a disposición de otros usuarios.

CE1.11 En un supuesto práctico, elaborar un documento a partir de varios ficheros correspondientes a partes del mismo, homogeneizando los formatos y utilizando documentos maestros y subdocumentos.

Contenidos

1. **Programa de tratamiento de textos.**
   - Entrada y salida del programa.
   - Descripción del Interface del procesador de texto.
   - Ventana de documento.
   - Barra de estado.
   - Ayuda de la aplicación de tratamiento de textos.
   - Barra de herramientas Estándar.
   - Uso de métodos de tecla abreviada.
   - Operaciones con el texto del documento.
     - Generalidades.
     - Modo Insertar texto.
     - Modo de sobrescribir.
     - Borrado de un carácter.
     - Desplazamiento del cursor.

cve: BOE-A-2011-10055

- Diferentes modos de seleccionar texto.
- Opciones de copiar y pegar.
- Búsqueda y reemplazado de texto.
- Uso y particularidades del portapapeles.
- Inserción de caracteres especiales.
- Inserción de fecha y hora.
- Deshacer y rehacer los últimos cambios.

- Operaciones con archivos de la aplicación.
  - Creación de un nuevo documento.
  - Apertura de un documento ya existente.
  - Guardado de los cambios realizados en un documento.
  - Duplicación un documento.
  - Cierre de un documento.
  - Compatibilidad de los documentos de distintas versiones y aplicaciones.
  - Manejo del Menú de ventana. Manejo de varios documentos.
- Corrección del texto.
  - Elección de Fuentes.
    - Tipo, estilo, tamaño, color, subrayado y efectos de fuente.
    - Espaciado entre caracteres.
    - Cambio de mayúsculas a minúsculas.
  - Manejo de Párrafos.
    - Alineación de párrafos.
    - Utilización de diferentes tipos de sangrías.
    - Espaciado de párrafos y líneas.
  - Inserción de Bordes y sombreados.
    - Bordes de párrafo y texto.
    - Sombreado de párrafo y texto.
  - Inserción de Numeración y viñetas.
    - Viñetas.
    - Listas numeradas.
    - Esquema numerado.
  - Manejo de Tabulaciones.
    - Tipos de tabulaciones.
    - Manejo de los tabuladores desde el cuadro de diálogo de tabuladores.
    - Uso de la regla para establecer y modificar tabulaciones.
- Configuración y visualización de páginas.
  - Configuración de página.
    - Márgenes.
    - Orientación de página
    - Tamaño de papel.
    - Diseño de página.
    - Uso de la regla para cambiar márgenes.
  - Visualización del documento.
  - Inserción de encabezados y pies de página.
  - Numeración de páginas.
  - Creación de bordes de página.
  - Inserción de saltos de página y de sección
  - Inserción de columnas periodísticas.
  - Inserción de notas al pie y al final.
- Creación de tablas.
  - Inserción o creación de tablas en un documento
  - Edición y movimiento dentro de una tabla.
  - Selección de celdas, filas, columnas, tabla.
  - Modificación del tamaño de filas y columnas.

cve: BOE-A-2011-10055

- Modificación de los márgenes de las celdas
- Aplicación de formato a una tabla.
- Cambio de la estructura de una tabla.

- Corrección de textos.
  - Selección del idioma.
  - Corrección de textos.
  - Corrección gramatical.
  - Empleo de las opciones de ortografía y gramática.
  - Uso del diccionario personalizado.
  - Autocorrección.
  - Elección de sinónimos.
  - Manejo del Traductor.
- Creación de Macros.
  - Grabadora de macros.
  - Utilización de macros.
- Impresión de documentos.
  - Impresión.
  - Configuración de la impresora.

2. Creación de sobres, etiquetas y documentos modelo.

- Creación del documento modelo para envío masivo: cartas, sobres, etiquetas o mensajes de correo electrónico.
- Selección de destinatarios mediante creación o utilización de archivos de datos.
- Creación de sobres y etiquetas, opciones de configuración.
- Combinación de correspondencia: salida a documento, impresora o correo electrónico.

3. Inserción de imágenes.

- Desde un archivo.
- Empleando imágenes prediseñadas.
- Utilizando el portapapeles.
- Ajuste de imágenes con el texto.
- Mejora de imágenes.
- Inserción y operaciones con Formas elaboradas.

4. Creación de estilos y manejo de plantillas.

- Estilos estándar.
- Asignación, creación, modificación y borrado de estilos.
- Manejo de Plantillas y asistentes.
  - Utilización de plantillas y asistentes del menú archivo nuevo.
  - Creación, guardado y modificación de plantillas de documentos.

5. Trabajo con documentos.

- Trabajo con documentos largos
  - Creación de tablas de contenidos e índices.
  - Realización de referencias cruzadas.
  - Confección de títulos numerados.
  - Confección de documentos maestros y subdocumentos.
- Fusión de documentos.
  - Con hojas de cálculo.
  - Con bases de datos.
  - Con gráficos.
  - Con presentaciones.
- Revisión de documentos y trabajo con documentos compartidos.
  - Gestión de versiones, control de cambios y revisiones.
  - Inserción de comentarios.

cve: BOE-A-2011-10055

- Comparación de documentos.
- Protección de todo o parte de un documento.

UNIDAD FORMATIVA 3

Denominación: ELABORACIÓN DE HOJAS DE CÁLCULO.

Código: UF0858

Duración: 50 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2 en lo referido a hojas de cálculo.

Capacidades y criterios de evaluación

C1: Elaborar documentos mediante aplicaciones ofimáticas de hoja de cálculo.

CE1.1 Explicar los conceptos básicos de una función: datos de entrada, función, salida

CE1.2 Organizar las carpetas y los documentos del ordenador para que tengan un acceso cómodo y eficaz desde la hoja de cálculo.

CE1.3 Realizar operaciones de localización, recuperación, nombrado y grabación de documentos desde una hoja de cálculo.

CE1.4 En diferentes supuestos prácticos de elaboración y edición de documentos usando las características proporcionadas por una hoja de cálculo:

- Incorporar los datos en sus diferentes formatos.
- Realizar los cálculos con los datos mediante fórmulas.
- Dar el formato adecuado para la correcta presentación de los datos.
- Verificar la validez de los datos mediante cálculos paralelos.
- Resolver problemas de referencias circulares, divisiones por cero, y otros con las utilidades proporcionadas por la aplicación.
- Usar referencias a otras hojas del documento y a hojas de otros documentos.
- Incorporar al documento elementos de otras aplicaciones (tablas, gráficas, trozos de texto).
- Incluir gráficos y mapas de distintos tipos con los datos de la hoja de cálculo usando los asistentes de la aplicación.

CE1.5 En diferentes supuestos prácticos, usar filtros, esquemas y operaciones de inmovilización de celdas para presentar de forma adecuada los datos.

CE1.6 Importar documentos procedentes de otros programas o de versiones anteriores usando las herramientas de la aplicación.

CE1.7 Imprimir documentos desde la hoja de cálculo, usando todas las posibilidades de la aplicación y de la impresora.

CE1.8 Crear funciones de usuario y macros sencillas y ponerlas a disposición de otros usuarios.

CE1.9 Elaborar plantillas siguiendo las instrucciones recibidas, haciendo especial hincapié en la protección de celdas y en la presentación clara para que un usuario las pueda usar de forma cómoda y sin posibilidad de error.

Contenidos

1. Aplicación de hoja de cálculo.

- Instalación e inicio de la aplicación.
- Configuración de la aplicación.
- Entrada y salida del programa.
- Descripción del interface de la hoja de cálculo.
- Ayuda de la aplicación de hoja de cálculo.
- Opciones de visualización.

cve: BOE-A-2011-10055

- Uso de métodos de tecla abreviada.
- Desplazamiento por la hoja de cálculo.
  - Mediante teclado y ratón.
  - Grandes desplazamientos.
  - Barras de desplazamiento.
- Introducción de datos en la hoja de cálculo.
  - Tipos de datos.
    - Numéricos.
    - Alfanuméricos.
    - Fecha/hora.
    - Fórmulas.
    - Funciones.
- Edición y modificación de la hoja de cálculo.
  - Selección de la hoja de cálculo.
    - Rangos.
    - Columnas.
    - Filas.
    - Hojas
  - Modificación de datos.
    - Edición del contenido de una celda.
    - Borrado del contenido de una celda o rango de celdas.
    - Uso del corrector ortográfico.
    - Uso de las utilidades de búsqueda y reemplazo.
  - Inserción y eliminación.
    - Celdas.
    - Filas.
    - Columnas.
    - Hojas de cálculo.
  - Copiado o reubicación de:
    - Celdas o rangos de celdas.
    - Hojas de cálculo.
  - Inmovilizado y protección de celdas.
- Almacenamiento y recuperación de un libro.
  - Creación de un nuevo libro.
  - Apertura de un libro ya existente.
  - Guardado de los cambios realizados en un libro.
  - Creación de un duplicado de un libro.
  - Cierre de un libro.
- Operaciones con rangos.
  - Relleno rápido de un rango.
  - Selección de varios rangos (rango múltiple, rango tridimensional).
  - Asignación de Nombres de rangos.
- Modificación de la apariencia de una hoja de cálculo
  - Formato de celda
    - Número.
    - Alineación.
    - Fuente.
    - Bordes.
    - Relleno.
    - Protección.
  - Anchura y altura de las columnas y filas
  - Ocultación y visualización de columnas, filas u hojas de cálculo.
  - Formato de la hoja de cálculo.
    - Tamaño y combinación de celdas.
    - Colores y texturas.

cve: BOE-A-2011-10055

- Tipos de líneas de separación.
- Cambio de nombre de una hoja de cálculo.
- Formatos condicionales.
- Autoformatos o estilos predefinidos.

- Manejo de Fórmulas.
  - Operadores y prioridad.
  - Escritura de fórmulas.
  - Copia de fórmulas.
  - Referencias relativas, absolutas y mixtas.
  - Referencias externas y vínculos
  - Resolución de errores en las fórmulas
    - Tipos de errores.
    - Herramientas de ayuda en la resolución de errores.
- Utilización de Funciones.
  - Empleo de Funciones matemáticas predefinidas.
  - Manejo de reglas para utilizar las funciones predefinidas.
  - Utilización de las funciones más usuales.
  - Uso del asistente para funciones.
  - Generación de funciones de usuario.
  - Utilización de funciones de rastreo de errores.
- Importación desde otras aplicaciones.
  - Bases de datos.
  - Presentaciones.
  - Documentos de texto.

2. Inserción de gráficos y otros elementos.

- Elementos de un gráfico.
- Creación de un gráfico.
- Modificación de un gráfico.
- Borrado de un gráfico.
- Inserción de otros elementos dentro de una hoja de cálculo
  - Inserción de imágenes.
  - Inserción de formas predefinidas.
  - Creación de texto artístico.
  - Inserción de otros elementos.
- Utilización de Plantillas y Macros.
  - Creación y uso de plantillas.
  - Creación y grabación de macros.
  - Utilización de macros.

3. Impresión de hojas de cálculo.

- Selección de Zonas de impresión.
- Selección de especificaciones de impresión.
- Configuración de página.
  - Márgenes.
  - Orientación.
  - Encabezados y pies y numeración de página.
- Vista preliminar.
- Formas de impresión.
- Configuración de impresora.

4. Trabajo con datos.

- Validaciones de datos.
- Realización de Esquemas.
- Creación de tablas o listas de datos.
- Ordenación de lista de datos, por uno o varios campos.
- Uso de Filtros.

cve: BOE-A-2011-10055

- Cálculo de Subtotales.

5. Revisión y trabajo con libros compartidos
- Gestión de versiones, control de cambios y revisiones
- Inserción de comentarios.
- Protección de una hoja de cálculo.
- Protección de un libro.
- Creación y uso de Libros compartidos.

UNIDAD FORMATIVA 4

Denominación: ELABORACIÓN DE PRESENTACIONES.

Código: UF0859

Duración: 30 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2 en lo referido a presentaciones.

Capacidades y criterios de evaluación

C1: Elaborar documentos mediante aplicaciones ofimáticas de presentaciones.

CE1.1 Explicar las partes de una diapositiva y los factores que se han de tener en cuenta para conseguir la correcta transmisión de la información en una presentación.

CE1.2 Organizar las carpetas y las presentaciones del ordenador para que tengan un acceso cómodo y eficaz desde la aplicación.

CE1.3 Realizar operaciones de localización, recuperación, nombrado y grabación de presentaciones desde la aplicación.

CE1.4 Elaborar plantillas de presentaciones usando las características proporcionadas por la aplicación.

CE1.5 En diferentes supuestos prácticos de elaboración y edición de presentaciones usando las características proporcionadas por la aplicación*:*
- Usar la plantilla que se establezca.
- Localizar en el catálogo disponible las figuras que más se adapten a lo requerido.
- Establecer la distribución de cuadros (textos, figuras, tablas y otros) sobre las diapositivas de acuerdo a lo requerido, usando
- diferentes colores, texturas, efectos y otras características proporcionadas por la aplicación
- Incorporar elementos de otras aplicaciones ofimáticas
- Usar las diferentes técnicas de transición entre diapositivas proporcionadas por la aplicación
- Usar las operaciones de edición que permita la aplicación para copiar, mover de sitio y modificar las dispositivas.

CE1.6 Comprobar, en un supuesto práctico, las características de la aplicación relacionadas con inclusión de comentarios y realización de ensayos.

CE1.7 Imprimir presentaciones desde la aplicación, en papel o transparencias, usando todas las posibilidades de la aplicación y de la impresora.

CE1.8 Conectar correctamente el equipo informático al de proyección para iniciar una presentación.

Contenidos

1. Diseño, organización y archivo de las presentaciones.
- La imagen corporativa de una empresa.
  - Importancia
  - Respeto por las normas de estilo de la organización

cve: BOE-A-2011-10055

- Diseño de las presentaciones
  - Claridad en la información.
  - La persuasión en la transmisión de la idea
- Evaluación de los resultados.
- Organización y archivo de las presentaciones.
  - Confidencialidad de la información.
- Entrega del trabajo realizado.

2. Aplicación de presentaciones.

- Ejecución de la aplicación para presentaciones.
- Salida de la aplicación para presentaciones.
- Creación de una presentación.
- Grabación de una presentación.
- Cierre de una presentación.
- Apertura de una presentación.
- Estructura de la pantalla.
- Descripción de las vistas de la aplicación.
  - Normal.
  - Clasificador de diapositivas.
  - Esquema.
- Acciones con diapositivas.
  - Inserción de nueva diapositiva.
  - Eliminación de diapositivas.
  - Duplicación de diapositivas
  - Ordenación de diapositivas.
- Trabajo con objetos.
  - Selección de objetos.
  - Desplazamiento de objetos.
  - Eliminación de objetos.
  - Modificación del tamaño de los objetos.
  - Duplicación de objetos.
  - Reubicación de objetos.
  - Alineación y distribución de objetos dentro de la diapositiva.
  - Trabajo con textos.
    - Inserción de texto (desde la diapositiva, desde el esquema de la presentación)
    - Modificación del formato del texto.
  - Selección de formatos de párrafos.
    - Alineación.
    - Listas numeradas.
    - Viñetas.
    - Estilos.
  - Manejo de Tablas.
    - Creación de tablas.
    - Operaciones con filas y columnas.
    - Alineación horizontal y vertical de las celdas.
  - Realización de Dibujos.
    - Líneas.
    - Rectángulos y cuadrados.
    - Círculos y elipses.
    - Autoformas.
    - Sombras y 3D.
    - Reglas y guías.
  - Utilización de Imágenes prediseñadas e insertadas.
  - Creación de gráficos
  - Creación de organigramas y diferentes estilos de diagramas.

cve: BOE-A-2011-10055

- Creación de Texto artístico.
- Inserción de sonidos y películas.
- Utilización de Formato de objetos.
  - Rellenos
  - Líneas
  - Efectos de sombra o 3D
- Documentación de la presentación.
  - Inserción de comentarios
  - Preparación de las Notas del orador
- Selección de Diseños o Estilos de Presentación.
  - Uso de plantillas de estilos.
  - Combinación de Colores.
  - Creación de Fondos de diapositivas.
  - Empleo de Patrones.

3. Impresión y presentación de diapositivas.

- Impresión y presentación de diapositivas en diferentes soportes.
  - Configuración de la página.
  - Encabezados, pies y numeración.
  - Configuración de los distintos formatos de impresión.
  - Selección de opciones de impresión.
- Presentación de diapositivas teniendo en cuenta lugar e infraestructura.
  - Animación de elementos.
  - Transición de diapositivas.
  - Selección de intervalos de tiempo.
  - Configuración de la presentación.
    - Presentación con orador
    - Presentación en exposición
    - Presentaciones personalizadas
  - Conexión a un proyector y configuración
  - Ensayo de la presentación
  - Proyección de la presentación.

UNIDAD FORMATIVA 5

Denominación: ELABORACIÓN Y MODIFICACIÓN DE IMÁGENES U OTROS ELEMENTOS GRÁFICOS.

Código: UF0860

Duración: 30 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2 en lo referido a imágenes y gráficos.

Capacidades y criterios de evaluación

C1: Elaborar gráficos mediante aplicaciones ofimáticas de elaboración o retocado de imágenes.

CE1.1 Describir las formas de representación de gráficos (mapas de bit, vectoriales) y los formatos más usuales.

CE1.2 Explicar el concepto de resolución en gráficos, las formas de compresión y las posibles pérdidas de calidad.

CE1.3 Explicar los conceptos básicos necesarios para obtener fotografías con cámaras digitales.

CE1.4 Explicar los conceptos de contraste, brillo, gamma y filtros asociados a imágenes.

cve: BOE-A-2011-10055

CE1.5 Organizar un catálogo de gráficos por contenidos que permita el acceso rápido y eficaz a las imágenes, gráficos y fotos incluidas en él.
CE1.6 Obtener imágenes mediante cámaras de fotografías digitales, escáneres, Internet u otros medios, e incorporarlas al catálogo.
CE1.7 Usar las herramientas disponibles para cambiar el formato de las imágenes y modificar su resolución para adaptar su tamaño a usos particulares, optimizando de esta forma la relación óptima de tamaño / calidad.
CE1.8 En diferentes supuestos prácticos, elaborar gráficos conforme a lo especificado, haciendo uso de todas las características que proporcione la aplicación de dibujo.
CE1.9 En diferentes supuestos prácticos, retocar fotografías conforme a lo especificado, haciendo uso de todas las características que proporcione la aplicación de edición de fotografías.

Contenidos

1. Obtención de imágenes

- Descripción de la imagen digital.
  - Formas de representación de gráficos e imágenes.
    - Mapas de bits.
    - Vectoriales.
    - Ventajas e inconvenientes de cada tipo.
  - Formatos usados para la representación de gráficos. Utilización.
  - Resolución y calidad de gráficos.
  - Formatos comprimidos. Perdidas de calidad en la compresión.
  - Modelos de color.
    - Escalas y gamas de colores.
    - Modelo de color RGB.
    - Modelo de color CMYK.
- Otros modelos.
- Técnica de escaneado.
- Cámaras digitales.
  - Componentes de una cámara digital.
  - Controles habituales.
  - LCD de estado de una cámara digital.
  - Instalación de pilas y memorias.
  - Configuración inicial.
  - Instalación del Software de la cámara digital.
  - Obtención de fotos y videoclips.
  - Conceptos básicos de obtención de fotos.
    - El enfoque.
    - Zoom óptico y digital.
    - El flash.
    - Modificación de la calidad de la imagen.
    - Modos de captura.
    - Ajustes equilibrio de blancos.
    - Velocidad ISO.
    - Ajustes de saturación y nitidez.
- Otros recursos.
- Guardar imágenes obtenidas en el sistema informático.
- Impresión de imágenes.
- Manejo de Catálogos de imágenes.
  - Creación de catálogos
  - Organización del catálogo
  - Uso del catálogo.
  - Incorporación de imágenes al catálogo.

cve: BOE-A-2011-10055

2. Utilización de las Aplicaciones de elaboración de gráficos.

- Descripción de la Interfaz Gráfica de Usuario.
- Utilización de las Herramientas para dibujar.
  - Líneas: rectas, curvas, quebradas.
  - Figuras geométricas.
  - Texto.

- Realización de Transformaciones.
  - Tamaño de los objetos.
  - Giros.
  - Unir y desunir objetos.
- Conexión y alineación entre figuras
- Agrupaciones y otras operaciones.
- Elección de colores y texturas.
- Utilización de Librerías de figuras.
- Importación y exportación de imágenes a diferentes formatos.

3. Utilización de Aplicaciones de retocado de fotografía.

- Descripción de la Interfaz Gráfica de Usuario.
- Utilización de herramientas para seleccionar y editar.
- Utilización de herramientas de transformación.
- Utilización de herramientas de color.
- Utilización de herramientas de pintura.
- Utilización de Filtros.
- Utilización de Librerías de fotos.
- Importación y exportación de imágenes a diferentes formatos.

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- UF0856	40	30
Unidad formativa 2 - UF0857	50	40
Unidad formativa 3 - UF0858	50	40
Unidad formativa 4 - UF0859	30	20
Unidad formativa 5 - UF0860	30	20

Secuencia:

Para el acceso a las Unidades Formativas 3, 4 y 5 es recomendable haber superado las Unidades Formativas 1 y 2.

Las tres últimas unidades formativas del módulo se pueden programar de manera independiente.

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 SISTEMAS MICROINFORMÁTICOS.

Código: MP0177

Duración: 40 horas

cve: BOE-A-2011-10055

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: Participar, de acuerdo con las instrucciones recibidas, en la instalación, configuración, puesta en marcha, y mantenimiento de una red de área local de acuerdo con los procedimientos establecidos en la empresa.

CE2.1 Interpretar la documentación técnica asociada a los elementos de comunicación.

CE2.2 Instalar y configurar los nodos de la red local, así como los gestores de protocolos y otros programas que soportan servicios de comunicaciones de acuerdo con los procedimientos establecidos.

CE2.3 Aplicar los procedimientos de prueba y verificación de los elementos de conectividad de la red utilizando las herramientas hardware y software necesarias.

CE2.4 Participar en la resolución de averías en la red local, utilizando las herramientas y procedimientos establecidos por la empresa.

CE2.5 Documentar el trabajo realizado de acuerdo con las prescripciones y procedimientos empresariales.

C3: Instalar, configurar y mantener paquetes informáticos de propósito general y aplicaciones específicas, de acuerdo con las instrucciones recibidas.

CE3.1 Instalar, configurar y actualizar aplicaciones ofimáticas y corporativas en un equipo informático de acuerdo con las especificaciones de la empresa y teniendo en cuenta las características del puesto de usuario.

CE3.2 Resolver los problemas de explotación de aplicaciones ante un mal funcionamiento del equipo, de acuerdo con los procedimientos establecidos y realizando la salvaguarda de información y la recuperación de la misma, en la medida de los posible.

C4: Facilitar y asistir al usuario en el uso de aplicaciones ofimáticas y corporativas.

CE4.1 Elaborar guías visuales con los conceptos básicos de uso de las aplicaciones ofimática y corporativas.

CE4.2 Adiestrar a los usuarios en el manejo de las aplicaciones ofimáticas con las que trabajan, resolviendo sus dudas o mediante la elaboración directa de trabajos.

C5: Participar en los proceso de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.

CE5.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.

CE5.2 Respetar los procedimientos y normas del centro de trabajo.

CE5.3 Emprender con diligencia las tareas según las instrucciones recibidas tratando de que se adecuen al ritmo de trabajo de la empresa.

CE5.4 Integrarse en los procesos de producción del centro de trabajo.

cve: BOE-A-2011-10055

CE5.5 Utilizar los canales de comunicación establecidos.
CE5.6 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. **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.

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	*Experiencia profesional requerida en el ámbito de la Unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con 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 de la familia profesional de informática y comunicaciones. • Certificados de profesionalidad de nivel 3 del área profesional de Sistemas y telemática	1 año	3 años
MF0220_2: Implantación de los elementos de la red local.	• 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 de la familia profesional de informática y comunicaciones. • Certificados de profesionalidad de nivel 3 del área profesional de Sistemas y telemática	1 año	3 años

cve: BOE-A-2011-10055

Módulos Formativos	Acreditación requerida	*Experiencia profesional requerida en el ámbito de la Unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0221_2: Instalación y configuración de aplicaciones informáticas.	• 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 de la familia profesional de informática y comunicaciones. • Certificados de profesionalidad de nivel 3 del área profesional de Sistemas y telemática	1 año	3 años
MF0222_2: Aplicaciones microinformáticas.	• 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 de la familia profesional de informática y comunicaciones. • Certificados de profesionalidad de nivel 3 del área profesional de Sistemas y telemática	1 año	3 años

* En los últimos tres años.

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

cve: BOE-A-2011-10055

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 ofimático, herramientas internet y programas de cifrado de correo. - Software de seguridad y antivirus. - Software para copias de seguridad y recuperación. - Software para la detección, diagnóstico y reparación. - Software para pruebas de conectividad. - Software de control de inventario de elementos de red local. - Impresora y periféricos. - Cámara digital. - Analizadores de red. - Certificadores 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.

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: Montaje y Reparación de Sistemas Microinformáticos.

Código: IFCT0309

Familia Profesional: Informática y Comunicaciones.

Área Profesional: Sistemas y telemática.

Nivel de cualificación profesional: 2

cve: BOE-A-2011-10055

Cualificación profesional de referencia:

IFC298_2 Montaje y Reparación de Sistemas Microinformáticos (Real Decreto 1201/2007, de 14 de septiembre).

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

UC0953_2: Montar equipos microinformáticos.
UC0219_2: Instalar y configurar el software base en sistemas microinformáticos.
UC0954_2: Reparar y ampliar equipamiento microinformático.

Competencia general

Montar, reparar y ampliar, equipos y componentes que forman un sistema microinformático, verificar la ausencia de interferencias entre ellos y asegurar su funcionamiento, reaccionando ante averías hardware y software detectadas y aplicando procedimientos correctivos.

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional tanto por cuenta propia, como por cuenta ajena en empresas o entidades públicas o privadas de cualquier tamaño, que disponen de equipos informáticos para su gestión, y en empresas o departamentos de informática.

Sectores productivos:

Se ubica sobre todo en el sector servicios, y principalmente en los siguientes tipos de empresas: empresas dedicadas a la comercialización, montaje y reparación de equipos y servicios microinformáticos; empresas que prestan servicios de asistencia técnica microinformática; 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.

Instalador de equipos microinformáticos.
Reparador de equipos microinformáticos.
Reparador de periféricos de sistemas microinformáticos.

Duración de la formación asociada: 510 horas

Relación de módulos formativos y de unidades formativas.

MF0953_2: Montaje de equipos microinformáticos. (150 horas)
- UF0861: Montaje y verificación de componentes. (90 horas)
- UF0862: Instalación y configuración de periféricos microinformáticos. (60 horas)

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)

MF0954_2: Reparación de equipamiento microinformático. (180 horas)
- UF0863: Reparación y ampliación de equipos y componentes hardware microinformáticos. (80 horas)
- UF0864: Resolución de averías lógicas en equipos microinformáticos. (30 horas)
- UF0865: Reparación de impresoras. (70 horas)

MP0179: Módulo de prácticas profesionales no laborales de Montaje y reparación de Sistemas Microinformáticos. (40 horas)

cve: BOE-A-2011-10055

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: MONTAR EQUIPOS MICROINFORMÁTICOS.

Nivel: 2

Código: UC0953_2

Realizaciones profesionales y criterios de realización

RP1: Montar los componentes hardware que forman un equipo microinformático siguiendo especificaciones establecidas, según necesidades de uso y en condiciones de seguridad.

CR1.1 Las especificaciones de montaje recibidas se interpretan, con objeto de identificar los componentes para realizar el ensamblado.

CR1.2 Las prestaciones y características de los componentes hardware se identifican de cara a su inclusión en el montaje del equipo microinformático.

CR1.3 La recepción de equipos y componentes se efectúa mediante los procedimientos de documentación, etiquetado, registro, almacenaje y manipulación establecidos, asegurando sus ubicaciones en las condiciones ambientales y de seguridad apropiadas según las normas establecidas.

CR1.4 Los componentes se ensamblan utilizando las herramientas y útiles apropiados, asegurando las conexiones entre ellos y verificando la sujeción, siguiendo los procedimientos establecidos por la organización, las recomendaciones de instalación del fabricante, y las medidas y elementos para la prevención de riesgos laborales.

CR1.5 Los componentes se ensamblan, tratando los embalajes, residuos y componentes desechables de acuerdo a las normativas medioambientales existentes, garantizando así la seguridad e higiene en el trabajo.

CR1.6 La identificación y etiquetado de cada uno de los componentes que forman el equipo montado, y del conjunto completo, se realiza haciendo uso de los sistemas de documentación externa e interna establecidos.

CR1.7 El resultado de los procedimientos de ensamblado y montaje del equipo, así como las incidencias detectadas, se documentan, para su uso posterior, siguiendo los modelos internos establecidos por la organización.

CR1.8 La documentación técnica específica asociada a los componentes hardware se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP2: Verificar el ensamblado de componentes, para asegurar la funcionalidad del sistema microinformático, siguiendo las especificaciones establecidas y de acuerdo a condiciones de seguridad.

CR2.1 El proceso de verificación de los componentes ensamblados se realiza siguiendo las pautas establecidas por la organización, estándares normalizados y normativa legal tanto en aspectos electrotécnicos, como de seguridad y de prevención de riesgos laborales.

CR2.2 El sistema operativo se implanta según las especificaciones recibidas, para comprobar que los componentes que utilizan drivers son reconocidos y no producen conflictos.

CR2.3 La integración de los componentes ensamblados en el equipo informático se realiza en la BIOS (Basic Input-Output System, sistema básico de entrada-salida) para obtener el máximo rendimiento del equipo, según el procedimiento establecido.

CR2.4 La verificación del ensamblado del equipo para asegurar que los componentes son reconocidos y habilitados se realiza comprobando los

cve: BOE-A-2011-10055

mensajes del POST (Power-On Self Test, test automático de encendido) y del sistema operativo según especificaciones técnicas y siguiendo el procedimiento establecido.
CR2.5 Los ajustes de los componentes, tanto firmware como hardware, se establecen de manera que se asegure el funcionamiento del equipo, según las especificaciones recibidas.
CR2.6 Los ensayos de estabilidad y seguridad de los equipos se realizan para verificar su funcionalidad siguiendo las recomendaciones de los fabricantes, propias de la empresa, estándares industriales y normativa vigente.
CR2.7 El software de medida se utiliza para realizar ensayos de rendimiento y evaluar y comparar las características de los equipos, según los procedimientos establecidos.
CR2.8 Los trabajos realizados así como las incidencias detectadas durante la verificación se documentan para su uso posterior, siguiendo los modelos internos establecidos por la organización derivando las incidencias al servicio correspondiente.

RP3: Instalar y configurar los periféricos del equipo microinformático, para su explotación, siguiendo especificaciones establecidas, según las necesidades de uso y en condiciones de seguridad.

CR3.1 La recepción y verificación de los dispositivos periféricos, su almacenaje y manipulación, se efectúan en las condiciones ambientales y de seguridad apropiadas, siguiendo el procedimiento establecido.
CR3.2 Los dispositivos periféricos, controladores de dispositivos y cableado de conexión que se van a instalar se verifican, para asegurar su compatibilidad y concordancia con las especificaciones recibidas, siguiendo procedimientos establecidos.
CR3.3 Los dispositivos periféricos se instalan utilizando las herramientas específicas, asegurando: su conexión con el equipo informático, suministro eléctrico, estabilidad, ergonomía y etiquetado, y aplicando criterios de seguridad, calidad y eficiencia, según procedimientos establecidos.
CR3.4 La configuración de cada periférico para la puesta en funcionamiento, se realiza siguiendo las instrucciones de la documentación técnica asociada y las especificaciones de la instalación.
CR3.5 Los controladores de dispositivos y las utilidades software asociadas al periférico, si fueran necesarias, se instalan y configuran para garantizar su explotación como componente del sistema, siguiendo especificaciones técnicas.
CR3.6 Las pruebas integrales para verificar el funcionamiento de los periféricos instalados se llevan a cabo según procedimientos establecidos.
CR3.7 Los trabajos realizados, así como las incidencias detectadas durante la instalación y configuración se documentan, para su uso posterior, siguiendo los modelos internos establecidos por la organización.
CR3.8 La documentación técnica específica asociada a los periféricos se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

Contexto profesional

Medios de producción

Elementos de protección (calzado aislante, gafas, guantes, descargador de electricidad estática, entre otros). Elementos de protección y seguridad personal. Elementos de protección de equipos. Herramientas y utillaje de uso común en mantenimiento eléctrico / electrónico. Herramientas específicas de medida y diagnóstico para montaje. Componentes informáticos: chasis, placas, fuentes de alimentación, tarjetas, soportes y memorias, entre otros. Periféricos: monitores, impresoras, escáneres, lectoras y cintas de backup, entre otros. Elementos de interconexión. Puestos con equipamiento especial para montaje. Equipos informáticos. Software de instalación y diagnóstico.

cve: BOE-A-2011-10055

Sistemas operativos instalados en soportes removibles preparados para su ejecución. Herramientas software de documentación. Herramientas de clonación.

Productos y resultados
Equipos informáticos ensamblados, instalados y verificados según las especificaciones recibidas. Equipos fiables que cumplen las normativas vigentes. Equipos documentados. Equipos con posibilidades de modificación y ampliación. Registro y almacenamiento de los elementos utilizados para el montaje.

Información utilizada o generada
Albaranes y documentación de recepción de equipos. Documentación de calibración de los equipos de medida. Normas sobre garantías (coberturas según los casos). Pruebas y control de muestras según normas de muestreo. Especificaciones para el montaje de equipos informáticos y dispositivos periféricos. Normas sobre el etiquetado y serialización de los componentes. Manuales de instalación e información técnica de los equipos y/o componentes. Manuales del software de base. Manuales del software específico. Catálogos de productos, proveedores, precios. Recomendaciones de montaje de los fabricantes. Soporte técnico del fabricante. Partes de trabajo. Partes de incidencias e histórico de incidencias de montaje. Documentación técnica y de prestaciones de los equipos. Guía de instalación y puesta en marcha del equipo. Normativas de seguridad e higiene. Normativas nacionales electrotécnicas. Normativas internacionales y estándares (ISO, EIA, IEEE, entre otros). Normativas internas de la organización. Normas para la protección contra descargas electroestáticas (ESD). Informes de prestaciones. Informes de incidencias del montaje, catalogados almacenados y controlados. Documentación del montaje (procesos, esquemas, memoria de componentes, entre otros) catalogada, almacenada y controlada. Documentación de la instalación y puesta en marcha del equipo para los clientes.

Unidad de competencia 2

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.

cve: BOE-A-2011-10055

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.
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.

cve: BOE-A-2011-10055

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. Informes de instalación, configuración y actualización del sistema operativo.

Unidad de competencia 3

Denominación: REPARAR Y AMPLIAR EQUIPAMIENTO MICROINFORMÁTICO.

Nivel: 2

Código: UC0954_2

Realizaciones profesionales y criterios de realización

RP1: Detectar averías en equipos microinformáticos y proceder a su solución, reparando o sustituyendo los componentes hardware averiados, siguiendo los procedimientos establecidos por la organización.

CR1.1 La causa del comportamiento anómalo se establece mediante la realización de pruebas funcionales iniciales para verificar los síntomas recogidos en el parte de averías y precisar las características de la misma, estableciendo la naturaleza física o lógica del problema valorando la posibilidad de reparación o sustitución, en función de los costes económicos de las mismas de manera que facilite la posterior documentación y gestión económica de la actuación.

CR1.2 Las herramientas software de diagnóstico se instalan y utilizan para determinar fallos intermitentes o bien problemas en el funcionamiento del sistema, según procedimiento establecido.

CR1.3 Las herramientas hardware de diagnóstico se instalan y utilizan, para detectar fallos en los componentes del sistema microinformático cuando el equipo no se enciende, según especificaciones técnicas establecidas.

CR1.4 Los componentes software afectados se reinstalan, actualizan o configuran con los parámetros indicados, para su funcionamiento, de acuerdo con las especificaciones técnicas recibidas.

CR1.5 Los componentes hardware averiados son reparados o sustituidos utilizando herramientas y dispositivos específicos, asegurando las conexiones eléctricas y electrónicas y la sujeción mecánica, confeccionando los cables necesarios para realizar las conexiones, si fuera el caso, para garantizar su funcionalidad en el sistema, siguiendo los procedimientos establecidos por la organización y aplicando criterios de funcionalidad, ergonomía, calidad, seguridad y eficiencia.

CR1.6 Las averías que no se han conseguido diagnosticar, se reportan al nivel de responsabilidad superior para su gestión, siguiendo los protocolos y procedimientos de actuación de la organización.

cve: BOE-A-2011-10055

CR1.7 Los embalajes, residuos y componentes desechables se tratan para su eliminación o reciclaje, de acuerdo a las normativas medioambientales sobre tratamiento de residuos.
CR1.8 Las pruebas de arranque y parada del sistema se realizan, para verificar y asegurar el funcionamiento de los equipos y componentes reparados o sustituidos, siguiendo los procedimientos establecidos.
CR1.9 La documentación realizada sobre la gestión de las incidencias producidas se registra para su uso posterior, siguiendo los modelos internos establecidos por la organización.

RP2: Ampliar equipos microinformáticos para añadir nuevas funcionalidades al sistema, de acuerdo a las especificaciones establecidas.

CR2.1 Las operaciones de actualización de componentes en equipos microinformáticos para la ampliación del mismo, se realizan comprobando las posibilidades de expansión y valorando los costes económicos, siguiendo el procedimiento establecido.
CR2.2 Los componentes se ensamblan utilizando las herramientas y útiles específicos para asegurar las conexiones entre ellos y verificar la sujeción, siguiendo la normativa de seguridad física, los procedimientos establecidos por la organización y las especificaciones técnicas del fabricante.
CR2.3 La compatibilidad de los nuevos componentes es verificada, para asegurar la integridad de los equipos y datos, comprobando el funcionamiento del equipo actualizado, siguiendo especificaciones técnicas establecidas.
CR2.4 La realización de copias de salvaguarda se realiza antes de la instalación de los componentes para asegurar la integridad del sistema, de acuerdo a las especificaciones recibidas.
CR2.5 El software asociado a la actualización se instala y configura para comprobar que los componentes añadidos son reconocidos y no producen conflictos, verificando y asegurando el funcionamiento del sistema mediante pruebas de arranque y parada, siguiendo el procedimiento establecido.
CR2.6 La documentación realizada sobre la ampliación y las incidencias que hayan podido producirse se registra, para su uso posterior, siguiendo los modelos internos establecidos por la organización.

RP3: Diagnosticar y reparar fallos lógicos en equipos microinformáticos, utilizando herramientas software específicas y siguiendo los procedimientos establecidos.

CR3.1 La causa del comportamiento anómalo se establece mediante la realización de pruebas funcionales iniciales, para verificar los síntomas recogidos en el parte de averías y precisar las características de la misma, estableciendo la naturaleza lógica del problema, siguiendo procedimientos establecidos.
CR3.2 Los procesos en ejecución se comprueban, para detectar consumos excesivos de recursos debido a posibles ataques de virus y programas maliciosos, siguiendo especificaciones técnicas establecidas.
CR3.3 El software de seguridad y detección (antivirus y antiespías) se utiliza, para diagnosticar y reparar posibles daños y pérdidas de información producidos por los virus y programas maliciosos, siguiendo el procedimiento establecido.
CR3.4 Las herramientas de recuperación de datos se utilizan para rescatar archivos borrados accidentalmente o afectados por alguna avería o incidencia, siguiendo los procedimientos establecidos.
CR3.5 El sistema de archivos se comprueba y verifica utilizando herramientas software específicas, con el fin de mantener la integridad del mismo, de acuerdo a las especificaciones técnicas recibidas.
CR3.6 Las aplicaciones afectadas se reinstalan o reconfiguran para su puesta en funcionamiento, siguiendo especificaciones técnicas recibidas y de acuerdo al procedimiento establecido.

cve: BOE-A-2011-10055

CR3.7 La documentación sobre la reparación que se ha realizado así como las incidencias detectadas, se registran para su uso posterior, siguiendo los modelos internos establecidos por la organización.
CR3.8 Las averías que no se han conseguido subsanar se reportan al nivel de responsabilidad superior para su gestión, siguiendo los protocolos y procedimientos de actuación establecidos por la organización.
CR3.9 La documentación técnica específica asociada se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP4: Identificar y solucionar averías en impresoras y otros dispositivos periféricos utilizando programas y útiles de ajuste, siguiendo las recomendaciones establecidas por los fabricantes.

CR4.1 La recepción de los periféricos averiados se efectúa mediante la descripción de la avería producida, utilizando documentación normalizada con objeto de establecer el mejor procedimiento de actuación posible, de acuerdo a la normativa de la organización.
CR4.2 La causa del comportamiento anómalo se establece mediante la realización de pruebas funcionales iniciales, para verificar los síntomas recogidos en el parte de averías y precisar las características de la misma, estableciendo la naturaleza del problema y la posibilidad de reparación con medios propios o en otras instalaciones de mayor nivel de especialización, según se indica en los protocolos de actuación de la organización.
CR4.3 El proceso de reparación y ajuste de los componentes de las impresoras y otros equipos periféricos se realiza, para garantizar el funcionamiento del dispositivo, siguiendo las pautas establecidas por la organización, estándares normalizados y normativa legal, tanto en aspectos electrotécnicos, como de seguridad y prevención de riesgos laborales.
CR4.4 Los componentes averiados se identifican y sustituyen utilizando herramientas específicas, con objeto de habilitar todas las funcionalidades del dispositivo, teniendo en cuenta las recomendaciones del fabricante, siguiendo los procedimientos establecidos por la organización y aplicando criterios de funcionalidad, ergonomía, calidad, seguridad y eficiencia.
CR4.5 Las averías que no se han conseguido aislar se reportan al nivel de responsabilidad superior para su gestión, siguiendo los protocolos y procedimientos de actuación de la organización.
CR4.6 Las pruebas de funcionamiento del periférico reparado se realizan para verificar y asegurar el funcionamiento de los mismos, siguiendo procedimientos establecidos.
CR4.7 La documentación de la reparación realizada, así como de las incidencias producidas, se registra para su uso posterior, siguiendo los protocolos y procedimientos de actuación establecidos por la organización.

Contexto profesional

Medios de producción

Equipos informáticos. Elementos de protección (calzado aislante, gafas, guantes, descargador de electricidad estática, entre otros). Herramientas y utillaje de uso común en mantenimiento eléctrico/electrónico. Componentes informáticos. Dispositivos periféricos. Impresoras. Sistemas operativos, controladores, programas de utilidad. Software antivirus y antiespia. Herramientas hardware de diagnóstico. Herramientas software de diagnóstico. Software libre para el mantenimiento informático.

