V. REQUISITOS MÍNIMOS DE ESPACIOS, INSTALACIONES Y EQUIPAMIENTO

Espacio Formativo	Superficie m² 15 alumnos	Superficie m² 25 alumnos
Aula taller de informática	60	75

Espacio Formativo	M1	M2	M3
Aula taller de informática	X	X	X

Espacio Formativo	Equipamiento
Aula taller de informática	– Equipos audiovisuales – PCs instalados en red, cañón de proyección e internet – Pizarras para escribir con rotulador – Rotafolios – Material de aula – Mesa y silla para formador – Mesas y sillas para alumnos – Aplicaciones de ofimática – Software de simulación de redes – Equipos y dispositivos de red: conmutadores, routers, puntos de acceso inalámbrico, – Medios de transmisión. – Testers, certificadores, … – Armarios de enracado de equipos – Equipos tipo PC con sistemas operativos windows y linux – Software de servicios de red

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 XI

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Gestión de Sistemas Informáticos

Código: IFCT0510

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y Telemática

cve: BOE-A-2011-19503

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC152_3 Gestión de sistemas informáticos (RD 1087/2005, de 16 de septiembre)

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

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

Competencia general:

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

Entorno Profesional:

Ámbito profesional:

Desarrolla su actividad profesional en empresas o entidades de naturaleza pública o privada de cualquier tamaño en el área de sistemas del departamento de informática.

Sectores productivos:

Se sitúa en todos los sectores del tejido empresarial dada su característica de transectorialidad que sobreviene de la necesidad de las organizaciones de tratar y administrar su información estén en el sector que estén. También 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 dedicadas a la comercialización de equipos informáticos.
Empresas que prestan servicios de asistencia técnica informática.

Ocupaciones o puestos de trabajo relacionados:

2721.1018 Administrador de sistemas de redes
Administrador de sistemas.
Responsable de informática.

Duración de la formación asociada: 500 horas.

Relación de módulos formativos y de unidades formativas:

MF0484_3: Administración hardware de un sistema informático (120 horas).
- UF1891: Dimensionar, instalar, y optimizar el hardware (70 horas)
- UF1892: Gestionar el crecimiento y las condiciones ambientales (50 horas)

MF0485_3: Administración software de un sistema informático (210 horas)
- UF1893: Instalación y parametrización del software (90 horas)
- UF1894: Mantenimiento del software (70 horas)
- UF1895: Auditorías y Continuidad de negocio (50 horas)

MF0486_3: (Transversal) Seguridad en equipos informáticos (90 horas).

cve: BOE-A-2011-19503

MP0398: Módulo de prácticas profesionales no laborales de Gestión de Sistemas Informáticos (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: ADMINISTRAR LOS DISPOSITIVOS HARDWARE DEL SISTEMA.

Nivel: 3

Código: UC0484_3

Realizaciones profesionales y criterios de realización

RP1: Elaborar y mantener inventarios de los componentes físicos del sistema para asegurar su localización y disponibilidad según las normas de la organización.

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

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

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

CR1.4 La documentación para la instalación del hardware se detalla y referencia en la documentación generada y se guardan convenientemente para su uso posterior.

CR1.5 La documentación técnica se interpreta correctamente tanto si está editada en castellano o en las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

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

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

CR2.2 las técnicas o herramientas de monitorización seleccionadas se emplean con destreza preparando el sistema para su monitorización, obteniéndose las estadísticas de rendimiento, programaciones de alertas y otros elementos de monitorización.

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

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

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

CR2.6 Los dispositivos físicos se parametrizan para mejorar el rendimiento y corregir las anomalías de funcionamiento detectadas en el sistema.

CR2.7 La documentación técnica se interpreta correctamente tanto si está editada en castellano o en 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-2011-19503

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

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

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

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

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

CR3.5 La integridad de la información y la continuidad en el funcionamiento del sistema quedan garantizadas durante la resolución de problemas o desajustes, tomando las medidas preventivas de seguridad necesarias y activando los posibles procedimientos de explotación alternativos.

CR3.6 La información original y copias de seguridad se restauran y actualizan para que el sistema vuelva a entrar en explotación siguiendo el protocolo de seguridad establecido.