Productos y resultados

Equipos informáticos reparados. Equipos informáticos ampliados. Impresoras y periféricos reparados y sustituidos.

cve: BOE-A-2011-10055

Información utilizada o generada

Especificaciones para el montaje de dispositivos periféricos. Documentación técnica asociada a la eliminación de virus y software maligno. Documentación técnica y de prestaciones de los dispositivos periféricos. Manuales técnicos de impresoras. Normas sobre el etiquetado y serialización de los componentes. Manuales de instalación e información técnica de los dispositivos periféricos. Manuales del software de base. Manuales del software específico. Catálogos de productos, proveedores, precios. Recomendaciones de montaje de los fabricantes. Soporte técnico del fabricante asociado a los dispositivos. Partes de trabajo. Normativas de seguridad e higiene. Normativas nacionales electrotécnicas. Normativas internaciones y estándares (ISO, EIA, IEEE, entre otras). Normativas internas de la empresa. Legislación sobre protección de datos y propiedad intelectual, normativa empresarial sobre confidencialidad de datos. Legislación sobre residuos. Documentación asociada a las ampliaciones y reparaciones realizadas.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: MONTAJE DE EQUIPOS MICROINFORMÁTICOS.

Código: MF0953_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0953_2 Montar equipos microinformáticos.

Duración: 150 horas

UNIDAD FORMATIVA 1

Denominación: MONTAJE Y VERIFICACIÓN DE COMPONENTES.

Código: UF0861

Duración: 90 horas

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

Capacidades y criterios de evaluación

C1: Clasificar los componentes que se utilizan en el montaje de los equipos microinformáticos, identificando sus parámetros funcionales y características, teniendo en cuenta sus especificaciones técnicas.

CE1.1 Identificar los formatos de chasis que se utilizan en la instalación de equipos informáticos, indicando sus características y funcionalidad.

CE1.2 Describir los tipos de fuentes de alimentación del mercado que se utilizan para la instalación en equipos microinformáticos, identificando sus parámetros funcionales y utilización, teniendo en cuenta sus especificaciones técnicas

CE1.3 Clasificar los tipos de placa base identificando sus características, conectividad y recomendaciones de uso, teniendo en cuenta sus especificaciones técnicas.

CE1.4 Describir los tipos de procesadores actuales detallando sus parámetros funcionales, recomendaciones de uso y su influencia en el rendimiento global del equipo.

cve: BOE-A-2011-10055

CE1.5 Identificar los tipos memoria RAM sus características, tecnología, parámetros funcionales y recomendaciones de uso para evaluar su influencia en el rendimiento global del equipo.
CE1.6 Definir los sistemas de almacenamiento masivo, indicando su tecnología, modo de conexión, parámetros funcionales, recomendaciones de uso y su influencia en el rendimiento global del equipo, para su utilización en el montaje de equipos microinformáticos.
CE1.7 Describir las características, parámetros funcionales e influencia, en el rendimiento global del equipo, de los adaptadores que se utilizan en la instalación de equipos microinformáticos para su conexión con otros dispositivos o con redes de comunicaciones.
CE1.8 Definir las características de los periféricos que se conectan a un equipo microinformático detallando sus particularidades y parámetros más significativos.
CE1.9 En supuestos prácticos, debidamente caracterizados, interpretar una solicitud de montaje de un equipo microinformático para proceder al ensamblado de los componentes, con objeto de garantizar la calidad del resultado:
- Buscar las características de los componentes en catálogos de distribuidores y fabricantes.
- Clasificar y seleccionar los componentes en función de las características establecidas en la solicitud, el presupuesto establecido y la homologación y garantía de los mismos.
- Comprobar la compatibilidad de los componentes.

C2: Instalar los elementos que componen los equipos microinformáticos, aplicando criterios de calidad, eficiencia y seguridad, de acuerdo a especificaciones técnicas recibidas.
CE2.1 Describir las características de un puesto de montaje de equipos microinformáticos y de las herramientas e instrumentos necesarios para realizar los procesos de ensamblado e instalación de componentes
CE2.2 Describir los procedimientos para la realización del montaje de equipos microinformáticos en función de su tecnología y características propias, teniendo en cuenta los criterios de calidad y seguridad definidos.
CE2.3 En supuestos prácticos, debidamente caracterizados, realizar el ensamblaje de un equipo microinformático para su utilización, de acuerdo a unas instrucciones recibidas:
- Identificar cada uno de los bloques funcionales que componen el ordenador y asociarlos con los componentes a ensamblar en el equipo.
- Elegir los componentes que formarán el equipo.
- Aplicar las medidas de seguridad establecidas.
- Interpretar la documentación técnica de los componentes a ensamblar
- Realizar el ensamblaje y ajuste de los componentes utilizando las herramientas y útiles necesarios.
- Realizar la documentación de todos los aspectos de la fase de montaje mediante el uso de documentos y plantillas establecidas.

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 el montaje de componentes.

C3: Verificar los equipos microinformáticos montados y asegurar su funcionalidad, estabilidad, seguridad y rendimiento, de acuerdo a las especificaciones dadas.
CE3.1 Describir los procedimientos de pruebas especificados para verificar la funcionalidad del montaje.
CE3.2 Identificar y aplicar la configuración inicial (SETUP) del equipo para optimizar su rendimiento, de acuerdo a las recomendaciones del fabricante, características técnicas y requisitos establecidos.

cve: BOE-A-2011-10055

CE3.3 Identificar los parámetros de configuración de la BIOS (Basic Input/Output System) asociados a cada uno de los componentes para que sean reconocidos por el equipo ensamblado.
CE3.4 Clasificar los mensajes de la BIOS para localizar posibles desajustes en el ensamblado de los componentes, teniendo en cuenta las especificaciones técnicas de los mismos.
CE3.5 Describir y aplicar los tipos de ensayos software que se realizan para verificar la funcionalidad de equipos utilizando software específico y de medida para evaluar las prestaciones.
CE3.6 En supuestos prácticos, debidamente caracterizados, realizar la verificación del montaje de un equipo microinformático para comprobar su funcionalidad, estabilidad, seguridad y rendimiento, de acuerdo a unas especificaciones recibidas.

- Ejecutar un sistema operativo desde un dispositivo de almacenamiento extraíble.
- Comprobar los mensajes del POST y del sistema operativo.
- Comprobar que los dispositivos adaptadores y periféricos son reconocidos y habilitados por el sistema, y no presentan conflictos.
- Realizar pruebas de arranque y parada para asegurar el funcionamiento del equipo.
- Realizar el diagnóstico de posibles conflictos utilizando herramientas software de verificación y diagnóstico.
- Realizar pruebas de estabilidad, seguridad y rendimiento utilizando las herramientas software específicas.
- Realizar la documentación de la instalación y configuración realizada y los resultados obtenidos utilizando unos formatos y plantillas dadas.

Contenidos

1. **Aplicación de medidas de seguridad contra el riesgo eléctrico.**
   - Seguridad eléctrica.
     - Medidas de prevención de riesgos eléctricos.
     - Daños producidos por descarga eléctrica.
     - Seguridad en el uso de componentes eléctricos.
   - Seguridad en el uso de herramientas manuales.
2. **Herramientas y componentes electrónicos.**
   - Electricidad estática. Descargas electrostáticas (ESD).
   - Estándares de la industria relacionados con la electrostática.
     - Manejo de dispositivos sensitivos a Descargas electrostáticas (ESDS). ANSI/EIA-625
     - Empaque de productos electrónicos para el envío. ANSI/EIA-541.
     - Símbolos y etiquetas para dispositivos sensitivos a electrostática. EIA-471.
     - Protección de dispositivos electrónicos de fenómenos electrostáticos. IEC 61340-5-1.
     - Otros estándares.
3. **Interpretación de la simbología aplicada a los componentes microinformáticos.**
   - Simbología estándar de los componentes.
     - Simbología eléctrica.
     - Simbología electrónica.
   - Simbología de homologaciones nacionales e internacionales.
     - La norma UNE-E-60617 (CEI-617).
     - Normativas internacionales y estándares: ISO, EIA, IEEE, etc.

cve: BOE-A-2011-10055

4. Componentes internos de un equipo microinformático.

- Arquitectura de un sistema microinformático.
- Componentes de un equipo informático, tipos, características y tecnologías.
  - El chasis.
    - Formatos y tipos.
    - Características básicas.
    - Funcionalidad.
  - La fuente de alimentación.
    - Tipos.
    - Potencia y tensiones.
    - Ventiladores.
  - La placa base.
    - Características. Factores de forma.
    - Elementos de una placa base.
      - Zócalo del microprocesador.
      - Ranuras para la memoria.
      - "Chipset".
      - El reloj.
      - La BIOS.
      - Ranuras de expansión.
      - Conectores externos.
      - Conectores internos.
      - Conectores eléctricos.
      - Jumpers y conmutadores DIP.
      - Otros elementos integrados.
      - Fabricantes.
  - El procesador.
    - Microprocesadores actuales.
    - Características principales.
    - Disipadores de calor y ventiladores.
    - Fabricantes.
  - La memoria.
    - Parámetros fundamentales.
    - Tipos, módulos de memoria y encapsulado.
  - Unidades de almacenamiento internas: tecnología, parámetros y conexión.
    - Disco duros.
    - Lectores y grabadores de CD-ROM y DVD.
    - Disqueteras.
    - Otros dispositivos magnéticos, ópticos o magneto-ópticos.
  - Tarjetas de expansión. Características, conexionado y conectores.
- Componentes OEM y RETAIL

5. Ensamblado de equipos y montaje de periféricos básicos

- El puesto de montaje.
  - Uso.
  - Dispositivos e instrumentos.
  - Herramientas para el montaje de equipos.
  - Seguridad.
- Guías de montaje.
- Elementos de fijación, tipos de tornillos.
- El proceso de ensamblado de un equipo microinformático.
  - Montaje del microprocesador.
  - Montaje de los módulos de memoria.
  - Montaje de la fuente de alimentación.

cve: BOE-A-2011-10055

- Montaje de la placa base.
- Montaje de los dispositivos de almacenamiento: Discos duros, unidades ópticas, etc.
- Cableado de los distintos componentes y dispositivos.
- Montaje de las tarjetas de expansión.

- El ensamblado fuera del chasis.
  - Comprobación de nuevos dispositivos.
  - Comprobación de componentes.
- Descripción de dispositivos periféricos básicos.
  - Tipos de dispositivos periféricos básicos.
  - Características técnicas y funcionales.
  - Parámetros de configuración.
  - Recomendaciones de uso.
  - Especificaciones técnicas.
- Instalación y prueba de periféricos básicos.
  - Procedimientos para el montaje de periféricos.
  - Identificación de los requisitos de instalación.
    -Documentación del fabricante.
    -Alimentación eléctrica.
    -Cableado.
    -Conexiones físicas.
    -Condiciones ambientales.
  - Instalación y configuración de periféricos básicos.
  - Instalación y configuración de la tarjeta gráfica.
  - Instalación de controladores y utilidades software.
  - Realización de pruebas funcionales y operativas.

6. Puesta en marcha y verificación de equipos informáticos.

- El proceso de verificación de equipos microinformáticos.
- Proceso de arranque de un ordenador.
  - Arranque a nivel eléctrico.
  - POST.
  - Señales de error del POST.
- Herramientas de diagnóstico y/o verificación de los sistemas operativos.
- Pruebas y mensajes con sistemas operativos en almacenamiento extraíble.
- Pruebas con software de diagnóstico.
- Pruebas de integridad y estabilidad en condiciones extremas.
- Pruebas de rendimiento.

7. Configuración de la BIOS.

- El SETUP. Versiones más utilizadas.
- El menú principal de configuración de la BIOS.
  - Configuración estándar de la CMOS.
  - Configuración avanzada de la BIOS.
  - Configuración avanzada del Chipset.
  - Configuración de los periféricos integrados.
  - Configuración de la gestión de la energía.
  - Configuración de dispositivos PnP/PCI.
  - Monitorización del sistema.
  - Establecimiento de contraseñas.
  - Valores por defecto.

8. Norma y reglamentos sobre Prevención de Riesgos laborales y ergonomía.

- Marco legal general.
  - Ley 31/1995, de Prevención de Riesgos Laborales.
  - R.D. 39/1997, Reglamento de los Servicios de Prevención.

cve: BOE-A-2011-10055

- Marco legal específico.
  - R.D. 485/1997, sobre disposiciones mínimas en materia de señalización de seguridad y salud en el trabajo.
  - R.D. 486/1997, por el que se establecen las disposiciones mínimas de seguridad en los lugares de trabajo.
  - R.D. 487/1997, sobre disposiciones mínimas de seguridad y salud relativas a la manipulación manual de cargas que entrañen riesgos, en particular dorsolumbares, para los trabajadores.
  - R.D. 488/1997, sobre disposiciones mínimas de seguridad relativas al trabajo con equipos que incluyen pantallas de visualización.
  - R.D. 556/1989, por el que se arbitran medidas mínimas sobre accesibilidad en los edificios.
  - Textos básicos y guías técnicas del INSHT sobre ergonomía.

9. Normas de protección del medio ambiente.

- Ley 10/1998, de Residuos. Definiciones. Categorías de residuos.
- Ley 11/1997, de Envases y Residuos de Envases y su desarrollo. Definiciones.
- R.D. 208/2005, sobre aparatos eléctricos y electrónicos y la gestión de sus residuos.
- Objeto, ámbito de aplicación y definiciones.
- Tratamiento de residuos.
- Operaciones de tratamiento: reutilización, reciclado, valorización energética y eliminación.
- Categorías de aparatos eléctricos o electrónicos.
- Tratamiento selectivo de materiales y componentes.
- Lugares de reciclaje y eliminación de residuos informáticos. Símbolo de recogida selectiva.
- R.D. 106/2008, sobre pilas y acumuladores y la gestión ambiental de sus residuos.
- Objeto, ámbito de aplicación, y definiciones.
- Tipos de pilas y acumuladores.
- Recogida, tratamiento y reciclaje.
- Símbolo de recogida selectiva.
- Normas sobre manipulación y almacenaje de productos contaminantes, tóxicos y combustibles. Las Fichas de Datos de Seguridad.
- Identificación de las sustancias o preparados.
  - Composición/información sobre componentes.
  - Identificación de los peligros.
  - Primeros auxilios.
  - Medidas de lucha contra incendios.
  - Medidas en caso de vertido o liberación accidental
  - Manipulación y almacenamiento.
  - Controles de exposición y protección personal.
  - Consideraciones sobre la eliminación.
  - Información relativa al transporte.
  - Información reglamentaria.

UNIDAD FORMATIVA 2

Denominación: INSTALACIÓN Y CONFIGURACIÓN DE PERIFÉRICOS MICROINFORMÁTICOS.

Código: UF0862

Duración: 60 horas

cve: BOE-A-2011-10055

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

Capacidades y criterios de evaluación:

C1: Instalar periféricos, para su explotación, en el equipo microinformático, de acuerdo a unas especificaciones dadas.

CE1.1 Clasificar los tipos de dispositivos periféricos, identificando sus características técnicas y funcionales, parámetros de configuración y recomendaciones de uso, teniendo en cuenta sus especificaciones técnicas.

CE1.2 Identificar los requisitos para realizar los procedimientos de instalación en lo que respecta a condiciones de alimentación eléctrica, cableado, conexiones físicas y circunstancias ambientales, según se indica en la documentación técnica proporcionada por el fabricante.

CE1.3 Describir los procedimientos para realizar la instalación de los controladores de dispositivos (drivers) y utilidades software necesarias para explotar las funcionalidades del periférico, teniendo en cuenta especificaciones técnicas del propio dispositivo.

CE1.4 Clasificar las pruebas funcionales y operativas que se realizarán con el periférico para asegurar su funcionamiento, de acuerdo a especificaciones técnicas

CE1.5 En casos prácticos en los que se cuenta con varios periféricos para proceder a su instalación y conexión al sistema microinformático, teniendo en cuenta las especificaciones técnicas de cada dispositivo.

- Comprobar que se dispone de los elementos para su instalación, tanto en lo que a cableado, conectores y elementos físicos respecta, como a dispositivos de almacenamiento (disquetes, discos u otros soportes) con los controladores de dispositivos (drivers) y utilidades software se requerirán para la instalación.
- Verificar que en el sistema microinformático se dispone de recursos para realizar la conexión con el dispositivo, tanto en lo que respecta a puertos, conectores o bahías, como en disponibilidad de clavijas de alimentación y otros requisitos ambientales.
- Realizar la instalación del dispositivo aplicando los medios de seguridad y protección especificados por la normativa y utilizando herramientas específicas para cada caso.
- Configurar el controlador de dispositivo (driver) en el sistema operativo.
- Aplicar los procedimientos de prueba funcional y operativa al dispositivo instalado.
- Documentar los procesos realizados y sus resultados.

CE1.1 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 de periféricos.

Contenidos

1. **Descripción de dispositivos periféricos.**
   - Tipos de dispositivos periféricos.
     - Impresoras.
     - Escáner.
     - Lectores ópticos.
     - Altavoces, micrófonos y dispositivos multimedia.
     - Lectoras de cintas de backup.
     - Otros.
   - Características técnicas y funcionales.
   - Parámetros de configuración.
   - Recomendaciones de uso.
   - Especificaciones técnicas.

cve: BOE-A-2011-10055

2. Instalación y prueba de periféricos.

- Procedimientos para el montaje de periféricos.
- Identificación de los requisitos de instalación.
  - Documentación del fabricante.
  - Alimentación eléctrica.
  - Cableado.
  - Conexiones físicas.
  - Condiciones ambientales.
- Instalación y configuración de periféricos.
- Instalación y configuración de tarjetas.
- Instalación de controladores y utilidades software.
- Realización de pruebas funcionales y operativas.

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 - UF0861	90	30
Unidad formativa 2 - UF0862	60	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.

MÓDULO FORMATIVO 2

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.

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.

cve: BOE-A-2011-10055

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.
- 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.

cve: BOE-A-2011-10055

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.

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.

cve: BOE-A-2011-10055

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

cve: BOE-A-2011-10055

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.
   - 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.

cve: BOE-A-2011-10055

- 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.

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-2011-10055

MÓDULO FORMATIVO 3

Denominación: REPARACIÓN DE EQUIPAMIENTO MICROINFORMÁTICO.

Código: MF0954_2

Nivel de cualificación profesional: 2

Asociado a la Unidad de Competencia:

UC0954_2 Reparar y ampliar equipamiento microinformático.

Duración: 180 horas

UNIDAD FORMATIVA 1

Denominación: REPARACIÓN Y AMPLIACIÓN DE EQUIPOS Y COMPONENTES HARDWARE MICROINFORMÁTICOS.

Código: UF0863

Duración: 80 horas

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

Capacidades y criterios de evaluación

C1: Describir los componentes eléctricos, electrónicos y electromecánicos contenidos dentro de los dispositivos de equipos microinformáticos susceptibles de ajuste, calibración y de producción de averías para discriminar causas de producción de incidencias.

CE1.1 Identificar los componentes de electrónica analógica y digital y sus aplicaciones más características, para asociar las métricas y equipamiento de medida necesario, para estimar la funcionalidad de un dispositivo, de acuerdo a sus especificaciones técnicas.

CE1.2 Interpretar los esquemas funcionales de los circuitos y componentes, y la simbología utilizada, relacionándolos con los elementos reales para aplicar los procedimientos de diagnóstico y verificación a equipos con incidencias funcionales.

CE1.3 Identificar los elementos eléctricos, electrónicos, ópticos y electromecánicos contenidos dentro de los dispositivos de un equipo informático susceptibles de ajuste, calibración y/o reparación, para efectuar las acciones de reparación o sustitución, en función de las informaciones obtenidas por medio de procesos de diagnóstico y especificaciones recibidas.

C2: Establecer la causa de la avería de los equipos y componentes del sistema microinformático, identificando su naturaleza mediante el uso de técnicas y herramientas especificadas.

CE2.1 Describir las características de un puesto de reparación de equipos microinformáticos y de las herramientas e instrumentos para realizar las tareas de detección de averías con la calidad, eficiencia y seguridad requeridas.

CE2.2 Describir las señales de alimentación, control y datos de los conectores, buses e interfaces de los componentes de un equipo informático, indicando el procedimiento y los dispositivos para la evaluación y estimación de sus parámetros funcionales, de acuerdo a especificaciones técnicas del dispositivo a monitorizar.

cve: BOE-A-2011-10055

CE2.3 Describir el procedimiento de desensamblaje de componentes, equipos microinformáticos y periféricos para poder realizar las actuaciones en los mismos.
CE2.4 Explicar la tipología y características de las averías en equipos microinformáticos describiendo las técnicas generales y los medios específicos para su localización con el fin de optimizar los procedimientos de reparación de averías.
CE2.5 Describir las características de las herramientas hardware y software que se utilizan para el diagnóstico de averías en el sistema microinformático, teniendo en cuenta sus especificaciones técnicas.
CE2.6 En un caso práctico, debidamente caracterizado, realizar la localización de una avería para aislar la causa que la produce y caracterizarla, de acuerdo a unas instrucciones recibidas:
- Establecer una primera hipótesis en función de la documentación aportada.
- Detectar los puntos críticos del equipo y/o componente mediante la consulta de los históricos de averías y las estadísticas de mantenimiento elaboradas al respecto.
- Identificar los síntomas y la naturaleza de la avería, caracterizándola por los efectos que produce.
- Efectuar medidas en los puntos de testeo establecidos por los fabricantes o definidos por el procedimiento especificado.
- Localizar el bloque funcional o componente responsable de la misma.
- Identificar los elementos de seguridad que deben ser tenidos en cuenta.
- Utilizar herramientas software de diagnóstico si se producen fallos intermitentes en el sistema.
- Utilizar herramientas hardware de diagnóstico si el equipo no enciende.
- Conectar un emulador y realizar pruebas comparativas con varias placas base.
- Realizar la documentación de las actividades realizadas y los resultados obtenidos utilizando los formatos y plantillas indicadas.

CE2.7 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 diagnóstico y resolución de averías.

C3: Aplicar los procedimientos para realizar el ajuste, reparación y verificación de los elementos averiados, garantizando el funcionamiento del equipo o componente.

CE3.1 Describir las herramientas y equipos para la reparación de averías de un equipo microinformático en función de los tipos de dispositivos a reparar, de acuerdo a las especificaciones técnicas de los propios equipos.
CE3.2 Describir los componentes de los dispositivos de un sistema microinformático susceptibles de ajuste, reparación y sustitución para la resolución de averías, en función de los tipos de dispositivos a reparar.
CE3.3 En un supuesto práctico, debidamente caracterizado, realizar la reparación de una avería producida en un elemento del sistema microinformático, siguiendo unos procedimientos dados:
- Identificar el componente causante de la avería.
- Aplicar las medidas de seguridad especificadas.
- Evaluar la sustitución del componente averiado o la posibilidad de su reparación.
- Establecer un presupuesto para la sustitución o reparación, valorando los costes de reparación, tanto de piezas como de mano de obra, según modelos económicos dados.
- Activar los mecanismos para garantizar la integridad de la información.
- Sustituir o reparar el elemento (físico o lógico) responsable de la avería.

cve: BOE-A-2011-10055

- Realizar las comprobaciones y los ajustes especificados en el software y en la configuración.
- Realizar pruebas de arranque y parada para comprobar el funcionamiento del elemento reparado.
- Reportar la avería a un nivel superior si fuera necesario.
- Documentar las actividades realizadas y los resultados obtenidos utilizando los formatos y plantillas indicadas.

CE3.4 Realizar la confección de diverso cableado informático mediante presión, crimpado o soldadura, de adaptadores, derivadores, conectores y latiguillos para cubrir necesidades específicas de conexión difíciles de obtener comercialmente, haciendo uso de las herramientas adecuadas y comprobando que la conectividad obtenida se corresponde con los esquemas teóricos de los mismos.

C4: Aplicar los procedimientos de ampliación de equipos informáticos garantizando el funcionamiento del equipo o componente, de acuerdo a unas especificaciones recibidas.

CE4.1 Identificar las características de los componentes sin documentación o carentes del software asociado o actualizado con objeto de realizar las operaciones para la ampliación del equipo mediante la interpretación de la información del etiquetado del fabricante (códigos, simbología) y la búsqueda y obtención de información a través de Internet teniendo en cuenta las especificaciones técnicas de las que dispongamos.

CE4.2 En un supuesto práctico, debidamente caracterizado, realizar la evaluación de la viabilidad de una ampliación para añadir nuevas funcionalidades a un equipo informático, en función de especificaciones funcionales recibidas:

- Identificar las necesidades y requisitos previos.
- Detectar las posibles interacciones con otros componentes del equipo.
- Evaluar la dificultad de obtención de los componentes.
- Estimar el aumento del rendimiento global que se obtiene.
- Realizar los procedimientos necesarios para evitar pérdidas de información.
- Estimar y documentar el coste económico de la actualización.

CE4.1 En un supuesto práctico, debidamente caracterizado, ampliar un equipo informático para aumentar las capacidades funcionales del mismo en función de unas especificaciones dadas y siguiendo los procedimientos indicados:

- Realizar la copia de seguridad de los datos del disco duro con objeto de garantizar la integridad de la información.
- Identificar los componentes a actualizar.
- Aplicar las medidas de seguridad establecidas.
- Realizar la ampliación, sustitución o actualización de los componentes especificados.
- Instalar y configurar el software asociado a los componentes actualizados.
- Realizar las comprobaciones y los ajustes tanto hardware como software para verificar la ampliación.
- Realizar la documentación de las actividades realizadas indicando la configuración inicial del equipo y la configuración después de la ampliación.

Contenidos

1. **Instrumentación básica aplicada a la reparación de equipos microinformáticos.**
   - Conceptos de electricidad y electrónica aplicada a la reparación de equipos microinformáticos.

cve: BOE-A-2011-10055

- Magnitudes eléctricas y su medida.
- Señales analógicas y digitales.
- Componentes analógicos.
- Electrónica digital
  - Sistemas de representación numérica y alfabética.
  - El circuito impreso.
  - Circuitos lógicos y funciones lógicas.
  - Principio de funcionamientos de circuitos integrados digitales
- Instrumentación básica.
  - Polímetro.
    - Descripción.
    - Medida de resistencias, tensiones e intensidades.
  - Osciloscopio.
    - Funcionamiento.
    - Terminología.
    - Puesta en funcionamiento. Sondas.
    - Controles de un osciloscopio.
    - Técnicas de medida.
  - Generador de baja frecuencia.
    - Descripción.
    - Utilización del Generador.

2. Funcionamiento de los dispositivos de un sistema informático.

- Esquemas funcionales de los dispositivos y periféricos en equipos informáticos.
- Componentes eléctricos. Funciones.
- Componentes electrónicos. Funciones.
- Componentes electromecánicos. Funciones.
- Los soportes de almacenamiento magnético.
  - Características.
  - Componentes.
  - Esquemas funcionales.

3. Tipos de averías en equipos microinformáticos.

- Tipología de las averías.
  - Clasificación.
  - Características.
- Averías típicas.
  - Lógicas
  - Físicas.
  - Procedimientos para su detección y corrección.

4. Diagnóstico y localización de averías en equipos informáticos.

- Organigramas y procedimientos para la localización de averías.
- El diagnóstico.
  - Técnicas de diagnóstico.
  - Software de medida.
  - Diagnóstico y detección.
- Herramientas software de diagnóstico.
  - Tipos.
  - Características.
  - Software comercial.
- Herramientas hardware de diagnóstico.
  - Tipos.
  - Características.
  - Tarjetas de diagnósticos POST.

cve: BOE-A-2011-10055

- Conectividad de los equipos informáticos
  - Medidas de señales de las interfases, buses y conectores de los diversos componentes.
    - De alimentación.
    - De control.
    - De datos.
- El conexionado externo e interno de los equipos informáticos.
  - Tipos de cables.
  - Tipos de conectores.
  - Significado de las patillas de las diversas interfaces y conectores.
- Técnicas de realización de diverso cableado.

5. Reparación del hardware de la unidad central.

- El puesto de reparación.
  - Características.
  - Herramientas de laboratorio.
  - Equipos de laboratorio.
- El presupuesto de la reparación.
  - Coste de componentes.
  - Criterios de tarificación.
    - Tiempos
    - Tipo de reparación
    - Tipo de componente.
- El procedimiento de reparación.
- Reparación de averías del hardware.
  - la fuente de alimentación.
  - La placa base.
  - Relacionadas con la memoria.
  - Unidades de almacenamiento.
  - Tarjetas de sonido.
  - Tarjetas gráficas.
  - Reparación de periféricos básicos y otros componentes hardware.

6. Ampliación de un equipo informático.

- Componentes actualizables.
  - Lógicos
  - Físicos.
- El procedimiento de ampliación.
  - Evaluación de la necesidad.
  - Compatibilidad de componentes.
  - Presupuesto de la ampliación.
  - Aseguramiento de la información.
- Ampliaciones típicas de equipos informáticos lógicas y físicas.

UNIDAD FORMATIVA 2

Denominación: RESOLUCIÓN DE AVERÍAS LÓGICAS EN EQUIPOS MICROINFORMÁTICOS.

Código: UF0864

Duración: 30 horas

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

cve: BOE-A-2011-10055

Capacidades y criterios de evaluación

C1: Recuperar la funcionalidad del equipo informático identificando y aplicando los procedimientos de reparación de averías lógicas de acuerdo a las especificaciones recibidas.

CE1.1 Distinguir los procedimientos que se utilizan para la resolución de averías lógicas según especificaciones recibidas.

CE1.2 Identificar los procesos que se ejecutan en un equipo para detectar posibles consumos excesivos de memoria y de procesador.

CE1.3 Reconocer los síntomas producidos por el ataque de virus y programas maliciosos que pueden afectar a los equipos informáticos para proceder a su eliminación utilizando software antivirus y antiespía según unas especificaciones establecidas.

CE1.4 Utilizar herramientas de recuperación de datos para recuperar archivos eliminados siguiendo unas especificaciones recibidas.

CE1.5 En supuestos prácticos, debidamente caracterizados, reparar un equipo informático con averías lógicas simuladas siguiendo unas especificaciones técnicas y procedimientos dados:

- Comprobar el sistema de archivos utilizando las herramientas software especificadas.
- Comprobar los procesos en ejecución.
- Comprobar y eliminar la presencia de virus y software espía utilizando las herramientas software indicadas.
- Reinstalar y configurar el software afectado.
- Realizar pruebas de arranque y parada para comprobar el funcionamiento del sistema.
- Reportar la avería a un nivel de responsabilidad superior, si fuera necesario.
- Documentar las actividades realizadas y los resultados obtenidos utilizando los formatos y plantillas dadas.

Contenidos

1. El administrador de tareas y herramientas de recuperación de datos.

- El administrador de tareas.
  - El administrador de tareas.
  - Programas.
  - Procesos.
  - Medidas de rendimiento.
- Instalación y utilización de herramientas de recuperación de datos.
  - La recuperación de datos. Concepto y funcionamiento.
  - Herramientas comerciales de recuperación de datos.
  - Instalación de herramientas.
  - Procedimiento de búsqueda y recuperación de datos.

2. Resolución de averías lógicas.

- El Master Boot Record (MBR), particiones y partición activa.
- Archivos de inicio del sistema.
- Archivos de configuración del sistema.
- Optimización del sistema.
- Copia de seguridad.
  - Transferencia de archivos.
  - Herramientas de back-up.
  - Clonación.
- Restablecimiento por clonación.
- Reinstalación, configuración y actualización de componentes de componentes software.

cve: BOE-A-2011-10055

3. Instalación y configuración del software antivirus.

- Virus informáticos.
  - Software malicioso: Conceptos y definiciones.
    - Evolución.
    - Virus, gusanos, troyanos, otros.
    - Vulnerabilidades en programas y parches.
    - Tipos de ficheros que pueden infectarse.
    - Medios de propagación.
    - Virus en correos, en programas y en documentos.
    - Ocultación del software malicioso.
    - Páginas web.
    - Correo electrónico.
    - Memoria principal del ordenador.
    - Sector de arranque.
    - Ficheros con macros.
  - Efectos y síntomas de la infección.
  - Virus informáticos y sistemas operativos.
  - Actualizaciones criticas de sistemas operativos.
  - Precauciones para evitar infección.
- Definición de software antivirus.
- Componentes activos de los antivirus.
  - Vacuna.
  - Detector.
  - Eliminador.
- Características generales de los paquetes de software antivirus.
  - Protección anti-spyware.
  - Protección contra el software malicioso.
  - Protección firewall.
  - Protección contra vulnerabilidades.
  - Protección contra estafas.
  - Actualizaciones automáticas.
  - Copias de seguridad y optimización del rendimiento del ordenador.
- Instalación de software antivirus.
  - Requisitos del sistema.
  - Instalación, configuración y activación del software.
  - Creación de discos de rescate.
  - Desinstalación.
- La ventana principal.
  - Estado de las protecciones. Activación y desactivación.
  - Tipos de análisis e informes.
  - Actualización automática y manual.
    - Actualización de patrones de virus y/ o ficheros identificadores de malware.
  - Configuración de las protecciones. Activación y desactivación.
  - Análisis, eliminación de virus y recuperación de los datos.
  - Actualizaciones.
  - Acceso a servicios.
    - Soporte.
    - Obtención de información.
  - Otras opciones.

UNIDAD FORMATIVA 3

Denominación: REPARACIÓN DE IMPRESORAS.

Código: UF0865

cve: BOE-A-2011-10055

Duración: 70 horas.

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

Capacidades y criterios de evaluación

C1: Aplicar los procedimientos de reparación de impresoras utilizando herramientas específicas, para ponerlas en funcionamiento, siguiendo unas especificaciones dadas.

CE1.1 Identificar los tipos de impresoras más utilizadas en el mercado distinguiendo las características entre ellas, según especificaciones técnicas.

CE1.2 Describir los bloques funcionales de cada tipo de impresora, así como el funcionamiento de sus componentes, según especificaciones técnicas de las mismas.

CE1.3 Reconocer los fallos de funcionamiento de cada tipo de impresora para reemplazar las partes causantes del fallo, teniendo en cuenta las características de la misma y siguiendo el procedimiento establecido.

CE1.4 Identificar los consumibles, sus tipos y procedimientos de sustitución para detectar y solucionar posibles averías en impresoras, teniendo en cuenta las características técnicas de las mismas.

CE1.5 Distinguir los procedimientos que se utilizan para la resolución de averías en impresoras, en función de sus especificaciones técnicas.

CE1.6 En supuestos prácticos, debidamente caracterizados, realizar la reparación de una impresora para su puesta en funcionamiento, siguiendo unas especificaciones técnicas y procedimientos dados:

- Realizar las pruebas establecidas para identificar la causa del fallo de la impresora.
- Identificar los componentes causantes del fallo.
- Realizar la reparación o sustitución del componente, o reportar la avería a un nivel de responsabilidad superior, si fuera necesario.
- Realizar pruebas de funcionamiento para verificar su funcionalidad.
- Documentar las actividades realizadas y los resultados obtenidos utilizando los formatos y plantillas establecidas.

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 la reparación de periféricos.

Contenidos

1. **Las impresoras.**
   - Las impresoras.
     - Parámetros básicos.
     - Los lenguajes de descripción de página.
     - La interfaz de conexión.
   - Tipos de impresoras. Características y diferencias.
     - Impresoras de impacto.
     - Impresoras de tinta.
     - Impresoras láser.
   - Marcas y modelos más usuales.
2. **Manipulación y sustitución de elementos consumibles.**
   - Tipos y características.
     - Cartuchos de tinta.
     - Cartuchos de tóner.
     - Formularios de papel
     - Pliegos de etiquetas adhesivas.
     - Sobres.

cve: BOE-A-2011-10055

- Otros.
- Conservación de elementos consumibles.
- Procedimientos de sustitución de elementos consumibles.
- Seguridad en procedimientos de manipulación y sustitución de elementos consumibles.

3. Reparación de impresoras matriciales.

- Impresoras matriciales. Funcionamiento y detalles técnicos.
- 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.
- Piezas de una impresora matricial.
- Especificaciones mecánicas, electrónicas, eléctricas y ambientales.
- Bloques funcionales y funcionamiento de sus componentes.
- Consumibles.
  - Tipos de consumibles.
    - Hojas sueltas.
    - Papel continuo.
    - Papel especial: etiquetas, impresos con copia, sobres.
  - Sustitución de consumibles.
    - Sustitución de cartuchos de cinta.
    - Sustitución de papel continuo.
- Mantenimiento preventivo y correctivo.
  - Limpieza de la impresora.
  - Lubricación.
  - Detección de problemas.
    - Indicadores de error.
    - Monitor de estados.
    - Auto test.
    - Volcado hexadecimal.
  - Resolución de problemas.
    - Problemas de alimentación.
    - Problemas de carga o de avance de papel.
    - Problemas en la posición de impresión.
    - Problemas de impresión o de la calidad de impresión.
    - Problemas de red.
    - Solución de atascos de papel.
    - Problemas con los accesorios opcionales.
    - Sustitución de kits de mantenimiento.
- Transporte de la impresora.

4. Reparación de 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.
- Especificaciones mecánicas, electrónicas, eléctricas y ambientales.
- Bloques funcionales y funcionamiento de sus componentes.
- Limpieza de la impresora.
- Lubricación.
- Consumibles.
  - Sustitución de consumibles.

cve: BOE-A-2011-10055

- 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.

- Mantenimiento preventivo y correctivo.
  - Revisión de los inyectores.
  - Limpieza del cabezal de inyección.
  - Alineación del cabezal de inyección.
  - Limpieza de la impresora.
  - Resolución de problemas.
    - Diagnóstico del problema.
    - Comprobación del estado de la impresora.
    - Atascos de papel.
    - Problemas con la calidad de impresión.
    - Problemas diversos de impresión.
    - El papel no avanza.
    - La impresora no imprime.
    - Otros problemas.
- Transporte de la impresora.

5. Reparación de 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.
- Piezas de una impresora láser.
- Especificaciones mecánicas, electrónicas, eléctricas y ambientales.
- Bloques funcionales y funcionamiento de sus componentes.
- Consumibles.
  - Sustitución de consumibles.
- Mantenimiento preventivo y correctivo.
  - Limpieza de elementos de la impresora.
  - Lubricación.
  - Sustitución de cartuchos de tóner.
  - Sustitución de la unidad fotoconductora.
  - Sustitución de la unidad fusora.
  - Sustitución del colector de tóner usado.
  - Resolución de problemas.
    - Diagnóstico del problema.
    - Comprobación del estado de la impresora.
    - Atascos de papel.
    - Impresión de una hoja de estado de la impresora.
    - Problemas de funcionamiento.
    - Problemas con la copia impresa.
    - Problemas de impresión a color.
    - Problemas con la calidad de impresión.
    - Problemas diversos de impresión.
    - Problemas de memoria.
    - Otros problemas.
- Transporte de la impresora.

Orientaciones metodológicas

Formación a distancia:

cve: BOE-A-2011-10055

Unidades formativas	Duración total en horas de las unidades formativas	N.º de horas máximas susceptibles de formación a distancia
Unidad formativa 1 - UF0863	80	20
Unidad formativa 2 - UF0864	30	10
Unidad formativa 3 - UF0865	70	10

Secuencia:

Las unidades formativas deberán superarse de forma correlativa.

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 MONTAJE Y REPARACIÓN DE SISTEMAS MICROINFORMÁTICOS.

Código: MP0179

Duración: 40 horas

Capacidades y criterios de evaluación

C1: Realizar, en un puesto de trabajo de una empresa, el montaje, instalación y verificación de los elementos que componen un sistema microinformático, siguiendo las instrucciones recibidas.

CE1.1 Obtener e interpretar la información necesaria para el montaje, instalación o verificación en las guías y/o catálogos de fabricantes y distribuidores.

CE1.2 Realizar el ensamblaje de equipos microinformáticos para su utilización utilizando las herramientas y útiles necesarios del puesto de trabajo.

CE1.3 Realizar la configuración del equipo, así como la carga del software de base.

CE1.4 Realizar la instalación de periféricos, configurándolo de manera adecuada.

CE1.5 Verificar el montaje e instalación realizando las pruebas oportunas, de acuerdo con las guías e información de los equipos, fabricantes y de la propia empresa.

C2: Instalar y configurar el software de base de acuerdo con los protocolos y procedimientos establecidos en la empresa.

CE2.1 Identificar las fases que intervienen en la instalación de sistema operativo comprobando los requisitos del equipo informático.

CE2.2 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.

CE2.3 Verificar el funcionamiento del equipo una vez realizada la instalación.

CE2.4 Utilizar las aplicaciones que proporcionan los sistemas operativos para la explotación del mismo.

CE2.5 Documentar el trabajo realizado de acuerdo con los procedimientos de la empresa.

C3: Realizar la reparación y ampliación de los equipos y componentes del sistema microinformático, utilizando los procedimientos, técnicas y herramientas especificadas, de acuerdo con las instrucciones recibidas.

cve: BOE-A-2011-10055

CE3.1 Establecer la causa de la avería de equipos y componentes mediante el uso de técnicas y herramientas hardware y software adecuadas, de acuerdo con los procedimientos de reparación establecidos.
CE3.2 Realizar el ajuste, reparación y verificación de los elementos averiados, garantizando el funcionamiento del equipo o componente, estableciendo un presupuesto de acuerdo con los modelos de la empresa.
CE3.3 Recuperar la funcionalidad del equipo informático eliminando la presencia de virus y software espía, reinstalando y configurando el software afectado.
CE3.4 Realizar la ampliación de equipos informáticos de acuerdo con las especificaciones proporcionadas.
CE3.5 Realizar la reparación de impresoras para su puesta en funcionamiento, de acuerdo con las especificaciones técnicas proporcionadas.

C4: Participar en los procesos de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.
CE4.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.
CE4.2 Respetar los procedimientos y normas del centro de trabajo.
CE4.3 Emprender con diligencia las tareas según las instrucciones recibidas tratando de que se adecuen al ritmo de trabajo de la empresa.
CE4.4 Integrarse en los procesos de producción del centro de trabajo.
CE4.5 Utilizar los canales de comunicación establecidos.
CE4.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. **Montar, reparar y ampliar, equipos y componentes que forman un sistema microinformático, siguiendo los procedimientos de la empresa.**
   - Montaje de equipos y sistemas microinformáticos en un puesto de montaje empresarial.
   - Instalación y configuración del software de base utilizado en la empresa.
   - Procedimientos de reparación de equipos y componentes microinformáticos aplicados en la empresa.
   - Procedimientos de etiquetado, embalaje, almacenamiento y traslado de equipos, periféricos y consumibles.

2. **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-2011-10055

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	*Experiencia profesional requerida en el ámbito de la Unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0953_2: Montaje de equipos microinformáticos.	• 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 de la familia profesional de Informática y comunicaciones. • Certificados de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones.	1 año	3 años
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 de la familia profesional de Informática y comunicaciones. • Certificados de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones.	1 año	3 años
MF0954_2: Reparación de equipamiento microinformático.	• 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 de la familia profesional de Informática y comunicaciones. • Certificados de profesionalidad de nivel 3 de la familia profesional de Informática y comunicaciones.	1 año	3 años

* En los últimos tres años.

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m² 15 alumnos	Superficie m² 25 alumnos
Aula de Informática	60	75
Aula Taller de Equipos Microinformáticos	90	90

Espacio Formativo	M1	M2	M3
Aula de Informática	X	X	X
Aula Taller de Equipos Microinformáticos	X		X

cve: BOE-A-2011-10055

Espacio Formativo	Equipamiento
Aula de Informática	- PCs instalados en red y conexión a Internet. - Software de base. - Software ofimático y herramientas internet. - Cañón de proyección. - Rotafolios. - Pizarra. - Material de aula. - Mesa y silla para el formador. - Mesa y silla para alumnos. - Mobiliario auxiliar para el equipamiento de aula.
Aula Taller de Equipos Microinformáticos	- Mobiliario específico de taller (Mesas de trabajo, estanterías y armarios, entre otros). - Cañón de proyección. - Armario de cableado con paneles de parcheado, y dispositivos de conexión a red. - Equipos informáticos y periféricos. - Componentes para el montaje de ordenadores. - Elementos y componentes para el mantenimiento preventivo y correctivo. - Sistemas operativos. - Herramientas y aplicaciones ofimáticas. - Herramientas de internet. - Software de clonación de equipos. - Programas y aplicaciones informáticas. - Herramientas hardware y software de testeo. - Herramientas de limpieza de soportes y periféricos. - Herramientas de etiquetado de productos. - Herramientas y utillaje de uso común para el montaje, mantenimiento y reparación de equipos y periféricos. - Instrumentación básica para la reparación de equipos microinformáticos. - Elementos de protección y seguridad. - Contenedores de reciclado de componentes: Pilas y baterías, papel, plásticos, metal.

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-2011-10055

ANEXO III

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Seguridad informática

Código: IFCT0109

Familia Profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC153_3 Seguridad informática (RD 1087/05 de 16 de septiembre)

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

UC0486_3: Asegurar equipos informáticos.
UC0487_3: Auditar redes de comunicación y sistemas informáticos.
UC0488_3: Detectar y responder ante incidentes de seguridad.
UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

Entorno Profesional:

Ámbito Profesional:

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

Sectores Productivos:

Está presente en múltiples sectores productivos, sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. También está presente en los siguientes tipos de empresas:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (outsourcing) de servicios.

cve: BOE-A-2011-10055

Ocupaciones o puestos de trabajo relacionados:

3820.1017 Programador de Aplicaciones Informáticas
3812.1014 Técnico en Informática de Gestión
Técnico en seguridad informática.
Técnico en auditoría informática.

Duración de la formación asociada: 500 horas

Relación de módulos formativos y de unidades formativas:

MF0486_3: Seguridad en equipos informáticos. (90 horas)
MF0487_3: Auditoría de seguridad informática. (90 horas)
MF0488_3: Gestión de incidentes de seguridad informática. (90 horas)
MF0489_3: Sistemas seguros de acceso y transmisión de datos. (60 horas)
MF0490_3: (Transversal) Gestión de servicios en el sistema informático. (90 horas)
MP0175: Modulo de prácticas profesionales no laborales de Seguridad informática. (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: ASEGURAR EQUIPOS INFORMÁTICOS

Nivel: 3

Código: UC0486_3

Realizaciones profesionales y criterios de realización

RP1: Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.

CR1.1 El plan de implantación del sistema informático de la organización se analiza comprobando que incorpora la información necesaria referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones entre otros, así como referencias de posibilidades de utilización de los equipos y restricciones de los mismos y protecciones contra agresiones de virus y otros elementos no deseados.

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

CR1.3 EL acceso a los servidores se realiza garantizando la confidencialidad e integridad de la conexión según las normas de seguridad de la organización.

CR1.4 Las políticas de usuario se analizan verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.

CR1.5 La política de seguridad es transmitida a los usuarios, asegurándose de su correcta y completa comprensión.

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

CR1.7 Las informaciones afectadas por la legislación de protección de datos se tratan verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.

cve: BOE-A-2011-10055

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

CR2.1 La ubicación del servidor en la red se realiza en una zona protegida y aislada según la normativa de seguridad y el plan de implantación de la organización.

CR2.2 Los servicios que ofrece el servidor se activan y configuran desactivando los innecesarios según la normativa de seguridad y plan de implantación de la organización.

CR2.3 Los accesos y permisos a los recursos del servidor por parte de los usuarios son configurados en función del propósito del propio servidor y de la normativa de seguridad de la organización.

CR2.4 Los mecanismos de registro de actividad e incidencias del sistema se activan y se habilitan los procedimientos de análisis de dichas informaciones.

CR2.5 Los módulos adicionales del servidor son analizados en base a sus funcionalidades y riesgos de seguridad que implican su utilización, llegando a una solución de compromiso.

CR2.6 Los mecanismos de autenticación se configuran para que ofrezcan niveles de seguridad e integridad en la conexión de usuarios de acuerdo con la normativa de seguridad de la organización.

CR2.7 Los roles y privilegios de los usuarios se definen y asignan siguiendo las instrucciones que figuren en la normativa de seguridad y el plan de explotación de la organización.

RP3: Instalar y configurar cortafuegos en equipos y servidores para garantizar la seguridad ante los ataques externos según las necesidades de uso y dentro de las directivas de la organización.

CR3.1 La topología del cortafuegos es seleccionada en función del entorno de implantación.

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

CR3.3 Los cortafuegos son instalados y configurados según el nivel definido en la política de seguridad.

CR3.4 Las reglas de filtrado y los niveles de registro y alarmas se determinan, configuran y administran según las necesidades dictaminadas por la normativa de seguridad de la organización.

CR3.5 Los cortafuegos son verificados con juegos de pruebas y se comprueba que superan las especificaciones de la normativa de seguridad de la organización.

CR3.6 La instalación y actualización del cortafuegos y los procedimientos de actuación con el mismo quedan documentados según las especificaciones de la organización.

CR3.7 Los sistemas de registro son definidos y configurados para la revisión y estudio de los posibles ataques, intrusiones y vulnerabilidades.

Contexto profesional

Medios de producción

Aplicaciones ofimáticas corporativas. Verificadores de fortaleza de contraseñas. Analizadores de puertos. Analizadores de ficheros de registro del sistema. Cortafuegos. Equipos específicos y/o de propósito general. Cortafuegos personales o de servidor. Sistemas de autenticación: débiles: basados en usuario y contraseña y robustos: basados en dispositivos físicos y medidas biométricas. Programas de comunicación con capacidades criptográficas. Herramientas de administración remota segura.

cve: BOE-A-2011-10055

Productos y resultados
Planes de implantación revisados según directivas de la organización. Informes de auditoría de servicios de red de sistemas informáticos. Mapa y diseño de la topología de cortafuegos corporativo. Guía de instalación y configuración de cortafuegos. Informe de actividad detectada en el cortafuegos. Mapa y diseño del sistema de copias de respaldo. Planificación de la realización de las copias de respaldo. Informe de realización de copias de respaldo. Normativa para la elaboración del diseño de cortafuegos. Elaboración de una operativa de seguridad acorde con la política de seguridad.

Información utilizada o generada
Política de seguridad de infraestructuras telemáticas. Manuales de instalación, referencia y uso de cortafuegos. Información sobre redes locales y de área extensa y sistemas de comunicación públicos y privados. Información sobre equipos y software de comunicaciones.
Normativa, reglamentación y estándares (ISO, EIA, UIT-T, RFC-IETF). Registro inventariado del hardware. Registro de comprobación con las medidas de seguridad aplicadas a cada sistema informático. Topología del sistema informático a proteger.

Unidad de competencia 2

Denominación: AUDITAR REDES DE COMUNICACIÓN Y SISTEMAS INFORMÁTICOS

Nivel: 3

Código: UC0487_3

Realizaciones profesionales y criterios de realización

RP1: Realizar análisis de vulnerabilidades, mediante programas específicos para controlar posibles fallos en la seguridad de los sistemas según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Las herramientas y los tipos de pruebas de análisis de vulnerabilidades se seleccionan y adecuan al entorno a verificar según las especificaciones de seguridad de la organización.

CR1.2 Los programas y las pruebas se actualizan para realizar ensayos consistentes con los posibles fallos de seguridad de las versiones de hardware y software instaladas en el sistema informático.

CR1.3 Los resultados de las pruebas se analizan y documentan conforme se indica en la normativa de la organización.

CR1.4 Los sistemas de acceso por contraseña se comprueban mediante herramientas específicas según las especificaciones de la normativa de seguridad.

CR1.5 La documentación del análisis de vulnerabilidades contiene referencias exactas de las aplicaciones y servicios que se han detectado funcionando en el sistema, el nivel de los parches instalados, vulnerabilidades de negación de servicio, vulnerabilidades detectadas y mapa de la red.

RP2: Verificar el cumplimiento de la normativa y requisitos legales vigentes en materia de protección de datos personales para asegurar la confidencialidad según las necesidades de uso y dentro de las directivas de la organización.

CR2.1 Los ficheros con datos de carácter personal son identificados y tienen asignado un responsable de seguridad según normativa legal.

CR2.2 El listado de personas autorizadas a acceder a cada fichero existe y se encuentra actualizado según normativa legal.

cve: BOE-A-2011-10055

CR2.3 El control de accesos a los ficheros se comprueba siguiendo el procedimiento establecido en la normativa de seguridad de la organización.
CR2.4 La gestión del almacenamiento de los ficheros y sus copias de seguridad se realiza siguiendo la normativa legal y de la organización.
CR2.5 El acceso telemático a los ficheros se realiza utilizando mecanismos que garanticen la confidencialidad e integridad cuando así lo requiera la normativa.
CR2.6 El informe de la auditoría recoge la relación de ficheros con datos de carácter personal y las medidas de seguridad aplicadas y aquellas pendientes de aplicación.

RP3: Comprobar el cumplimiento de la política de seguridad establecida para afirmar la integridad del sistema según las necesidades de uso y dentro de las directivas de la organización.
CR3.1 Los procedimientos de detección y gestión de incidentes de seguridad se desarrollan y se incluyen en la normativa de seguridad de la organización.
CR3.2 Los puntos de acceso de entrada y salida de la red son verificados para que su uso se circunscriba a lo descrito en la normativa de seguridad de la organización.
CR3.3 Los programas de seguridad y protección de sistemas se activan y actualizan según las especificaciones de los fabricantes.
CR3.4 Los puntos de entrada y salida de la red adicionales son autorizados y controlados en base a las especificaciones de seguridad y al plan de implantación de la organización.
CR3.5 Los procesos de auditoría informática son revisados, tanto los de carácter interno, como aquellos realizados por personal externo a la organización.
CR3.6 Los procedimientos de las políticas de seguridad se verifican en su cumplimiento por parte de los usuarios.

Contexto profesional

Medios de producción
Aplicaciones ofimáticas corporativas
Analizadores de vulnerabilidades.
Herramientas para garantizar la confidencialidad de la información.
Programas que garantizan la confidencialidad e integridad de las comunicaciones.
Aplicaciones para gestión de proyectos.
Programas de análisis de contraseñas.

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

Información utilizada o generada
Normativa sobre protección de datos personales.
Política de seguridad de la empresa.
Metodologías de análisis de seguridad (OSSTM, BS7799/ISO17799).
Boletines de seguridad y avisos de vulnerabilidades disponibles en formato electrónico.
Topología del sistema informático a proteger.

Unidad de competencia 3

Denominación: DETECTAR Y RESPONDER ANTE INCIDENTES DE SEGURIDAD

cve: BOE-A-2011-10055

Nivel: 3

Código: UC0488_3

Realizaciones profesionales y criterios de realización

RP1: Implantar procedimientos para la respuesta ante incidentes e implantar mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.

CR1.1 Los procedimientos de detección y respuesta de incidentes están documentados, indican los roles y responsabilidades de seguridad e implementan los requerimientos de la política de seguridad de la organización.

CR1.2 Los sistemas se modelan para detectar signos de comportamiento sospechoso seleccionando los mecanismos de registro a activar, observando las alarmas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones.

CR1.3 Los mecanismos de registro del sistema se activan y se planifican los procedimientos de análisis de los mismos según las especificaciones de seguridad de la organización.

CR1.4 Los sistemas de detección de intrusos se instalan, actualizan y configuran en función de las especificaciones de seguridad de la organización.

CR1.5 Los procedimientos de restauración del sistema informático se verifican para la recuperación del mismo ante un incidente grave dentro de las necesidades de la organización.

RP2: Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.

CR2.1 Las herramientas utilizadas para detectar intrusiones son analizadas para determinar que no han sido comprometidas ni afectadas por programas maliciosos.

CR2.2 Los parámetros de funcionamiento sospechoso se analizan con herramientas específicas según la normativa de seguridad.

CR2.3 Los componentes software del sistema se verifican periódicamente en lo que respecta a su integridad usando programas específicos.

CR2.4 Las pruebas realizadas a los dispositivos de protección física del sistema informático verifican el correcto funcionamiento de los mismos según la normativa de seguridad de la organización.

CR2.5 Los sucesos y signos extraños que pudieran considerarse una alerta son recogidos en el informe diario de actividad.

RP3: Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la organización.

CR3.1 La detección de un incidente de seguridad produce la realización de los procedimientos recogidos en los protocolos de la normativa de seguridad de la organización.

CR3.2 El sistema vulnerado, se aísla y se procede a recoger la información para el análisis forense de la misma según los procedimientos de la normativa de seguridad de la organización.

CR3.3 El sistema atacado se analiza mediante herramientas de detección de intrusos según los procedimientos de seguridad de la organización.

CR3.4 La intrusión es contenida mediante la aplicación de las medidas establecidas en la normativa de seguridad de la organización.

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

cve: BOE-A-2011-10055

CR3.6 Los daños causados se determinan y se planifican las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado según las normas de calidad y el plan de explotación de la organización.

Contexto profesional

Medios de producción
Aplicaciones ofimáticas corporativas. Analizadores de vulnerabilidades. Herramientas para garantizar la confidencialidad de la información. Programas que garantizan la confidencialidad e integridad de las comunicaciones. Aplicaciones para gestión de proyectos. Programas de análisis de contraseñas. Software de monitorización de redes. Software de flujo de trabajo para envío de alarmas e incidencias a responsables. IDS y sus consolas. Consola de SNMP.

Productos y resultados
Informes de análisis de vulnerabilidades. Relación de contraseñas débiles. Registro de ficheros de datos de carácter personal, según normativa vigente. Informe de auditoría de servicios y puntos de acceso al sistema informático. Registro de actividad. Documento de seguridad. Registro de alarmas.

Información utilizada o generada
Normativa sobre protección de datos personales. Política de seguridad de la empresa. Metodologías de análisis de seguridad (OSSTM, BS7799/ISO17799). Boletines de seguridad y avisos de vulnerabilidades, en su mayoría redactados en inglés, y disponibles en formato electrónico. Documento de trabajo en base a la política de seguridad. Normativa de detección de intrusos. Normativa de prevención de amenazas de seguridad.

Unidad de competencia 4

Denominación: DISEÑAR E IMPLEMENTAR SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Nivel: 3

Código: UC0489_3

Realizaciones profesionales y criterios de realización

RP1: Implantar políticas de seguridad y cifrado de información en operaciones de intercambio de datos para obtener conexiones seguras según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Las comunicaciones con otras compañías o a través de canales inseguros utilizan redes privadas virtuales para garantizar la confidencialidad e integridad de dichas conexiones durante el tránsito a través de redes públicas según las especificaciones de la normativa de seguridad y el diseño de redes de la organización.

CR1.2 Los requerimientos para implantar la solución de red privada virtual se seleccionan y comunican al operador de telefonía para lograr soluciones adecuadas al plan de seguridad.

CR1.3 Las técnicas de protección de conexiones inalámbricas disponibles en el mercado son evaluadas y se seleccionan aquellas más idóneas, teniendo en cuenta el principio de proporcionalidad y las normas de seguridad de la organización.

cve: BOE-A-2011-10055

CR1.4 Los servicios accesibles a través de la red telemática que emplean técnicas criptográficas para garantizar la integridad y confidencialidad de las comunicaciones son implantados según parámetros de la normativa de seguridad de la organización.
CR1.5 Los servicios accesibles a través de la red telemática que no incorporan técnicas criptográficas para garantizar la seguridad de las comunicaciones utilizan servicios de encapsulación.
CR1.6 Los servicios que incorporan soporte para certificados digitales para identificación del servidor, se emplean para garantizar al usuario la identidad del servidor.

RP2: Implantar sistemas de firma digital para asegurar la autenticidad, integridad y confidencialidad de los datos que intervienen en una transferencia de información utilizando sistemas y protocolos criptográficos según las necesidades de uso y dentro de las directivas de la organización.
CR2.1 El acceso a servicios a través de la red telemática utiliza autenticación basada en certificados digitales de identidad personal.
CR2.2 El proceso de obtención y verificación de firmas se aplica en caso de ser necesario según los requerimientos del sistema informático y los procesos de negocio
CR2.3 La transmisión de mensajes de correo electrónico utilizan certificados digitales para firmar y cifrar su contenido.
CR2.4 Los sistemas de firma digital de documentos mediante certificados digitales se implantan según la normativa de seguridad de la organización.
CR2.5 Los sistemas de sellado digital de tiempo, para garantizar la existencia de un documento en una determinada fecha, se implantan según las normas de seguridad de la organización.
CR2.6 Los componentes web son firmados digitalmente para garantizar la integridad de dichos componentes.

RP3: Implementar infraestructuras de clave pública para garantizar la seguridad según los estándares del sistema y dentro de las directivas de la organización.
CR3.1 La jerarquía de certificación se diseña en función de las necesidades de la organización y del uso que se vaya a dar a los certificados.
CR3.2 La declaración de prácticas de certificación y la política de certificación se redacta de forma que definen los procedimientos y derechos y obligaciones de los responsables de la autoridad de certificación y de los usuarios.
CR3.3 El sistema de autoridad de certificación se instala siguiendo las indicaciones del fabricante.
CR3.4 El certificado de la autoridad de certificación y la política de certificación se disponen a los usuarios en la forma y modo necesario, siguiendo las directrices contenidas en la declaración de prácticas de certificación.
CR3.5 La clave privada de la autoridad de certificación se mantiene segura y con las copias de respaldo establecidas en la declaración de prácticas de certificación.
CR3.6 La emisión de certificados digitales se realiza según los usos que va a recibir el certificado y siguiendo los procedimientos indicados en la declaración de prácticas de certificación.
CR3.7 El servicio de revocación de certificados mantiene accesible la información sobre validez de los certificados emitidos por la autoridad de certificación según lo indicado en la declaración de prácticas de certificación.

cve: BOE-A-2011-10055

Contexto profesional

Medios de producción
Programas para conexión segura. Sistemas para implantar autoridades de certificación digital. Servidores y clientes de redes privadas virtuales (VPN). Soportes seguros para certificados digitales. Servidores web con soporte SSL/TLS. Encapsuladores de tráfico con soporte criptográfico (HW y SW). Programas de conexión segura a servicios telemáticos. Interfaces de correo electrónico con soporte para correo seguro.

Productos y resultados
Política de certificación. Declaración de prácticas de certificación. Listado de certificados emitidos y certificados revocados. Guías y recomendaciones de implantación de sistemas de comunicación seguros. Guías de utilización de certificados digitales.

Información utilizada o generada
Normativa legal sobre firma digital. Estándares y recomendaciones, generalmente redactadas en inglés. Manuales de instalación de infraestructuras de clave pública (PKI).

Unidad de competencia 5

Denominación: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Los procesos que intervienen en el sistema son identificados para evaluar parámetros de rendimiento.

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

CR1.3 Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización.

CR1.4 Las herramientas de monitorización se implantan y configuran determinando los niveles de las alarmas en función del plan de explotación de la organización.

RP2: Administrar los dispositivos de almacenamiento según las necesidades de uso y dentro de las directivas de la organización.

CR2.1 Los dispositivos de almacenamiento se configuran para ser usados en los distintos sistemas operativos utilizados en el sistema informático.

CR2.2 La estructura de almacenamiento se define y se implanta atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de uso de la organización.

CR2.3 Los requerimientos de nomenclatura de objetos y restricciones de uso de cada dispositivo de almacenamiento se documentan adecuadamente.

CR2.4 Los dispositivos de almacenamiento se integran para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

cve: BOE-A-2011-10055

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.

CR3.1 El acceso de los usuarios al sistema informático se configura para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.

CR3.2 El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.

CR3.3 Los recursos disponibles para los usuarios se limitan con las herramientas adecuadas en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.

CR4.1 Los dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.

CR4.2 Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.

CR4.3 Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización.

Contexto profesional

Medios de producción

Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

Productos y resultados

Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada

Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: SEGURIDAD EN EQUIPOS INFORMÁTICOS

Código: MF0486_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

cve: BOE-A-2011-10055

UC0486_3: Asegurar equipos informáticos

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los planes de implantación de la organización para identificar los elementos del sistema implicados y los niveles de seguridad a implementar.

CE1.1 Identificar la estructura de un plan de implantación, explicando los contenidos que figuran en cada sección.

CE1.2 Distinguir los sistemas que pueden aparecer en el plan de implantación, describiendo las funcionalidades de seguridad que implementan.

CE1.3 Describir los niveles de seguridad que figuran en el plan de implantación, asociándolos a los permisos de acceso para su implantación.

CE1.4 En un supuesto práctico en el que se pide analizar el plan de implantación y sus repercusiones en el sistema:

- Determinar los sistemas implicados en el plan de implantación.
- Analizar los requisitos de seguridad de cada sistema.
- Describir las medidas de seguridad a aplicar a cada sistema.
- Cumplimentar los formularios para la declaración de ficheros de datos de carácter personal.

C2: Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores según especificaciones de seguridad.

CE2.1 Describir las características de los mecanismos de control de acceso físico, explicando sus principales funciones.

CE2.2 Exponer los mecanismos de traza, asociándolos al sistema operativo del servidor.

CE2.3 Identificar los mecanismos de control de acceso lógico, explicando sus principales características (contraseñas, filtrado de puertos IP entre otros).

CE2.4 En un supuesto práctico de implantación de un servidor según especificaciones dadas:

- Determinar la ubicación física del servidor para asegurar su funcionalidad.
- Describir y justificar las medidas de seguridad física a implementar que garanticen la integridad del sistema.
- Identificar los módulos o aplicaciones adicionales para implementar el nivel de seguridad requerido por el servidor.
- Determinar las amenazas a las que se expone el servidor, evaluando el riesgo que suponen, dado el contexto del servidor.
- Determinar los permisos asignados a los usuarios y grupos de usuarios para la utilización del sistema.

C3: Evaluar la función y necesidad de cada servicio en ejecución en el servidor según las especificaciones de seguridad.

CE3.1 Identificar los servicios habituales en el sistema informático de una organización, describiendo su misión dentro de la infraestructura informática y de comunicaciones.

CE3.2 Identificar y describir los servicios necesarios para el funcionamiento de un servidor, en función de su misión dentro del sistema informático de la organización.

CE3.3 Describir las amenazas de los servicios en ejecución, aplicando los permisos más restrictivos, que garantizan su ejecución y minimizan el riesgo.

CE3.4 En un supuesto práctico de implantación de un servidor con un conjunto de servicios en ejecución con correspondencias a un plan de explotación dado:

- Indicar las relaciones existentes entre dicho servidor y el resto del sistema informático de la organización.

cve: BOE-A-2011-10055

- Extraer del plan de implantación los requisitos de seguridad aplicables al servidor.
- Determinar los servicios mínimos necesarios para el funcionamiento del sistema.

C4: Instalar, configurar y administrar un cortafuegos de servidor con las características necesarias según especificaciones de seguridad.

CE4.1 Clasificar los tipos de cortafuegos, de red y locales, hardware y software, de paquetes y aplicación, describiendo sus características y funcionalidades principales.

CE4.2 Describir las reglas de filtrado de un cortafuegos de servidor, explicando los parámetros principales.

CE4.3 Explicar el formato de traza de un cortafuegos de servidor, reflejando la información de seguridad relevante.

CE4.4 A partir de un supuesto práctico de instalación de un cortafuegos de servidor en un escenario de accesos locales y remotos:

- Determinar los requisitos de seguridad del servidor.
- Establecer las relaciones del servidor con el resto de equipos del sistema informático.
- Elaborar el listado de reglas de acceso a implementar en el servidor.
- Componer un plan de pruebas del cortafuegos implementado.
- Ejecutar el plan de pruebas, redactando las correcciones necesarias para corregir las deficiencias detectadas.

Contenidos

1. **Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos**
   - Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
   - Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
   - Salvaguardas y tecnologías de seguridad más habituales
   - La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

2. **Análisis de impacto de negocio**
   - Identificación de procesos de negocio soportados por sistemas de información
   - Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
   - Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

3. **Gestión de riesgos**
   - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
   - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
   - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

4. **Plan de implantación de seguridad**
   - Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
   - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
   - Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

cve: BOE-A-2011-10055

5. Protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

6. Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas

- Determinación de los perímetros de seguridad física
- Sistemas de control de acceso físico mas frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos
- Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
- Exposición de elementos mas frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
- Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
- Elaboración de la normativa de seguridad física e industrial para la organización
- Sistemas de ficheros más frecuentemente utilizados
- Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización
- Configuración de políticas y directivas del directorio de usuarios
- Establecimiento de las listas de control de acceso (ACLs) a ficheros
- Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
- Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
- Sistemas de autenticación de usuarios débiles, fuertes y biométricos
- Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
- Elaboración de la normativa de control de accesos a los sistemas informáticos

7. Identificación de servicios

- Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
- Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
- Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

8. Robustecimiento de sistemas

- Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
- Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
- Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
- Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

cve: BOE-A-2011-10055

- Actualización de parches de seguridad de los sistemas informáticos
- Protección de los sistemas de información frente a código malicioso
- Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
- Monitorización de la seguridad y el uso adecuado de los sistemas de información

9. Implantación y configuración de cortafuegos

- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
- Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
- Definición de reglas de corte en los cortafuegos
- Relación de los registros de auditoría del cortafuegos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas del cortafuegos

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0486_3	90	40

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: AUDITORÍA DE SEGURIDAD INFORMÁTICA

Código: MF0487_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0487_3: Auditar redes de comunicación y sistemas informáticos

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecuen a las especificaciones de seguridad informática.

CE1.1 Explicar las diferencias entre vulnerabilidades y amenazas.

CE1.2 Enunciar las características de los principales tipos de vulnerabilidades y programas maliciosos existentes, describiendo sus particularidades.

cve: BOE-A-2011-10055

CE1.3 Describir el funcionamiento de una herramienta de análisis de vulnerabilidades, indicando las principales técnicas empleadas y la fiabilidad de las mismas.
CE1.4 Seleccionar la herramienta de auditoría de seguridad más adecuada en función del servidor o red y los requisitos de seguridad.
CE1.5 A partir de un supuesto práctico, ante un sistema informático dado en circunstancias de implantación concretas:
- Establecer los requisitos de seguridad que debe cumplir cada sistema.
- Crear una prueba nueva para la herramienta de auditoría, partiendo de las especificaciones de la vulnerabilidad.
- Elaborar el plan de pruebas teniendo en cuenta el tipo de servidor analizado.
- Utilizar varias herramientas para detectar posibles vulnerabilidades
- Analizar el resultado de la herramienta de auditoría, descartando falsos positivos.
- Redactar el informe de auditoría, reflejando las irregularidades detectadas, y las sugerencias para su regularización.

C2: Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.
CE2.1 Explicar la normativa legal vigente (autonómica, nacional, europea e internacional) aplicable a datos de carácter personal.
CE2.2 Exponer los trámites legales que deben cumplir los ficheros con datos de carácter personal, teniendo en cuenta la calidad de los mismos.
CE2.3 Describir los niveles de seguridad establecidos en la normativa legal vigente asociándolos a los requisitos exigidos.
CE2.4 A partir de un supuesto práctico, en el que se cuenta con una estructura de registro de información de una organización:
- Identificar los ficheros con datos de carácter personal, justificando el nivel de seguridad que le corresponde.
- Elaborar el plan de auditoría de cumplimiento de legislación en materia de protección de datos de carácter personal.
- Revisar la documentación asociada a los ficheros con datos de carácter personal, identificando las carencias existentes.
- Elaborar el informe correspondiente a los ficheros de carácter personal, indicando las deficiencias encontradas y las correcciones pertinentes.

C3: Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.
CE3.1 Identificar las fases del análisis de riesgos, describiendo el objetivo de cada una de ellas.
CE3.2 Describir los términos asociados al análisis de riesgos (amenaza, vulnerabilidad, impacto y contramedidas), estableciendo la relación existente entre ellos.
CE3.3 Describir las técnicas de análisis de redes, explicando los criterios de selección.
CE3.4 Describir las topologías de cortafuegos de red comunes, indicando sus funcionalidades principales.

Contenidos

1. Criterios generales comúnmente aceptados sobre auditoría informática
- Código deontológico de la función de auditoría
- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- Criterios a seguir para la composición del equipo auditor

cve: BOE-A-2011-10055

- Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
- Tipos de muestreo a aplicar durante el proceso de auditoría
- Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

2. Aplicación de la normativa de protección de datos de carácter personal

- Principios generales de protección de datos de carácter personal
- Normativa europea recogida en la directiva 95/46/CE
- Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
- Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

3. Análisis de riesgos de los sistemas de información

- Introducción al análisis de riesgos
- Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
- Particularidades de los distintos tipos de código malicioso
- Principales elementos del análisis de riesgos y sus modelos de relaciones
- Metodologías cualitativas y cuantitativas de análisis de riesgos
- Identificación de los activos involucrados en el análisis de riesgos y su valoración
- Identificación de las amenazas que pueden afectar a los activos identificados previamente
- Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
- Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
- Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
- Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
- Determinación de la probabilidad e impacto de materialización de los escenarios
- Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
- Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
- Relación de las distintas alternativas de gestión de riesgos

cve: BOE-A-2011-10055

- Guía para la elaboración del plan de gestión de riesgos
- Exposición de la metodología NIST SP 800-30
- Exposición de la metodología Magerit versión 2

4. **Uso de herramientas para la auditoría de sistemas**
   - Herramientas del sistema operativo tipo Ping, Traceroute, etc.
   - Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
   - Herramientas de análisis de vulnerabilidades tipo Nessus
   - Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
   - Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
   - Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

5. **Descripción de los aspectos sobre cortafuegos en auditorías de Sistemas Informáticos.**
   - Principios generales de cortafuegos
   - Componentes de un cortafuegos de red
   - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
   - Arquitecturas de cortafuegos de red
   - Otras arquitecturas de cortafuegos de red

6. **Guías para la ejecución de las distintas fases de la auditoría de sistemas de información**
   - Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
   - Guía para la elaboración del plan de auditoría
   - Guía para las pruebas de auditoría
   - Guía para la elaboración del informe de auditoría

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0487_3	90	40

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 3

Denominación: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Código: MF0488_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0488_3: Detectar y responder ante incidentes de seguridad

cve: BOE-A-2011-10055

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.

CE1.1 Describir las técnicas de detección y prevención de intrusos, exponiendo los principales parámetros que pueden emplearse como criterios de detección.

CE1.2 Determinar el número, tipo y ubicación de los sistemas de detección de intrusos, garantizando la monitorización del tráfico indicado en el plan de implantación.

CE1.3 Seleccionar las reglas del sistema de detección de intrusos, en función del sistema informático a monitorizar.

CE1.4 Determinar los umbrales de alarma del sistema, teniendo en cuenta los parámetros de uso del sistema.

CE1.5 Elaborar reglas de detección, partiendo de la caracterización de las técnicas de intrusión.

CE1.6 A partir de un supuesto práctico convenientemente caracterizado en el que se ubican servidores con posibilidad de accesos locales y remotos:

- Instalar y configurar software de recolección de alarmas.
- Configurar diferentes niveles de recolección de alarmas.

CE1.7 En una colección de supuestos prácticos en un entorno controlado de servidores en varias zonas de una red departamental con conexión a Internet:

- Decidir áreas a proteger.
- Instalar un sistema de detección de intrusos.
- Definir y aplicar normas de detección.
- Verificar funcionamiento del sistema atacando áreas protegidas.
- Elaborar un informe detallando conclusiones.

C2: Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.

CE2.1 Analizar la información de los sistemas de detección de intrusos, extrayendo aquellos eventos relevantes para la seguridad.

CE2.2 Analizar los indicios de intrusión, indicando los condicionantes necesarios para que la amenaza pueda materializarse.

CE2.3 Clasificar los elementos de las alertas del sistema de detección de intrusiones, estableciendo las posibles correlaciones existentes entre ellos, distinguiendo las alertas por tiempos y niveles de seguridad.

CE2.4 A partir de un supuesto práctico, en el que realizan intentos de intrusión al sistema informático:

- Recopilar las alertas de los sistemas de detección de intrusiones.
- Relacionar los eventos recogidos por los sistemas de detección de intrusiones.
- Determinar aquellas alertas significativas.
- Elaborar el informe correspondiente indicando las posibles intrusiones y el riesgo asociado para la seguridad del sistema informático de la organización.

CE2.5 Establecer procesos de actualización de las herramientas de detección de intrusos para asegurar su funcionalidad según especificaciones de los fabricantes.

C3: Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

cve: BOE-A-2011-10055

CE3.1 Describir las fases del plan de actuación frente a incidentes de seguridad, describiendo los objetivos de cada fase.
CE3.2 Indicar las fases del análisis forense de equipos informáticos, describiendo los objetivos de cada fase.
CE3.3 Clasificar los tipos de evidencias del análisis forense de sistemas, indicando sus características, métodos de recolección y análisis.
CE3.4 Describir las distintas técnicas para análisis de programas maliciosos, indicando casos de uso.
CE3.5 En un supuesto práctico, en el que se ha producido una intrusión en un sistema informático:
- Realizar la recogida de evidencias volátiles.
- Realizar la recogida de evidencias no volátiles.
- Análisis preliminar de las evidencias.
- Análisis temporal de actividad del sistema de ficheros.
- Elaborar el informe final, recogiendo las evidencias encontradas, las posibles vulnerabilidades utilizadas para la intrusión y la actividad realizada por el intruso que ha sido detectada en el sistema.

CE3.6 Estandarizar métodos de recuperación de desastres de equipos informáticos ante la detección de intrusiones.

Contenidos

1. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- Identificación y caracterización de los datos de funcionamiento del sistema
- Arquitecturas más frecuentes de los sistemas de detección de intrusos
- Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

2. Implantación y puesta en producción de sistemas IDS/IPS
- Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
- Definición de políticas de corte de intentos de intrusión en los IDS/IPS
- Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
- Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
- Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

3. Control de código malicioso
- Sistemas de detección y contención de código malicioso
- Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
- Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
- Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
- Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

cve: BOE-A-2011-10055

- Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

4. Respuesta ante incidentes de seguridad

- Procedimiento de recolección de información relacionada con incidentes de seguridad
- Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
- Proceso de verificación de la intrusión
- Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

5. Proceso de notificación y gestión de intentos de intrusión

- Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
- Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
- Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
- Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
- Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
- Establecimiento del nivel de intervención requerido en función del impacto previsible
- Guía para la investigación y diagnostico del incidente de intento de intrusión o infecciones
- Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
- Proceso para la comunicación del incidente a terceros, si procede
- Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

6. Análisis forense informático

- Conceptos generales y objetivos del análisis forense
- Exposición del Principio de Lockard
- Guía para la recogida de evidencias electrónicas:
  - Evidencias volátiles y no volátiles
  - Etiquetado de evidencias
  - Cadena de custodia
  - Ficheros y directorios ocultos
  - Información oculta del sistema
  - Recuperación de ficheros borrados
- Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
- Guía para la selección de las herramientas de análisis forense

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0488_3	90	40

cve: BOE-A-2011-10055

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: SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

Código: MF0489_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos

Duración: 60 horas

Capacidades y criterios de evaluación

C1: Evaluar las técnicas de cifrado existentes para escoger la necesaria en función de los requisitos de seguridad exigidos.

CE1.1 Describir las diferencias entre los algoritmos de cifrado de clave privada y los de clave pública, indicando sus diferentes usos.
CE1.2 Identificar los diferentes modos de cifrado, describiendo las características principales.
CE1.3 Clasificar los diferentes algoritmos de clave privada, describiendo sus fases de ejecución.
CE1.4 Clasificar los diferentes algoritmos de clave pública, describiendo sus fases de ejecución.
CE1.5 Identificar los diferentes protocolos de intercambio de claves, describiendo su funcionamiento.

C2: Implantar servicios y técnicas criptográficas en aquellos servicios que lo requieran según especificaciones de seguridad informática.

CE2.1 Justificar la necesidad de utilizar técnicas criptográficas en las comunicaciones entre sistemas informáticos en función de los canales utilizados.
CE2.2 Definir las técnicas de cifrado para conectar de forma segura dos redes describiendo las funcionalidades y requisitos necesarios.
CE2.3 Definir las técnicas empleadas para conectar de forma segura dos equipos (túneles SSL y SSH), describiendo las funcionalidades y requisitos necesarios.
CE2.4 En un caso práctico, en el que se desea establecer una comunicación segura entre dos sistemas informáticos:

- Analizar los requisitos de seguridad de la arquitectura de comunicaciones propuesta.
- Indicar la solución más indicada, justificando la selección.
- Instalar los servicios de VPN e IPSec para conectar redes.
- Instalar los servicios de túneles SSL o SSH para conectar equipos distantes.

C3: Utilizar sistemas de certificados digitales en aquellas comunicaciones que requieran integridad y confidencialidad según especificaciones de seguridad.

cve: BOE-A-2011-10055

CE3.1 Identificar los atributos empleados en los certificados digitales para servidor, describiendo sus valores y función.
CE3.2 Describir los modos de utilización de los certificados digitales, asociándolos a las especificaciones de seguridad: confidencialidad, integridad y accesibilidad.
CE3.3 Describir la estructura de un sistema de sellado digital, indicando las funciones de los elementos que la integran.

C4: Diseñar e implantar servicios de certificación digital según necesidades de explotación y de seguridad informática.
CE4.1 Describir la estructura de la infraestructura de clave pública, indicando las funciones de los elementos que la integran.
CE4.2 Describir los servicios y obligaciones de la autoridad de certificación, relacionándolos con la política de certificado y la declaración de prácticas de certificación.
CE4.3 Identificar los atributos obligatorios y opcionales de un certificado digital, describiendo el uso habitual de dichos atributos.
CE4.4 Describir la estructura de una infraestructura de gestión de privilegios, indicando las funciones de los elementos que la integran.
CE4.5 Determinar los campos de los certificados de atributos, describiendo su uso habitual y la relación existente con los certificados digitales.
CE4.6 En un caso práctico, en el que se desea establecer un sistema de certificación para un sistema informático:
- Diseñar una infraestructura de clave pública, en función de las especificaciones.
- Justificar la jerarquía de autoridades de certificación diseñada.
- Emitir los certificados siguiendo los procedimientos indicados en la Declaración de Prácticas de Certificación.

Contenidos

1. Criptografía
- Perspectiva histórica y objetivos de la criptografía
- Teoría de la información
- Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos
- Elementos fundamentales de la criptografía de clave privada y de clave publica
- Características y atributos de los certificados digitales
- Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente
- Algoritmos criptográficos mas frecuentemente utilizados
- Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización
- Elementos fundamentales de las funciones resumen y los criterios para su utilización
- Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica
- Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización
- Criterios para la utilización de técnicas de cifrado de flujo y de bloque
- Protocolos de intercambio de claves
- Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop

cve: BOE-A-2011-10055

2. Aplicación de una infraestructura de clave pública (PKI)

- Identificación de los componentes de una PKI y su modelo de relaciones
- Autoridad de certificación y sus elementos
- Política de certificado y declaración de practicas de certificación (CPS)
- Lista de certificados revocados (CRL)
- Funcionamiento de las solicitudes de firma de certificados (CSR)
- Infraestructura de gestión de privilegios (PMI)
- Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales
- Aplicaciones que se apoyan en la existencia de una PKI

3. Comunicaciones seguras

- Definición, finalidad y funcionalidad de redes privadas virtuales
- Protocolo IPSec
- Protocolos SSL y SSH
- Sistemas SSL VPN
- Túneles cifrados
- Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0489_3	60	40

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 5

Denominación: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

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

cve: BOE-A-2011-10055

usuarios afectados entre otros) para determinar su influencia en el rendimiento del sistema.

CE1.2 Describir cada una de las herramientas provistas por el sistema para la gestión de procesos con objeto de permitir la intervención en el rendimiento general del sistema.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema.

CE1.4 En un supuesto práctico en el que se cuenta con un sistema informático con una carga de procesos debidamente caracterizada:

- Utilizar las herramientas del sistema para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar las operaciones de activación, desactivación y modificación de prioridad entre otras con un proceso utilizando las herramientas del sistema.
- Monitorizar el rendimiento del sistema mediante herramientas específicas y definir alarmas, que indiquen situaciones de riesgo.

C2: Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

CE2.1 Identificar los distintos sistemas de archivo utilizables en un dispositivo de almacenamiento dado para optimizar los procesos de registro y acceso a los mismos.

CE2.2 Explicar las características de los sistemas de archivo en función de los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento en el sistema informático asociando los dispositivos con los distintos sistemas de archivos existentes.

CE2.4 En un supuesto práctico en el que se dispone de un sistema de almacenamiento de la información con varios dispositivos:

- Realizar el particionamiento, en los casos que sea necesario, y la generación de la infraestructura de los sistemas de archivo a instalar en cada dispositivo.
- Implementar la estructura general de almacenamiento integrando todos los dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado.

C3: Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

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

CE3.2 Describir las herramientas que se utilizan en la gestión de permisos a usuarios para el uso de los recursos del sistema.

CE3.3 En un supuesto práctico en el que se cuenta con derecho de administración de usuarios:

- Identificar los posibles accesos de un usuario al sistema.
- Modificar los permisos de utilización de un recurso del sistema a un usuario.
- Definir limitaciones de uso de un recurso del sistema a los usuarios.

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

CE4.1 Explicar los parámetros de configuración y funcionamiento de los dispositivos de comunicaciones para asegurar su funcionalidad dentro del sistema.

cve: BOE-A-2011-10055

CE4.2 Relacionar los servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos con objeto de analizar y evaluar el rendimiento.
CE4.3 En un supuesto práctico en el que tomamos un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:
- Identificar los dispositivos de comunicaciones y describir sus características.
- Verificar el estado de los servicios de comunicaciones.
- Evaluar el rendimiento de los servicios de comunicaciones.
- Detectar y documentar las incidencias producidas en el sistema.

Contenidos

1. **Gestión de la seguridad y normativas**
   - Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
   - Metodología ITIL Librería de infraestructuras de las tecnologías de la información
   - Ley orgánica de protección de datos de carácter personal.
   - Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

2. **Análisis de los procesos de sistemas**
   - Identificación de procesos de negocio soportados por sistemas de información
   - Características fundamentales de los procesos electrónicos
     - Estados de un proceso,
     - Manejo de señales, su administración y los cambios en las prioridades
   - Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
   - Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
   - Técnicas utilizadas para la gestión del consumo de recursos

3. **Demostración de sistemas de almacenamiento**
   - Tipos de dispositivos de almacenamiento más frecuentes
   - Características de los sistemas de archivo disponibles
   - Organización y estructura general de almacenamiento
   - Herramientas del sistema para gestión de dispositivos de almacenamiento

4. **Utilización de métricas e indicadores de monitorización de rendimiento de sistemas**
   - Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
   - Identificación de los objetos para los cuales es necesario obtener indicadores
   - Aspectos a definir para la selección y definición de indicadores
   - Establecimiento de los umbrales de rendimiento de los sistemas de información
   - Recolección y análisis de los datos aportados por los indicadores
   - Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

5. **Confección del proceso de monitorización de sistemas y comunicaciones**
   - Identificación de los dispositivos de comunicaciones
   - Análisis de los protocolos y servicios de comunicaciones

cve: BOE-A-2011-10055

- Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
- Procesos de monitorización y respuesta
- Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
- Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
- Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
- Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

6. Selección del sistema de registro de en función de los requerimientos de la organización

- Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
- Análisis de los requerimientos legales en referencia al registro
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
- Asignación de responsabilidades para la gestión del registro
- Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
- Guía para la selección del sistema de almacenamiento y custodia de registros

7. Administración del control de accesos adecuados de los sistemas de información

- Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
- Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
- Requerimientos legales en referencia al control de accesos y asignación de privilegios
- Perfiles de de acceso en relación con los roles funcionales del personal de la organización
- Herramientas de directorio activo y servidores LDAP en general
- Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
- Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0490_3	90	40

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-2011-10055

MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES DE SEGURIDAD INFORMÁTICA

Código: MP0175

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Proporcionar soporte técnico en materia de seguridad.