CR3.7 El almacenamiento de las copias se supervisa, comprobando que se cumplen los estándares de seguridad establecidos por la organización.

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

CR3.9 La documentación técnica se interpreta correctamente tanto si está editada en castellano o en las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

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

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

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

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

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

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

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

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

cve: BOE-A-2011-19503

CR5.1 Las especificaciones técnicas de los dispositivos y el plan general de seguridad de la organización se conocen e interpretan adecuadamente para la adecuación del sistema.
CR5.2 Los requerimientos ambientales y condiciones de alimentación eléctrica de los dispositivos físicos se establecen y contrastan con las posibilidades de la instalación para evitar incidencias e interrupciones en el servicio.
CR5.3 Las condiciones de ergonomía, seguridad, y aprovechamiento del espacio disponible se establecen para la correcta ubicación de los equipos y dispositivos físicos.

Contexto profesional

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

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

Información utilizada o generada

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

Unidad de competencia 2

Denominación: INSTALAR, CONFIGURAR Y ADMINISTRAR EL SOFTWARE DE BASE Y DE APLICACIÓN DEL SISTEMA.

Nivel: 3

Código: UC0485_3

Realizaciones profesionales y criterios de realización

RP1: Instalar y configurar el sistema operativo de servidor para asegurar la funcionalidad del sistema según las necesidades de la organización.
CR1.1 El sistema operativo del servidor se instala siguiendo los procedimientos y lo indicado en la documentación técnica.

cve: BOE-A-2011-19503

CR1.2 La verificación de los componentes del sistema operativo y controladores de dispositivos se realiza mediante pruebas de arranque y parada, y la utilización de herramientas software de verificación y diagnóstico, de modo que se pueda comprobar que los componentes son reconocidos y habilitados y no aparecen conflictos según lo dispuesto por la organización.
CR1.3 Los parámetros del sistema operativo se configuran para garantizar la integridad y fiabilidad del sistema según el plan de seguridad de la organización.
CR1.4 La configuración de los parámetros de red se establece para conectar el servidor según el diseño de red del sistema y los estándares y normas de seguridad y calidad de la organización.
CR1.5 Los diferentes grupos y usuarios se crean para permitir la utilización del sistema según las necesidades de la organización y el plan de seguridad del sistema.
CR1.6 Las actualizaciones necesarias del sistema operativo del servidor se llevan a cabo con eficacia, asegurando la integridad del sistema, la idoneidad de las mismas y siguiendo las normas de seguridad de la organización.
CR1.7 Los detalles relevantes de la instalación, así como las incidencias durante el proceso, se reflejan en la documentación, según el procedimiento establecido por la organización.
CR1.8 La documentación técnica se interpreta correctamente tanto si está editada en castellano o en las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

RP2: Elaborar y mantener inventarios del software del sistema para garantizar su localización y disponibilidad según las normas de la organización.

CR2.1 El software y sus versiones se enumeran de forma exhaustiva para mantener un inventario de las aplicaciones y sistemas operativos disponibles en el sistema.
CR2.2 La configuración actual del software de base y aplicación se registra y documenta de forma clara y completa para facilitar las labores de recuperación en caso de fallos.
CR2.3 La información del software instalado se enumera en relación con cada usuario para permitir el control de instalaciones de aplicaciones no permitidas.
CR2.4 El número de instalaciones, su situación e identificación se controlan por cada producto software para llevar a cabo un control exhaustivo de licencias cumpliendo la legislación vigente sobre propiedad intelectual.
CR2.5 Los privilegios de acceso de los usuarios del sistema a recursos software se registran para el control de acceso, según el plan de seguridad del sistema y las leyes de datos vigentes.
CR2.6 Las aplicaciones de inventariado automático se utilizan para mantener actualizada la información acerca del software del sistema.