CE1.1. Proporcionar asistencia técnica en el diseño y configuración de soluciones de seguridad.

CE1.2. Dar soporte a otras áreas en las tareas de diseño y reingeniería de procesos para aportar la visión de seguridad.

CE1.3. Actuar como enlace entre las distintas áreas de la compañía para coordinar medidas de seguridad multidepartamentales.

CE1.4. Analizar las reglas específicas desarrolladas por las áreas técnicas específicas para las herramientas de seguridad corporativas.

CE1.5. Coordinar el uso de las herramientas de cifrado y la gestión de las claves

CE1.6. Dar soporte técnico a los comités de dirección que proceda.

CE1.7. Evaluar y mantenerse permanentemente informado de los errores, informes, noticias, boletines, etc. de seguridad recibidos y dar el primer nivel de soporte y distribución.

CE1.8. Desarrollar las políticas y procedimientos operativos en materia de seguridad de la información y dar soporte a las distintas áreas de la organización para su puesta en producción.

C2: Verificar la correcta aplicación de las medidas de seguridad.

CE2.1. Realizar las verificaciones necesarias para determinar el grado de vulnerabilidad de las distintas plataformas tecnológicas, así como el resto de revisiones periódicas de seguridad de los sistemas de información.

CE2.2. Mantener actualizado el análisis de riesgos de la organización

CE2.3. Coordinar las auditorías técnicas de seguridad.

C3: Participar en los procesos 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. Revisión de la situación de la seguridad de la información

- Revisión de las normas internas de seguridad
- Revisión de la gestión de usuarios, privilegios y política de contraseñas
- Revisión de las copias de seguridad
- Revisión de las incidencias que se han producido

cve: BOE-A-2011-10055

- Revisión de la situación con respecto a la protección frente a código malicioso
- Revisión de la seguridad de las redes de datos
- Revisión de la seguridad de servidores y puestos de trabajo
- Revisión de la seguridad física, suministro eléctrico, climatización y protección de incendios según proceda

2. Configuración de reglas de relacionadas con la seguridad
- Configuración de la seguridad de el/los router
- Configuración de la seguridad de el/los switch
- Configuración de la seguridad de el/los cortafuegos
- Configuración de la seguridad de el/los sistema de detección de intrusos
- Configuración de la seguridad de el/los antivirus

3. Comunicación de los aspectos relacionados con la seguridad
- Establecimiento de canales para mantener a la organización actualizada en materia de seguridad
- Establecimiento de los canales internos para coordinar la seguridad entre los departamentos de la organización

4. Monitorización de la seguridad
- Monitorización de las comunicaciones
- Monitorización del rendimiento de sistemas

5. Aplicación de la normativa y metodología de seguridad
- Aplicación de códigos de buenas practicas de seguridad a la gestión diaria de los sistemas de información
- Integración de los requerimientos de seguridad en los procesos de negocio de la organización

6. 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 del proceso productivo de la organización.
- Utilización 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.

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	*Experiencia profesional en el ámbito de la unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0486_3: Asegurar equipos 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.	1 año	3 años

cve: BOE-A-2011-10055

Módulos Formativos	Acreditación requerida	*Experiencia profesional en el ámbito de la unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0487_3: Auditoría de seguridad informática	• 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.	2 años	4 años
MF0488_3: Gestión de incidentes de seguridad informática	• 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.	1 año	3 años
MF0489_3: Sistemas seguros de acceso y transmisión de datos	• 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.	1 año	3 años
MF0490_3: Gestión de servicios en el sistema informático	• 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.	2 años	4 años

* En los últimos tres años.

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTOS

Espacio Formativo	Superficie m^2 15 alumnos	Superficie m^2 25 alumnos
Aula de gestión	45	60

Espacio Formativo	M1	M2	M3	M4	M5
Aula de gestión	X	X	X	X	X

Espacio Formativo	Equipamiento
Aula de gestión	- Equipos audiovisuales - PCs instalados en red, cañón de proyección e internet - Software especifico de la especialidad - Pizarras para escribir con rotulador - Rotafolios - Material de aula - Mesa y sillas para formador - Mesas y sillas para alumnos

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

cve: BOE-A-2011-10055

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 IV

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: IMPLANTACIÓN Y GESTIÓN DE ELEMENTOS INFORMÁTICOS EN SISTEMAS DOMÓTICOS/INMÓTICOS, DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Código: IFCT0409

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y Telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC365_3 Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia (RD 1701/2007, de 14 diciembre)

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

UC0490_3: Gestionar servicios en el sistema informático
UC1219_3: Implantar y mantener sistemas domóticos-inmóticos
UC1220_3: Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia

Competencia general:

Integrar y mantener elementos informáticos y de comunicaciones en sistemas de automatización de edificios domóticos e inmóticos, de control de accesos y presencia y de videovigilancia a nivel de hardware y software, asegurando el funcionamiento de los distintos módulos que los componen, en condiciones de calidad y seguridad, cumpliendo la normativa y reglamentación vigentes.

cve: BOE-A-2011-10055

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional tanto por cuenta propia, como por cuenta ajena en empresas o entidades publicas o privadas de cualquier tamaño, dedicadas al diseño, implementación y mantenimiento de sistemas domóticos/inmóticos, de control de accesos y presencia, y videovigilancia.

Sectores productivos:

Se ubica sobre todo en el sector servicios, y principalmente en empresas cuya actividad tenga como objetivo el proveer y mantener servicios relacionados con la automatización de viviendas y edificios, así como con la seguridad privada, relativos a la implementación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia.

Ocupaciones o puestos de trabajo relacionados:

Integrador de elementos informáticos en sistemas domóticos/inmóticos.
Integrador de elementos informáticos en sistemas de control de accesos y presencia, y en sistemas de videovigilancia.
Experto de mantenimiento de elementos informáticos en sistemas de control de accesos y presencia, y en sistemas de videovigilancia.

Duración de la formación asociada: 540 horas.

Relación de módulos formativos y de unidades formativas:

MF0490_3: (Transversal) Gestión de servicios en el sistema informático (90 horas)
MF1219_3: Implantación y mantenimiento de sistemas domóticos/inmóticos (150 horas)
- UF1134: Instalación y puesta en marcha de un proyecto domótico / inmótico (80 horas)
- UF1135: Conectividad del proyecto domótico: redes, sistemas y protocolos de comunicación; pasarelas (40 horas)
- UF1136: Documentación, mantenimiento y gestión de incidencias en un proyecto domótico (30 horas)

MF1220_3: Implantación y mantenimiento de sistemas de control de accesos y presencia, y de video vigilancia (220 horas)
- UF1137: Instalación y puesta en marcha de un sistema de Video Vigilancia y seguridad (90 horas)
- UF1138: Instalación y puesta en marcha de un sistema de Control de Acceso y presencia (90 horas)
- UF1139: Mantenimiento y gestión de Incidencias en proyectos de Video Vigilancia, control de accesos, y presencia (40 horas)

MP0236: Módulo de prácticas profesionales no laborales de Implantación y gestión de elementos informáticos en sistemas domóticos/inmóticos, de control de accesos y presencia, y de videovigilancia (80 horas)

cve: BOE-A-2011-10055

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso y dentro de las directivas de la organización.

CR1.1. Los procesos que intervienen en el sistema son identificados para evaluar parámetros de rendimiento.

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

CR1.3. Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización.

CR1.4. Las herramientas de monitorización se implantan y configuran determinando los niveles de las alarmas en función del plan de explotación de la organización.

RP2: Administrar los dispositivos de almacenamiento según las necesidades de uso y dentro de las directivas de la organización.

CR2.1. Los dispositivos de almacenamiento se configuran para ser usados en los distintos sistemas operativos utilizados en el sistema informático.

CR2.2. La estructura de almacenamiento se define y se implanta atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de uso de la organización.

CR2.3. Los requerimientos de nomenclatura de objetos y restricciones de uso de cada dispositivo de almacenamiento se documentan adecuadamente.

CR2.4. Los dispositivos de almacenamiento se integran para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.

CR3.1. El acceso de los usuarios al sistema informático se configura para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.

CR3.2. El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.

CR3.3. Los recursos disponibles para los usuarios se limitan con las herramientas adecuadas en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.

CR4.1. Los dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.

CR4.2. Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.

cve: BOE-A-2011-10055

CR4.3. Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización

Contexto profesional

Medios de producción
Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

Productos y resultados
Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada
Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

Unidad de competencia 2

Denominación: IMPLANTAR Y MANTENER SISTEMAS DOMÓTICOS/INMÓTICOS

Nivel: 3

Código: UC1219_3
Realizaciones profesionales y criterios de realización

RP1: Configurar y parametrizar los equipos y dispositivos del sistema domótico/inmótico para su puesta en servicio, de acuerdo a los requisitos funcionales del proyecto.

CR1.1 Las especificaciones recogidas en el proyecto de instalación y/o de integración del sistema domótico/inmótico a implantar se interpretan con objeto de identificar la arquitectura, componentes y tecnologías que intervienen en el sistema.

CR1.2 La comprobación y verificación de la ubicación e instalación de los equipos, dispositivos e infraestructura se realiza para garantizar la configuración, programación y puesta en marcha del sistema domótico / inmótico, de acuerdo a los requisitos funcionales del proyecto.

CR1.3 La configuración y parametrización física y lógica de los equipos y dispositivos que forman el sistema domótico/inmótico se planifica y se realiza, para su puesta en servicio, cumpliendo los requisitos funcionales fijados por el proyecto y de acuerdo a los procedimientos establecidos por la organización.

CR1.4 La configuración de las diferentes pasarelas residenciales, en su caso, se realiza para conectar las distintas redes internas que componen el sistema domótico/inmótico con las redes públicas de datos, para acceder a los servicios que proporcionan y permitir el acceso bidireccional al sistema desde el exterior de acuerdo a especificaciones del proyecto.

CR1.5 La puesta en marcha del sistema domótico/inmótico se realiza, siguiendo el protocolo de pruebas establecido por la organización y de acuerdo a las especificaciones funcionales del proyecto.

cve: BOE-A-2011-10055

CR1.6 El informe de puesta en marcha del sistema domótico/inmótico se elabora, incluyendo la configuración de los equipos, de los dispositivos y las pruebas de puesta en marcha realizadas, con objeto de registrar la información para su uso posterior, según normas de la organización.
CR1.7 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP2: Elaborar y mantener inventarios de los equipos y dispositivos, y del software que componen el sistema domótico/inmótico, para garantizar su identificación y localización, siguiendo las normas establecidas por la organización.
CR2.1 El inventario de componentes hardware y aplicaciones software se elabora para registrar las características, localización y estado de los mismos, según las normas de la organización.
CR2.2 Las configuraciones de los equipos y aplicaciones del sistema domótico/inmótico se registran en el inventario, según procedimiento establecido por la organización, para facilitar las labores de recuperación en caso de fallos.
CR2.3 El inventario se mantiene actualizado registrando todos los cambios producidos en el sistema domótico/inmótico, tanto a nivel de hardware, como de software y de configuración, según procedimiento establecido por la organización.
CR2.4 Los manuales técnicos de los dispositivos y equipos del sistema domótico/inmótico se registran y se referencian en la documentación generada, para su uso posterior, de acuerdo al procedimiento establecido por la organización.

RP3: Ajustar el software de control y crear programas para añadir funcionalidades al sistema domótico/inmótico, integrándolas en la aplicación de monitorización y control (software de control) utilizando herramientas de programación y estándares software de desarrollo, de acuerdo a especificaciones técnicas y necesidades del sistema.
CR3.1 La configuración y parametrización del software de control del sistema se planifica y se realiza para su puesta en funcionamiento, de acuerdo a los requisitos funcionales fijados por el proyecto, los protocolos de configuración establecidos por los elementos software del sistema domótico/inmótico y los procedimientos establecidos por la organización.
CR3.2 La comprobación y verificación de la ubicación e instalación de los equipos de monitorización y control del sistema, se realizan para garantizar su configuración, programación y puesta en marcha, siguiendo especificaciones técnicas del proyecto.
CR3.3 La programación de funcionalidades del software de control se realiza teniendo en cuenta las distintas técnicas y lenguajes de desarrollo y estándares de referencia de sistemas de control domótico/inmótico, utilizando las herramientas proporcionadas por el sistema, según especificaciones técnicas y necesidades de uso.
CR3.4 La pasarela residencial, en su caso, se configura implementando nuevos servicios y aplicaciones, utilizando estándares software de desarrollo de estos servicios, según necesidades especificadas.
CR3.5 Las pruebas de puesta en marcha de las funcionalidades de visualización y control del sistema, se realizan para verificar que cumplen las especificaciones del proyecto, siguiendo el protocolo establecido por la organización.
CR3.6 El informe de puesta en marcha de la aplicación de monitorización y control se elabora, incluyendo las actividades realizadas y las incidencias detectadas, para su uso posterior, siguiendo las normas establecidas por la organización.

RP4: Mantener el sistema domótico/inmótico tanto a nivel hardware como software para garantizar su funcionamiento, de acuerdo a requisitos funcionales y criterios de calidad establecidos en el proyecto.

cve: BOE-A-2011-10055

CR4.1 Los procedimientos específicos de mantenimiento de los equipos y dispositivos que componen el sistema domótico/inmótico se definen para garantizar su funcionalidad, teniendo en cuenta las especificaciones técnicas de los mismos.
CR4.2 El plan de mantenimiento preventivo del sistema domótico/inmótico se elabora para garantizar la continuidad en la prestación del servicio, de acuerdo con los procedimientos específicos requeridos por los componentes del sistema, y por la organización.
CR4.3 La localización de averías y reparación o sustitución de los componentes hardware y software del sistema informático que soporta el sistema domótico/inmótico se realiza para mantenerlo operativo, utilizando herramientas específicas, aplicando los procedimientos normalizados y cumpliendo las normas de seguridad establecidas por la organización.
CR4.4 El manual de identificación y resolución de incidencias del sistema domótico/inmótico se elabora y se actualiza cada vez que se detecte una incidencia nueva, indicando la información más relevante respecto a la misma, de acuerdo con los procedimientos específicos requeridos por los componentes del sistema, indicando tareas, tiempos y resultados previstos.

Contexto profesional

Medios de producción
Ordenador portátil, PC de sobremesa y periféricos. Aplicaciones informáticas propietarias para configuración de sistemas domóticos. Bases de datos software de elementos hardware. Aplicaciones informáticas para diseño 2D y 3D. Aplicaciones informáticas para la gestión del mantenimiento. Instrumentos de medida: polímetro, cronómetro, luxómetro, entre otras. Estándares de referencia para desarrollo de sistemas domóticos/inmóticos. Equipos y dispositivos de sistemas domóticos/inmóticos. Software de control de sistemas domóticos/inmódicos.

Productos y resultados
Configuración y puesta en marcha del sistema inmótico/domótico. Mantenimiento preventivo de los componentes hardware y software del sistema domótico/inmótico. Mantenimiento correctivo de los componentes hardware y software del sistema domótico/inmótico.

Información utilizada o generada
Proyecto de ingeniería del sistema domótico/inmótico. Documentación técnica, manuales de instalación y uso de elementos hardware del sistema domótico/inmótico. Documentación técnica, manuales de instalación y uso de las aplicaciones software del sistema domótico/inmótico. Documentación de instalación eléctrica de los elementos hardware del sistema domótico/inmótico. Reglamento electrotécnico de baja tensión (REBT). Reglamento de infraestructuras comunes de telecomunicaciones (ICT). Pliegos de especificaciones del sistema domótico/inmótico. Planificación de la configuración y parametrización del sistema domótico/inmótico. Documentación de la topología, configuración de los elementos (parámetros, valores, direcciones IP, direcciones físicas) del sistema domótico/inmótico. Documento de procedimiento de pruebas de puesta en marcha del sistema domótico/inmótico. Acta de puesta en marcha y entrega del sistema. Documento de procedimiento de acciones de mantenimiento del sistema domótico/inmótico. Informes/actas/partes de mantenimiento preventivo y correctivo del sistema domótico/inmótico. Manual de usuario de funcionamiento del sistema domótico: hardware y software de control del sistema domótico/inmótico.

cve: BOE-A-2011-10055

Unidad de competencia 3

Denominación: IMPLANTAR Y MANTENER SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Nivel: 3

Código: UC1220_3

Realizaciones profesionales y criterios de realización

RP1: Interpretar las especificaciones técnicas del proyecto y verificar su instalación para implementar el sistema de control de accesos y presencia, y videovigilancia, según necesidades de la organización.

CR1.1 El análisis de riesgo y las especificaciones recogidas en el proyecto de instalación del sistema de control de accesos y presencia, y videovigilancia a implementar, se interpretan con objeto de identificar la arquitectura y componentes del sistema a implantar.

CR1.2 La planificación de las operaciones a desarrollar se realiza de acuerdo con los recursos humanos y materiales disponibles, para optimizar el proceso de implementación de los sistemas, teniendo en cuenta el marco de la reglamentación vigente y las especificaciones del diseño.

CR1.3 La infraestructura (cableado, armarios de conexiones, alimentaciones eléctricas) y los equipos de control, los elementos de captación y de accionamiento (barreras, cerraderos eléctricos, portillones de paso, tornos y molinillos, entre otros) de los sistemas de control de accesos y presencia, se verifican a lo largo del proceso de implantación para garantizar su integración y funcionalidad, siguiendo especificaciones descritas en la documentación del proyecto del sistema.

CR1.4 La infraestructura (cableados, armarios de conexiones, alimentaciones eléctricas), las características y ubicación de las cabinas de los elementos de captación de imagen (cámaras y domos, entre otros), de los detectores de presencia, de los equipos de tratamiento de señales(multiplexores, secuenciadores, matrices, videograbadores, videowall y teclados, entre otros) y dispositivos de visualización (monitores) de los sistemas de videovigilancia, se verifican a lo largo del proceso de montaje en lo que respecta a características funcionales, elementos y zonas a proteger para asegurar la funcionalidad del sistema, siguiendo las especificaciones de proyecto del sistema.

CR1.5 Los equipos y dispositivos instalados que componen el sistema de control de accesos y presencia se ajustan y configuran, para probar su funcionalidad y asegurar su funcionamiento, de acuerdo a especificaciones técnicas de proyecto del sistema.

CR1.6 Los equipos y dispositivos instalados, así como los elementos motorizados del sistema de videovigilancia se ajustan y configuran, para garantizar la integración de los mismos y la consecución de los objetivos del sistema, de acuerdo a las características funcionales y técnicas prescritas en la documentación técnica y de diseño.

CR1.7 Las actividades realizadas se documentan en formato normalizado para su uso posterior, siguiendo el procedimiento establecido por la organización.

RP2: Implementar los sistemas de control de accesos y presencia en la organización, de acuerdo a los requisitos y especificaciones de diseño establecidos en el proyecto.

CR2.1 Los equipos informáticos y periféricos asociados se configuran físicamente, y se instalan y configuran las aplicaciones de control y gestión de usuarios de acuerdo con los perfiles de acceso establecidos en las especificaciones del diseño,

cve: BOE-A-2011-10055

para garantizar la seguridad y fiabilidad de la información del sistema, teniendo en cuenta las especificaciones de la organización y la normativa vigente.

CR2.2 Los terminales de control de accesos y presencia de los usuarios y sus elementos biométricos, se programan y parametrizan para cumplimentar las normas de control de accesos y presencia, de acuerdo con los perfiles y niveles de acceso prescritos en las especificaciones del proyecto del sistema.

CR2.3 La aplicación software que centraliza el control del sistema, se instala y configura, y se verifica que es compatible con los equipos que tiene que controlar, para ratificar la funcionalidad del sistema de control de accesos y presencia, de acuerdo con los parámetros prefijados en las especificaciones de diseño.

CR2.4 La carga inicial de los datos del sistema de control de accesos y presencia se realiza y verifica para asegurar su integridad y el cumplimiento de la normativa legal vigente sobre protección de datos, según la política de seguridad de la organización.

CR2.5 La información registrada en el sistema se trata con herramientas de consulta y generación de informes para una distribución de la misma, garantizando la continuidad de la prestación de los servicios y la seguridad en los accesos y usos de dicha información, cumpliendo las normativas de protección de datos y de acuerdo a los planes de contingencias y seguridad de la organización.

CR2.6 La herramienta de generación de copias de seguridad de los controles y registros realizados, se integra con el sistema y se configura para que los usuarios tengan acceso, de acuerdo a los planes de seguridad y a la normativa legal vigente sobre protección de datos.

CR2.7 El informe de puesta en marcha se confecciona para que recoja con precisión los parámetros de funcionalidad, de acuerdo con lo establecido en la documentación del sistema, así como los ajustes realizados y las modificaciones que se sugieren para el análisis de riesgo.

CR2.8 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP3: Implementar los sistemas de videovigilancia en la organización, de acuerdo a los requisitos y especificaciones de diseño establecidos en el proyecto.

CR3.1 Los equipos informáticos y periféricos asociados se configuran físicamente, y se instalan y configuran las aplicaciones de control, gestión y planimetría, de acuerdo con las secuencias de visualización y la calidad de las imágenes requeridas establecidas en las especificaciones, para garantizar la funcionalidad del sistema y la integración de sus elementos.

CR3.2 La aplicación software (gestión de cámaras, proceso de grabación, planimetría, acceso remoto) que centraliza el control del sistema de videovigilancia se instala, configura y verifica para comprobar que cumple los parámetros prefijados y es compatible con los equipos que tiene que controlar, de acuerdo a especificaciones técnicas.

CR3.3 La información registrada y grabada se trata con parámetros de confidencialidad, para garantizar la continuidad de la prestación de los servicios de visualización y grabación de imágenes de las zonas establecidas, según el plan de contingencia vigente en la organización para los sistemas de información y teniendo en cuenta la legislación sobre protección de datos.

CR3.4 La herramienta de generación de copias de seguridad de las grabaciones realizadas se integra con el sistema y se configura, para que los usuarios tengan acceso al sistema, de acuerdo a los planes de seguridad y cumpliendo la normativa legal vigente sobre protección de datos.

CR3.5 El informe de puesta en marcha del se confecciona para que recoja con precisión los parámetros de funcionalidad de acuerdo con lo establecido en la documentación del sistema, así como los ajustes realizados y las modificaciones que se sugieren para el análisis de riesgo.

cve: BOE-A-2011-10055

CR3.6 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP4: Mantener los sistemas de control de accesos y presencia, y de videovigilancia, para asegurar su funcionalidad, de acuerdo con lo establecido en la documentación técnica del proyecto.

CR4.1 El plan de mantenimiento preventivo se interpreta para garantizar la continuidad en la prestación del servicio, de acuerdo con los procedimientos específicos requeridos por los componentes del sistema, indicando claramente la periodicidad de su aplicación.

CR4.2 Los procedimientos específicos de mantenimiento preventivo de los sistemas de control de accesos y presencia se ejecutan, para garantizar la funcionalidad óptima de los mismos, según lo indicado en el plan de mantenimiento.

CR4.3 Los procedimientos específicos de mantenimiento preventivo de los sistemas de videovigilancia se ejecutan, de acuerdo con los equipos y dispositivos que conforman las distintas partes del sistema, para garantizar la continuidad en la prestación del servicio y la funcionalidad de cada uno de los componentes, según lo indicado en las especificaciones funcionales y el plan de mantenimiento.

CR4.4 Los procedimientos específicos de mantenimiento se revisan periódicamente para adaptar el sistema a los cambios incluidos en el análisis de riesgo y, para detectar deficiencias y proponer mejoras de seguridad, siguiendo las indicaciones de los fabricantes y normativa de la organización.

CR4.5 La localización de averías y reparación de los sistemas de control de accesos y presencia, y de videovigilancia se realiza aplicando sistemáticamente los procedimientos normalizados por la organización, respetando las normas de seguridad y los tiempos establecidos, para evitar interrupciones en la prestación del servicio y minimizar el impacto de éstas cuando se produzcan.

CR4.6 Las actualizaciones de los componentes hardware y software de los sistemas de control de accesos y presencia, y de videovigilancia, se realizan para añadir mejoras y corregir posibles fallos, teniendo en cuenta las especificaciones técnicas de los fabricantes y normativa de la organización.

CR4.7 El plan de mantenimiento preventivo de los sistemas de control de accesos y presencia, y de videovigilancia, se actualiza para recoger con precisión los resultados obtenidos en la aplicación del plan de mantenimiento preventivo, así como las intervenciones realizadas frente a disfunciones y averías del sistema, de acuerdo a los planes de contingencias de la organización.

CR4.8 La documentación generada en la aplicación de los procedimientos de mantenimiento preventivo se recoge en los registros normalizados para su almacenamiento y posterior tratamiento y distribución, siguiendo el protocolo establecido por la organización.

Contexto profesional

Medios de producción

Equipos informáticos y periféricos. Herramientas ofimáticas. Herramientas software de planificación. Aplicaciones informáticas para la gestión de los sistemas de control de accesos y detección de presencia. Aplicaciones informáticas para la gestión de cámaras de videovigilancia y planimetría. Instrumentos de medida: polímetro, téster de cableado coaxial, certificador de cableado, monitor de vídeo portátil, luxómetro. Equipos para control de accesos y presencia: cabezales lectores de tarjetas (banda magnética, proximidad, chip), lectores biométricos, centrales de control, actuadores (electrocerraderos, barreras), detectores de presencia. Equipos para sistemas de videovigilancia: cámaras analógicas, cámaras IP, ópticas para las cámaras, cabinas para las cámaras, posicionadores, teclados de control, multiplexores, secuenciadores,

cve: BOE-A-2011-10055

grabadores de imagen analógicos y digitales, monitores analógicos y TFT, soportes de grabación (cintas, CD, DVD).

Productos y resultados
Planificación, ejecución y seguimiento de la implementación de los sistemas de control de accesos y presencia, y de videovigilancia. Verificación y puesta en marcha de los sistemas de control de accesos y presencia, y de videovigilancia. Procedimientos de intervención preventiva y correctiva requeridos para el mantenimiento de los sistemas de control de accesos y presencia, y de videovigilancia. Mantenimiento preventivo de los sistemas de control de accesos y presencia, y de videovigilancia. Reparación de averías en los sistemas de control de accesos y presencia, y de videovigilancia.

Información utilizada o generada
Análisis de riesgo. Especificaciones técnicas de los proyectos de instalación. Documentación técnica de los equipos y dispositivos y recomendaciones de los fabricantes, en soporte impreso o electrónico. Manuales de instalación y guías de usuario. Reglamentación sobre seguridad privada. Manuales de uso y funcionamiento de los equipos y dispositivos. Manuales del software asociado. Información sobre la configuración de red y direccionamiento IP. Informes de puesta en marcha de los sistemas. Partes de servicio e intervención para el mantenimiento de los sistemas. Legislación vigente sobre protección de datos y seguridad privada.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

CE1.1 Identificar los procesos del sistema y los parámetros que los caracterizan (procesos padre, estado del proceso, consumo de recursos, prioridades y usuarios afectados entre otros) para determinar su influencia en el rendimiento del sistema.

CE1.2 Describir cada una de las herramientas provistas por el sistema para la gestión de procesos con objeto de permitir la intervención en el rendimiento general del sistema.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema.

CE1.4 En un supuesto práctico en el que se cuenta con un sistema informático con una carga de procesos debidamente caracterizada:

cve: BOE-A-2011-10055

- Utilizar las herramientas del sistema para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar las operaciones de activación, desactivación y modificación de prioridad entre otras con un proceso utilizando las herramientas del sistema.
- Monitorizar el rendimiento del sistema mediante herramientas específicas y definir alarmas, que indiquen situaciones de riesgo.

C2: Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

CE2.1 Identificar los distintos sistemas de archivo utilizables en un dispositivo de almacenamiento dado para optimizar los procesos de registro y acceso a los mismos.

CE2.2 Explicar las características de los sistemas de archivo en función de los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento en el sistema informático asociando los dispositivos con los distintos sistemas de archivos existentes.

CE2.4 En un supuesto práctico en el que se dispone de un sistema de almacenamiento de la información con varios dispositivos:

- Realizar el particionamiento, en los casos que sea necesario, y la generación de la infraestructura de los sistemas de archivo a instalar en cada dispositivo.
- Implementar la estructura general de almacenamiento integrando todos los dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado.

C3: Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

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

CE3.2 Describir las herramientas que se utilizan en la gestión de permisos a usuarios para el uso de los recursos del sistema.

CE3.3 En un supuesto práctico en el que se cuenta con derecho de administración de usuarios:

- Identificar los posibles accesos de un usuario al sistema.
- Modificar los permisos de utilización de un recurso del sistema a un usuario.
- Definir limitaciones de uso de un recurso del sistema a los usuarios.

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

CE4.1 Explicar los parámetros de configuración y funcionamiento de los dispositivos de comunicaciones para asegurar su funcionalidad dentro del sistema.

CE4.2 Relacionar los servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos con objeto de analizar y evaluar el rendimiento.

CE4.3 En un supuesto práctico en el que tomamos un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:

- Identificar los dispositivos de comunicaciones y describir sus características.
- Verificar el estado de los servicios de comunicaciones.
- Evaluar el rendimiento de los servicios de comunicaciones.
- Detectar y documentar las incidencias producidas en el sistema.

cve: BOE-A-2011-10055

Contenidos

1. **Seguridad y normativas en sistemas informáticos**
   - Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
   - Metodología ITIL Librería de infraestructuras de las tecnologías de la información
   - Ley orgánica de protección de datos de carácter personal.
   - Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

2. **Procesos de sistemas informáticos**
   - Identificación de procesos de negocio soportados por sistemas de información
   - Características fundamentales de los procesos electrónicos
     - □ Estados de un proceso,
     - □ Manejo de señales, su administración y los cambios en las prioridades
   - Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
   - Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
   - Técnicas utilizadas para la gestión del consumo de recursos

3. **Sistemas de almacenamiento de sistemas informáticos**
   - Tipos de dispositivos de almacenamiento más frecuentes
   - Características de los sistemas de archivo disponibles
   - Organización y estructura general de almacenamiento
   - Herramientas del sistema para gestión de dispositivos de almacenamiento

4. **Utilización de métricas e indicadores de monitorización de rendimiento de sistemas**
   - Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
   - Identificación de los objetos para los cuales es necesario obtener indicadores
   - Aspectos a definir para la selección y definición de indicadores
   - Establecimiento de los umbrales de rendimiento de los sistemas de información
   - Recolección y análisis de los datos aportados por los indicadores
   - Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

5. **Confección del proceso de monitorización de sistemas y comunicaciones**
   - Identificación de los dispositivos de comunicaciones
   - Análisis de los protocolos y servicios de comunicaciones
   - Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
   - Procesos de monitorización y respuesta
   - Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
   - Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
   - Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
   - Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

cve: BOE-A-2011-10055

6. **Selección del sistema de registro de en función de los requerimientos de la organización**
   - Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
   - Análisis de los requerimientos legales en referencia al registro
   - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
   - Asignación de responsabilidades para la gestión del registro
   - Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
   - Guía para la selección del sistema de almacenamiento y custodia de registros

7. **Administración del control de accesos adecuados de los sistemas de información**
   - Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
   - Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
   - Requerimientos legales en referencia al control de accesos y asignación de privilegios
   - Perfiles de de acceso en relación con los roles funcionales del personal de la organización
   - Herramientas de directorio activo y servidores LDAP en general
   - Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
   - Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0490_3	90	40

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: IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DOMÓTICOS/INMÓTICOS

Código: MF1219_3

Nivel de cualificación profesional: 3

cve: BOE-A-2011-10055

Asociado a la Unidad de Competencia:

UC1219_3 Implantar y mantener sistemas domóticos/inmóticos.

Duración: 150 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y PUESTA EN MARCHA DE UN PROYECTO DOMÓTICO / INMÓTICO

Código: UF1134

Duración: 80 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP3 excepto en lo referente a la configuración y conectividad de las pasarelas de comunicación.

Capacidades y criterios de evaluación

C1: Interpretar las especificaciones técnicas y funcionales de un proyecto de instalación y/o de integración de sistemas domóticos/inmóticos.

CE1.1 Describir los requisitos funcionales del proyecto domótico/inmótico, detallando los equipos y dispositivos involucrados en cada una de las funcionalidades.

CE1.2 Identificar las distintas tecnologías utilizadas en instalaciones de sistemas domóticos / inmóticos.

CE1.3 Distinguir y clasificar las distintas arquitecturas y medios de transmisión utilizados (par trenzado, vía radio, red eléctrica) en los sistemas domóticos.

CE1.4 Verificar los elementos que componen la instalación e infraestructura de un sistema domótico/inmótico para la puesta en servicio y su configuración, de acuerdo con las especificaciones funcionales del proyecto.

CE1.5 En un caso práctico, debidamente caracterizado, a partir de la documentación técnica que define el proyecto de instalación y/o integración de un sistema domótico/inmótico:

- Identificar los requisitos funcionales del proyecto.
- Identificar los elementos del sistema domótico/inmótico, tanto hardware como software.
- Identificar las distintas redes que forman el sistema domótico/inmótico.
- Comprobar que los elementos del sistema cumplen con los requisitos funcionales.
- Verificar visualmente la instalación.
- Documentar los trabajos realizados según unas especificaciones dadas.

C2: Identificar los parámetros funcionales de los equipos y dispositivos del sistema domótico/inmótico y, en un caso práctico, realizar su puesta en servicio, de acuerdo a las especificaciones técnicas del proyecto.

CE2.1 Identificar las características de los estándares y protocolos implicados en el sistema domótico/inmótico para su correcta configuración.

CE2.2 Describir las características técnicas y funcionales de los equipos y dispositivos del sistema domótico/inmótico, incluyendo el estándar domótico o sistema propietario al que pertenecen, identificando los parámetros de

cve: BOE-A-2011-10055

configuración e indicando el impacto que supone en un proyecto una modificación del mismo.
CE2.3 Configurar los componentes hardware y software del sistema domótico/inmótico, utilizando las herramientas específicas del sistema al que pertenecen.
CE2.4 En un caso práctico, debidamente caracterizado, configurar y parametrizar los equipos y dispositivos que forman el sistema domótico/inmótico, a poner en servicio, de acuerdo a especificaciones técnicas:
- Identificar los equipos y dispositivos del sistema domótico a implantar y poner en servicio.
- Configurar los elementos hardware y software del sistema domótico/inmótico utilizando las herramientas software propietarias.
- Probar la funcionalidad de los equipos del sistema.
- Elaborar un informe de puesta en marcha del sistema.

CE2.5 Interpretar la documentación inherente a los equipos y dispositivos, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.

C3: Identificar los parámetros y herramientas de configuración del software de control, y añadir nuevas funcionalidades al sistema domótico/inmótico, de acuerdo a especificaciones técnicas dadas.

CE3.1 Explicar las características y funcionalidades del software de configuración del sistema domótico/inmótico, en función de sus especificaciones técnicas.
CE3.2 Identificar los equipos y el software de control del sistema domótico/inmótico, con sus características y funcionalidades, incluyendo el estándar domótico o sistema propietario al que pertenecen.
CE3.3 Describir los parámetros de configuración de cada módulo del software de control del sistema domótico/inmótico, indicando el impacto que supone en un proyecto una modificación del mismo, teniendo en cuenta especificaciones técnicas y funcionales.
CE3.4 Identificar las herramientas de programación que proporcionan los sistemas domóticos/inmóticos, en función de los estándares domóticos y sistemas propietarios a los que pertenecen.
CE3.5 En un caso práctico, debidamente caracterizado, configurar el software de control y añadir nuevas funcionalidades al sistema domótico/inmótico, de acuerdo a especificaciones técnicas dadas:
- Verificar los equipos que van a contener el software de control.
- Instalar y configurar el software de control.
- Añadir nuevas funcionalidades utilizando las herramientas de programación o configuración propias del sistema.
- Aplicar técnicas de desarrollo para añadir las nuevas funcionalidades al sistema.
- Realizar pruebas para verificar las funcionalidades del software de control.
- Elaborar el informe de puesta en marcha siguiendo los formatos especificados.

Contenidos

1. Conceptos generales de la domótica / Inmótica
- Definición de conceptos relacionados con domótica.
- Aplicación de la domótica a la vivienda como parte del “hogar digital”.
- Descripción de las diferentes redes que forman un edificio y su integración con la domótica.
- Análisis del ámbito de aplicación y ejemplos de aplicación.
- Desarrollo histórico y estado actual de la domótica.
- Análisis de los actores Influyentes de la domótica.

cve: BOE-A-2011-10055

- Identificación de los organismos y asociaciones relacionados con la domótica.

2. Aplicación de Electricidad y Electrónica a los Sistemas Domóticos
- Relación de los conceptos y elementos electrónicos / eléctricos básicos.
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes (incluso en otros idiomas).
- Análisis de los sistemas de control básicos (autómatas) y su evolución hacia sistemas domóticos.

3. Estudio y Clasificación de los diferentes Sistemas Domóticos más representativos
- Clasificación de los sistemas domóticos según su medio de transmisión.
- Clasificación según su arquitectura.
- Clasificación según su Topología.
- Clasificación según su protocolo.
  - Sistemas estándar.
  - Sistemas Propietarios.
- Análisis, evaluación y acometida de un proyecto domótico:
  - Restricciones del protocolo y de su funcionalidad.
  - Restricciones propias de los aparatos y dispositivos.
  - Parámetros a evaluar del medio físico de comunicación (distancias, interferencias, atenuaciones, etc.).
  - Identificación de la problemática debida al medio y la localización del sistema (entorno).
  - Protecciones de los aparatos (Ips).
  - Valoración de la influencia del factor humano.

4. Elementos del Proyecto / Sistema domótico
- Descripción de los componentes HARDWARE (Dispositivos) del sistema domótico.
- Descripción y características del Medio de transmisión (soporte de comunicación) del sistema domótico.
- Análisis, descripción y características del SOFTWARE Programación y parametrización de los elementos del sistema domótico.
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas).
- Interpretación de un proyecto domótico.

5. Requisitos y necesidades del sistema domótico
- Definición de la topología de las instalaciones convencionales.
- Análisis de las necesidades de adaptación de las instalaciones a las nuevas tecnologías.
- Modificaciones y requisitos necesarios para integrar sistemas domóticos.
- Estudio de la aplicación de la normativa aplicable en instalaciones domóticas:
  - REBT “Reglamento Electrónico de Baja tensión”.
  - ICT “Infraestructura Común de Telecomunicaciones”.
  - Normativa Mundial y Europea.
- Análisis de la relación de las instalaciones domóticas y la actual normativa ICT.
  - Necesidades de normalización y reglamentación.
  - Adaptación para llegar a la IHD “Infraestructura del Hogar Digital”.

cve: BOE-A-2011-10055

6. **Funcionalidades y valores añadidos de la domótica**
   - Funcionalidad de las instalaciones previo a los sistemas domóticos.
   - Aportaciones y mejoras en seguridad.
   - Mejoras en el confort.
   - Eficiencia energética y control de recursos.
   - Comunicación y redes, ocio y multimedia.

7. **Control y gestión de un sistema domótico:**
   - Diseño de una visualización o unidad funcional de control y gestión del sistema.
   - Gestión de la climatización e iluminación.
   - Gestión inteligente de recursos: eficiencia energética.
   - Tratamiento de datos en la red domótica: horarios y eventos.
   - Definición y estudio de necesidades de escenas y macros en un sistema domótico.
   - Descripción y definición de los sistemas de captura de medidas y almacenamiento de datos, consumos e históricos en un sistema domótico.
   - Definición de las funciones lógicas y temporizaciones del sistema domótico.

8. **Simulación del desarrollo de un proyecto domótico siguiendo las pautas que se indiquen.**
   - Observación del proyecto de forma global: sistemas que involucra, dispositivos a instalar, espacios reservados, infraestructura, canalizaciones y conectividad de los elementos para hacerse a la idea del alcance del mismo.
   - Realización de un estudio previo de las necesidades, características y funcionalidades del proyecto a implantar. Comprobación que el sistema nos aporta todo lo que necesitamos.
   - Análisis de la solución propuesta e instalación física de los dispositivos y la totalidad de sus conexiones, tanto con el sistema domótico como con el resto de sistemas involucrados.
   - Programación del sistema domótico.
   - Comprobación de que el sistema funcione según exigencias del proyecto, y en caso contrario, aplicación de los métodos de detección y corrección de errores, para posteriormente volver a comprobar el sistema.
   - Realización del informe de la puesta en marcha y la documentación necesaria.

UNIDAD FORMATIVA 2

Denominación: CONECTIVIDAD DEL PROYECTO DOMÓTICO: REDES, SISTEMAS Y PROTOCOLOS DE COMUNICACIÓN; PASARELAS

Código: UF1135

Duración: 40 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP3 en lo referente a pasarelas de comunicación.

Capacidades y criterios de evaluación

C1: Dotar de comunicación (monodireccional o bidireccional) a una instalación domótica mediante la configuración y parametrización de las diferentes pasarelas, redes de comunicación y/o sistemas con los que se necesita interacción según las especificaciones y necesidades del proyecto técnico para permitir los servicios y funcionalidades allí definidos.

cve: BOE-A-2011-10055

CE1.1 Identificar las distintas redes del sistema así como las interconexiones entre los elementos de cada una de ellas y las necesidades de comunicación del sistema.
CE1.2 Explicar las características y funcionalidades de las pasarelas de comunicación identificando los diferentes tipos, tecnologías y parámetros de configuración y conexión del sistema domótico con las redes externas.
CE1.3 Describir los servicios que se pueden añadir al sistema domótico/inmótico a través de las pasarelas de comunicación.
CE1.4 En un caso práctico, debidamente caracterizado, configurar y parametrizar y poner en servicio las pasarelas que dotan al sistema domótico/inmótico de conectividad, de acuerdo a especificaciones técnicas.

Contenidos

1. **Relación de las redes de comunicación con la domótica**
   - Descripción de las diferentes redes de comunicación existentes en el mercado.
   - Evaluación de las necesidades del sistema según las indicaciones del proyecto.
   - Valoración de las posibilidades y ventajas de una vivienda / edificio inteligente con capacidad de comunicación bidireccional.