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

CR3.1 La instalación del software corporativo se lleva a cabo con eficacia asegurando la integridad del sistema, cumpliendo los requisitos establecidos por la organización y siguiendo lo indicado en la documentación técnica.
CR3.2 La verificación del funcionamiento del software en el conjunto del sistema se realiza según los procedimientos de seguridad y calidad establecidos por la organización y el propio fabricante.
CR3.3 El software corporativo se configura con parámetros adecuados según el plan de seguridad del sistema y las necesidades de la organización.
CR3.4 Las actualizaciones necesarias del software corporativo se llevan a cabo con eficacia, asegurando la integridad del sistema, la idoneidad de las mismas y siguiendo las normas de seguridad de la organización.

cve: BOE-A-2011-19503

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

CR3.6 La documentación técnica se interpreta correctamente tanto si está editada en castellano o en las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

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

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

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

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

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

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

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

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

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

CR5.3 Los programas de comprobación a utilizar se establecen para obtener parámetros del rendimiento del sistema.

CR5.4 Los modelos que representan al sistema se realizan para obtener parámetros de rendimiento del mismo.

CR5.5 Los sistemas de simulación del sistema se configuran para obtener parámetros del rendimiento del mismo.

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

CR5.7 Los componentes hardware se reconfiguran, eliminan o añaden de acuerdo al análisis realizado para la mejora del rendimiento de las aplicaciones.

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

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

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

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

cve: BOE-A-2011-19503

CR6.4 La planificación del sistema de identificación y almacenamiento de los soportes se realiza en función de las especificaciones de calidad de la organización.
CR6.5 La documentación de los procedimientos de obtención y verificación de copias de respaldo así como la de los planes de contingencias y resolución de incidencias se confecciona según la normativa de la organización.

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

CR7.1 El plan de auditoría con las pruebas funcionales necesarias y periodos de realización se implementa, de forma que garantice el óptimo rendimiento del sistema.
CR7.2 La comprobación de incidencias se realiza para verificar, precisar y minimizar efectos negativos sobre el sistema.
CR7.3 El diagnostico y localización de funcionamientos indeseados se realiza utilizando los equipos y las herramientas necesarias, y se aplica el correspondiente procedimiento correctivo en un tiempo adecuado.
CR7.4 El informe de auditoría se realiza en el formato normalizado que permita recoger la información requerida para la actuación del repositorio de incidencias.
CR7.5 La documentación técnica se interpreta correctamente tanto si está editada en castellano o en las lenguas oficiales de las Comunidades Autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.

Contexto profesional

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

Productos y resultados
Sistema operativo y aplicaciones configurados y parametrizados de acuerdo a las necesidades. Inventarios software y de configuración de aplicaciones del sistema. Copias de seguridad. Documentación de instalación, configuración y parte de incidencias del software de base del sistema. Documentación de instalación, configuración y parte de incidencias del software de aplicación corporativo. Guías de instalación y configuración de aplicaciones y software de base para el personal de apoyo. Plan de asistencia y entrenamiento de usuarios. Copias de seguridad realizadas, archivadas y documentadas.

Información utilizada o generada
Manuales de instalación del sistema operativo. Manual de operación del sistema operativo. Manuales de instalación de aplicaciones. Manuales de operación de realización de copias de seguridad. Normas de seguridad (plan de seguridad) y calidad de la organización. Manuales de herramientas administrativas. Manuales de ayuda en línea. Asistencia técnica en línea. Planes de explotación e implantación de la organización. Legislación sobre protección de datos y propiedad intelectual, normativa empresarial sobre la confidencialidad de datos.

Unidad de competencia 3

Denominación: ASEGURAR EQUIPOS INFORMÁTICOS.

cve: BOE-A-2011-19503

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.

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.

cve: BOE-A-2011-19503

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.

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.

III. FORMACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

MÓDULO FORMATIVO 1

Denominación: ADMINISTRACIÓN HARDWARE DE UN SISTEMA INFORMÁTICO.

Código: MF0484_3

cve: BOE-A-2011-19503

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

UC0484_3: Administrar los dispositivos hardware del sistema.

Duración: 120 horas

UNIDAD FORMATIVA 1

Denominación: DIMENSIONAR, INSTALAR Y OPTIMIZAR EL HARDWARE

Código: UF1891

Duración: 70 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP1, RP2 y RP3

Capacidades y criterios de evaluación

C1: Identificar los componentes hardware del sistema distinguiendo sus características y detallando parámetros y procedimientos de instalación.

CE1.1 Analizar y explicar los fundamentos de la arquitectura física de un sistema informático precisando las distintas partes que lo componen.

CE1.2 Enumerar y definir las funciones que realizan cada uno de los componentes hardware de un sistema informático explicando sus características.