2. **Integración de la domótica con redes de comunicación y otras tecnologías a gestionar y / o monitorizar: Configuración de la/s pasarela/s:**
   - Red TCP/IP (WAN y LAN)
   - Red telefónica RTC
   - Red multimedia – Hogar Digital
   - Red GSM / GPRS
   - Redes PAN: BlueTooth
   - Red IR
   - Integración de cámaras y sistemas de seguridad
   - Tecnologías Inalámbricas
   - Sistemas de proximidad y control de acceso
   - Pasarelas a otras redes de gestión: Iluminación, Clima.
   - Sistemas de Interacción para personas con discapacidades o minusvalías. Parametrización de interfaces de control adaptado del entorno, avisos y vigilancia.
   - Otras tecnologías a considerar

UNIDAD FORMATIVA 3

Denominación: DOCUMENTACIÓN, MANTENIMIENTO Y GESTIÓN DE INCIENCIAS EN UN PROYECTO DOMÓTICO

Código: UF1136

Duración: 30 horas

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

Capacidades y criterios de evaluación

C1: Identificar los procedimientos y herramientas de gestión de inventarios, y elaborar y mantener el inventario del sistema domótico/inmótico siguiendo especificaciones dadas.

cve: BOE-A-2011-10055

CE1.1 Identificar los pasos que se deben seguir en el procedimiento de inventariado de un sistema domótico/inmótico, tanto durante su implantación inicial como durante su posterior mantenimiento.
CE1.2 Describir las características y funcionalidades de las herramientas software que se utilizan para la gestión de inventarios.
CE1.3 Describir los procedimientos de extracción de información a inventariar de los elementos que componen los sistemas domóticos/inmóticos, en función de sus especificaciones técnicas.
CE1.4 En un caso práctico, debidamente caracterizado, elaborar y mantener el inventario de los equipos y dispositivos que forman el sistema domótico/inmótico:
- Identificar los equipos y dispositivos, así como las configuraciones y software asociado a inventariar.
- Utilizar herramientas software específicas de gestión de inventarios.
- Registrar toda la información del sistema y los cambios que se produzcan en el inventario.
- Realizar pruebas para verificar las funcionalidades del software de control.
- Elaborar el informe de puesta en marcha siguiendo los formatos especificados.

C2: Elaborar y aplicar procedimientos de mantenimiento del sistema domótico/inmótico, teniendo en cuenta los criterios de calidad establecidos en el proyecto y las recomendaciones de fabricantes de los elementos que lo componen.
CE2.1 Identificar y detallar las operaciones de mantenimiento preventivo del sistema domótico/inmótico y de cada uno de los equipos y dispositivos que lo forman, en función de las especificaciones técnicas de los mismos.
CE2.2 Describir los procedimientos normalizados y las herramientas que se utilizan para localizar y solucionar las averías de los componentes del sistema domótico/inmótico, tanto a nivel hardware como software.
CE2.3 En un caso práctico, debidamente caracterizado, mantener el sistema domótico/inmótico de acuerdo a especificaciones técnicas dadas:
- Identificar las tareas de mantenimiento de los equipos y dispositivos implicados.
- Elaborar el plan de mantenimiento de cada uno de los elementos del sistema.
- Utilizar herramientas específicas para localizar averías hardware y software.
- Resolver las incidencias que se produzcan aplicando los procedimientos normalizados.
- Actualizar el manual de identificación y detección de incidencias.

Contenidos

1. Documentación de una instalación domótica/inmótica.
- Uso de Herramientas de generación de informes
- Verificación del estado final de la instalación y actualización del proyecto incluyendo las modificaciones respecto al proyecto original
- Desarrollo del Inventario final de dispositivos y aparatos: Software y Hardware
- Realización de una copia de seguridad y respaldo de configuraciones de los diferentes dispositivos y sistemas integrados en el proyecto.
- Creación y mantenimiento del libro de incidencias
- Creación del manual de usuario de la instalación
- Elaboración de la documentación correspondiente al proyecto que se indique

cve: BOE-A-2011-10055

2. **Mantenimiento de una instalación domótica/inmótica.**
   - Puesta a punto de la instalación y protocolo de pruebas.
   - Mantenimiento de un sistema domótico a Nivel Hardware
   - Mantenimiento de un sistema domótico a Nivel Software
   - Tele-mantenimiento (Programación y mantenimiento a distancia)
   - Mantenimiento de prevención de la instalación mediante gestión domótica.

3. **Gestión de incidencias en una instalación domótica/inmótica.**
   - Detección de fallos en un sistema domótico
   - Localización de problemática debida al hardware:
     - □ Fallo de Dispositivos o conexiones
     - □ Fallos en el medio de transmisión
     - □ Fallos originados por el entorno y la localización del sistema
   - Localización de problemática debida al software:
     - □ Fallos de comunicación y protocolo
     - □ Fallos de funcionalidad
     - □ Estados no evaluados previamente
   - Solución: Procedimientos y recomendaciones para reponer dispositivos (o añadirlos) en la instalación
   - Solución: Procedimientos y recomendaciones para actualizar, modificar software o firmware en la instalación

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Unidades formativa 1 – UF1134	80	30
Unidades formativa 2 – UF1135	40	10
Unidades formativa 3 - UF1136	30	20

Secuencia

Para acceder a la unidad formativa 2 debe haberse superado la unidad formativa 1.
Para acceder a la unidad formativa 3 debe haberse superado la unidad formativa 2.

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 3

Denominación: IMPLANTACIÓN Y MANTENIMIENTO DE SISTEMAS DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEO VIGILANCIA

Código: MF1220_3

cve: BOE-A-2011-10055

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC1220_3 Implantar y mantener sistemas de control de accesos y presencia, y de videovigilancia.

Duración: 220 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE VIDEO VIGILANCIA Y SEGURIDAD

Código: UF1137

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 en lo referente a videovigilancia y con la RP3.

Capacidades y criterios de evaluación

C1: Interpretar las especificaciones técnicas y funcionales del proyecto de instalación del sistema de videovigilancia, así como del análisis de riesgo identificando la información necesaria para llevar a cabo su implantación.

CE1.1 Describir las características y especificaciones técnicas del proyecto de instalación del sistema de videovigilancia.

CE1.2 Explicar las características, funciones y elementos del análisis de riesgo para llevar a cabo la implantación de un sistema de videovigilancia teniendo en cuenta las especificaciones técnicas del proyecto.

CE1.3 Describir las técnicas de planificación de proyectos necesarias para llevar a cabo la implantación del sistema: recursos humanos, plazos de entrega, costes establecidos y justificación de variaciones entre otros.

CE1.4 En un caso práctico, a partir de la documentación técnica que define el proyecto de instalación de videovigilancia, debidamente caracterizado, identificar y describir:

- La ubicación de los equipos y dispositivos de los distintos subsistemas.
- Los medios y herramientas necesarios para aplicar los procesos de implementación.
- El sistema de distribución de energía, los elementos de protección y el sistema de alimentación ininterrumpida.
- Las envolventes, cuadros, armarios y elementos del cableado.
- El tipo de canalizaciones y su distribución en plantas, distribución horizontal y vertical.
- Las características de los cableados y conexionado de los elementos.
- Los sistemas de identificación y señalización de conductores y de los elementos de conexión de los equipos presentes en la instalación.
- Los equipos informáticos y periféricos utilizados para la administración del sistema.
- La aplicación informática de configuración, gestión y supervisión de los subsistemas, así como los controladores (manejadores de dispositivos o drivers) debidamente actualizados.

C2: Identificar la infraestructura y verificar la instalación del sistema de videovigilancia para su implantación, de acuerdo a especificaciones técnicas.

cve: BOE-A-2011-10055

CE2.1 Identificar los equipos, dispositivos y elementos que componen la infraestructura del sistema de videovigilancia, así como las conexiones con otros sistemas o redes de comunicación.
CE2.2 Describir la interconexión entre los recintos de cableado y/o entre los edificios donde se encuentran los equipos del sistema de videovigilancia.
CE2.3 Explicar técnicas de ajuste físico de los equipos, dispositivos y elementos que componen la infraestructura del sistema de videovigilancia, así como las conexiones con otros sistemas o redes de comunicación.
CE2.4 Explicar la necesidad de integrar el sistema de videovigilancia.
CE2.5 En un caso práctico, debidamente caracterizado, verificar la instalación del sistema de videovigilancia, según especificaciones técnicas del proyecto:
- Identificar los equipos y dispositivos que componen los sistemas.
- Comprobar las conexiones eléctricas y de cableado entre equipos y dispositivos.
- Verificar el ajuste de los equipos y dispositivos de los sistemas.
- Documentar los trabajos realizados según formatos especificados.

C3: Poner en servicio los equipos y dispositivos del sistema de videovigilancia, así como sus aplicaciones y configuraciones, teniendo en cuenta las especificaciones técnicas asociadas.
CE3.1 Describir las características y funcionalidades de los dispositivos y equipos que forman el sistema de videovigilancia, identificando sus parámetros de configuración.
CE3.2 Identificar las funciones principales que realiza el sistema informático que se utiliza para la gestión y supervisión del sistema de videovigilancia.
CE3.3 Explicar las características y funcionalidades de las aplicaciones de control, gestión y planimetría que se utilizan en el sistema de videovigilancia, identificando los parámetros de instalación y configuración.
CE3.4 Describir la funcionalidad de la aplicación software que centraliza el control del sistema de videovigilancia, identificando los parámetros de instalación y configuración.
CE3.5 Citar la legislación sobre protección de datos a la hora de tratar la información registrada y grabada en el sistema de videovigilancia.
CE3.6 Describir la funcionalidad de las herramientas de generación de copias de seguridad que se utilizan en los sistemas de videovigilancia, identificando los parámetros de instalación y configuración.
CE3.7 En un caso práctico, debidamente caracterizado, de poner en servicio el sistema de videovigilancia, de acuerdo a las especificaciones del proyecto:
- Identificar los dispositivos y equipos del sistema de videovigilancia.
- Configurar el sistema informático.
- Instalar las aplicaciones software de todo el sistema de videovigilancia.
- Configurar los parámetros del sistema de CCTV en las controladoras.
- Configurar los parámetros del sistema de CCTV en los servidores de grabación.
- Probar la funcionalidad del sistema.
- Elaborar el plan de documentación a través del diario de Ingeniería
- Elaborar el documento de seguridad teniendo en cuenta las normas marcadas por la LOPD.

CE3.8 Interpretar la documentación inherente a los equipos y dispositivos, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.

cve: BOE-A-2011-10055

Contenidos

1. **Sistemas de videovigilancia**
   - Definición de sistemas de CCTV y video vigilancia
   - Aplicación de los sistemas de video a la seguridad
   - Identificación de los principales campos de aplicación mediante el estudio de casos reales
   - Descripción de la evolución de los sistemas de video vigilancia

2. **Video y tratamiento de la imagen**
   - Definición de los conceptos de luz, imagen y video
   - Descripción de los tipos de lentes y sus características principales
   - Análisis de la señal de video e imagen analógica
     - □ Formación, tratamiento y transmisión de la imagen analógica
     - □ Características y formatos de video analógico
     - □ Ventajas e inconvenientes del video analógico
   - Análisis de la señal de video e imagen Digital
     - □ Formación, tratamiento y transmisión de la imagen digital
     - □ Características y formatos de video analógico
     - □ Ventajas e inconvenientes del video digital
   - Parámetros de evaluación de las señales de video

3. **Sistemas de Video Vigilancia y seguridad Analógicos**
   - Hardware: cámaras y dispositivos de sistema
   - Soporte, cableado y topología del sistema analógico de video vigilancia
   - Configuración, métodos de gestión y visualización en sistemas analógicos
   - Topología, escalabilidad e Infraestructura de un sistema analógico
   - Características del sistema analógico

4. **Sistemas de Video Vigilancia y seguridad Digitales**
   - Hardware: cámaras y dispositivos de sistema
   - Soporte, cableado, tecnologías de transporte y topología del sistema digital de video vigilancia
   - Configuración, métodos de gestión y visualización en sistemas digitales
   - Topología, escalabilidad e Infraestructura de un sistema digital
   - Características del sistema digital y conectividad con otras redes
   - Integración analógica en el mundo digital: Sistemas mixtos

5. **Almacenamiento de la Información obtenida**
   - Sistemas de almacenamiento en formato analógico
   - Sistemas de almacenamiento formato digital
   - Dimensionado del sistema de almacenamiento en función de los requerimientos del proyecto
   - Protección y seguridad de los datos e información aportada por el sistema:
     - □ Protección mediante un sistema de alimentación ininterrumpida los dispositivos de toda la instalación de video vigilancia
     - □ Copias de seguridad y sistemas de prevención de pérdidas de datos
     - □ Redundancia
     - □ Acceso protegido y gestión de privilegios en los sistemas de videovigilancia
     - □ Autentificación de la información. Marca de Agua
     - □ Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

cve: BOE-A-2011-10055

6. Funcionalidades y Gestión del sistema de Video Vigilancia

- Métodos de Grabación
  - □ A demanda
  - □ Planificada
  - □ Continua
  - □ Por eventos
  - □ Detección de movimiento
- Configuraciones de visualización
- Búsqueda inteligente de eventos
- Generación de eventos
- Seguridad: Gestión de alertas y avisos; Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
- Análisis, proceso y obtención de información relevante: Video Inteligente: Video procesado por herramientas de software informático:
  - □ Conteo de personas
  - □ Reconocimiento Facial
  - □ Seguimiento de objetos y personas
  - □ Lector de Matriculas
  - □ Avisos sobre objetos que desaparecen / aparecen
  - □ Análisis de trayectorias y recorridos
  - □ Obtención de informes y estadísticas
  - □ Detección de situaciones anómalas
  - □ Procesado de Imagen
  - □ Otras

7. Planificación del proceso de acometida e implantación de un proyecto de video vigilancia

- Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de video vigilancia
  - □ Restricciones de los sistemas y de funcionalidad
  - □ Limitaciones de los dispositivos de captación de video, transmisión de video, comunicación y almacenamiento.
  - □ Problemática del medio de comunicación (distancias, interferencias, atenuaciones, etc.)
  - □ Problemática debida al medio y la localización del sistema (entorno)
  - □ Protecciones de los aparatos (Ips)
  - □ Factor Humano
- Evaluación de los niveles de riesgo y tipos de amenazas
- Evaluación de las necesidades de vigilancia y nivel de protección
- Análisis de la situación: ¿Qué hay que vigilar?
- Planteamiento: ¿Cómo y cuándo vigilar? ¿Desde dónde vigilar? ¿Quién ha de vigilar?
- Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
- Planteamiento de las funcionalidades del sistema
- Integración con otros sistemas y redes: reacciones y posibilidades ante una detección o evento
- Criterios de selección del dispositivos
- Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
- Estimación de tiempos de ejecución, recursos y personal necesario
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
- Comprobación del cumplimiento de la Normativa y reglamentación sobre Seguridad Privada y Ley Orgánica de Protección de Datos

cve: BOE-A-2011-10055

- Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
- Documentación generada o utilizada en el proceso:
  - □ Usada:
    - Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
    - Proyecto de las instalaciones a Vigilar
    - Normativa técnica
    - Normativa legal aplicada
  - □ Generada
    - Informe de puesta en marcha
    - Libro de seguimiento e incidencias
    - Reflejo fiel del estado final de la instalación
    - Informe de configuración del sistema
    - Informe de seguridad acorde con la LOPD

8. **Simulación del desarrollo de un proyecto de videovigilancia siguiendo las pautas que se indiquen**
   - Observación del proyecto de forma global: sistemas que involucra, dispositivos a instalar, espacios reservados, infraestructura, canalizaciones y conectividad de los elementos para hacerse a la idea del alcance del mismo.
   - Realización de un estudio previo de las necesidades, características y funcionalidades del proyecto a implantar. Comprobación que el sistema nos aporta todo lo que necesitamos.
   - Análisis de la solución propuesta e instalación física de los dispositivos y la totalidad de sus conexiones, tanto con el sistema de videovigilancia como con el resto de sistemas involucrados
   - Parametrización y ajuste del sistema de videovigilancia
   - Comprobación de que el sistema funcione según exigencias del proyecto, y en caso contrario, aplicación de los métodos de detección y corrección de errores, para posteriormente volver a comprobar el sistema.
   - Realización del informe de la puesta en marcha y la documentación necesaria

UNIDAD FORMATIVA 2

Denominación: INSTALACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE CONTROL DE ACCESOS Y PRESENCIA

Código: UF1138

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 en lo referente a control de accesos y presencia y con la RP2.

Capacidades y criterios de evaluación

C1: Interpretar las especificaciones técnicas y funcionales de un proyecto de instalación de sistemas de control de accesos y presencia así como del análisis de riesgo identificando la información necesaria para llevar a cabo su implantación.

CE1.1 Describir las características y especificaciones técnicas del proyecto de instalación del sistema de control de accesos y presencia.

CE1.2 Explicar las características, funciones y elementos del análisis de riesgo para llevar a cabo la implantación y el mantenimiento de un sistema de control de accesos y presencia teniendo en cuenta las especificaciones técnicas del proyecto.

cve: BOE-A-2011-10055

CE1.3 Describir las técnicas de planificación de proyectos necesarias para llevar a cabo la implantación del sistema: recursos humanos, plazos de entrega, costes establecidos y justificación de variaciones entre otros.

CE1.4 En un caso práctico, a partir de la documentación técnica que define el proyecto de instalación y mantenimiento de un sistema de control de accesos y presencia, debidamente caracterizado, identificar y describir:

- La ubicación de los equipos y dispositivos de los distintos subsistemas.
- Los medios y herramientas necesarios para aplicar los procesos de implementación.
- El sistema de distribución de energía, los elementos de protección y el sistema de alimentación ininterrumpida.
- Las envolventes, cuadros, armarios y elementos del cableado.
- El tipo de canalizaciones y su distribución en plantas, distribución horizontal y vertical.
- Las características de los cableados y conexionado de los elementos.
- Los sistemas de identificación y señalización de conductores y de los elementos de conexión de los equipos presentes en la instalación.
- Los equipos informáticos y periféricos utilizados para la administración del sistema.
- La aplicación informática de configuración, gestión y supervisión de los drivers debidamente actualizados.

C2: Identificar la infraestructura y verificar la instalación de los sistemas de control de accesos y presencia para su implantación, de acuerdo a especificaciones técnicas.

CE2.1 Identificar los equipos, dispositivos y elementos que componen la infraestructura de los sistemas de control de accesos y presencia así como las conexiones con otros sistemas o redes de comunicación.

CE2.2 Describir la interconexión entre los recintos de cableado y/o entre los edificios donde se encuentran los equipos del sistema de control de accesos y presencia.

CE2.3 Explicar técnicas de ajuste físico de los equipos, dispositivos y elementos que componen la infraestructura de los sistemas de control de accesos y presencia así como las conexiones con otros sistemas o redes de comunicación.

CE2.4 Explicar la necesidad de integrar el sistema de control de accesos y presencia.

CE2.5 En un caso práctico, debidamente caracterizado, verificar la instalación de los sistemas de control de accesos y presencia, y de videovigilancia, según especificaciones técnicas del proyecto:

- Identificar los equipos y dispositivos que componen los sistemas.
- Comprobar las conexiones eléctricas y de cableado entre equipos y dispositivos.
- Verificar el ajuste de los equipos y dispositivos de los sistemas.
- Documentar los trabajos realizados según formatos especificados.

C3: Poner en servicio los equipos y dispositivos del sistema de control de accesos y presencia, así como sus aplicaciones y configuraciones, teniendo en cuenta las especificaciones técnicas asociadas.

CE3.1 Describir las características y funcionalidades de los dispositivos y equipos que forman el sistema de control de accesos y presencia, identificando sus parámetros de configuración.

CE3.2 Identificar las funciones principales que realiza el sistema informático que se utiliza para la gestión y supervisión del sistema de control de accesos y presencia.

CE3.3 Explicar las características y funcionalidades de las aplicaciones software del sistema de control de accesos y presencia, tanto el software que centraliza

cve: BOE-A-2011-10055

el sistema como el software de control y gestión de usuarios, identificando sus parámetros de instalación y configuración.
CE3.4 Programar y parametrizar los terminales de control de accesos y presencia, y sus elementos biométricos, siguiendo prescripciones técnicas del proyecto.
CE3.5 Explicar los procesos de carga inicial del sistema de control de accesos y presencia.
CE3.6 Describir la funcionalidad de las herramientas de generación de copias de seguridad que se utilizan en los sistemas de control de accesos y presencia, identificando los parámetros de instalación y configuración.
CE3.7 Realizar consultas e informes de la información registrada en el sistema de control de accesos y presencia, utilizando herramientas específicas propias del sistema, teniendo en cuenta la legislación sobre protección de datos.
CE3.8 En un caso práctico, debidamente caracterizado, poner en servicio el sistema de control de accesos y presencia, de acuerdo a especificaciones técnicas del proyecto:
- Identificar los dispositivos y equipos del sistema.
- Configurar el sistema informático.
- Instalar las aplicaciones software de todo el sistema de control de accesos y presencia.
- Configurar los parámetros del sistema de control de accesos en las controladoras y terminales de control de accesos.
- Configurar los parámetros del sistema de control de accesos en los servidores.
- Configurar los parámetros del sistema de control de accesos en los portillones.
- Probar la funcionalidad del sistema.
- Elaborar el plan de documentación a través del diario de ingeniería.
- Elaborar el documento de seguridad teniendo en cuenta las normas marcadas por la LOPD.

CE3.9 Interpretar la documentación inherente a los equipos y dispositivos, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda.

Contenidos

1. **Sistemas de control de acceso y presencia**
   - Definición de los sistemas de control de acceso y presencia. Características más importantes.
   - Valoración de las necesidades y razones para la integración de un sistema de control de accesos y presencia
   - Identificación de los principales campos de aplicación mediante el estudio de casos reales

2. **Componentes y características de los sistemas y dispositivos que forman el control de acceso y presencia.**
   - Sistemas mecánicos automatizados integrados en la gestión de accesos
     - □ Electro cerraduras
     - □ Puertas y Barreras
     - □ Torniquetes y Tornos
     - □ Rampas y Elevadores
     - □ Sistemas diseñados para minusválidos
     - □ Otros tipos de activaciones o eventos
   - Dispositivos, Sistemas y tecnologías de identificación / autentificación
     - □ Relojes de control y / o tarificación
     - □ Teclados: Códigos y contraseñas de acceso

cve: BOE-A-2011-10055

- □ Lectores de tarjeta
  - Códigos de barra
  - Banda Magnética
- □ Lectores de proximidad
  - Tarjetas o chips de proximidad. Tecnología RFID
  - Bluetooth
  - Otras
- □ Sensores Biométricos e Identidad biométrica; Como identificar a través de rasgos y factores únicos en cada persona
  - Lector de Huella digital
  - Lector de Palma o estructura de la mano
  - Reconocimiento Facial
  - Reconocimiento del Iris
  - Reconocimiento de retina
  - Sistemas de reconocimiento de voz

- Dispositivos, Software y datos de control del sistema
  - □ Hardware de control e integración de sistema
  - □ Conectividad y cableado. Infraestructura, funcionamiento y topología de los sistemas de control de acceso y presencia
  - □ Punto de gestión y monitorización del sistema:
    - Configuración y parametrización del sistema
    - Solución Hardware o Software.
    - Herramientas de extracción de informes
    - Software de tratamiento de datos.
    - Bases de datos e información de control

3. Funcionalidades y Aplicaciones de los sistemas de control de acceso y presencia

- Control, monitorización y gestión de prioridades de acceso en instalaciones, identificación de las personas y datos relevantes que acceden, conocer el estado de los accesos y tener la posibilidad de gestionarlos.
- Control de horarios y eficiencia en empresas o procesos productivos.
- Tratamiento de datos:
  - □ Generación de estadísticas y datos de ocupación
  - □ Tarificación de servicios y tiempos
- Sistemas de localización, control y detección de personas en un entorno cerrado; control de errantes no intrusivo
- Sistemas de control médico, acceso a datos y posibilidad de actualización de información automatizado. (Aplicable o otros procesos similares)
- Gestión de alarmas y eventos
  - □ Accesos no deseados
  - □ Alertas no permitidos o fuera de horario
  - □ Alarmas de averías o mal funcionamiento del sistema
  - □ Interacción con otros sistemas y/o redes de comunicación o CRA (Centrales receptoras de alarmas)
- Soluciones de control logístico y de distribución
- Soluciones de Gestión de Asistencia a Eventos

4. Protección y seguridad del sistema y de los datos e información aportada por el sistema:

- Protección, mediante un sistema de alimentación ininterrumpida, de los dispositivos de toda la instalación de control de accesos y presencia
- Copias de seguridad y sistemas de prevención de pérdidas de datos
- Redundancia

cve: BOE-A-2011-10055

- Acceso protegido y gestión de privilegios en los sistemas de gestión y monitorización del sistema de control de accesos y presencia
  - □ Copias seguridad actualizadas de la información de control del sistema. Accesos, zonas de vigilancia, Bases de datos, horarios, etc.

5. Proceso de acometida e implantación de un proyecto de control de accesos y presencia

- Evaluación de las recomendaciones y puntos clave previos a acometer un proyecto de control de accesos y presencia
  - □ Restricciones de los sistemas y de su funcionalidad
  - □ Problemática del medio de comunicación (número máximo de dispositivos, distancias, interferencias, atenuaciones, etc.)
  - □ Problemática debida al medio y la localización del sistema (entorno)
  - □ Protecciones de los aparatos (Ips)
  - □ Factor Humano
- Evaluación de los niveles de riesgo y tipos de amenazas
- Evaluación de las necesidades y definición del servicio y funcionalidades a implantar
- Interpretación y evaluación del proyecto y la infraestructura necesaria para acometerlo
- Estimación de tiempos de ejecución, recursos y personal necesario
- Interpretación de manuales así como de las características y funciones de los aparatos proporcionados por los fabricantes. (incluso en otros idiomas)
- Análisis de la situación: ¿Qué accesos hay que controlar?
- Planteamiento y planificación: ¿Cómo y cuándo se controlan? ¿Desde dónde controlar y gestionar el sistema?
- Estructuración del sistema y búsqueda de la ubicación optima de los dispositivos
- Planteamiento de las funcionalidades del sistema
- Integración con otros sistemas y redes: Reacciones y posibilidades ante una detección o evento
- Comprobación el cumplimiento de la normativa y reglamentación sobre seguridad privada y Ley Orgánica de Protección de Datos
- Configuración del sistema y puesta en marcha tanto del software como del hardware, según las especificaciones y funcionalidades requeridas.
- Documentación generada o utilizada en el proceso:
  - □ Usada:
    - Proyecto: memoria, planos, pliego de condiciones y requisitos necesarios
    - Proyecto de las instalaciones a controlar
    - Normativa técnica
    - Normativa legal aplicada
  - □ Generada
    - Informe de puesta en marcha
    - Libro de Seguimiento e incidencias
    - Reflejo fiel del estado final de la instalación
    - Informe de Configuración del sistema
    - Informe de seguridad acorde con la LOPD

6. Simulación del desarrollo de un proyecto de control de accesos y presencia siguiendo las pautas que se indiquen

- Observación del proyecto de forma global: sistemas que involucra, dispositivos a instalar, espacios reservados, infraestructura, canalizaciones y conectividad de los elementos para hacerse a la idea del alcance del mismo.

cve: BOE-A-2011-10055

- Realización de un estudio previo de las necesidades, características y funcionalidades del proyecto a implantar. Comprobación que el sistema nos aporta todo lo que necesitamos.
- Análisis de la solución propuesta e instalación física de los dispositivos y la totalidad de sus conexiones, tanto con el sistema de control de accesos como con el resto de sistemas involucrados
- Parametrización y ajuste del sistema de control de accesos
- Comprobación de que el sistema funcione según exigencias del proyecto, y en caso contrario, aplicación de los métodos de detección y corrección de errores, para posteriormente volver a comprobar el sistema.
- Realización del informe de la puesta en marcha y la documentación necesaria

UNIDAD FORMATIVA 3

Denominación: MANTENIMIENTO Y GESTIÓN DE INCIDENCIAS EN PROYECTOS DE VIDEO VIGILANCIA, CONTROL DE ACCESOS Y PRESENCIA

Código: UF1139

Duración: 40 horas

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

Capacidades y criterios de evaluación

C1: Describir los procedimientos de mantenimiento y resolver las incidencias de los sistemas de control de accesos y presencia, y de videovigilancia, para mantener operativo el sistema.

CE1.1 Describir los procesos de mantenimiento de los equipos y dispositivos que forman los sistemas de control de accesos y detección de presencia, y de videovigilancia identificando los parámetros de funcionalidad óptima.

CE1.2 Elaborar y actualizar los procedimientos de mantenimiento estableciendo el número de revisiones preventivas y las acciones a realizar en cada revisión del sistema.

CE1.3 Identificar nuevas funcionalidades y mejoras de los componentes hardware y software de los sistemas de control de accesos y detección de presencia, y de videovigilancia que existen en el mercado, para proponer actualizaciones compatibles.

CE1.4 Clasificar la tipología y características de las averías de naturaleza física y lógica que se presentan en los sistemas de control de accesos y detección de presencia, y de videovigilancia.

CE1.5 Describir las técnicas generales y los medios técnicos específicos necesarios para la localización de averías de naturaleza física y lógica en los sistemas de control de accesos y detección de presencia, y de videovigilancia.

CE1.6 En varios casos prácticos simulados, debidamente caracterizados, para el diagnóstico, localización y resolución de averías en los sistemas de control de accesos y presencia, y de videovigilancia:

- Interpretar la documentación del sistema, identificando los distintos bloques funcionales y componentes específicos que lo componen.
- Identificar los síntomas de la avería caracterizándola por los efectos que produce.
- Realizar un plan de intervención en el sistema para determinar la causa o causas que producen la avería.

cve: BOE-A-2011-10055

- Localizar el elemento (físico o lógico) responsable de la avería y realizar la sustitución (mediante la utilización de componentes similares o equivalentes) o modificación del elemento, configuración y/o programa, aplicando los procedimientos requeridos y en un tiempo adecuado.
- Realizar las comprobaciones, modificaciones y ajustes de los parámetros del sistema, según las especificaciones de la documentación técnica del mismo, utilizando las herramientas apropiadas, que permitan su puesta a punto en cada caso.
- Elaborar un informe-memoria de las actividades desarrolladas y resultados obtenidos, estructurándolo en los apartados necesarios para una adecuada documentación de las mismas (descripción del proceso seguido, medios utilizados, medidas, explicación funcional y esquemas).

Contenidos

1. Procesos de mantenimiento en sistemas de videovigilancia

- Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
  - □ Mantenimiento de cámaras y dispositivos hardware de tratamiento de video
  - □ Comprobación de dispositivos de interconexión, sujeción, cableado e infraestructura de monitorización y control
  - □ Mantenimiento de sistemas de almacenamiento
  - □ Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
- Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento del software del sistema. Verificación de que funciona según los requisitos especificados
  - □ Comprobación del funcionamiento del software de gestión, visualización, grabación y tratamiento de datos del sistema de videovigilancia
  - □ Comprobación de la correcta parametrización a nivel software de los dispositivos del sistema: cámaras, servidores, comunicación, etc.
  - □ Actualización en caso necesario del software de gestión
  - □ Comprobación del sistema de copias de seguridad y el acceso a información del sistema.
  - □ Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
  - □ Actualización del firmware de los dispositivos que lo requieran
- Comprobación del correcto funcionamiento de integración con los sistemas y redes de comunicación conectados y certificación del cumplimiento de la Ley Orgánica de protección de datos y normativas técnicas.
  - □ Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
    - Pasarelas de comunicación
    - Módulos de entradas y salidas interconectadas entre sistemas
  - □ Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
  - □ Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
- Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
- Comprobar que el personal al cargo hace un correcto uso del sistema, en caso negativo, aconsejar alternativas correctas, enseñar o referencias a los manuales de manejo.

cve: BOE-A-2011-10055

2. **Incidencias y alertas en proyectos de video vigilancia**
   - Incidencias de fallos en hardware: Proceso de reinstalación de dispositivos averiados
   - Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
   - Tratamiento de errores o alertas de mal funcionamiento.
     - □ Sistemas y herramientas de detección de errores, tanto a nivel de hardware como software
     - □ Procesos de depuración y reconfiguración del sistema
     - □ Prueba y puesta en marcha de la nueva configuración del sistema
   - Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
     - □ Cambio de escenario a vigilar debido a muebles, árboles, arbustos u otros obstáculos físicos para el correcto funcionamiento del sistema.
     - □ Alteración de la estructura a vigilar. Procesos de reposicionamiento y nueva configuración del sistema
     - □ Gestión de cambios en la configuración requerida por la dirección del lugar
   - Avisos, Gestión y modificaciones en remoto del sistema de video vigilancia
   - Generación de la nueva documentación o actualización de la documentación ya existente tras las operaciones de gestión de incidencias
   - Actualización y mejora del estado del sistema de videovigilancia
   - Evaluación del estado del sistema
   - Propuestas de mejora del sistema
   - Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de video vigilancia

3. **Procesos y tareas de mantenimiento en sistemas de control de accesos y presencia**
   - Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento de los dispositivos hardware del sistema.
     - □ Mantenimiento mecánico de los dispositivos físicos de control de accesos: Barreras, puertas, tornos y resto de dispositivos mecánicos del sistema
     - □ Mantenimiento eléctrico y electrónico de las automatizaciones de control: Cerraduras, tarjetas y componentes electrónicos e informáticos del sistema
     - □ Comprobación de los sistemas de identificación y autentificación: Verificar funcionamiento y funcionalidad de teclados, lectores de tarjetas, proximidad, biométricos y resto de dispositivos identificación y autentificación
     - □ Comprobación de Dispositivos de interconexión, sujeción, Cableado e infraestructura de monitorización, avisos y control
     - □ Mantenimiento de Soporte del sistema de Gestión y almacenamiento de datos
     - □ Mantenimiento de los Sistemas de protección y alimentación ininterrumpida o SAI.
   - Definición de las tareas y procesos de mantenimiento e inspección del correcto funcionamiento del software del sistema. Verificación de que funciona según los requisitos especificados
     - □ Comprobación del funcionamiento del software de gestión, monitorización y herramientas de tratamiento de datos, creación de informes y estadísticas, etc. Para que funcionen según las especificaciones de proyecto
     - □ Comprobación la correcta parametrización a nivel software de los dispositivos del sistema
     - □ Actualización en caso necesario del software de gestión
     - □ Comprobación del sistema de copias de seguridad y el acceso a información del sistema.

cve: BOE-A-2011-10055

- □ Comprobación del sistema de seguridad, nivel de privilegios y protección del sistema
- □ Actualización del firmware de los dispositivos que lo requieran

- Comprobación del correcto funcionamiento de integración con los sistemas y redes de comunicación conectados y certificación del cumplimiento de la Ley Orgánica de protección de datos y normativas técnicas.
  - □ Mantenimiento del hardware y dispositivos físicos de comunicación o integración con otras redes:
    - Pasarelas de comunicación
    - Módulos de entradas y salidas interconectadas entre sistemas
  - □ Pruebas y protocolos de evaluación y correcto funcionamiento de la comunicación a nivel software
  - □ Actualizar el sistema para seguir cumpliendo con la normativa técnica y legal en el momento de realizar el mantenimiento en caso de necesitarla
- Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de mantenimiento
- Comprobación que el personal al cargo hace un correcto uso del sistema, en caso negativo, aconsejar alternativas correctas, enseñar o referencias a los manuales de manejo.

4. Gestión de incidencias y alertas

- Incidencias de fallos en hardware: Proceso de Re instalación de dispositivos averiados
- Incidencias de fallos en Software: Proceso de reconfiguración / actualización / sustitución del software de gestión.
- Tratamiento de errores o alertas de mal funcionamiento.
  - □ Sistemas y herramientas de Detección de errores, tanto a nivel de hardware como software
  - □ Procesos de Depuración y reconfiguración del sistema
  - □ Prueba y puesta en marcha de la nueva configuración del sistema
- Incidencias de Modificación del entorno. Adaptación a las nuevas configuraciones.
  - □ Alteración de la estructura a controlar. Procesos de reposicionamiento y nueva configuración del sistema
  - □ Gestión de cambios en la configuración requerida por la dirección del lugar
- Avisos, Gestión y modificaciones en remoto del sistema de control de accesos y presencia
- Generación de la nueva documentación o Actualización de la documentación ya existente tras las operaciones de gestión de incidencias
- Actualización y mejora del estado del sistema de control de accesos
- Evaluación del estado del sistema
- Propuestas de mejora del sistema
- Aplicación de nuevas funcionalidades: Procesos para la actualización / ampliación / integración del sistema de control de accesos

Orientaciones metodológicas

Formación a distancia:

Unidades formativas	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Unidades formativa 1 – UF1137	90	40
Unidades formativa 2 – UF1138	90	40
Unidades formativa 3 – UF1139	40	20

cve: BOE-A-2011-10055

Secuencia

Para acceder a la unidad formativa 3 debe haberse superado la unidad formativa 1 y la 2.

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 DE PRÁCTICAS PROFESIONALES NO LABORALES IMPLANTACIÓN Y GESTIÓN DE ELEMENTOS INFORMÁTICOS EN SISTEMAS DOMÓTICOS/ INMÓTICOS, DE CONTROL DE ACCESOS Y PRESENCIA, Y DE VIDEOVIGILANCIA

Código: MP0236

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Analizar un proyecto de domótica e inmótica, de video vigilancia, y control de accesos y presencia en un caso real.

CE1.1 Analizar los distintos protocolos y procesos llevados a cabo desde el planteamiento inicial de un proyecto hasta su finalización, poniendo especial atención en la forma profesional de realizar todas las operaciones implicadas en el proceso. Tanto desde el punto de vista de hardware (conexiones, empalmes, distribución inteligente de aparatos, precauciones a tomar, etc.) como software, métodos de programación, formas de mejorar la eficiencia de la instalación, etc.
CE1.2 Identificar los dispositivos o los sistemas con los que trabaje la empresa y saber concretar su ámbito de aplicación y las funcionalidades que aportan al proyecto.
CE1.3 Justificar el diseño y la documentación de un proyecto nuevo, ya sea de Domótica y/o Video Vigilancia y/o Control de Accesos y Presencia.
CE1.4 Identificar el conexionado físico de una instalación de acuerdo con la documentación de proyecto.
CE1.5 Participar en la programación de los distintos dispositivos, recibiendo información tutelada mientras se lleva a cabo la puesta a punto de una instalación real.

C2: Proporcionar soporte técnico y gestionar la incidencias en sistemas de Domótica, Video Vigilancia, y Control de Accesos y Presencia.

CE2.1 Reconocer un sistema instalado y en funcionamiento, identificar los diferentes dispositivos que lo componen y la topología que conforman.
CE2.2 Analizar la infraestructura del sistema, las canalizaciones y cableados de alimentación y comunicación de los diferentes dispositivos que forman el sistema.
CE2.3 Detectar el origen de un mal funcionamiento, así como identificar los métodos de reparación realizando las operaciones de sustitución, reconfiguración o integración que fuesen necesarias.
CE2.4 Realizar las tareas de mantenimiento y supervisión periódicas necesarias para el correcto funcionamiento de los sistemas instalados, ayudando a redactar la documentación necesaria.

cve: BOE-A-2011-10055

C3: Actualizar, ampliar e integrar nuevos sistemas o funcionalidades en instalaciones existentes

CE3.1 Aprender a evaluar el impacto que produce en una instalación existente la implementación de un nuevos sistemas o funcionalidades.
CE3.2 Evaluar las necesidades de infraestructura al implementar nuevos sistemas en instalaciones existentes.
CE3.3 Participar en la integración de un nuevo sistema dentro de una instalación existente
CE3.4 Ayudar a evaluar y comprobar el correcto funcionamiento e interacción funcional óptima de los nuevos sistemas con las instalaciones existentes.
CE3.5 Aprender a detectar los posibles conflictos que pueden presentarse al implementar un nuevo sistema con los sistemas ya dispuestos en la instalación.

C4: Participar en los procesos de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.

CE4.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.
CE4.2 Respetar los procedimientos y normas del centro de trabajo.
CE4.3 Emprender con diligencia las tareas según las instrucciones recibidas, tratando de que se adecuen al ritmo de trabajo de la empresa.
CE4.4 Integrarse en los procesos de producción del centro de trabajo.
CE4.5 Utilizar los canales de comunicación establecidos.
CE4.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. **Desarrollo de nuevos proyectos domoticos e inmóticos**
   - Análisis detallado de los diferentes sistemas que ofrece el mercado con los que trabaja la empresa en cuestión.
   - Utilización de las herramientas necesarias para la instalación de esos sistemas. Tanto hardware como software
   - Análisis de las necesidades, características y peculiaridades de un nuevo proyecto.
   - Desarrollo de los diferentes documentos que conforman el proyecto.
   - Observación del proceso de Instalación y conexión de los diferentes dispositivos.
   - Análisis de la programación y puesta a punto del sistema. Cooperación de manera no intrusiva siguiendo las indicaciones del tutor de empresa
   - Participación en los procesos de detección y gestión de incidencias
   - Participación en la redacción y actualización de la documentación relevante para el proyecto y final de obra.

2. **Mantenimiento de instalaciones domóticas e inmóticas existentes.**
   - Identificación de los sistemas instalados y en funcionamiento. Identificando los diferentes dispositivos y redes que integran el sistema
   - Análisis de la infraestructura de registros, conductos y espacios de reserva que forman la instalación.
   - Análisis de la topología de la red de alimentación y comunicación del sistema.
   - Detección de fallos en el sistema, ya sean de software o hardware.
   - Subsanación de los fallos detectados.
   - Desarrollo de la documentación necesaria para el registro documental del proyecto.
   - Realización de tareas de mantenimiento para el correcto funcionamiento de los sistemas.

cve: BOE-A-2011-10055

- Análisis de las funcionalidades que ofrece un sistema instalado, así como de las posibles mejoras que podrían incorporarse.
- Optimización de las funcionalidades de los diferentes dispositivos.

3. Implantación de nuevos sistemas en instalaciones domóticas e inmóticas
- Compatibilidad entre sistemas existentes y sistemas a implantar.
- Análisis de las necesidades de infraestructura al implementar nuevos sistemas.
- Identificación de los valores añadidos que surgen al implementar nuevos sistemas en combinación con los ya existentes.
- Solución de conflictos entre los sistemas recién implementados y los ya existentes.
- Creación de la documentación necesaria para reflejar correctamente las modificaciones realizadas en la instalación al implementar un nuevo sistema.

4. 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 del proceso productivo de la organización.
- Utilización 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 ambienta

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	Experiencia profesional requerida en el ámbito de la unidad de competencia
MF0490_3: Gestión de servicios en el sistema informático	• 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.	2 años
MF1219_3: Implantación y mantenimiento de sistemas domóticos/inmóticos	• 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.	2 años
MF1220_3: Implantación y mantenimiento de sistemas de control de accesos y presencia, y de videovigilancia.	• 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.	2 años

cve: BOE-A-2011-10055

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m² 15 alumnos	Superficie m² 25 alumnos
Aula de gestión	45	60
Taller de comunicaciones	80	150

Espacio Formativo	M1	M2	M3
Aula de gestión	X	X	X
Taller de comunicaciones		X	X

Espacio Formativo	Equipamiento
Aula de gestión	- Equipos audiovisuales - Cañón con proyección - Pantalla para proyección - Rotafolios o pizarra con rotuladores - Ordenador en funciones de servidor para casos prácticos - Ordenadores en funciones de puesto en red para los casos prácticos - Material de aula - Mesa y silla para formador - Mesas y sillas para alumnos
Taller de comunicaciones	- Instrumentos de medida: polímetro, téster de cableado coaxial, certificador de cableado, monitor de vídeo portátil, luxómetro. - Instrumentos de Taller de Electricidad, Electrónica e Informática. - Paneles de trabajo adaptados según el sistema o sistemas domóticos seleccionados para la formación - Equipos para control de accesos y presencia: cabezales lectores de tarjetas (banda magnética, proximidad, chip), lectores biométricos, centrales de control, actuadores (electro cerraduras, barreras), detectores de presencia. - Equipos para sistemas de videovigilancia: cámaras analógicas, cámaras IP, ópticas para las cámaras, cabinas para las cámaras, posicionadores, teclados de control, multiplexores, secuenciadores, grabadores de imagen analógicos y digitales, monitores analógicos y TFT, soportes de grabación (cintas, CD,DVD) - Ordenador configurado específicamente para la impartición de este certificado (del mismo modo que los ordenadores del aula de gestión) - Acceso a Internet, telefónico y conectividad GSM/GPRS/UMTS (tarjetas SIM)

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.

cve: BOE-A-2011-10055

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 V

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: ADMINISTRACIÓN DE SERVICIOS DE INTERNET

Código: IFCT0509

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC156_3 Administración de servicios Internet (RD 1087/05, de 16 de septiembre)

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

UC0495_3: Instalar, configurar y administrar el software para gestionar un entorno Web.
UC0496_3: Instalar, configurar y administrar servicios de mensajería electrónica.
UC0497_3: Instalar, configurar y administrar servicios de transferencia de archivos y multimedia.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Instalar, configurar, administrar y mantener servicios comunes de provisión e intercambio de información utilizando los recursos de comunicaciones que ofrece Internet.