CE1.3 Clasificar según su tipología cada uno de los componentes hardware de un sistema informático atendiendo a sus características, utilidad y propósitos.

CE1.4 Detallar las características técnicas y procedimientos de instalación y configuración de los componentes hardware de un sistema informático según especificaciones de funcionalidades dadas.

CE1.5 Distinguir y explicar los tipos de dispositivos físicos y técnicas de comunicación posibles entre los diferentes componentes hardware de un sistema informático, describiendo sus principales características y tipología.

CE1.6 Definir y clasificar los diferentes tipos de dispositivos periféricos atendiendo a su propósito, describiendo las diferentes técnicas utilizadas para realizar la comunicación con los mismos y las tecnologías disponibles en controladores de entrada/salida.

CE1.7 Identificar y clasificar los diferentes dispositivos físicos disponibles para conectar el sistema a través de una red de comunicaciones.

CE1.8 A partir de un supuesto práctico de identificación y registro de dispositivos hardware:

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

C2: Seleccionar y aplicar los procedimientos y técnicas de monitorización del rendimiento de los dispositivos para ajustar los parámetros de configuración y asegurar la ausencia de conflictos.

CE2.1 Enumerar y definir las métricas de rendimiento comúnmente utilizadas para medir el rendimiento de un sistema.

cve: BOE-A-2011-19503

CE2.2 Caracterizar y analizar los principales procedimientos y técnicas de monitorización utilizados para medir las prestaciones de un sistema.
CE2.3 Aplicar las técnicas y herramientas seleccionadas para conseguir un rendimiento óptimo y determinar el estado del sistema analizando los resultados de las mediciones del rendimiento e indicando si este se encuentra saturado, equilibrado o infrautilizado.
CE2.4 Representar gráficamente el rendimiento del sistema según los datos obtenidos de la monitorización.
CE2.5 Analizar las alarmas obtenidas en la monitorización y describir los principales problemas de configuración relativos a dispositivos hardware conocidos explicando las soluciones más comunes.
CE2.6 En una serie de supuestos prácticos de monitorización y ajuste de sistemas:
- Seleccionar las métricas del rendimiento a utilizar según las necesidades del sistema.
- Obtener mediciones del rendimiento del sistema utilizando con destreza las herramientas necesarias para llevarlo a cabo.
- Analizar las mediciones obtenidas, documentándolas y presentándolas para facilitar la toma de decisiones acerca del sistema.
- Configurar los parámetros del sistema necesarios para que se cumplan los requisitos de rendimiento.
- Reconfigurar el sistema dependiendo de las alarmas obtenidas en las mediciones.
- Indicar y documentar las limitaciones que existen en el intento de mejorar las prestaciones de un sistema.

C3: Integrar e implantar en el sistema informático dispositivos hardware que garanticen la continuidad en la prestación de servicios y la seguridad de los datos.
CE3.1 Identificar las diferentes soluciones hardware disponibles para asegurar la continuidad del funcionamiento del sistema, describiendo sus principales características y configuraciones
CE3.2 Definir las diferentes soluciones hardware disponibles para asegurar la recuperación del sistema ante situaciones imprevistas, describiendo sus principales características y configuraciones.
CE3.3 Identificar las políticas de seguridad y protección de datos y su relación en la recuperación y continuidad de servicios y aplicaciones según la normativa de seguridad informática.
CE3.4 En un supuesto práctico, implementar y configurar soluciones para asegurar la continuidad del funcionamiento del sistema, dados unos requisitos previos:
- Analizar el sistema para determinar las necesidades y disposición de sistemas de alimentación ininterrumpida.
- Instalar adecuadamente las unidades de alimentación y los estabilizadores de tensión respetando las características técnicas de los aparatos y cumpliendo las normas relativas a seguridad en el puesto de trabajo.
- Parametrizar y monitorizar los dispositivos instalados, adecuándolos al sistema para garantizar su total compatibilidad, óptimo funcionamiento, control y gestión de los mismos.
- Realizar un plan de intervención y activación de posibles mecanismos alternativos
- Documentar la instalación de los dispositivos físicos detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.