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional en empresas o entidades de naturaleza pública o privada de cualquier tamaño que cuenten con infraestructura de redes intranet, internet o extranet para realizar intercambio de informaciones, la actividad se realiza en el área de sistemas del departamento de informática desempeñando su trabajo tanto por cuenta ajena como por cuenta propia.

Sectores productivos:

Dada la amplia distribución de los servicios de Internet se observa un fundamento transectorial en esta cualificación, con especial relevancia en el sector servicios, ubicándose en los siguientes tipos de empresas:
Organismos públicos y empresas de cualquier sector productivo que por su tamaño y organización necesiten disponer de servicios propios basados en tecnologías de Internet.

cve: BOE-A-2011-10055

Empresas proveedoras de servicios Internet.
Empresas de externalización de servicios (outsourcing) y centros de datos.
Empresas dedicadas al desarrollo de páginas y aplicaciones Web.

Ocupaciones o puestos de trabajo relacionados:

Administrador de servicios de Internet.
Administrador de entornos Web (webmaster).
Administrador de servicios de mensajería electrónica (postmaster).
Técnico de sistemas de Internet.

Duración de la formación asociada: 590 horas

Relación de módulos formativos y de unidades formativas:

MF0495_3: Administración de servicios Web (180 horas)
- UF1271: Instalación y configuración del software de servidor Web (90 horas)
- UF1272: Administración y auditoría de los servicios Web (90 horas)

MF0496_3: Administración de servicios de mensajería electrónica (120 horas).
- UF1273: Selección, instalación y configuración del software de servidor de mensajería electrónica (60 horas)
- UF1274: Administración y auditoría de los servicios de mensajería electrónica (60 horas)

MF0497_3: Administración de servicios de transferencia de archivos y contenidos multimedia (120 horas).
- UF1275: Selección, instalación, configuración y administración de los servidores de transferencia de archivos (70 horas)
- UF1276: Selección, instalación, configuración y administración de los servidores multimedia (50 horas)

MF0490_3: (Transversal) Gestión de servicios en el sistema informático (90 horas)

MP0267: Módulo de prácticas profesionales no laborales de Administración de servicios de internet (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: INSTALAR, CONFIGURAR Y ADMINISTRAR EL SOFTWARE PARA GESTIONAR UN ENTORNO WEB

Nivel: 3

Código: UC0495_3

Realizaciones profesionales y criterios de realización

RP1: Instalar y configurar el software de servidor Web para permitir el acceso a las informaciones publicadas según las políticas de seguridad de la empresa.

CR1.1 Los documentos de especificación del servicio a prestar son interpretados identificando las características que debe reunir el entorno de explotación.

CR1.2 El servidor Web se elige e instala, configurando el hardware, software, parámetros de conectividad y permisos del sistema de acuerdo con las

cve: BOE-A-2011-10055

especificaciones del fabricante, el plan de implantación y la normativa de seguridad y calidad de la organización.
CR1.3 Los certificados para servidor seguro se solicitan a la autoridad certificadora y se instalan y mantienen siguiendo los requisitos de seguridad especificados para el servicio y las políticas de la organización.
CR1.4 El contenido a publicar se instala en el servidor siguiendo las especificaciones de diseño y la política de seguridad de la organización.
CR1.5 La verificación de la instalación y configuración del servidor Web se realiza mediante la ejecución de una serie de pruebas según normas de calidad de la organización.
CR1.6 Los datos finales de configuración, ubicación de los contenidos, URLs de acceso y seguridad se documentan siguiendo las normas internas de la organización.
CR1.7 El manual de operación se redacta para permitir la recuperación ante fallos del servicio, de forma que se garanticen los parámetros establecidos de disponibilidad y calidad del servicio.
CR1.8 La documentación técnica de los distintos servidores Web que pueden ser utilizados se interpreta tanto si está editada en castellano o las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

RP2: Instalar y configurar los módulos y extensiones del servidor Web para atender funcionalidades añadidas según las necesidades de los lenguajes y herramientas utilizadas en el desarrollo de la información a publicar.
CR2.1 Los módulos y extensiones a instalar en el entorno de explotación se eligen buscando la mayor concordancia entre especificaciones de diseño y de fabricante, y siguiendo las políticas de la organización.
CR2.2 La configuración hardware, software, de conectividad y permisos del servidor se definen de acuerdo con los requisitos de diseño y de fabricante.
CR2.3 Los módulos y extensiones se instalan siguiendo las directrices del fabricante y la política de seguridad de la organización.
CR2.4 El contenido adicional a publicar se instala en el servidor siguiendo las especificaciones de diseño y la política de seguridad de la organización.
CR2.5 Los módulos y extensiones del servidor Web instalados y configurados se prueban para demostrar su funcionalidad y correcta integración según las normas de calidad de la organización.
CR2.6 Los datos finales de configuración, ubicación de los contenidos, URLs de acceso y seguridad se documentan siguiendo las normas internas de la organización.
CR2.7 El manual de operación se redacta para permitir la correcta recuperación ante fallos del servicio, de forma que se garanticen los parámetros establecidos de disponibilidad y calidad del servicio.
CR2.8 La documentación técnica de los distintos módulos y extensiones del servidor Web que pueden ser utilizados se interpreta tanto si está editada en castellano o las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

RP3: Administrar y auditar los servicios Web para asegurar y optimizar su rendimiento según las necesidades de uso y los planes de explotación de la organización.
CR3.1 La ejecución de los servicios Web y los módulos software instalados se comprueban realizando la batería de pruebas especificada en el diseño y por las normas de calidad de la organización.
CR3.2 Los parámetros de calidad de servicio y de usabilidad se comprueban utilizando las herramientas software adecuadas según las normas de la organización.

cve: BOE-A-2011-10055

CR3.3 Los fallos de ejecución y de rendimiento del servidor Web se diagnostican indicando si se trata de un problema de configuración, de desarrollo o de recursos y redactando el correspondiente informe de incidencias y la posible solución los mismos.
CR3.4 El contenido a publicar se actualiza siguiendo las políticas de la organización y teniendo en cuenta la normativa legal vigente.
CR3.5 El servidor de estadísticas del servicio Web se elige e instala buscando la mayor concordancia entre especificaciones de diseño y de fabricante, y siguiendo las políticas de la organización.
CR3.6 Las fuentes de datos, la periodicidad de análisis, los tipos de informes y los permisos se configuran en el servidor de estadísticas siguiendo las especificaciones de diseño y la política de seguridad de la organización.
CR3.7 Los parámetros de configuración se ajustan para solventar o mejorar los posibles fallos de ejecución o rendimiento, siguiendo las especificaciones de diseño y del fabricante y cumpliendo las normas internas de seguridad y calidad.
CR3.8 La aplicación de los procedimientos de operación del servicio se comprueba realizando inspecciones periódicas y simulando averías según los procedimientos de seguridad de la organización.
CR3.9 La documentación de configuración y los procedimientos de operación se actualizan con los cambios que se produzcan en la resolución de incidencias.

RP4: Instalar, configurar y administrar el servidor de aplicaciones y la conexión con sistemas gestores de bases de datos para permitir la ejecución de aplicaciones e interacción con bases de datos según las necesidades de la organización.

CR4.1 El servidor de aplicaciones y software de conexión de acceso a bases de datos a instalar en el entorno de explotación se eligen buscando la mayor concordancia entre especificaciones de diseño y de fabricante, y siguiendo las políticas de la organización.
CR4.2 La configuración software, de conectividad y permisos se definen de acuerdo con los requisitos de diseño y de fabricante y las normas de implantación de la organización.
CR4.3 El software de servidor de aplicaciones y la conexión a las bases de datos se configura siguiendo las directrices del fabricante y la política de seguridad de la organización.
CR4.4 Las aplicaciones del servicio se instalan en el servidor de aplicaciones siguiendo las especificaciones de diseño y la política de seguridad de la organización.
CR4.5 La ejecución de módulos software tanto de cliente como de servidor y la conexión a las bases de datos se comprueba realizando la batería de pruebas especificada en el diseño y por las normas internas de la organización.
CR4.6 Los datos finales de configuración y seguridad se documentan siguiendo las normas internas de la organización.
CR4.7 El manual de operación se redacta para permitir la correcta recuperación ante fallos del servicio de forma que se garanticen los parámetros establecidos de disponibilidad y calidad del servicio.
CR4.8 La documentación técnica de los servidores Web y de aplicaciones, y de los sistemas gestores de bases de datos que pueden ser utilizados se interpreta tanto si está editada en castellano o las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

cve: BOE-A-2011-10055

Contexto profesional

Medios de producción
Equipos informáticos, generalmente, de tipo servidor. Sistemas operativos y parámetros de configuración. Software de servidores: Web, de aplicaciones, de estadísticas. Paquetes de software con funcionalidades adicionales. Módulos de conexión a base de datos: ODBC y JDBC entre otros. Certificados digitales. Cortafuegos. Sistemas gestores de bases de datos. Herramientas de seguridad.

Productos y resultados
Servicios Web para todo tipo de ámbito Internet, intranet o extranet. Servicios Web para todo tipo de contenido: contenido estático o dinámico y aplicaciones. Servicios Web seguros. Servicios de alojamiento/hosting Web.

Información utilizada o generada
Documentación de diseño del servicio. Documentación de productos software. Normas internas de calidad y seguridad. Acuerdos de nivel de servicio (SLAs). Documentación de configuración de sistemas y servicios. Documentación de trazabilidad, actualización y mantenimiento. Baterías de pruebas. Manuales de uso y funcionamiento de los sistemas informáticos. Manuales de instalación y configuración del software asociado a esta unidad de competencia. Manuales de operación de los sistemas gestores de bases de datos. Manuales de los lenguajes y herramientas utilizados para generar la información a publicar. Manual de administración del software asociado a esta unidad de competencia. Materiales de cursos de formación. Sistemas de ayuda del software. Soportes técnicos de asistencia. Plan de pruebas e informe de fallos. Normativa legal de publicación de información. Normativa legal de propiedad de la información. Manual de operación del servidor Web. Histórico de sucesos.

Unidad de competencia 2

Denominación: INSTALAR, CONFIGURAR Y ADMINISTRAR SERVICIOS DE MENSAJERÍA ELECTRÓNICA

Nivel: 3

Código: UC0496_3

Realizaciones profesionales y criterios de realización

RP1: Instalar y configurar los servicios de mensajería electrónica para proporcionar facilidades de intercomunicación a los usuarios según las directivas de la organización.

CR1.1 Los documentos de especificación del servicio a prestar son interpretados correctamente identificando las características que debe reunir el entorno de explotación.

CR1.2 El servidor de mensajería electrónica se elige, instala y configura el hardware, software, conectividad y permisos en el equipo informático siguiendo las especificaciones del fabricante y según las especificaciones de la organización.

CR1.3 Los elementos de seguridad se instalan y configuran siguiendo las directrices del fabricante, las especificaciones del servicio y política de seguridad de la organización.

CR1.4 La verificación de la instalación y configuración de los servidores de mensajería electrónica se realiza mediante la ejecución de una serie de pruebas.

CR1.5 Los datos finales de configuración y de seguridad se documentan siguiendo las normas internas de la organización.

cve: BOE-A-2011-10055

CR1.6 La documentación técnica de los distintos servidores de mensajería electrónica que pueden ser utilizados se interpreta tanto si está editada en castellano o las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

RP2: Administrar servicios de mensajería electrónica para asegurar la distribución de los mensajes entre usuarios según las políticas de la organización.

CR2.1 Los perfiles y cuentas de usuario, buzones, administradores, moderadores, listas y salas se configuran en el servidor correspondiente, siguiendo las especificaciones de diseño y la política de seguridad de la organización.

CR2.2 El manual de operación se redacta para permitir la correcta recuperación ante fallos del servicio de forma que se garanticen los parámetros establecidos de disponibilidad y calidad del servicio.

CR2.3 Las alarmas de los programas de seguridad se configuran según los parámetros establecidos por la normativa de seguridad de la empresa.

RP3: Auditar los servicios de mensajería electrónica para garantizar la calidad del servicio y diagnosticar y solucionar los fallos en el mismo según las necesidades de la organización.

CR3.1 Los servicios de mensajería electrónica se auditan para garantizar un rendimiento óptimo de los servidores de mensajería electrónica según las necesidades de la organización.

CR3.2 Los parámetros de calidad de servicio se comprueban utilizando las herramientas software adecuadas según la normativa de seguridad de la organización.

CR3.3 Los fallos de ejecución y rendimiento se diagnostican correctamente identificando el origen del problema e indicando la posible solución del mismo, documentando el proceso según las normas y el plan de calidad de la organización.

CR3.4 Los parámetros de configuración se ajustan para solventar o mejorar los posibles fallos de ejecución o rendimiento, siguiendo las especificaciones de diseño y del fabricante y cumpliendo las normas internas de seguridad y calidad.

CR3.5 La documentación de configuración y los procedimientos de operación se actualizan con los cambios que se produzcan en la resolución de incidencias.

CR3.6 La información expuesta en los servidores de mensajería electrónica según los planes de la organización no infringe ninguna normativa legal.

Contexto profesional

Medios de producción

Equipos informáticos, generalmente, de tipo servidor. Software de servidores: correo, mensajería electrónica instantánea, news, foros, chat, y peer-to-peer entre otros. Cortafuegos. Sistemas operativos y parámetros de configuración. Herramientas de seguridad informática.

Productos y resultados

Servicios de mensajería electrónica personal. Servicios de comunidad virtual. Servicios de intercambio de archivos. Servicios de boletines.

Información utilizada o generada

Documentación de diseño del servicio. Documentación de productos software. Normas internas de calidad y seguridad. Acuerdos de nivel de servicio (SLAs). Documentación de configuración de sistemas y servicios. Manuales de uso y funcionamiento de los sistemas informáticos. Manuales de instalación del software asociado a esta unidad de competencia. Manuales de administración del software asociado a esta unidad de competencia. Materiales de cursos de formación. Sistemas de ayuda del software. Soportes técnicos de asistencia. Plan de pruebas e informe de fallos. Normativa legal de

cve: BOE-A-2011-10055

publicación de información. Normativa legal de propiedad de la información. Manuales de operación de los servidores de mensajería electrónica. Histórico de sucesos.

Unidad de competencia 3

Denominación: INSTALAR, CONFIGURAR Y ADMINISTRAR SERVICIOS DE TRANSFERENCIA DE ARCHIVOS Y MULTIMEDIA

Nivel: 3

Código: UC0497_3

Realizaciones profesionales y criterios de realización

RP1: Instalar, configurar servicios de transferencia de archivos para facilitar el uso de repositorios de información según necesidades de la organización.

CR1.1 El servidor de transferencia de archivos se elige, instala y se configura el hardware, software, parámetros de conectividad y permisos del sistema de acuerdo con las especificaciones del fabricante, requisitos del servicio y normativas de implantación y seguridad de la organización.

CR1.2 La estructura de directorios, los contenidos y los permisos se implantan en el servidor siguiendo las especificaciones de diseño, la política de seguridad de la organización y la normativa legal vigente.

CR1.3 La verificación de la instalación y la configuración del servidor de transferencia de archivos se realiza mediante la ejecución de las pruebas necesarias según las normativas de calidad e implantación de la organización.

CR1.4 Los parámetros de calidad del servicio se verifican mediante la ejecución de pruebas del sistema según las normativas de calidad y seguridad de la organización.

CR1.5 Los datos finales de configuración, estructura de directorios, URLs de acceso y seguridad se documentan siguiendo las normas internas de la organización.

RP2: Administrar servicios de transferencia de archivos en función de las necesidades especificadas en el plan de explotación de la organización.

CR2.1 El manual de operación se redacta para permitir la correcta recuperación ante fallos del servicio de forma que se garanticen los parámetros establecidos de disponibilidad y calidad del servicio.

CR2.2 La aplicación de los procedimientos de operación del servicio se comprueba realizando inspecciones periódicas y simulando averías.

CR2.3 La configuración de los registros del sistema (logs) y de las alarmas en la ejecución del servicio se realizan teniendo en cuenta los parámetros de rendimiento exigidos en el plan de explotación.

CR2.4 Las ubicaciones de la información servida se controlan y auditan tanto en lo que respecta a los contenidos como en los permisos definidos en ellas según las especificaciones de seguridad de la organización.

CR2.5 Los fallos de ejecución y rendimiento se diagnostican y se documentan indicando las causas de la incidencia y su posible solución según la normativa de la organización.

RP3: Instalar, configurar servicios de audio y video de acuerdo con las especificaciones dadas y teniendo en cuenta los anchos de banda disponibles en las líneas de comunicaciones.

cve: BOE-A-2011-10055

CR3.1 Los documentos de especificación del servicio a prestar son interpretados correctamente identificando las características que debe reunir el entorno de explotación.
CR3.2 Los servidores de transferencia de audio y vídeo bajo demanda y videoconferencia se eligen, instalan y se configuran el hardware, software, los parámetros de conectividad y los permisos del sistema de acuerdo con los requisitos del fabricante, las especificaciones del servicio y la normativa de implantación y seguridad de la organización.
CR3.3 La estructura y ubicación de contenidos, los parámetros de conexión y los permisos se configuran en los servidores de audio y video bajo demanda y videoconferencia siguiendo las especificaciones de diseño y la política de seguridad de la organización y según la normativa legal vigente confeccionando la documentación relativa a la configuración realizada.
CR3.4 La verificación de la instalación y la configuración de los servidores de audio y video bajo demanda y videoconferencia se realizan mediante la ejecución de las pruebas necesarias según las normativas de calidad e implantación de la organización.
CR3.5 Los parámetros de calidad del servicio se verifican mediante la realización de las pruebas necesarias según las normativas de calidad y seguridad de la organización.

RP4: Administrar servicios de audio y vídeo según especificaciones del plan de explotación de la organización y requisitos impuestos por los recursos disponibles.
CR4.1 El manual de operación se redacta para permitir la recuperación ante fallos del servicio, de forma que se garanticen los parámetros establecidos de disponibilidad y calidad del servicio.
CR4.2 La aplicación de los procedimientos de operación del servicio se comprueba realizando inspecciones periódicas y simulando averías.
CR4.3 Los fallos de ejecución y rendimiento se diagnostican y reparan indicando si se trata de un problema de configuración, de recursos del sistema, del software de servidor o de conectividad y redactando el correspondiente informe de incidencias.
CR4.4 Los consumos de recursos se controlan asignando número máximo de usuarios concurrentes a los servicios y disponibilidades máximas de consuma de ancho de banda en las líneas de comunicaciones según especificaciones del plan de explotación de la organización

Contexto profesional

Medios de producción
Equipos informáticos de tipo servidor. Líneas de comunicaciones. Software de servidores: directorio, FTP, streaming de audio y vídeo, videoconferencia y entornos de trabajo colaborativo en tiempo real entre otros. Paquetes de software con funcionalidades adicionales. Cortafuegos. Herramientas de seguridad. Sistemas operativos y parámetros de configuración.

Productos y resultados
Servicios de transferencia de archivos. Servicios de audio y vídeo bajo demanda. Servicios de videoconferencia y entornos de trabajo colaborativo.

Información utilizada o generada
Documentación de diseño del servicio. Documentación de productos software. Normas internas de calidad y seguridad. Acuerdos de nivel de servicio (SLAs). Documentación de configuración de sistemas y servicios. Manuales de uso y funcionamiento de los sistemas informáticos. Manuales de instalación del software asociado a esta unidad

cve: BOE-A-2011-10055

de competencia. Manuales de administración del software asociado a esta unidad de competencia. Materiales de cursos de formación. Sistemas de ayuda del software asociado a esta unidad de competencia. Soportes técnicos de asistencia. Plan de pruebas e informe de fallos. Normativa legal de publicación de información. Normativa legal de propiedad de la información. Manuales de operación de los servidores asociados a esta unidad de competencia. Histórico de sucesos.

Unidad de competencia 4

Denominación: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Los procesos que intervienen en el sistema son identificados para evaluar parámetros de rendimiento.

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

CR1.3 Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización.

CR1.4 Las herramientas de monitorización se implantan y configuran determinando los niveles de las alarmas en función del plan de explotación de la organización.

RP2: Administrar los dispositivos de almacenamiento según las necesidades de uso y dentro de las directivas de la organización.

CR2.1 Los dispositivos de almacenamiento se configuran para ser usados en los distintos sistemas operativos utilizados en el sistema informático.

CR2.2 La estructura de almacenamiento se define y se implanta atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de uso de la organización.

CR2.3 Los requerimientos de nomenclatura de objetos y restricciones de uso de cada dispositivo de almacenamiento se documentan adecuadamente.

CR2.4 Los dispositivos de almacenamiento se integran para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.

CR3.1 El acceso de los usuarios al sistema informático se configura para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.

CR3.2 El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.

CR3.3 Los recursos disponibles para los usuarios se limitan con las herramientas adecuadas en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.

CR4.1 Los dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.

cve: BOE-A-2011-10055

CR4.2 Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.
CR4.3 Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización.

Contexto profesional

Medios de producción

Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

Productos y resultados

Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

Información utilizada o generada

Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: ADMINISTRACIÓN DE SERVICIOS WEB

Código: MF0495_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0495_3: Instalar, configurar y administrar el software para gestionar un entorno Web

Duración: 180 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE DE SERVIDOR WEB

Código: UF1271

cve: BOE-A-2011-10055

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1 y RP2
Capacidades y criterios de evaluación

C1: Seleccionar el servidor Web, sus módulos y extensiones para verificar que cumplen los requisitos de ejecución de las aplicaciones Web dadas.

CE1.1 Describir los parámetros de funcionamiento de un servidor Web en un escenario de instalación dado.

CE1.2 Describir las características de un servidor Web comparándolo con otros servidores Web existentes en el mercado.

CE1.3 Identificar y describir las funciones de los módulos y extensiones más habituales en los servidores Web.

CE1.4 Relacionar los parámetros cuantitativos y cualitativos de configuración con los requisitos de sistema correspondientes.

CE1.5 A partir de un supuesto práctico en el que se cuenta con un servicio Web en producción:

- Identificar la funcionalidad requerida en el servidor Web.
- Estimar la carga y el rendimiento esperado.
- Identificar el nivel y los requisitos de seguridad.
- Seleccionar el servidor Web y las extensiones necesarias.
- Estimar los requisitos de sistema e indicar las plataformas hardware y software más adecuadas.

C2: Instalar y configurar el servidor Web en el sistema informático para ofrecer funcionalidades de distribución de información.

CE2.1 Describir los mecanismos de autenticación de usuarios y de acceso a los contenidos.

CE2.2 Describir los procesos de arranque y parada, y de rotación de los registros (logs).

CE2.3 A partir de un supuesto práctico de servicio Web a instalar según premisas de funcionamiento estipuladas:

- Comprobar que el sistema reúne las características necesarias para la instalación del servidor Web y el servicio especificado.
- Establecer en el sistema la estructura de almacenamiento de los recursos, los permisos de acceso y ejecución y las variables de entorno necesarios.
- Instalar el software del servidor y establecer los procesos de arranque y parada, y de rotación de registros de acuerdo con las especificaciones del administrador del sistema informático.
- Configurar en el servidor Web los mecanismos de acceso: protocolos, direcciones IP, dominios, servidores virtuales y puertos según indicaciones recibidas por el administrador de la red.
- Habilitar los mecanismos especificados de autenticación de usuarios.
- Verificar la instalación del servidor Web y de las funcionalidades esperadas.
- Generar la documentación de operación y recuperación ante fallos.

CE2.4 Explicar el concepto, características y funcionalidad de los certificados de servidores seguros.

CE2.5 Describir los pasos a seguir para solicitar, instalar y mantener certificados de servidor seguro.

C3: Instalar, configurar e integrar los módulos y extensiones del servidor Web en el sistema informático.

cve: BOE-A-2011-10055

CE3.1 Describir las funciones de los principales módulos y extensiones de los servidores Web destinados a cubrir funcionalidades específicas en un sitio Web dado.
CE3.2 Identificar los parámetros de configuración de los principales módulos y extensiones de los servidores Web a instalar en función de las especificaciones recibidas.
CE3.3 Describir la interrelación de los módulos y extensiones con el servidor Web y otros posibles servicios y aplicaciones, tanto del propio sistema como de sistemas externos.
CE3.4 A partir de un supuesto práctico de servicio Web a instalar en un escenario de distribución de información debidamente caracterizado:
- Implantar el software de los módulos y extensiones del servidor Web.
- Configurar los permisos de acceso y ejecución de los recursos adicionales.
- Configurar los parámetros que optimicen el rendimiento del conjunto.
- Configurar y comprobar la comunicación con otros servicios y aplicaciones, locales o remotos.
- Detallar las pruebas a realizar para comprobar la correcta instalación y configuración de los módulos y extensiones del servidor Web.
- Cumplimentar la documentación de operación y recuperación ante fallos.

Contenidos

1. **Conceptos básicos de sistemas de servidores.**
   - Sistemas operativos soportados.
   - Fundamentos de TCP/IP
   - Estructura Cliente / Servidor.

2. **Manejo del protocolo http.**
   - Funcionamiento y estructura.
   - Descripción de peticiones o request methods.
   - Códigos de estado.
   - Cabeceras.
   - Codificación del contenido. Páginas de códigos.
   - Realización de peticiones HTTP en Internet mediante un proxy, livehttpheaders o método similar, analizando el protocolo utilizado.

3. **Selección del servidor Web.**
   - Parámetros de funcionamiento.
   - Características del servidor Web.
   - Funcionalidades principales.
   - Requisitos del sistema:
     - Hardware.
     - Software.
     - Conectividad.

4. **Instalación y configuración básica del servidor Web.**
   - Instalación del servidor Web:
     - Procedimientos de instalación.
     - Instalación del servidor en el sistema operativo.
     - Verificación de la instalación.
   - Control del servicio. Inicio y parada.
   - Creación de entradas DNS
   - Parámetros básicos de configuración:
     - Descripción de los parámetros básicos.
     - Alojamiento virtualizado (virtual hosting)

cve: BOE-A-2011-10055

- Alojamiento virtualizado basado en nombres (Name-based virtual hosting)
- Logging

- Directivas básicas de configuración:
  - Puerto de escucha
  - Directorio raíz
  - Otras directivas básicas de configuración.
- Herramientas de configuración.
- Mantenimiento del servicio.

5. Módulos y extensiones del servidor Web.

- Descripción de los módulos y extensiones del servidor Web.
- Soporte a lenguajes:
  - CGI
  - Motores de script (ASP.NET, PHP...)

6. Análisis de la seguridad del servidor Web

- Descripción de los conceptos básicos del servidor web:
  - Rutas y permisos. Permiso de lectura vs permiso de ejecución.
  - Listado de directorios.
  - Tipos MIME permitidos.
- Control de acceso por IP origen.
- Control de acceso por usuarios:
  - Métodos de intercambio de credenciales (Autenticación Básica /Digest / NTLM)
  - Almacén de credenciales. (LDAP, Base de datos, ficheros de texto, Windows)
  - Configuración de directorios protegidos con contraseña.
- Identificación de las Conexiones seguras mediante https:
  - Certificados de seguridad.
  - Algoritmos de cifrado.
  - Entidades de certificación
  - Generación de un CSR
  - Generación de un certificado auto-firmado.
  - Instalación de un certificado.
  - Control de acceso por certificado de cliente.

UNIDAD FORMATIVA 2

Denominación: ADMINISTRACIÓN Y AUDITORÍA DE LOS SERVICIOS WEB

Código: UF1272

Duración: 90 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP3 y RP4
Capacidades y criterios de evaluación

C1: Administrar los contenidos gestionados por el servidor Web, los accesos realizados y el rendimiento según especificaciones de diseño normativa de la organización y legislación vigente.

CE1.1 Describir procedimientos de actualización de contenidos y control de versiones según procedimientos.

CE1.2 Describir las técnicas de gestión de permisos: perfiles, grupos y roles entre otros atendiendo a las especificaciones de las normas internas de seguridad informática.

cve: BOE-A-2011-10055

CE1.3 Explicar los procedimientos de optimización del rendimiento del servidor Web y sus complementos en el sistema informático.
CE1.4 Describir la función y características principales de un servidor de estadísticas Web.
CE1.5 A partir de un supuesto práctico de servicio Web en producción:
- Definir la organización de los contenidos en el servidor Web.
- Establecer los procedimientos de actualización y control de versiones.
- Analizar los parámetros de rendimiento del servidor Web.
- Establecer planes de actuación para adaptar el servidor a las variaciones de uso y planes de contingencias.

CE1.6 Explicar la normativa legal vigente que afecta a la información publicada en el servidor Web.

C2: Instalar, configurar y administrar el servidor de aplicaciones en el sistema informático como proveedor de datos para los servicios Web.
CE2.1 Describir las funciones de un servidor de aplicaciones y sus parámetros de configuración.
CE2.2 Explicar el procedimiento de implantación de aplicaciones en un servidor de aplicaciones.
CE2.3 A partir de un supuesto práctico de servicio Web a instalar con conexión a bases de datos y contando con un servidor de aplicaciones:
- Implantar el software del servidor de aplicaciones y los módulos de acceso a base de datos.
- Configurar los parámetros que optimicen el rendimiento del conjunto.
- Implantar la aplicación del servicio Web en el servidor, comprobando el correcto arranque, funcionamiento y parada.
- Configurar y comprobar la comunicación con otros servicios y aplicaciones, locales o remotos.
- Verificar la instalación del servidor de aplicaciones.
- Generar la documentación de operación y recuperación ante fallos.

C3: Seleccionar, instalar y configurar los métodos de acceso a sistemas gestores de bases de datos para utilizar sus recursos en sitios Web dinámicos.
CE3.1 Describir los métodos de acceso a sistemas gestores de bases de datos más usuales y sus procedimientos de conexión con un servidor Web.
CE3.2 Describir la interrelación y mecanismos de comunicación entre los distintos elementos de una arquitectura Web en tres capas.
CE3.3 A partir de un supuesto práctico de servicio Web a instalar con conexión a bases de datos:
- Implantar los módulos de acceso a base de datos.
- Configurar los parámetros que optimicen el rendimiento del sistema de acceso a bases de datos.
- Configurar y comprobar la comunicación con otros servicios y aplicaciones, locales o remotos.
- Verificar la conexión a la base de datos y la aplicación del servicio Web.
- Generar la documentación de operación y recuperación ante fallos.

C4: Aplicar procedimientos de auditoría y resolución de incidencias en la explotación de un servicio Web.
CE4.1 Describir y clasificar los elementos determinantes del rendimiento de una plataforma Web.
CE4.2 Explicar los procedimientos de cuantificación y medida de la calidad de servicio prestada.
CE4.3 Explicar los procedimientos de diagnóstico de incidencias en entornos de producción de servicios Web.

cve: BOE-A-2011-10055

CE4.4 Describir detalladamente las técnicas de resolución de incidencias en entornos de producción de servicios Web.
CE4.5 En un supuesto práctico en el que disponemos de un servicio Web en producción:
- Verificar que las operaciones definidas en los manuales de procedimiento se realizan puntual y convenientemente.
- Establecer los mecanismos de medición del rendimiento y disponibilidad del servicio.
- Analizar los parámetros de calidad del servicio para determinar el grado de cumplimiento de las especificaciones.
- Aplicar las medidas correctoras de las deficiencias encontradas.

CE4.6 En un supuesto práctico en el que contamos con un servicio Web en situación de incidencia:
- Aplicar las técnicas y herramientas de diagnóstico que permitan identificar la causa del mal funcionamiento.
- Aplicar medidas urgentes de contención para mantener el máximo nivel de servicio posible y limitar los posibles daños.
- Establecer los procedimientos para la resolución definitiva del problema y la recuperación de la situación previa a la incidencia.
- Analizar la causa de la incidencia y establecer los procedimientos para prevenir otra situación similar o resolverla en menor tiempo.

CE4.7 Definir los pasos a seguir en la instalación y configuración de un servidor de estadísticas.

Contenidos

1. Administración de contenidos del servidor Web.
- Procedimientos de actualización de contenidos:
  - FTP
  - FTPS
  - SFTP
  - Introducción a sistemas de gestión de contenidos (CMS)
- Organización de contenidos.
- Control de versiones.
- Técnicas de gestión de permisos:
  - Perfiles.
  - Grupos.
  - Roles.
- Procedimientos de optimización del rendimiento del servidor Web:
  - Técnicas de optimización.
  - Parámetros de calidad de servicio y usabilidad.
  - Pruebas de optimización.
  - Simulación de generación de carga Web con herramientas específicas.
- Servidores de estadísticas:
  - Estructura y campos de un fichero de log.
  - Concepto de sesión.
  - Mecanismos de seguimiento de sesiones.
  - Instalación de un analizador de logs sencillo
- Normativa legal relacionada con la publicación de contenidos Web:
  - Salvaguarda de logs.
  - LOPD.

2. Servidor de aplicaciones de servicios Web.
- Descripción de funciones y parámetros de configuración:
  - Parámetros recomendados según el escenario.

cve: BOE-A-2011-10055

- Procedimientos de implantación:
  - Comprobación de arranque, funcionamiento y parada.
  - Verificación de la instalación.
- Análisis y elaboración de la documentación de operación.

3. Acceso a sistemas gestores de bases de datos.

- Motores de base de datos de uso más frecuente en aplicaciones Web (ORACLE, SQL Server, mySQL):
  - Protocolos de acceso.
  - Modelos de seguridad (Por IP, por usuario contraseña, seguridad integrada, combinación de estas...)
- Bibilotecas de acceso:
  - ODBC, JDBC, DSN-Less ODBC, OleDB.
  - Implantar módulos de acceso (Instalar controladores ODBC, crear un DSN,...)
- Mecanismos de comunicación en una arquitectura Web en 3 capas:
  - SOAP, RPC, WebServices.
- Verificación de la conexión a la base de datos.

4. Descripción de arquitecturas distribuidas en múltiples servidores.

- Modelo de 3 capas.
- Tolerancia a fallos.
- Reparto de carga.
- Almacenes de estado de sesión. (ASP.NET state service…)
- Almacenes de caché. (Memcached…)
- Servidores Proxy.

5. Gestión de actualizaciones de servidores y aplicaciones.

- Entorno de desarrollo y preproducción.
- Procedimientos de despliegue de actualizaciones.

6. Auditoría y resolución de incidentes sobre servicios Web.

- Medición de la calidad del servicio prestada:
  - Parámetros de calidad.
  - Disponibilidad del servicio.
  - Acuerdos de prestación de Servicio (SLAs).
- Gestión de vulnerabilidades en aplicaciones Web:
  - Herramientas de detección de vulnerabilidades en aplicaciones Web (P.e. Nikto).
- Diagnóstico de incidentes en producción:
  - Monitorización.
  - Herramientas de medición del rendimiento (Contadores del sistema windows, apache mod_status...)
- Técnicas de resolución de incidentes:
  - Medidas de contención. Workarounds.
  - Análisis causa - raíz.
  - Gestión proactiva de problemas

Orientaciones metodológicas

Formación a distancia:

cve: BOE-A-2011-10055

Unidades formativas	Duración total en horas de las unidades formativas	N.º de horas máximas susceptibles de formación a distancia
Unidad formativa 1 - UF1271	90	40
Unidad formativa 2 - UF1272	90	30

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.

MÓDULO FORMATIVO 2

Denominación: ADMINISTRACIÓN DE SERVICIOS DE MENSAJERÍA ELECTRÓNICA

Código: MF0496_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0496_3: Instalar, configurar y administrar servicios de mensajería electrónica.

Duración: 120 horas

UNIDAD FORMATIVA 1

Denominación: SELECCIÓN, INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE DE SERVIDOR DE MENSAJERÍA ELECTRÓNICA

Código: UF1273

Duración: 60 horas

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

Capacidades y criterios de evaluación

C1: Seleccionar los servidores de mensajería electrónica en función de las necesidades de la organización.

CE1.1 Describir el funcionamiento básico de los servidores de correo electrónico, foros, chat y mensajería electrónica instantánea.

CE1.2 Describir las características más significativas de los servidores de mensajería electrónica, para determinar su adecuación a un determinado servicio.

CE1.3 Relacionar los parámetros cuantitativos y cualitativos de configuración de los servidores de mensajería electrónica con los requisitos de sistema correspondientes.

CE1.4 A partir de un supuesto práctico de servicio de mensajería electrónica a instalar:

- Identificar la funcionalidad requerida en la especificación del servicio.

cve: BOE-A-2011-10055

- Estimar la carga y el rendimiento previsto.
- Identificar el nivel y los requisitos de seguridad.
- Seleccionar el servidor o servidores más adecuados a los requisitos.
- Estimar los requisitos de sistema e indicar las plataformas hardware y software más adecuadas.

C2: Instalar y configurar los servidores de mensajería electrónica en el sistema informático.

CE2.1 Explicar los métodos de configuración en el sistema: almacenamiento de los recursos, perfiles de usuario, permisos de acceso y ejecución y variables de entorno, entre otros para adecuar los parámetros de instalación y configuración del servidor de mensajería electrónica.

CE2.2 Describir los mecanismos de autenticación de usuarios y su correlación con el servicio de mensajería electrónica.

CE2.3 Explicar los mecanismos de acceso a los servidores: protocolos, direccionamiento y puertos, entre otros para acceder al servicio de mensajería electrónica.

CE2.4 Describir los procesos de arranque y parada, y de rotación de registros en lo que se refiere al servicio de mensajería electrónica.

CE2.5 A partir de un supuesto práctico de servicio de mensajería electrónica a instalar:

- Comprobar que el sistema reúne las características necesarias para la instalación de los servidores.
- Establecer en el sistema la estructura de almacenamiento de los recursos, los permisos de acceso y ejecución y las variables de entorno necesarios.
- Instalar el software del servidor y establecer los procesos de arranque y parada, y de rotación de registros (logs).
- Configurar en el servidor de mensajería electrónica los mecanismos de acceso: protocolos, direcciones IP, dominios y puertos.
- Establecer la configuración del servidor DNS para la localización del servicio.
- Habilitar los mecanismos especificados de autenticación de usuarios.
- Verificar la instalación del servidor de mensajería electrónica.
- Generar la documentación de operación y recuperación ante fallos.

Contenidos

1. Conceptos básicos sobre mensajería electrónica.

- Correo Electrónico:
  - Formato de un mensaje de correo.
  - Flujo de un mensaje de correo.
  - Protocolos de red: DNS. SMTP. POP. IMAP. Otros protocolos propietarios.
  - Aplicaciones Cliente y Servidor: MUA. MTA. Servidores POP/IMAP y otros
  - Amenazas y métodos de contención: Spam y Virus. Filtros antivirus/ antispam, SPF, Domain Keys, SenderId. Otras amenazas.
- Mensajería electrónica instantánea.
- Foros.
- Chat.
- Listas de correo.

2. Instalación de un sistema de correo.

- Diseño del sistema correo:
  - Requisitos funcionales, operativos y de seguridad.
  - Normativa legal.
  - Selección hardware y software.
- Instalación del operativo del servidor:
  - Instalación mínima.

cve: BOE-A-2011-10055

- Securización (bastionamiento).
- Instalación y configuración del servidor SMTP (MTA):
  - Instalación software.
  - Configuración como MX: Parámetros de configuración. Protocolos y puertos de acceso. Dominios y cuentas.
  - Configuración como MTA: Parámetros de configuración. Protocolos y puertos de acceso. Autenticación de usuarios .
  - Instalación y configuración de un sistema de filtros antivirus/antispam.
  - Procesos de arranque y parada.
  - Registros (logs).
- Instalación y configuración del servidor POP/IMAP:
  - Instalación software.
  - Parámetros de configuración. Protocolos y puertos de acceso.
  - Autenticación de usuarios.
  - Procesos de arranque y parada.
  - Registros (logs).
- Instalación y configuración del servidor Web (Webmail):
  - Instalación software.
  - Parámetros de configuración. Protocolos y puertos de acceso.
  - Autenticación de usuarios.
  - Procesos de arranque y parada.
  - Registros (logs).
- Elaboración del Manual de Operación.

UNIDAD FORMATIVA 2

Denominación: ADMINISTRACIÓN Y AUDITORÍA DE LOS SERVICIOS DE MENSAJERÍA ELECTRÓNICA

Código: UF1274

Duración: 60 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2 y RP3.

Capacidades y criterios de evaluación

C1: Administrar los servidores de mensajería electrónica para asegurar la continuidad en el servicio según las especificaciones de seguridad.

CE1.1 Definir los procedimientos de gestión de cuentas de usuarios en el servicio de mensajería electrónica.

CE1.2 Explicar las técnicas de administración de recursos de almacenamiento y gestión de buzones para el servidor de mensajería electrónica.

CE1.3 Describir la comunicación de los servidores de mensajería electrónica con otros servidores y aplicaciones.

CE1.4 Explicar las técnicas de protección informática del servicio y de los usuarios según las especificaciones de las normas de seguridad informática.

CE1.5 Describir las medidas para optimización del rendimiento de los servidores.

CE1.6 A partir de un supuesto práctico de servicio de mensajería electrónica en producción:

- Definir la política de gestión de cuentas de usuarios.
- Implantar las herramientas de seguridad más adecuadas a los requisitos del servicio y las condiciones de operación.
- Analizar los parámetros de rendimiento del servidor.

cve: BOE-A-2011-10055

- Establecer planes de actuación para adaptar el servidor a las variaciones de uso y planes de contingencia.

CE1.7 Explicar la normativa legal vigente que afecta a la información manejada por el servidor de mensajería electrónica.

C2: Aplicar procedimientos de auditoría y resolución de incidencias en servicios de mensajería electrónica.

CE2.1 Describir y clasificar los elementos determinantes del rendimiento de un servidor de mensajería electrónica.

CE2.2 Explicar los procedimientos de cuantificación y medición de la calidad de servicio prestada.

CE2.3 Explicar los procedimientos de diagnóstico de incidencias en entornos de producción de servicios de mensajería electrónica.

CE2.4 Describir detalladamente las técnicas de resolución de incidencias en entornos de producción de servicios de mensajería electrónica.

CE2.5 A partir de un supuesto práctico de servicio de mensajería electrónica en producción:

- Verificar que las operaciones definidas en los manuales de procedimiento se realizan puntual y convenientemente.
- Establecer los mecanismos de medición del rendimiento y disponibilidad del servicio.
- Analizar los parámetros de calidad del servicio para determinar el grado de cumplimiento de las especificaciones.
- Aplicar las medidas correctoras de las deficiencias encontradas.

CE2.6 A partir de un supuesto práctico de servicio de mensajería electrónica en producción en situación de incidencia:

- Aplicar las técnicas y herramientas de diagnóstico que permitan identificar la causa del mal funcionamiento.
- Aplicar medidas urgentes de contención para mantener el máximo nivel de servicio posible y limitar los posibles daños.
- Establecer los procedimientos para la resolución definitiva del problema y la recuperación de la situación previa a la incidencia.
- Analizar la causa de la incidencia y establecer los procedimientos para prevenir otra situación similar o resolverla en menor tiempo.

Contenidos

1. Administración del sistema de correo.

- Administración del sistema:
  - Gestión de cuentas de usuario.
  - Administración de recursos de almacenamiento.
  - Gestión de buzones.
- Optimización del rendimiento del sistema:
  - Elementos determinantes del rendimiento: Hardware. Sistema Operativo. Aplicaciones.
  - Ajustes de rendimiento del Sistema Operativo.
  - Ajustes de rendimiento de las aplicaciones: Servidor SMTP. Servidor POP/IMAP. Servidor Web, filtros antivirus/antispam.
  - Escalado de un sistema de correo: Separación de servicios. Balanceo de carga, alta disponibilidad.
- Monitorización del sistema:
  - Configuración de un sistema de monitorización.
  - Monitorización de los parámetros de rendimiento más importantes del sistema.
- Securización del sistema:

cve: BOE-A-2011-10055

- Adecuación a la Normativa legal (LSSI,LOPD) y a las políticas de seguridad de la organización.
- Códigos de buenas prácticas (ISO 27002)
- Recuperación ante desastres y continuidad de los servicios.
- Copias de Seguridad.
- Gestión de actualizaciones.
- Protección servicios: Firewall. Herramientas seguridad (Nmap, Nessus/ OpenVAS, Brutus).

2. **Auditoría y resolución de incidencias sobre los servicios de mensajería electrónica.**
   - Auditoría:
     - Plan de Pruebas.
     - Disponibilidad del servicio.
     - Acuerdos de prestación de Servicio (SLAs).
     - Alta disponibilidad en sistemas de correo.
   - Técnicas de resolución de incidentes:
     - Medidas de contención. Workarounds.
     - Análisis causa – raíz.
     - Gestión proactiva de problemas.
   - Análisis y utilización de herramientas para la resolución de incidencias:
     - Monitorización.
     - Logs.
     - Herramientas del Sistemas Operativo.
     - Herramientas de las aplicaciones.

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 - UF1273	60	30
Unidad formativa 2 - UF1274	60	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.

MÓDULO FORMATIVO 3

Denominación: ADMINISTRACIÓN DE SERVICIOS DE TRANSFERENCIA DE ARCHIVOS Y CONTENIDOS MULTIMEDIA

Código: MF0497_3

Nivel de cualificación profesional: 3

cve: BOE-A-2011-10055

Asociado a la Unidad de Competencia:

UC0497_3: Instalar, configurar y administrar servicios de transferencia de archivos y multimedia.

Duración: 120 horas

UNIDAD FORMATIVA 1

Denominación: SELECCIÓN, INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LOS SERVIDORES DE TRANSFERENCIA DE ARCHIVOS

Código: UF1275

Duración: 70 horas

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

Capacidades y criterios de evaluación

C1: Seleccionar los servidores de transferencia de archivos en función de los requisitos demandados por la organización.

CE1.1 Describir el funcionamiento de los servidores de transferencia de archivos

CE1.2 Describir las características más significativas de los servidores de transferencia de archivos, para determinar su adecuación a un determinado servicio.

CE1.3 Relacionar los parámetros cuantitativos y cualitativos de configuración de los servidores de transferencia de archivos con los requisitos de sistema correspondientes.

CE1.4 A partir de un supuesto práctico de servicio de transferencia de archivos a instalar:

- Identificar la funcionalidad requerida en la especificación de los servicios.
- Estimar la carga y el rendimiento esperado.
- Identificar el nivel y los requisitos de seguridad.
- Seleccionar el servidor o servidores más adecuados a los requisitos.
- Estimar los requisitos de sistema e indicar las plataformas hardware y software más adecuadas.

C2: Instalar, configurar e integrar el servidor de transferencia de archivos en el sistema informático.

CE2.1 Explicar los métodos de configuración en el sistema del servidor de transferencia de archivos, tales como almacenamiento de los recursos, perfiles de usuario, permisos de acceso y variables de entorno entre otros.

CE2.2 Describir los mecanismos habituales de autenticación de usuarios en estos servidores.

CE2.3 Explicar los mecanismos de acceso a los servidores: protocolos, direccionamiento, puertos en estos servidores.

C3: Administrar los recursos y elementos manejados por el servidor para asegurar la continuidad del servicio, su adecuado rendimiento y las especificaciones de seguridad.

CE3.1 Describir procedimientos de actualización de contenidos y control de versiones

CE3.2 Describir las técnicas de gestión de permisos y cuentas de usuarios.

CE3.3 Explicar las técnicas de administración de recursos de almacenamiento.

CE3.4 Describir las medidas para optimización del rendimiento de los servidores.

cve: BOE-A-2011-10055

CE3.5 A partir de un supuesto práctico de servicio de transferencia de archivos en producción:
- Definir la organización de los contenidos en el servidor de transferencia de archivos.
- Establecer los procedimientos de actualización y control de versiones.
- Implantar el sistema de control de acceso a la información.
- Analizar los parámetros de rendimiento del servidor.
- Establecer planes de actuación para adaptar el servidor a las variaciones de uso.

CE3.6 Explicar la normativa legal vigente que afecta a la información publicada en el servidor de transferencia de archivos.

C4: Aplicar procedimientos de auditoría y resolución de incidencias en el servicio de transferencia de archivos.

CE4.1 Describir y clasificar los elementos determinantes del rendimiento de un servidor de transferencia de archivos.

CE4.2 Explicar los procedimientos de cuantificación y medición de la calidad de servicio prestada.

CE4.3 Explicar los procedimientos de diagnóstico de incidencias en entornos de producción de servicios de transferencia de archivos.

CE4.4 Describir detalladamente las técnicas de resolución de incidencias en entornos de producción de servicios de transferencia de archivos.

CE4.5 A partir de un supuesto práctico de servicio de transferencia de archivos en producción:
- Verificar que las operaciones definidas en los manuales de procedimiento se realizan puntual y convenientemente.
- Establecer los mecanismos de medición del rendimiento y disponibilidad del servicio.
- Analizar los parámetros de calidad del servicio para determinar el grado de cumplimiento de las especificaciones.
- Aplicar las medidas correctoras de las deficiencias encontradas.

CE4.6 A partir de un supuesto práctico de servicio de transferencia de archivos en producción en situación de incidencia:
- Aplicar las técnicas y herramientas de diagnóstico que permitan identificar la causa del mal funcionamiento.
- Aplicar medidas urgentes de contención para mantener el máximo nivel de servicio posible y limitar los posibles daños.
- Establecer los procedimientos para la resolución definitiva del problema y la recuperación de la situación previa a la incidencia.
- Analizar la causa de la incidencia y establecer los procedimientos para prevenir otra situación similar o resolverla en menor tiempo.

Contenidos

1. Características de los distintos servidores de transferencia de archivos.
- Transferencia de archivos en Internet.
- Formatos de archivos.
- Protocolos específicos de transferencia de archivos.
- Aplicaciones. Servidor y Cliente.
- Ancho de banda y tipos de accesos.
- Servicios de ficheros:
  - NFS.
  - CIFS / Samba.
  - Samba.

cve: BOE-A-2011-10055

2. **Instalación y Configuración de servidores de transferencia de archivos.**
   - Funcionamiento y tipos de servidores.
   - Plataformas habituales HW y SW:
     - Requisitos HW habituales
     - Requisitos SW habituales
   - Características y parámetros de configuración principales:
     - Direccionamiento.
     - Puertos.
     - Encriptación. Permisos.
     - Cuotas.
   - Gestión del almacenamiento:
     - Cuotas y watermarks.
     - Almaceramiento externo.
     - Directorios virtuales
   - Configuración del acceso:
     - Creación de usuarios y permisos.
     - Acceso anónimo.
     - Acceso autenticado.
     - Máscaras de creación automática de permisos.
     - Seguridad de acceso.
   - Requisitos de sistema para la instalación de servidores de transferencia de archivos en distintas plataformas:

3. **Administración del servidor**
   - Actualización de contenidos.
   - Control de versiones.
   - Cuentas de usuarios.
   - Registros del sistema (logs).

4. **Auditoría del servicio.**
   - Metodología de medición y evaluación de la calidad de servicio.
   - Rendimientos del servidor.
   - Parámetros de calidad.
   - Plan de Pruebas.
   - Disponibilidad del servicio.
   - SLAs.
   - Alta disponibilidad en transferencia de archivos.
   - Normativa legal vigente sobre la información publicada en servidores de transferencia de archivos.

5. **Técnicas de resolución de incidentes.**
   - Técnicas de diagnóstico de incidentes.
   - Medidas de contención. Workarounds.
   - Análisis causa – raíz.
   - Gestión proactiva de problemas.
   - Herramientas para la resolución de incidencias:
     - Monitorización.
     - Logs.

UNIDAD FORMATIVA 2

Denominación: SELECCIÓN, INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LOS SERVIDORES MULTIMEDIA

Código: UF1276

cve: BOE-A-2011-10055

Duración: 50 horas

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

Capacidades y criterios de evaluación

C1: Seleccionar los servidores de contenidos multimedia en función de los requisitos demandados por la organización.

CE1.1 Describir el funcionamiento de los servidores de contenidos multimedia.

CE1.2 Describir las características más significativas de los servidores de contenidos multimedia, para determinar su adecuación a un determinado servicio.

CE1.3 Relacionar los parámetros cuantitativos y cualitativos de configuración de los servidores de contenidos multimedia con los requisitos de sistema correspondientes.

CE1.4 A partir de un supuesto práctico de servicio de contenidos multimedia a instalar:

- Identificar la funcionalidad requerida en la especificación de los servicios.
- Estimar la carga y el rendimiento esperado.
- Identificar el nivel y los requisitos de seguridad.
- Seleccionar el servidor o servidores más adecuados a los requisitos.
- Estimar los requisitos de sistema e indicar las plataformas hardware y software más adecuadas.

C2: Instalar, configurar e integrar el servidor de contenidos multimedia en el sistema informático.

CE2.1 Explicar los métodos de configuración en el sistema del servidor de contenidos multimedia, tales como almacenamiento de los recursos, perfiles de usuario, permisos de acceso y variables de entorno entre otros.

CE2.2 Describir los mecanismos habituales de autenticación de usuarios en estos servidores.

CE2.3 Explicar los mecanismos de acceso a los servidores: protocolos, direccionamiento, puertos en estos servidores.

CE2.4 A partir de un supuesto práctico de servicio multimedia a instalar:

- Comprobar que el sistema reúne las características necesarias para la instalación de los servidores.
- Establecer en el sistema la estructura de almacenamiento de los recursos, los permisos de acceso y las variables de entorno necesarios.
- Instalar el software del servidor y establecer los procesos de arranque y parada, y de rotación de registros (logs).
- Configurar en el servidor los mecanismos de acceso: protocolos, direcciones IP, URLs de acceso, dominios y puertos.
- Habilitar los mecanismos especificados de autenticación de usuarios.
- Verificar la instalación del servidor multimedia.
- Generar la documentación de operación y recuperación ante fallos.

C3: Administrar los recursos y elementos manejados por el servidor para asegurar la continuidad del servicio, su adecuado rendimiento y las especificaciones de seguridad.

CE3.1 Describir procedimientos de actualización de contenidos y control de versiones

CE3.2 Describir las técnicas de gestión de permisos y cuentas de usuarios.

CE3.3 Explicar las técnicas de administración de recursos de almacenamiento.

CE3.4 Describir la comunicación de los servidores multimedia con otros servidores y aplicaciones.

CE3.5 Describir las medidas para optimización del rendimiento de los servidores.

cve: BOE-A-2011-10055

CE3.6 A partir de un supuesto práctico de servicio multimedia en producción:
- Definir la organización de los contenidos en el servidor multimedia.
- Establecer los procedimientos de actualización y control de versiones.
- Implantar el sistema de control de acceso a la información.
- Analizar los parámetros de rendimiento del servidor.
- Establecer planes de actuación para adaptar el servidor a las variaciones de uso.

CE3.7 Explicar la normativa legal vigente que afecta a la información publicada en el servidor de contenidos multimedia.

C4: Aplicar procedimientos de auditoría y resolución de incidencias en el servicio de contenidos multimedia.

CE4.1 Describir y clasificar los elementos determinantes del rendimiento de un servidor multimedia.

CE4.2 Explicar los procedimientos de cuantificación y medición de la calidad de servicio prestada.

CE4.3 Explicar los procedimientos de diagnóstico de incidencias en entornos de producción de servicios multimedia.

CE4.4 Describir detalladamente las técnicas de resolución de incidencias en entornos de producción de servicios multimedia.

CE4.5 A partir de un supuesto práctico de servicio multimedia en producción:
- Verificar que las operaciones definidas en los manuales de procedimiento se realizan puntual y convenientemente.
- Establecer los mecanismos de medición del rendimiento y disponibilidad del servicio.
- Analizar los parámetros de calidad del servicio para determinar el grado de cumplimiento de las especificaciones.
- Aplicar las medidas correctoras de las deficiencias encontradas.

CE4.6 A partir de un supuesto práctico de servicio multimedia en producción en situación de incidencia:
- Aplicar las técnicas y herramientas de diagnóstico que permitan identificar la causa del mal funcionamiento.
- Aplicar medidas urgentes de contención para mantener el máximo nivel de servicio posible y limitar los posibles daños.
- Establecer los procedimientos para la resolución definitiva del problema y la recuperación de la situación previa a la incidencia.
- Analizar la causa de la incidencia y establecer los procedimientos para prevenir otra situación similar o resolverla en menor tiempo.

Contenidos

1. **Características de los distintos servidores de transferencia de archivos multimedia.**
   - Tipos de archivos y contenidos multimedia.
   - Protocolos específicos de transferencia de archivos multimedia.
   - Aplicaciones para servicios multimedia:
     - Windows Media.
     - Real Time.
     - Flash.
     - Otros.
   - Ancho de banda y tipos de accesos para contenidos multimedia.
   - Streaming:
     - Difusión.
     - Emisión.

cve: BOE-A-2011-10055

2. **Instalación y configuración de servidores de transferencia de archivos multimedia.**
   - Funcionamiento y tipos de servidores multimedia.
   - Plataformas habituales HW y SW para multimedia:
     - Requisitos HW habituales.
     - Requisitos SW habituales.
   - Características y parámetros de configuración principales:
     - Direccionamiento.
     - Puertos.
     - Permisos.
   - Configuración del acceso a contenidos multimedia:
     - Acceso anónimo.
     - Acceso autenticado.
     - Máscaras de creación automática de permisos.
     - Seguridad de acceso.
   - Requisitos de sistema para la instalación de servidores de transferencia de archivos multimedia en distintas plataformas:

3. **Administración del servidor multimedia.**
   - Actualización de contenidos multimedia.
   - Control de versiones.
   - Cuentas de usuarios.
   - Registros del sistema (logs).

4. **Auditoría del servicio multimedia.**
   - Medición y evaluación de la calidad de servicios multimedia.
   - Rendimiento y parámetros específicos del servidor multimedia.
   - Pruebas específicas para servicios multimedia.
   - Disponibilidad de servicios multimedia.
   - Alta disponibilidad en servicios de transferencia de archivos multimedia.

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 - UF1275	70	30
Unidad formativa 2 - UF1276	50	20

Secuencia:

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

Criterios de acceso para los alumnos

Según 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: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

cve: BOE-A-2011-10055

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

CE1.1 Identificar los procesos del sistema y los parámetros que los caracterizan (procesos padre, estado del proceso, consumo de recursos, prioridades y usuarios afectados entre otros) para determinar su influencia en el rendimiento del sistema.

CE1.2 Describir cada una de las herramientas provistas por el sistema para la gestión de procesos con objeto de permitir la intervención en el rendimiento general del sistema.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema.

CE1.4 En un supuesto práctico en el que se cuenta con un sistema informático con una carga de procesos debidamente caracterizada:

- Utilizar las herramientas del sistema para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar las operaciones de activación, desactivación y modificación de prioridad entre otras con un proceso utilizando las herramientas del sistema.
- Monitorizar el rendimiento del sistema mediante herramientas específicas y definir alarmas, que indiquen situaciones de riesgo.

C2: Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

CE2.1 Identificar los distintos sistemas de archivo utilizables en un dispositivo de almacenamiento dado para optimizar los procesos de registro y acceso a los mismos.

CE2.2 Explicar las características de los sistemas de archivo en función de los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento en el sistema informático asociando los dispositivos con los distintos sistemas de archivos existentes.

CE2.4 En un supuesto práctico en el que se dispone de un sistema de almacenamiento de la información con varios dispositivos:

- Realizar el particionamiento, en los casos que sea necesario, y la generación de la infraestructura de los sistemas de archivo a instalar en cada dispositivo.
- Implementar la estructura general de almacenamiento integrando todos los dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado.

C3: Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

cve: BOE-A-2011-10055

CE3.1 Identificar las posibilidades de acceso al sistema distinguiendo los accesos remotos de los accesos locales.
CE3.2 Describir las herramientas que se utilizan en la gestión de permisos a usuarios para el uso de los recursos del sistema.
CE3.3 En un supuesto práctico en el que se cuenta con derecho de administración de usuarios:
- Identificar los posibles accesos de un usuario al sistema.
- Modificar los permisos de utilización de un recurso del sistema a un usuario.
- Definir limitaciones de uso de un recurso del sistema a los usuarios.

C4: Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados.
CE4.1 Explicar los parámetros de configuración y funcionamiento de los dispositivos de comunicaciones para asegurar su funcionalidad dentro del sistema.
CE4.2 Relacionar los servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos con objeto de analizar y evaluar el rendimiento.
CE4.3 En un supuesto práctico en el que tomamos un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:
- Identificar los dispositivos de comunicaciones y describir sus características.
- Verificar el estado de los servicios de comunicaciones.
- Evaluar el rendimiento de los servicios de comunicaciones.
- Detectar y documentar las incidencias producidas en el sistema.

Contenidos

1. Gestión de la seguridad y normativas
- Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
- Metodología ITIL Librería de infraestructuras de las tecnologías de la información
- Ley orgánica de protección de datos de carácter personal.
- Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

2. Análisis de los procesos de sistemas
- Identificación de procesos de negocio soportados por sistemas de información
- Características fundamentales de los procesos electrónicos:
  - Estados de un proceso,
  - Manejo de señales, su administración y los cambios en las prioridades
- Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
- Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
- Técnicas utilizadas para la gestión del consumo de recursos

3. Demostración de sistemas de almacenamiento
- Tipos de dispositivos de almacenamiento más frecuentes
- Características de los sistemas de archivo disponibles
- Organización y estructura general de almacenamiento
- Herramientas del sistema para gestión de dispositivos de almacenamiento

cve: BOE-A-2011-10055

4. **Utilización de métricas e indicadores de monitorización de rendimiento de sistemas**
   - Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información
   - Identificación de los objetos para los cuales es necesario obtener indicadores
   - Aspectos a definir para la selección y definición de indicadores
   - Establecimiento de los umbrales de rendimiento de los sistemas de información
   - Recolección y análisis de los datos aportados por los indicadores
   - Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

5. **Confección del proceso de monitorización de sistemas y comunicaciones**
   - Identificación de los dispositivos de comunicaciones
   - Análisis de los protocolos y servicios de comunicaciones
   - Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
   - Procesos de monitorización y respuesta
   - Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
   - Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
   - Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
   - Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

6. **Selección del sistema de registro de en función de los requerimientos de la organización**
   - Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
   - Análisis de los requerimientos legales en referencia al registro
   - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
   - Asignación de responsabilidades para la gestión del registro
   - Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
   - Guía para la selección del sistema de almacenamiento y custodia de registros

7. **Administración del control de accesos adecuados de los sistemas de información**
   - Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
   - Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
   - Requerimientos legales en referencia al control de accesos y asignación de privilegios
   - Perfiles de de acceso en relación con los roles funcionales del personal de la organización
   - Herramientas de directorio activo y servidores LDAP en general
   - Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
   - Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

cve: BOE-A-2011-10055

Orientaciones metodológicas

Formación a distancia:

Módulo formativo	Número de horas totales del módulo	Nº. de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0490_3	90	40

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 DE PRÁCTICAS PROFESIONALES NO LABORALES DE ADMINISTRACIÓN DE SERVICIOS DE INTERNET

Código: MP0267

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Proporcionar soporte técnico en la implementación y administración de servicios Web, mensajería electrónica y transferencia de archivos.

CE1.1 Proporcionar asistencia técnica en el diseño y configuración de servicios Web (Apache e IIS).

CE1.2 Proporcionar asistencia técnica en el diseño y configuración de servicios de mensajería electrónica.

CE1.3 Proporcionar asistencia técnica en el diseño y configuración de servicios de transferencia de archivos.

C2: Participar con el soporte adecuado de los procesos de auditoría y mantenimiento de servicios Web, mensajería electrónica y transferencia de archivos.

CE2.1 Colaborar en el mantenimiento de los servicios Web de la empresa, monitorizando los sistemas correspondientes, y participando con el departamento técnico en la resolución de incidencias.

CE2.2 Colaborar en el mantenimiento de los servicios de mensajería electrónica de la empresa, monitorizando los sistemas correspondientes, y participando con el departamento técnico en la resolución de incidencias.

CE2.3 Colaborar en el mantenimiento de los servicios de transferencia de archivos de la empresa, monitorizando los sistemas correspondientes, y participando con el departamento técnico en la resolución de incidencias.

C3: Participar en los procesos 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.

cve: BOE-A-2011-10055

CE3.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. **Implementación y administración de Servicios Web.**
   - Comprobar requisitos de instalación, y dar soporte en la elección del servidor.
   - Colaborar en la instalación y configuración de servidores Web.
   - Dar soporte en las verificaciones y testeos, así como la documentación del sistema.

2. **Implementación y administración de Servicios de mensajería electrónica.**
   - Comprobar requisitos de instalación, y dar soporte en la elección del servidor.
   - Colaborar en la instalación y configuración de servicios de mensajería electrónica.
   - Dar soporte en las verificaciones y testeos, así como la documentación del sistema.

3. **Implementación y administración de Servicios de transferencia de archivos.**
   - Comprobar requisitos de instalación, y dar soporte en la elección del servidor.
   - Colaborar en la instalación y configuración de los servicios de transferencia de archivos.
   - Ayudar en la instalación y configuración de servicios de transferencia de archivos multimedia, teniendo en cuenta sus particularidades.
   - Dar soporte en las verificaciones y testeos, así como la documentación del sistema.

4. **Auditoría y mantenimiento de Servicios Web, mensajería electrónica y transferencia de archivos.**
   - Dar soporte en el análisis de rendimiento y optimización del sistema.
   - Colaborar en las actualizaciones del sistema y su monitorización, así como en el proceso de resolución de incidencias.
   - Participar en la generación de toda la documentación.

5. **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 del proceso productivo de la organización.
   - Utilización 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.

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	Experiencia profesional requerida en el ámbito de la unidad de competencia
MF0495_3: Instalar, configurar y administrar el software para gestionar un entorno Web	• 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.	1 año

cve: BOE-A-2011-10055

Módulos Formativos	Acreditación requerida	Experiencia profesional requerida en el ámbito de la unidad de competencia
MF0496_3: Instalar, configurar y administrar servicios de mensajería electrónica	• 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.	1 año
MF0497_3: Instalar, configurar y administrar servicios de transferencia de archivos y multimedia	• 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.	1 año
MF0490_3: Gestionar servicios en el sistema informático	• 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.	2 años

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m^2 15 alumnos	Superficie m^2 25 alumnos
Aula de gestión	45	60

Espacio Formativo	M1	M2	M3	M4
Aula de gestión	X	X	X	X

Espacio Formativo	Equipamiento
Aula de gestión	- Equipos audiovisuales - Cañón y pantalla de proyección - Ordenador en funciones de servidor para casos prácticos - Ordenadores en funciones de puesto en red para los casos prácticos - Internet - Pizarra para escribir con rotulador o Rotafolios - Material de aula - Mesa y silla para formador - Mesas y sillas para alumnos

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

cve: BOE-A-2011-10055

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 VI

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: PROGRAMACIÓN DE SISTEMAS INFORMÁTICOS

Código: IFCT0609

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC303_3 Programación de sistemas informáticos (RD 1201/2007, de 14 de septiembre)

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

UC0490_3: Gestionar servicios en el sistema informático.
UC0964_3: Crear elementos software para la gestión del sistema y sus recursos
UC0965_3: Desarrollar elementos software con tecnologías de programación basada en componentes.

Competencia general:

Desarrollar componentes software a partir de unas especificaciones concretas, proporcionando funciones de administración y supervisión del sistema operativo, para la gestión de los recursos de un sistema informático y la interacción con otros sistemas utilizando tecnologías de desarrollo orientadas a objetos y a componentes.

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional tanto por cuenta propia, como 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 o de desarrollo 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 que tienen como objetivo de negocio la comercialización de servicios de

cve: BOE-A-2011-10055

análisis, diseño y construcción de aplicaciones informáticas; grandes organizaciones, siendo parte del equipo de programación y mantenimiento de sistemas informáticos.

Ocupaciones o puestos de trabajo relacionados:

2711.1019 Analista de Sistemas, nivel superior
2712.1030 Analista Programador, nivel medio
2712.1012 Analista de Aplicaciones, nivel medio
3820.1017 Programador de Aplicaciones Informáticas
Programador de sistemas.
Programador de componentes.

Duración de la formación asociada: 590 horas

Relación de módulos formativos y de unidades formativas:

MF0490_3: (Transversal) Gestión de servicios en el sistema informático. (90 horas)
MF0964_3: Desarrollo de elementos software para gestión de sistemas. (210 horas)
- UF1286: Desarrollo y optimización de componentes software para tareas administrativas de sistemas. (90 horas)
- UF1287: Desarrollo de componentes software para el manejo de dispositivos (drivers). (60 horas)
- UF1288: Desarrollo de componentes software para servicios de comunicaciones. (60 horas)

MF0965_3: Desarrollo de software basado en tecnologías orientadas a componentes. (210 horas)
- UF1289: Diseño de elementos software con tecnologías basadas en componentes (90 horas)
- UF1290: Implementación e integración de elementos software con tecnologías basadas en componentes (90 horas)
- UF1291: Despliegue y puesta en funcionamiento de componentes software (30 horas)

MP0274: Módulo de prácticas profesionales no laborales de Programación de Sistemas informáticos (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: GESTIONAR SERVICIOS EN EL SISTEMA INFORMÁTICO

Nivel: 3

Código: UC0490_3

Realizaciones profesionales y criterios de realización

RP1: Gestionar la configuración del sistema para asegurar el rendimiento de los procesos según las necesidades de uso y dentro de las directivas de la organización.

CR1.1 Los procesos que intervienen en el sistema son identificados para evaluar parámetros de rendimiento.

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

cve: BOE-A-2011-10055

CR1.3 Las prioridades de ejecución de los procesos se adecuan en función de las especificaciones del plan de explotación de la organización.
CR1.4 Las herramientas de monitorización se implantan y configuran determinando los niveles de las alarmas en función del plan de explotación de la organización.

RP2: Administrar los dispositivos de almacenamiento según las necesidades de uso y dentro de las directivas de la organización.
CR2.1 Los dispositivos de almacenamiento se configuran para ser usados en los distintos sistemas operativos utilizados en el sistema informático.
CR2.2 La estructura de almacenamiento se define y se implanta atendiendo a las necesidades de los distintos sistemas de archivos y a las especificaciones de uso de la organización.
CR2.3 Los requerimientos de nomenclatura de objetos y restricciones de uso de cada dispositivo de almacenamiento se documentan adecuadamente.
CR2.4 Los dispositivos de almacenamiento se integran para ofrecer un sistema funcional al usuario según las especificaciones de la organización.

RP3: Gestionar las tareas de usuarios para garantizar los accesos al sistema y la disponibilidad de los recursos según especificaciones de explotación del sistema informático.
CR3.1 El acceso de los usuarios al sistema informático se configura para garantizar la seguridad e integridad del sistema según las especificaciones de la organización.
CR3.2 El acceso de los usuarios a los recursos se administra mediante la asignación de permisos en función de las necesidades de la organización.
CR3.3 Los recursos disponibles para los usuarios se limitan con las herramientas adecuadas en base a lo especificado en las normas de uso de la organización.

RP4: Gestionar los servicios de red para asegurar la comunicación entre sistemas informáticos según necesidades de explotación.
CR4.1 Los dispositivos de comunicaciones son verificados en lo que respecta a su configuración y rendimiento según las especificaciones de la organización.
CR4.2 Los servicios de comunicaciones son identificados en el sistema con sus procesos correspondientes para analizar los consumos de recursos y verificar que están dentro de lo permitido por las especificaciones del plan de explotación de la organización.
CR4.3 Las incidencias en los servicios de comunicaciones se detectan y se documentan para informar a los responsables de la explotación del sistema y de la gestión de las comunicaciones según los protocolos de la organización.

Contexto profesional

Medios de producción

Sistemas operativos. Herramientas de administración de usuarios y gestión de permisos a recursos. Herramientas de control de rendimiento. Herramientas de monitorización de procesos. Herramientas de monitorización de uso de memoria. Herramientas de monitorización de gestión de dispositivos de almacenamiento. Herramientas de gestión de usuarios.

Productos y resultados

Sistema operando correctamente. Rendimiento del sistema adecuado a los parámetros de explotación. Sistema seguro e íntegro en el acceso y utilización de recursos. Servicios de comunicaciones en funcionamiento.

cve: BOE-A-2011-10055

Información utilizada o generada

Manuales de explotación del sistema operativo y de los dispositivos. Plan de explotación de la organización. Manuales de las herramientas de monitorización utilizadas. Gráficas y análisis de rendimiento. Listados de acceso y restricciones de usuarios. Informe de incidencias. Protocolo de actuación ante incidencias.

Unidad de competencia 2

Denominación: CREAR ELEMENTOS SOFTWARE PARA LA GESTIÓN DEL SISTEMA Y SUS RECURSOS

Nivel: 3

Código: UC0964_3

Realizaciones profesionales y criterios de realización

RP1: Desarrollar componentes software que implementen servicios y herramientas de gestión del sistema operativo, utilizando lenguajes orientados a la programación de sistemas, para soportar tareas administrativas según necesidades funcionales dadas.

CR1.1 Las especificaciones técnicas del servicio o herramienta de gestión a implementar, se analizan para identificar los recursos para el desarrollo del componente según necesidades funcionales detectadas.

CR1.2 Los diagramas y la documentación previa al desarrollo se realizan, para ser utilizados como soporte de la creación de los componentes según especificaciones de la organización.

CR1.3 El desarrollo del código del componente se realiza, asistido por el uso de herramientas editoras y depuradoras para optimizar los rendimientos según especificaciones de la organización.

CR1.4 Los componentes software que implementan los servicios y herramientas de gestión se programan, para dar soporte a las funciones definidas de acuerdo a las especificaciones técnicas del diseño suministrado.

CR 1.5 El plan de prueba se elabora con el fin de comprobar la funcionalidad de los componentes desarrollados, según especificaciones y criterios de calidad establecidos.

CR1.6 Los componentes software de servicios y de herramientas desarrollados se prueban y depuran, para corregir los errores utilizando las herramientas de depuración del entorno de programación según los criterios de calidad establecidos.

CR1.7 La documentación de los componentes software de servicios y herramientas de gestión se realiza, para cumplimentar el registro de la información producida siguiendo los patrones, normativa y procedimientos especificados en el diseño.

CR1.8 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP2: Codificar y utilizar funciones de las librerías del sistema en el desarrollo de componentes software, para optimizar los desarrollos según especificaciones técnicas y funcionales.

CR2.1 Las funciones documentadas de las librerías del sistema se identifican y catalogan, para facilitar la localización de la información de las mismas según necesidades de desarrollo.

cve: BOE-A-2011-10055

CR2.2 Las funciones de las librerías del sistema se utilizan en la elaboración de nuevos componentes software, para mejorar los rendimientos de los desarrollos mediante la reutilización del código escrito y probado, según las especificaciones técnicas de cada función y los requisitos de invocación de las mismas.

CR2.3 Los componentes software se desarrollan con los requisitos especificados, para ser incluidos en librerías para su posterior uso y distribución, según necesidades y especificaciones técnicas.

CR2.4 Las pruebas funcionales y estructurales del componente realizado se planifican y se realizan, para comprobar y asegurar los objetivos del desarrollo según especificaciones técnicas y de calidad de la organización.

CR2.5 La documentación de las librerías del sistema operativo desarrolladas se realiza, para cumplimentar las necesidades de registro siguiendo los patrones, normativa y procedimientos especificados en el diseño.

RP3: Elaborar componentes software utilizando lenguajes orientados a la programación de sistemas, según especificaciones establecidas para manejar dispositivos hardware.

CR3.1 La documentación técnica con las especificaciones de los dispositivos hardware se interpreta, para identificar las características y los parámetros de la programación del manejador de dispositivo, de acuerdo al diseño suministrado.

CR3.2 La documentación técnica de las herramientas software a utilizar y del sistema operativo se interpreta, para identificar las características y los parámetros de la programación del manejador de dispositivo de acuerdo al diseño suministrado.

CR3.3 Las herramientas de programación se utilizan para desarrollar y depurar los posibles errores del código desarrollado, según criterios de calidad de la organización.

CR3.4 Las pruebas del manejador del dispositivo elaborado se planifican y se realizan en los posibles escenarios en los que puede ser implantado, para asegurar su funcionalidad y la ausencia de conflictos con el resto de los componentes del sistema, según especificaciones técnicas y normativa de calidad de la organización.

CR3.5 La documentación técnica y de usuario del manejador desarrollado, se confecciona según los parámetros y la normativa de la organización.

CR3.6 La documentación técnica específica asociada, se interpreta, en su caso, en la lengua extranjera de uso más frecuente en el sector.

RP4: Confeccionar componentes software que implementen servicios de comunicaciones, para enlazar distintos sistemas según estándares de desarrollo.

CR4.1 Las especificaciones del servicio se interpretan para discriminar los elementos que intervendrán en el desarrollo del componente como puertos de comunicaciones entre los sistemas y protocolos estándares seleccionados, entre otros, según especificaciones y necesidades del servicio.

CR4.2 El desarrollo del componente se realiza en entornos cliente/servidor, para implementar las funcionalidades del servicio de comunicaciones según especificaciones técnicas y funcionales aportadas.

CR4.3 La codificación del componente se realiza utilizando herramientas de programación y depuración, para optimizar la fase de desarrollo según especificaciones de la organización.

CR4.4 El componente se somete a baterías de pruebas en réplicas de los posibles escenarios de su implantación posterior, para asegurar la funcionalidad e integridad según criterios de calidad y seguridad de la organización.

CR4.5 La documentación del desarrollo y pruebas realizadas se confecciona siguiendo los patrones, normativa y procedimientos especificados en el diseño.

cve: BOE-A-2011-10055

Contexto profesional

Medios de producción

Cortafuegos antivirus y servidores proxy.
Entornos integrados de desarrollo.
Equipos informáticos, periféricos y dispositivos hardware.
Herramientas de control de cambios.
Herramientas de prueba.
Herramientas de depuración.
Herramientas de desarrollo o entornos integrados (IDE).
Herramientas de distribución de aplicaciones.
Herramientas de documentación de elementos de programación.
Herramientas ofimáticas.
Lenguajes 4GL.
Lenguajes estructurados.
Lenguajes orientados a objetos.
Lenguajes de programación concurrentes.

Productos y resultados

Código ejecutable y código fuente del software desarrollado.
Procedimientos y casos de prueba desarrollados.
Programas de prueba.
Sistema operativo y aplicaciones configurados y parametrizados de acuerdo a las necesidades.

Información utilizada o generada

Documentación sobre los casos y datos de prueba desarrollados.
Documentación técnica del diseño del software a desarrollar.
Documentación técnica y de usuario del software desarrollado.
Manuales de funcionamiento del software.
Manuales de interfaces de programación (API) del sistema operativo.
Manuales de la herramienta de programación empleada.
Manuales de uso del sistema operativo.
Manuales del entorno de programación (IDE).
Manuales del lenguaje de programación empleado.
Manuales técnicos del dispositivo hardware a programar.
Normas corporativas de desarrollo de software, de pruebas, de control de calidad.
Sistemas de ayuda de las aplicaciones informáticas.
Soportes técnicos para asistencia (telefónica, Internet, mensajería y foros, entre otros).

Unidad de competencia 3

Denominación: DESARROLLAR ELEMENTOS SOFTWARE CON TECNOLOGÍAS DE PROGRAMACIÓN BASADA EN COMPONENTES

Nivel: 3

Código: UC0965_3

Realizaciones profesionales y criterios de realización

RP1: Realizar el diseño del componente software, para su posterior desarrollo según la tecnología de componentes especificada.

cve: BOE-A-2011-10055

Contexto profesional

Medios de producción
Entornos integrados de desarrollo.
Equipos informáticos y periféricos de comunicaciones.
Herramientas de control de cambios.
Herramientas de depuración.
Herramientas de desarrollo o entornos integrados (IDE).
Herramientas de distribución de aplicaciones.
Herramientas de documentación de elementos de programación.
Herramientas de gestión de cambios, incidencias y configuración.
Herramientas de prueba.
Herramientas ofimáticas.
Lenguajes 4GL.
Lenguajes de manipulación de datos.
Lenguajes estructurados.
Lenguajes orientados a objetos.
Servicios de transferencia de ficheros y mensajería.
Sistemas operativos y parámetros de configuración.

Productos y resultados
Código ejecutable y código fuente del software desarrollado.
Paquete de instalación y/o despliegue del software desarrollado.
Procedimientos y casos de prueba.
Programas de prueba realizados.
Sistema informático en funcionamiento con un rendimiento óptimo y una utilización adecuada de sus recursos.
Sistema operativo y aplicaciones configurados y parametrizados de acuerdo a las necesidades.

Información utilizada o generada
Documentación sobre los casos y datos de prueba desarrollados.
Documentación técnica del diseño del software a desarrollar.
Documentación técnica y de usuario del software desarrollado.
Manuales de interfaces de programación (API) del sistema operativo.
Manuales de uso del sistema operativo. Manuales de uso y funcionamiento de los sistemas informáticos.
Manuales del entorno de programación (IDE).
Manuales del lenguaje de programación.
Manuales del lenguaje de programación empleado.
Manuales técnicos de los dispositivos de comunicaciones sobre los que se vaya a programar.
Normas corporativas de desarrollo de software, de pruebas, de control de calidad.
Soportes técnicos de asistencia (telefónica, Internet, mensajería y foros, entre otros).

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Código: MF0490_3

cve: BOE-A-2011-10055

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0490_3: Gestionar servicios en el sistema informático

Duración: 90 horas

Capacidades y criterios de evaluación

C1: Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

CE1.1 Identificar los procesos del sistema y los parámetros que los caracterizan (procesos padre, estado del proceso, consumo de recursos, prioridades y usuarios afectados entre otros) para determinar su influencia en el rendimiento del sistema.

CE1.2 Describir cada una de las herramientas provistas por el sistema para la gestión de procesos con objeto de permitir la intervención en el rendimiento general del sistema.

CE1.3 Explicar técnicas de monitorización y herramientas destinadas a evaluar el rendimiento del sistema.

CE1.4 En un supuesto práctico en el que se cuenta con un sistema informático con una carga de procesos debidamente caracterizada:

- Utilizar las herramientas del sistema para identificar cuantos procesos activos existen y las características particulares de alguno de ellos.
- Realizar las operaciones de activación, desactivación y modificación de prioridad entre otras con un proceso utilizando las herramientas del sistema.
- Monitorizar el rendimiento del sistema mediante herramientas específicas y definir alarmas, que indiquen situaciones de riesgo.

C2: Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

CE2.1 Identificar los distintos sistemas de archivo utilizables en un dispositivo de almacenamiento dado para optimizar los procesos de registro y acceso a los mismos.

CE2.2 Explicar las características de los sistemas de archivo en función de los dispositivos de almacenamiento y sistemas operativos empleados.

CE2.3 Describir la estructura general de almacenamiento en el sistema informático asociando los dispositivos con los distintos sistemas de archivos existentes.

CE2.4 En un supuesto práctico en el que se dispone de un sistema de almacenamiento de la información con varios dispositivos:

- Realizar el particionamiento, en los casos que sea necesario, y la generación de la infraestructura de los sistemas de archivo a instalar en cada dispositivo.
- Implementar la estructura general de almacenamiento integrando todos los dispositivos y sus correspondientes sistemas de archivos.
- Documentar los requerimientos y restricciones de cada sistema de archivos implantado.

C3: Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

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

cve: BOE-A-2011-10055

CE3.2 Describir las herramientas que se utilizan en la gestión de permisos a usuarios para el uso de los recursos del sistema.
CE3.3 En un supuesto práctico en el que se cuenta con derecho de administración de usuarios:
- Identificar los posibles accesos de un usuario al sistema.
- Modificar los permisos de utilización de un recurso del sistema a un usuario.
- Definir limitaciones de uso de un recurso del sistema a los usuarios.

C4: Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados.
CE4.1 Explicar los parámetros de configuración y funcionamiento de los dispositivos de comunicaciones para asegurar su funcionalidad dentro del sistema.
CE4.2 Relacionar los servicios de comunicaciones activos en el sistema con los dispositivos utilizados por ellos con objeto de analizar y evaluar el rendimiento.
CE4.3 En un supuesto práctico en el que tomamos un sistema informático conectado con el exterior por medio de varias líneas de comunicaciones:
- Identificar los dispositivos de comunicaciones y describir sus características.
- Verificar el estado de los servicios de comunicaciones.
- Evaluar el rendimiento de los servicios de comunicaciones.
- Detectar y documentar las incidencias producidas en el sistema.

Contenidos

1. Gestión de la seguridad y normativas en sistemas informáticos
- Norma ISO 27002 Código de buenas practicas para la gestión de la seguridad de la información
- Metodología ITIL Librería de infraestructuras de las tecnologías de la información
- Ley orgánica de protección de datos de carácter personal.
- Normativas mas frecuentemente utilizadas para la gestión de la seguridad física

2. Análisis de los procesos de sistemas informáticos
- Identificación de procesos de negocio soportados por sistemas de información
- Características fundamentales de los procesos electrónicos:
  - Estados de un proceso,
  - Manejo de señales, su administración y los cambios en las prioridades
- Determinación de los sistemas de información que soportan los procesos de negocio y los activos y servicios utilizados por los mismos
- Análisis de las funcionalidades de sistema operativo para la monitorización de los procesos y servicios
- Técnicas utilizadas para la gestión del consumo de recursos

3. Demostración de sistemas informáticos de almacenamiento
- Tipos de dispositivos de almacenamiento más frecuentes
- Características de los sistemas de archivo disponibles
- Organización y estructura general de almacenamiento
- Herramientas del sistema para gestión de dispositivos de almacenamiento

4. Utilización de métricas e indicadores de monitorización de rendimiento de sistemas informáticos
- Criterios para establecer el marco general de uso de métricas e indicadores para la monitorización de los sistemas de información

cve: BOE-A-2011-10055

- Identificación de los objetos para los cuales es necesario obtener indicadores
- Aspectos a definir para la selección y definición de indicadores
- Establecimiento de los umbrales de rendimiento de los sistemas de información
- Recolección y análisis de los datos aportados por los indicadores
- Consolidación de indicadores bajo un cuadro de mandos de rendimiento de sistemas de información unificado

5. Confección del proceso de monitorización de sistemas y comunicaciones

- Identificación de los dispositivos de comunicaciones
- Análisis de los protocolos y servicios de comunicaciones
- Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
- Procesos de monitorización y respuesta
- Herramientas de monitorización de uso de puertos y servicios tipo Sniffer
- Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
- Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
- Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

6. Selección del sistema de registro de en función de los requerimientos de la organización

- Determinación del nivel de registros necesarios, los periodos de retención y las necesidades de almacenamiento
- Análisis de los requerimientos legales en referencia al registro
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros
- Asignación de responsabilidades para la gestión del registro
- Alternativas de almacenamiento para los registros del sistemas y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad
- Guía para la selección del sistema de almacenamiento y custodia de registros

7. Administración del control de accesos adecuados de los sistemas de información

- Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
- Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
- Requerimientos legales en referencia al control de accesos y asignación de privilegios
- Perfiles de de acceso en relación con los roles funcionales del personal de la organización
- Herramientas de directorio activo y servidores LDAP en general
- Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
- Herramientas de Sistemas de punto único de autenticación Single Sign On (SSO)

Orientaciones metodológicas

Formación a distancia:

cve: BOE-A-2011-10055

Módulo formativo	Número de horas totales del módulo	N.º de horas máximas susceptibles de formación a distancia
Módulo formativo - MF0490_3	90	40

Criterios de acceso para los alumnos

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

MÓDULO FORMATIVO 2

Denominación: DESARROLLO DE ELEMENTOS SOFTWARE PARA GESTIÓN DE SISTEMAS

Código: MF0964_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0964_3 Crear elementos software para la gestión del sistema y sus recursos

Duración: 210 horas

UNIDAD FORMATIVA 1

Denominación: DESARROLLO Y OPTIMIZACIÓN DE COMPONENTES SOFTWARE PARA TAREAS ADMINISTRATIVAS DE SISTEMAS

Código: UF1286

Duración: 90 horas

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

Capacidades y criterios de evaluación

C1: Analizar las especificaciones técnicas proporcionadas para el desarrollo a realizar, comprobando su validez y optimización.

CE1.1 Clasificar las principales arquitecturas de sistemas operativos (monolítico, modular, microkernel, sistemas distribuidos) y sus características, para identificar las necesidades de gestión y administración de dichos sistemas según especificaciones técnicas.

CE1.2 Explicar los apartados de un análisis de requisitos, detallando los diagramas básicos utilizados para la especificación funcional y de datos según metodologías y estándares de diseño.

CE1.3 Analizar las especificaciones técnicas del servicio o herramienta de gestión que se desea implementar, para identificar los recursos requeridos del componente según las especificaciones funcionales dadas.

CE1.4 Realizar los diagramas previos a la fase de desarrollo siguiendo las especificaciones técnicas y criterios de calidad especificados.

cve: BOE-A-2011-10055

CE1.5 En un supuesto práctico, para interpretar un análisis de requisitos dado para el desarrollo de un elemento software, teniendo en cuenta las necesidades de administración de los recursos del sistema informático:
- Definir los módulos software a realizar a partir de las especificaciones técnicas y catálogo de requisitos.
- Establecer las relaciones entre módulos determinando entradas, salidas y flujos de datos según el diseño funcional y las especificaciones del sistema.
- Determinar las estructuras necesarias para representar la información especificada en los requisitos.
- Crear las estructuras necesarias para realizar el seguimiento de requisitos durante la codificación del elemento software según unos criterios de calidad especificados.

C2: Desarrollar elementos software destinados a la gestión de los recursos del sistema, mediante herramientas y lenguajes de programación de sistemas.

CE2.1 Enumerar las herramientas y lenguajes estructurados, orientados al desarrollo de programas para la gestión de recursos del sistema, detallando sus características.

CE2.2 Describir las técnicas de funcionamiento y principios de los sistemas de memoria, detallando su organización en jerarquías, para desarrollar elementos software que las utilicen según las especificaciones funcionales aportadas.

CE2.3 Clasificar las arquitecturas de entrada/salida, de buses y de microprocesadores en sistemas, explicando las técnicas y procesos funcionales utilizados para el desarrollo de los elementos software, según unas especificaciones funcionales dadas.

CE2.4 Distinguir las funciones de las librerías del sistema para la elaboración de nuevos componentes software, reutilizando el código ya desarrollado e implementando nuevos elementos en dichas librerías u obteniendo componentes aislados, según unos criterios de optimización y calidad especificados.

CE2.5 Describir los tipos de pruebas, tanto funcionales como estructurales, y los procesos de depuración a los que debe ser sometido un componente desarrollado y las herramientas utilizadas, para verificar su funcionalidad e integración con el resto de componentes del sistema, según unos criterios de calidad especificados.

CE2.6 Clasificar las herramientas utilizadas en las fases de desarrollo: generación del código, creación de los módulos ejecutables, control de versiones, depuración y pruebas, documentación y empaquetado para su distribución para optimizar la generación y asegurar la calidad de los productos del desarrollo, según unos criterios de seguridad y calidad especificados.

CE2.7 En varios supuestos prácticos para desarrollar elementos software para la gestión de los recursos del sistema, dadas unas especificaciones técnicas:
- Diseñar los algoritmos asociados al elemento software utilizando técnicas de desarrollo estructurado.
- Codificar los módulos software a partir de los algoritmos diseñados utilizando herramientas y lenguajes estructurados.
- Codificar estructuras de datos utilizando las funcionalidades proporcionadas por el lenguaje estructurado.
- Utilizar los recursos y librerías disponibles en las herramientas de desarrollo para realizar la codificación de los algoritmos.
- Diseñar y codificar los manejadores de errores necesarios para garantizar el óptimo funcionamiento del módulo software.
- Diseñar y codificar componentes que permitan el acceso concurrente a los recursos del sistema.
- Depurar los módulos desarrollados utilizando las herramientas disponibles.

cve: BOE-A-2011-10055

- Diseñar y aplicar baterías de pruebas sobre los módulos desarrollados para comprobar su correcto funcionamiento y documentar los resultados obtenidos.
- Documentar los módulos desarrollados para facilitar su revisión y futuras modificaciones y ampliaciones.
- Realizar la implantación de los módulos documentando el proceso y las incidencias detectadas.

CE2.8 Interpretar la documentación técnica asociada a las herramientas y lenguajes de programación, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda en el desarrollo.

Contenidos

1. **Descripción de los servicios, estructura y administración de Sistemas Operativos**
   - Definición y conceptos básicos sobre Sistemas Operativos:
     - Descripción de los servicios básicos ofrecidos por un Sistema Operativo
     - Gestión de memoria. Memoria virtual
     - Ejecución de programas y gestión de procesos
     - Gestión del almacenamiento. Sistemas de Archivos
     - Gestión de dispositivos de entrada/salida
     - Gestión de red
     - Gestión de errores
     - Gestión de la seguridad
     - Auditoría (logs del sistema)
     - Procesos de arranque (boot) y finalización del sistema (shutdown)
   - Características estructurales de los Sistemas Operativos:
     - Sistemas monolíticos
     - Microkernels
     - Sistemas modulares y por capas
     - Máquinas virtuales
     - Sistemas distribuidos
   - Herramientas administrativas de uso común en Sistemas Operativos:
     - Interfaces de usuario gráficos
     - Intérpretes de comandos

2. **Programación de sistemas operativos. Lenguajes y librerías de uso común**
   - Las llamadas al sistema (System Calls):
     - Definición
     - Uso directo y mediante Application Programming Interfaces (APIs)
     - Principales tipos de llamadas al sistema:
       - Control de procesos
       - Gestión de ficheros
       - Gestión de dispositivos
       - Información del sistema
       - Comunicaciones
     - Descripción y uso de las APIs estándar de uso común para llamadas a sistema:
       - Win32 API (Sistemas Windows)
       - POSIX API (Sistemas Unix, Linux, Mac)
       - Java API (Multiplataforma)
   - Programas de utilidades y comandos del sistema:
     - Principales tipos:
       - Operaciones con ficheros y directorios
       - Funciones de estado

cve: BOE-A-2011-10055

- Edición y manipulación de ficheros
- Soporte para lenguajes de programación (compiladores, enlazadores, ensambladores, intérpretes, etc.)
- Ejecución de programas
- Comunicaciones, mensajería, intercambio remoto de archivos, etc.

○ Uso de utilidades y comandos mediante lenguajes de script de uso común
- Windows scripting
- Linux/Unix scripting

3. El ciclo de vida del software de gestión de sistemas

- Modelos del ciclo de vida del software.
  - ○ En cascada (waterfall)
  - ○ Iterativo
  - ○ Incremental
  - ○ En V
  - ○ Basado en componentes (CBSE)
  - ○ Desarrollo rápido (RAD)
  - ○ Ventajas e inconvenientes. Pautas para la selección de la metodología más adecuada.
- Descripción de las fases en el ciclo de vida del software:
  - ○ Análisis y especificación de requisitos
    - Tipos de requisitos : funcionales/ no funcionales, de usuario, de interfaz, de seguridad y de rendimiento
    - Modelos para el análisis de requisitos
    - Documentación de requisitos
    - Validación de requisitos
    - Gestión de requisitos
  - ○ Diseño:
    - Modelos para el diseño de sistemas : contexto y arquitectura, procesos, datos, objetos, interfaces de usuario ,componentes y despliegues
    - Diagramas de diseño: diagramas de entidad-relación, diagramas de flujo, diagramas de contexto y UML. Diagramas UML de uso común en diseño de sistemas
    - Documentación: herramientas de generación de documentación y documentación el código
  - ○ Implementación. Conceptos generales de desarrollo de software:
    - Principios básicos del desarrollo de software
    - Técnicas de desarrollo de software : basadas en prototipos, basadas en componentes, métodos de desarrollo rápido y otras técnicas de desarrollo
  - ○ Validación, verificación y pruebas:
    - Validación y verificación de sistemas: planificación, métodos formales de verificación y métodos automatizados de análisis
    - Pruebas de software: tipos, diseño de pruebas, ámbito de aplicación, automatización de pruebas, herramientas y estándares sobre pruebas de software.
- Calidad del software:
  - ○ Principios de calidad del software
  - ○ Métricas y calidad del software:
    - Concepto de métrica y su importancia en la medición de la calidad
    - Principales métricas en las fases del ciclo de vida software
  - ○ Estándares para la descripción de los factores de Calidad:
    - ISO-9126
    - Otros estándares. Comparativa

cve: BOE-A-2011-10055

4. Desarrollo del software de gestión de sistemas

- Análisis de especificaciones para el desarrollo de software de gestión de sistemas:
  - Identificación de los componentes necesarios según las especificaciones
  - Análisis de los componentes reutilizables
  - Análisis de la integración de los componentes en la arquitectura del sistema
  - Identificación de los modelos funcionales y de datos de los componentes
- Técnicas de programación presentes en lenguajes de uso común aplicables al desarrollo de software de gestión de sistemas:
  - Programación estructurada:
    - Tipos primitivos y estructurados
    - Variables. Ámbito de utilización
    - Operadores aritméticos y lógicos
    - Estructuras de control. Bucles, condicionales y selectores
    - Funciones y procedimientos. Parámetros por valor y referencia.
    - Recursividad
    - Programación de elementos básicos: cadenas, fechas y ficheros.
    - Conversiones de tipos
    - Manejo de errores (excepciones)
    - Lenguajes estructurados de uso común
  - Programación orientada a objetos:
    - Clases y objetos
    - Herencia, polimorfismo y sobrecarga dinámica de métodos
    - Propiedades: selectores (get), modificadores (set) y referencias (let)
    - Lenguajes orientados a objetos de uso común
- Técnicas de programación de software de gestión de sistemas:
  - Reutilización de código.
    - Uso de librerías del sistema
    - Llamadas a utilidades y aplicaciones del sistema
  - Técnicas específicas aplicables a los servicios básicos del sistema:
    - Programación de la gestión de los procesos: multitarea, control de bloqueos(deadlock) y comunicación entre procesos
    - Programación de la gestión de memoria: jerarquías de memoria, paginación de memoria, segmentación de memoria, intercambio(swapping), compartición de memoria, seguridad y memoria virtual
    - Programación de los sistemas de archivos: acceso a archivos y directorios, atributos y mecanismos de protección
    - Programación de los sistemas de entrada y salida: gestión de interrupciones, acceso directo a memoria (DMA) , puertos de entrada/salida y asignación de memoria
    - Programación de la seguridad: control de variables, control de desbordamiento de búferes , aserciones, precondiciones y post-condiciones.
  - Técnicas de optimización
- Control de calidad del desarrollo del software de gestión de sistemas:
  - Métricas aplicables
  - Verificación de requisitos
  - Proceso de mejora continua
- Herramientas de uso común para el desarrollo de software de sistemas:
  - Editores orientados a lenguajes de programación
  - Compiladores y enlazadores
  - Generadores de programas

cve: BOE-A-2011-10055

- Depuradores
- De prueba y validación de software
- Optimizadores de código
- Empaquetadores
- Generadores de documentación de software
- Despliegue de software:
  - Gestores y repositorios de paquetes. Versionado y control de dependencias
  - Distribución de software
  - Gestores de actualización de software
- De control de versiones
- Entornos integrados de desarrollo (IDE) de uso común:
  - Específicos de sistemas Windows
  - Específicos de sistemas Unix
  - Multiplataforma

UNIDAD FORMATIVA 2

Denominación: DESARROLLO DE COMPONENTES SOFTWARE PARA EL MANEJO DE DISPOSITIVOS (DRIVERS)

Código: UF1287

Duración: 60 horas

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

Capacidades y criterios de evaluación

C1: Utilizar las técnicas y estándares utilizadas en el desarrollo, distribución e implantación de manejadores de dispositivos (drivers), para la integración de periféricos en el sistema informático según especificaciones técnicas y funcionales dadas.

CE1.1 Interpretar la documentación técnica de las herramientas software a utilizar y del sistema operativo donde se implementará el manejador de dispositivo, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda, para identificar las características y los parámetros para la programación del manejador de dispositivo de acuerdo al diseño suministrado.

CE1.2 Utilizar las técnicas, estándares y herramientas de programación para desarrollar el manejador de dispositivo y depurar los posibles errores en el código desarrollado, según especificaciones técnicas de las herramientas y necesidades funcionales dadas.

CE1.3 Realizar las pruebas del manejador del dispositivo elaborado en los posibles escenarios en los que puede ser implantado, para asegurar su funcionalidad y la ausencia de conflictos con el resto de los elementos del sistema según especificaciones técnicas y normativa de calidad dadas.

CE1.4 Confeccionar la documentación técnica y de usuario del manejador desarrollado según unos parámetros y una normativa dadas.

CE1.5 En un supuesto práctico para modificar un manejador de dispositivo en el que se va a realizar un cambio en su diseño, de acuerdo a unas especificaciones funcionales dadas:

- Modificar el código para incorporar los cambios necesarios siguiendo los criterios de calidad especificados.
- Comprobar, mediante la realización de pruebas, que la modificación ha sido incorporada con éxito y que no ha alterado la funcionalidad del resto de manejadores, en particular, y del sistema en general.

cve: BOE-A-2011-10055

- Realizar la actualización de toda la documentación que se vea afectada por el cambio propuesto.
- Diseñar el manejador del dispositivo utilizando técnicas de desarrollo estructurado y los estándares adecuados para el tipo de dispositivo.
- Codificar manejadores de dispositivos utilizando la herramienta seleccionada, aplicando el diseño previamente obtenido y utilizando lenguajes estructurados.
- Implantar el manejador del dispositivo documentando el código generado, los resultados obtenidos y las incidencias detectados.

Contenidos

1. El núcleo del sistema operativo
- Arquitectura general del núcleo
- Subsistemas del núcleo:
  - Gestión de procesos
  - Gestión de memoria
  - Sistemas de ficheros
  - Control de dispositivos
  - Comunicaciones
- Aspectos de seguridad sobre el desarrollo de elementos del núcleo
- Consideraciones sobre compatibilidad de versiones del núcleo

2. Programación de controladores de dispositivo
- Funcionamiento general de un controlador de dispositivo
- Principales tipos de controladores de dispositivo:
  - Carácter
  - Bloque
  - Paquete
- Técnicas básicas de programación de controladores de dispositivos
  - Estructuras básicas de datos de dispositivos
  - Gestión de errores de dispositivos
  - Gestión de memoria de dispositivos
  - Control de interrupciones
  - Gestión de puertos de entrada y salida
  - Uso de Acceso directo a memoria (DMA) y buses
- Técnicas de depuración y prueba:
  - Impresión de trazas
  - Monitorización de errores
  - Técnicas específicas de depuración de controladores en sistemas operativos de uso común:
    - Windows
    - Unix
  - Aplicación de estándares de calidad del software al desarrollo de controladores de dispositivos
- Compilación y carga de controladores de dispositivos
- Distribución de controladores de dispositivo
- Particularidades en el desarrollo de dispositivos en sistemas operativos de uso común:
  - Sistemas Windows
  - Sistemas Unix
  - Modos de instalación de controladores de dispositivo en sistemas operativos de uso común. Dispositivos Plug & Play:
    - Instalación de dispositivos en Windows
    - Instalación de dispositivos en Sistemas Unix

cve: BOE-A-2011-10055

- Herramientas:
  - Entornos de desarrollo de controladores de dispositivo en sistemas operativos de uso común
  - Herramientas de depuración y verificación de controladores de dispositivos
- Documentación de manejadores de dispositivo:
  - Elaboración de especificaciones técnicas siguiendo directrices específicas de sistemas operativos de uso común
  - Elaboración de manual de instalación
  - Elaboración de manual de uso

UNIDAD FORMATIVA 3

Denominación: DESARROLLO DE COMPONENTES SOFTWARE PARA SERVICIOS DE COMUNICACIONES

Código: UF1288

Duración: 60 horas

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

Capacidades y criterios de evaluación

C1: Implementar servicios de comunicaciones entre sistemas aplicando las técnicas y estándares de desarrollo de elementos software, de acuerdo a unas especificaciones técnicas y funcionales dadas.

CE1.1 Clasificar las arquitecturas de servicios de comunicaciones para distinguir servicios prestados en entornos cliente/servidor de entornos entre iguales (punto a punto).

CE1.2 Describir los protocolos y puertos utilizados para la comunicación entre sistemas, teniendo en cuenta el soporte que ofrecen a los servicios de comunicaciones.

CE1.3 Identificar las principales API's (Aplication Program Interface) y librerías y su uso para el desarrollo mediante programación estructurada.

CE1.4 Realizar la codificación del componente utilizando herramientas de programación y depuración adecuadas para optimizar la fase de desarrollo según unas especificaciones técnicas dadas.

CE1.5 Someter al componente a baterías de pruebas en réplicas de los posibles escenarios de su implantación posterior, para verificar la ausencia de conflictos y su integración con el resto de componentes del sistema, según unos criterios de calidad y seguridad dados.

CE1.6 Clasificar los estándares definidos para el desarrollo de servicios de comunicaciones entre sistemas según diferentes criterios: organizaciones de estandarización, tipos de servicios y protocolos soportados, entre otros.

CE1.7 Enumerar los principales problemas de seguridad en el ámbito de las comunicaciones y describir las estrategias a aplicar, para el desarrollo de componentes que implementen servicios seguros según estándares y especificaciones dadas.

CE1.8 En varios supuestos prácticos donde se van a desarrollar componentes para el establecimiento de servicios de comunicaciones entre sistemas, dadas unas especificaciones técnicas:

- Seleccionar la herramienta adecuada para el desarrollo de los componentes de comunicaciones.

cve: BOE-A-2011-10055

- Diseñar el componente utilizando técnicas de desarrollo estructurado y los estándares definidos.
- Codificar el elemento software utilizando la herramienta seleccionada, aplicando el diseño previamente obtenido y utilizando lenguajes estructurados.
- Depurar y probar el componente garantizando su óptimo funcionamiento.
- Diseñar baterías de posibles ataques contra el servicio y probarlas para detectar posibles vulnerabilidades.
- Implantar los componentes para verificar el servicio de comunicaciones documentando los resultados e incidencias detectados.
- Documentar el código desarrollado, las pruebas realizadas y el resultado de los procesos de implantación de los componentes.

Contenidos

1. Programación concurrente

- Programación de procesos e hilos de ejecución:
  - Gestión de procesos
  - Hilos y sincronización
- Programación de eventos asíncronos:
  - Señales
  - Temporizadores
- Mecanismos de comunicación entre procesos:
  - Tuberías (pipes)
  - Semáforos
  - Compartición de memoria
  - Mensajes
- Sincronización:
  - Funciones de sincronización entre hilos
  - Problemas de sincronización. Bloqueos (Deadlocks)
- Acceso a dispositivos:
  - Funciones de lectura y escritura
  - Puertos de entrada y salida

2. Fundamentos de comunicaciones

- Modelos de programación en red:
  - El modelo cliente/servidor
  - El modelo de objetos distribuidos
  - Modelos basados en mensajes. Introducción a los Servicios web
- El nivel físico:
  - Dispositivos físicos
  - Protocolos de nivel físico
- El nivel de enlace:
  - Redes Ethernet
  - Direcciones físicas
- El nivel de transporte:
  - El protocolo TCP/IP
  - Esquemas de direccionamiento
  - El nivel de transporte. Protocolos TCP y UDP. Otros protocolos de uso común.
  - Puertos
  - Servicios de red básicos

3. Programación de servicios de comunicaciones

- Aplicaciones y utilidades de comunicaciones. Estándares de comunicaciones:
  - Organismos de estandarización de comunicaciones

cve: BOE-A-2011-10055

- Comunicaciones en sistemas operativos de uso común
- Tipos de servicios de comunicaciones
- Protocolos de comunicaciones de uso común
- Estándares de comunicaciones inalámbricas

- Librerías de comunicaciones de uso común:
  - APIs para entornos Windows
  - APIs para entornos Unix
- Programación de componentes de comunicaciones:
  - Programación de sockets:
    - Funciones básicas
    - Ejemplos de utilización. Sockets TCP y UDP
    - Programación cliente/servidor mediante sockets
  - Programación de manejadores de protocolos
- Técnicas de depuración de servicios de comunicaciones:
  - Directrices para el diseño de pruebas
  - Exploración de vulnerabilidades y puertos
  - Revisión de logs
  - Otras técnicas de depuración
  - Herramientas de prueba y depuración de servicios de comunicaciones
- Rendimiento en las comunicaciones:
  - Calidad de servicio IP
  - Control del ancho de banda
  - Herramientas de monitorización de redes

4. Seguridad en las comunicaciones

- Principios de seguridad en las comunicaciones:
  - Mecanismos de seguridad
  - Principales vulnerabilidades y amenazas
- Herramientas para la gestión de la seguridad en red. Scanners
- Seguridad IP
- Seguridad en el nivel de aplicación. El protocolo SSL
- Seguridad en redes inalámbricas

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 – UF1286	90	40
Unidad formativa 2 – UF1287	60	30
Unidad formativa 3 – UF1288	60	30

Secuencia:

Para acceder a las Unidades formativas 2 y 3 debe haberse superado la Unidad formativa 1

Criterios de acceso para los alumnos

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

cve: BOE-A-2011-10055

MÓDULO FORMATIVO 3

Denominación: DESARROLLO DE SOFTWARE BASADO EN TECNOLOGÍAS ORIENTADAS A COMPONENTES

Código: MF0965_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0965_3 Desarrollar elementos software con tecnologías de programación basada en componentes

Duración: 210 horas

UNIDAD FORMATIVA 1

Denominación: DISEÑO DE ELEMENTOS SOFTWARE CON TECNOLOGÍAS BASADAS EN COMPONENTES

Código: UF1289

Duración: 90 horas

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

Capacidades y criterios de evaluación

C1: Identificar las características y arquitecturas de las tecnologías de desarrollo, orientadas a componentes para la creación y modificación de elementos software integrados en estos entornos, según estándares y normalizaciones existentes.

CE1.1 Describir las técnicas y métodos de desarrollo involucrados en el paradigma del desarrollo, orientado a componentes para la confección y modificación elementos software, según los estándares de esta tecnología.

CE1.2 Clasificar las herramientas y lenguajes orientados a objetos utilizados en el desarrollo orientado a componentes, describiendo sus características para identificar las que son específicas para la creación o modificación de los elementos software, según las especificaciones funcionales dadas.

CE1.3 Clasificar los estándares de modelos de componentes, describiendo las pasarelas para interoperar entre componentes heterogéneos, para realizar las tareas de integración de los elementos desarrollados según especificaciones funcionales y técnicas.

CE1.4 Identificar las técnicas de diagramación y documentación para el desarrollo de software basado en tecnologías orientadas a componentes, según estándares de diseño de metodologías orientadas a componentes.

CE1.5 En un caso práctico para desarrollar componentes dentro de una arquitectura dada y contando con unas especificaciones funcionales precisas:

- Realizar la diagramación y documentación previa al desarrollo del componente, para optimizar los procesos de creación del componente según especificaciones recibidas.
- Identificar los diferentes interfaces y técnicas utilizadas para la intercomunicación de componentes, para poder aplicarlas al desarrollo de nuevos componentes.

cve: BOE-A-2011-10055

- Definir los interfaces del componente software a desarrollar para la intercomunicación con el resto de componentes del sistema, según especificaciones técnicas de la arquitectura de componentes y necesidades funcionales.
- Diseñar la estructura del componente utilizando los estándares de creación de componentes, según especificaciones técnicas de la arquitectura utilizada y necesidades funcionales.
- Confeccionar la documentación del diseño realizado siguiendo los patrones, normativa y procedimientos especificados.

Contenidos

1. La orientación a objetos

- Principios de la orientación a objetos. Comparación con la programación estructurada:
  - Ocultación de información (information hiding)
  - El tipo abstracto de datos (ADT). Encapsulado de datos.
  - Paso de mensajes
- Conceptos básicos de orientación a objetos:
  - Clases:
    - Atributos, variables de estado y variables de clase
    - Métodos. Requisitos e invariantes.
    - Gestión de excepciones
    - Agregación de clases
  - Objetos:
    - Creación y destrucción de objetos
    - Llamada a métodos de un objeto
    - Visibilidad y uso de las variables de estado
    - Referencias a objetos
    - Persistencia de objetos
    - Optimización de memoria y recolección de basura (garbage collection)
  - Herencia:
    - Concepto de herencia. Superclases y subclases.
    - Herencia múltiple
    - Clases abstractas
    - Tipos de herencia: herencia de implementación, herencia de interfaces y de tipos y otros tipos de herencia
    - Polimorfismo y enlace dinámico (dynamic binding)
    - Directrices para el uso correcto de la herencia
  - Modularidad:
    - Librerías de clases. Ámbito de utilización de nombres
    - Ventajas de la utilización de modulos o paquetes
  - Genericidad y sobrecarga:
    - Concepto de genericidad
    - Concepto de Sobrecarga. Tipos de sobrecarga
    - Comparación entre genericidad y sobrecarga
- Desarrollo orientado a objetos:
  - Lenguajes de desarrollo orientado a objetos de uso común
  - Herramientas de desarrollo
- Lenguajes de modelización en el desarrollo orientado a objetos:
  - El lenguaje unificado de modelado (UML)
  - Diagramas para la modelización de sistemas orientados a objetos

cve: BOE-A-2011-10055

2. La orientación a componentes

- Fundamentos conceptuales:
  - Definición de componente
  - Comparación entre componentes y objetos
  - Módulos
  - Interfaces:
    - Tipos de interfaces
    - Versionado de interfaces
    - Interfaces como contratos
  - Escalado de componentes
  - Estado de componentes
- Arquitecturas de componentes:
  - Basadas en objetos. Composición y uso de objetos
  - Multicapa
  - Basadas en middleware
  - Basadas en objetos distribuidos
- Diseño de componentes:
  - Principios de diseño de componentes:
    - Dependencias no cíclicas
    - Principio “open/closed”
    - Reusabilidad
    - Configurabilidad
    - Abstracción
    - Dependencias
  - Técnicas de reusabilidad:
    - Patrones
    - Librerías
    - Interfaces
    - Protocolos y esquemas de mensajes
    - Uso de lenguajes de programación
    - Estructuras y jerarquías de estructuras
    - Arquitecturas de sistemas
  - Modelo de componente:
    - Especificación de servicios: transacciones, seguridad, persistencia y acceso remoto
    - Especificación de Interface
    - Especificación de la implementación
    - Especificación de las unidades de despliegue (modulos)
  - Modelos de integración de componentes:
    - Referencias e identidad de objetos, componentes e interfaces
    - Servicios de localización
    - Modelos de intercambio: objetos distribuidos, capa intermedia (Middleware) e interacción e integración mediante servicios web
    - Comparación entre métodos de intercambio en las principales infraestructuras de componentes: OMG: CORBA, OMA, Java: JavaBeans, EJBs y Microsoft: COM, OLE/ActiveX, .NET
  - Diagramación y documentación de componentes:
    - Modelo de información: diagramas conceptuales, diagramas de arquitectura de componentes y diagramas de despliegue.
    - Modelo dinámico: diagramas de interacción y de actividad, diagramas de casos de uso y diagramas de estado.

cve: BOE-A-2011-10055

UNIDAD FORMATIVA 2

Denominación: IMPLEMENTACIÓN E INTEGRACIÓN DE ELEMENTOS SOFTWARE CON TECNOLOGÍAS BASADAS EN COMPONENTES

Código: UF1290

Duración: 90 horas

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

Capacidades y criterios de evaluación

C1: Construir elementos software a partir de las especificaciones de necesidades y con las condiciones de desarrollo de la tecnología de componentes utilizada.

CE1.1 Explicar los enfoques de desarrollo e implementación para la creación de componentes aplicando el principio de reutilización.

CE1.2 Describir el proceso de adaptación de un componente existente para incluirlo en la arquitectura en la que se quiere reutilizar, según especificaciones técnicas de la tecnología de componentes utilizada.

CE1.3 Enunciar las características del proceso de diseño de un nuevo componente para incluirlo en la arquitectura en la que se quiere utilizar, garantizando su futura reutilización.

CE1.4 Clasificar las herramientas de programación y depuración para optimizar la fase de desarrollo de los componentes según unas especificaciones dadas.

CE1.5 Identificar los elementos y parámetros de la interfaz del componente, para su desarrollo con herramientas y lenguajes específicos, para implementar la vía de comunicaciones con el resto de componentes según los estándares de definición de interfaces de la arquitectura.

CE1.6 Realizar los procesos de instalación del componente, comprobando que ejecuta las acciones requeridas y su disponibilidad para las aplicaciones que lo invoquen, según especificaciones técnicas de la arquitectura.

CE1.7 En un caso practico para desarrollar componentes software reutilizables, dadas unas especificaciones funcionales y técnicas:

- Diseñar el nuevo componente para que cumpla las especificaciones funcionales dadas.
- Comprobar que la funcionalidad del componente diseñado puede ser extendida para futuras reutilizaciones.
- Implementar el componente utilizando herramientas y lenguajes orientados a objeto.
- Depurar y probar el componente desarrollado utilizando las herramientas disponibles.
- Documentar el componente y sus interfaces para facilitar su futura reutilización.

CE1.8 En un caso practico para desarrollar software reutilizando componentes, dadas unas especificaciones funcionales y técnicas:

- Utilizar repositorios de componentes para localizar aquellos que se ajusten a las especificaciones dadas y puedan ser reutilizados.
- Diseñar las modificaciones que se van a realizar sobre el componente existente para que cumpla las especificaciones dadas.
- Modificar el componente utilizando herramientas y lenguajes orientados a objeto.
- Depurar y probar el componente modificado utilizando las herramientas disponibles.
- Documentar las modificaciones realizadas sobre el componente y sus interfaces para facilitar su futura reutilización.

cve: BOE-A-2011-10055

CE1.9 Interpretar la documentación técnica asociada a las herramientas de programación, incluso si está editada en la lengua extranjera de uso más frecuente en el sector, utilizándola de ayuda en el desarrollo.

Contenidos

1. Desarrollo de componentes

- Lenguajes de desarrollo de componentes.:
  - Comparativa con lenguajes orientados a objetos
  - Lenguajes orientados a componentes:
    - Descripción de intefaces
    - Ensamblado
    - Descripción de arquitectura
- Requisitos principales del desarrollo orientado a componentes:
    - Modularidad
    - Despliegue independiente
    - Reemplazabilidad
    - Seguridad
    - Separación entre interfaz e implementación
- Infraestructuras (frameworks) de componentes:
  - Modelos de infraestruturas de componentes:
    - Orientados a conexión
    - Orientados a contexto
    - Orientados a aspectos
  - Descripción de las intraestructuras de componentes de uso común:
    - OMG: CORBA, OMA
    - Java: JavaBeans, EJBs
    - Microsoft: COM, OLE/ActiveX, .NET
- Métodos de desarrollo de componentes:
  - Uso de lenguajes orientados a objetos
  - Selección de infraestructuras de componentes
- Construcción de software mediante componentes:
    - Definición de interfaces. Lenguajes de descripción de interfaces
    - Reutilización de componentes.
    - Técnicas de ensamblado en infraestructuras de uso común
- Técnicas específicas de desarrollo:
  - Componentes en la capa de servidor web. Páginas dinámicas
  - Componentes en la capa de servidor de aplicaciones.
  - Componentes en la capa de aplicación cliente:
    - Componentes de interfaz gráfico
    - Componentes orientados a documento
  - Componentes en la capa de servicios web
  - Componentes para dispositivos móviles
- Herramientas para el desarrollo de componentes:
  - Entornos integrados de desarrollo de componentes
  - Configuración e instalación de herramientas de uso común:
    - Entorno Java
    - Entorno .NET
  - Gestión del ciclo de vida en el desarrolo de componentes mediante herramientas de uso común:
    - Uso de repositorios de componentes. Registro de componentes
    - Reutilización de componentes para la construcción de sistemas software
    - Definición de metadatos de componente. Descriptores de interfaces
    - Modelo de seguridad

cve: BOE-A-2011-10055

- Instalación de componentes
- Depuración y prueba de componentes

2. **Componentes distribuidos**
   - Programación distribuida en infraestructuras de uso común:
     - Programación multihilo (multithreading)
     - Comunicaciones síncronas y asíncronas
   - Modelos de intercambio:
     - Llamadas a procedimientos remotos
     - Orientados a mensajes
     - Orientados a recursos

UNIDAD FORMATIVA 3

Denominación: DESPLIEGUE Y PUESTA EN FUNCIONAMIENTO DE COMPONENTES SOFTWARE

Código: UF1291

Duración: 30 horas

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

Capacidades y criterios de evaluación

C1: Aplicar los procedimientos de despliegue e integración del componente en un entorno de tecnología orientada a componentes, según especificaciones técnicas de la arquitectura.

CE1.1 Describir las técnicas disponibles para realizar el proceso de búsqueda de componentes, que satisfagan los requisitos impuestos en el diseño inicial.

CE1.2 Clasificar los métodos de evaluación y selección de componentes, basándose en una serie de requisitos impuestos por las especificaciones iniciales de diseño.

CE1.3 Realizar las pruebas estructurales para verificar que el componente seleccionado se comunica con el resto de componentes y que no produce conflictos, según criterios de calidad y seguridad dados, y del diseño preeliminar.

CE1.4 Definir los procedimientos para el despliegue y adaptación para realizar la implantación del elemento software, según requisitos del componente desarrollado y siguiendo criterios de calidad, seguridad y especificaciones de la arquitectura.

CE1.5 Describir los procesos de integración, configuración e interconexión de los componentes seleccionados, para que permitan construir la aplicación final según los criterios de calidad y seguridad especificados en el diseño inicial.

CE1.6 Monitorizar el rendimiento de los componentes desarrollados o seleccionados para asegurar su integración en el sistema, de acuerdo a criterios de calidad y seguridad.

CE1.7 Realizar la documentación del despliegue y la implantación siguiendo los patrones, normativa y procedimientos especificados.

CE1.8 En un supuesto práctico debidamente caracterizado, utilizar las herramientas de desarrollo para realizar el desarrollo y despliegue de un componente software según unas especificaciones funcionales y técnicas dadas:

- Extraer la información relativa al diseño de un componente.
- Codificar el componente según especificaciones funcionales y técnicas.
- Realizar las pruebas estructurales según normativa y criterios de calidad establecidos.

cve: BOE-A-2011-10055

- Incorporar el despliegue, adaptación, configuración e integración del componente según especificaciones técnicas y de implantación del desarrollo.
- Trazar las pruebas del componente según normativas de calidad y seguridad dadas.
- Configurar la herramienta para la realización de baterías de pruebas automáticas según normativa y criterios de calidad dados.
- Elaborar documentación mediante las plantillas facilitadas o incorporadas en la propia herramienta.
- Generar informes de calidad y métricas, e interpretar los resultados.

Contenidos

1. Despliegue de componentes
- Modelos de despliegue:
  - Diseño sin repositorio:
    - Diseño y ejecución sin despliegue
    - Ejemplos: UML
  - Diseño con repositorio sólo para el depósito de componentes:
    - Tipos de contenedores
    - Ejemplos: EJBs, .NET, CCM, Servicios web
  - Despliegue con repositorio:
    - Composición y depósito de componentes
    - Ejemplo: JavaBean
  - Diseño con repositorio:
    - Tipos de conectores
    - Ejemplos: Koala

2. Selección de componentes
- Tipos:
  - Componentes comerciales:
    - Sin posibilidad de modificaciones (COTS)
    - Con posibilidad de adaptaciones (MOTS)
  - Componentes de fuente abierta
  - Ventajas e inconvenientes
- Métodos de personalización de componentes:
  - Parametrización
  - Uso de extensiones (plugins)
- Criterios de selección de componentes reutilizables:
  - Adaptabilidad
  - Auditabilidad
  - Estandarización
  - Características de concurrencia
  - Rendimiento
  - Consumo de recursos
  - Seguridad
  - Características de mantenimiento y actualización
- Proceso de selección de componentes:
  - Evaluación de componentes según requisitos
  - Diseño y codificación (código de enlace):
    - Enlace de componentes con otros sistemas
    - Integración
    - Configuración
  - Diseño de pruebas
  - Detección de fallos

cve: BOE-A-2011-10055

- Mantenimiento y gestión de configuraciones
- Actualización de componentes
- Métodos de selección de uso común:
  - CAP (COTS Acquisition Process)
  - RUP (Rational Unified Process)

3. Control de calidad de componentes

- Métodos de evaluación de calidad de componentes. Estándares de calidad
- Categorías y métricas de evaluación
- Proceso de validación y medición de calidad:
  - Pruebas de conformidad a requisitos funcionales
  - Pruebas de integración con otros sistemas
  - Pruebas de aspectos no funcionales:
    - Rendimiento
    - Seguridad
    - Integración
- Documentación de componentes
- Descripción funcional
- Descripción de aspectos no funcionales
- Descripción del proceso de instalación y despliegue:
  - Descripción del empaquetamiento (packaging)
  - Requisitos de implantación
  - Parametrización y ajuste

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 – UF1289	90	40
Unidad formativa 2 – UF1290	90	40
Unidad formativa 3 – UF1291	30	20

Secuencia:

Para acceder a las 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 en certificado de profesionalidad de la familia profesional al que acompaña este anexo.

MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES DE PROGRAMACIÓN DE SISTEMAS INFORMÁTICOS

Código: MP0274

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Colaborar en el desarrollo y análisis de sistemas informáticos.
CE1.1 Analizar los requisitos de desarrollo de los sistemas corporativos.

cve: BOE-A-2011-10055

CE1.2 Evaluar el análisis y diseño de los sistemas conforme a los requisitos establecidos.
CE1.3 Verificar el uso y reutilización de componentes software en la realización de los sistemas corporativos.
CE1.4 Apoyar en el desarrollo y mantenimiento de los sistemas software
CE1.5 Colaborar en la realización de documentación del software
CE1.6 Investigar nuevas herramientas o actualizaciones de las existentes para mejorar la productividad en el desarrollo
CE1.7 Facilitar la coordinación entre los grupos de diseño, desarrollo, instalación y despliegue de software

C2: Auditar la calidad y seguridad de los sistemas software
CE2.1 Clasificar los sistemas software según su criticidad y valor para la empresa
CE2.2 Proporcionar apoyo en la realización de auditorías de software para la verificación y mejora de de la calidad y seguridad del software
CE2.3 Realizar pruebas según normativa y criterios de calidad establecidos en la empresa
CE2.4 Proporcionar asistencia en la aplicación de las medidas de mejora de la calidad y seguridad del software corporativo

C3: Participar en los procesos 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. **Análisis del ciclo de vida de software**
   - Definición de requisitos funcionales
   - Metodologías de diseño
   - Lenguajes y herramientas de desarrollo corporativos
   - Procedimientos de depuración y prueba de software
   - Procesos de instalación y despliegue
   - Normalización y reutilización de componentes corporativos
   - Criterios para la actualización del software
   - Normas de documentación

2. **Desarrollo y reutilización de componentes corporativos**
   - Utilización de herramientas de desarrollo en las distintas fases del ciclo de vida software según las normas corporativas
   - Realización de diagramas de diseño
   - Validación de requisitos
   - Coordinación entre diferentes equipos o programadores para la construcción de sistemas software
   - Realización de pruebas y validación de requisitos

cve: BOE-A-2011-10055

3. **Auditorías de calidad y seguridad**
   - Aplicación de la normativa de calidad
   - Realización de planes de auditoría
   - Revisión de la seguridad del software
   - Análisis del rendimiento del software
   - Evaluación del nivel de integración y optimización en la construcción del software
   - Identificación de aspectos de mejora
   - Realización de informes

4. **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 del proceso productivo de la organización.
   - Utilización 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.

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	Experiencia profesional requerida en el ámbito de la unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0490_3: Gestionar servicios en el sistema informático	• 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.	2 años	4 años
MF0964_3: Desarrollo de elementos software para gestión de sistemas	• 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.	1 año	3 años
MF0965_3: Desarrollo de software basado en tecnologías orientadas a componentes	• 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.	1 año	3 años

V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m^2 15 alumnos	Superficie m^2 25 alumnos
Aula de gestión	45	60

cve: BOE-A-2011-10055

Espacio Formativo	M1	M2	M3
Aula de gestión	X	X	X

Espacio Formativo	Equipamiento
Aula de gestión	- Equipos audiovisuales - PCs instalados en red, con conexión a Internet - PC con funciones de servidor - Cañón de proyección - Software específico de la especialidad - Pizarras para escribir con rotulador - Rotafolios - Material de aula - Mesa y silla para formador - Mesas y sillas para alumnos

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-2011-10055