CE3.5 En varios supuestos prácticos de implementación y configuración de soluciones para la recuperación del sistema ante situaciones imprevistas, dados unos requisitos de seguridad a cumplir:

cve: BOE-A-2011-19503

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

Contenidos

1. Clasificar e inventariar el hardware

- Identificar y clasificar el hardware:
  - Conocer los distintos tipos de hardware según finalidad.
  - Conocer la arquitectura de servidores y PCs.
  - Diferenciar los componentes identificando sus funciones.
  - Clasificar los componentes según características, utilidad, y propósito.
  - Instalar y sustituir componentes en un sistema informáticos, atendiendo a la documentación del fabricante y a las normas de la organización.
- Establecer la conectividad del hardware:
  - Diferenciar los diferentes buses de comunicación en un sistema informático.
  - Distinguir los distintos tipos de conectividad con los dispositivos periféricos.
  - Identificar los distintos tipos de conectividad y tecnologías de conectividad entre los elementos hardware que componen la arquitectura de una plataforma para la prestación de un servicio.
  - Establecer la conectividad entre PCs y/o servidores.
  - Conectar los servidores con equipos de almacenamiento externo.
  - Diseñar la conexión con equipos de copia de seguridad.
  - Establecer la conexión con Internet.
  - Elegir e instalar el controlador de entrada/salida más adecuado según la finalidad perseguida.
- Documentar e inventariar el hardware:
  - Enumerar los equipos detallando componentes, estado, y ubicación.
  - Documentar las configuraciones y parametrizaciones.
  - Documentar las conectividades.
  - Etiquetar el hardware.
- Mantener el inventario:
  - Actualizarlo con las altas, bajas, y modificaciones.
  - Auditar el inventario.

cve: BOE-A-2011-19503

2. **Monitorizar el rendimiento**
   - Diseñar la monitorización:
     - Distinguir los distintos tipos de monitorizaciones según su finalidad. Diseñar la monitorización externa para garantizar la disponibilidad del sistema y diseñar la monitorización para la gestión de capacidad del sistema.
     - Seleccionar técnicas o herramientas en función de las características del hardware.
     - Definir parámetros a monitorizar. Conocer los parámetros habituales a monitorizar.
     - Monitorizar la CPU, RAM, y discos del sistema.
     - Monitorizar la conectividad.
     - Monitorizar los servicios.
     - Seleccionar los elementos a monitorizar y los umbrales de aviso según los procedimientos definidos por la organización.
     - Establecer las alertas: Configurar alertas ante la indisponibilidad de servicio y configurar alertas para garantizar la correcta gestión de capacidad según los procedimientos definidos en la organización.
   - Monitorizar el sistema:
     - Obtener estadísticas de rendimiento.
     - Interpretar correctamente los informes gráficos de uso.
   - Diagnosticar el estado del sistema:
     - Analizar el rendimiento: Comparar los valores obtenidos con el histórico de uso del sistema y localizar los cuellos de botella del sistema.
     - Proponer mejoras.
     - Evaluar la viabilidad de sustitución o ampliación de los elementos hardware que causan los cuellos de botella, por otros de superior rendimiento que cumplan la misma función.
     - Evaluar alternativas de diseño a la arquitectura que se adecuen mejor a las necesidades de rendimiento del sistema.
   - Optimizar la parametrización para implementar un mejor rendimiento:
     - Revisar la configuración de la BIOS del sistema.
     - Revisar la documentación del fabricante en busca de nuevas versiones de firmware que obtengan mejor rendimiento.

3. **Diseñar e implementar arquitecturas tolerantes a fallos**
   - Instalar los elementos hardware del sistema atendiendo a las especificaciones del fabricante y a las normas de la organización.
   - Verificar el correcto funcionamiento del sistema tras su instalación.
   - Diseñar los puntos de tolerancia a fallos del sistema:
     - Definir e implementar la tolerancia a fallos eléctricos.
     - Definir e implementar la tolerancia a fallos de disco, y de conectividad.
   - Conocer los procedimientos de respaldo y de recuperación de fallos definidos en la empresa:
     - Externalizar y salvaguardar las copias según los procedimientos vigentes en la organización.
     - Facilitar a los técnicos de copias de seguridad los soportes que contiene las copias necesarias para la restauración del servicio.
     - Instalar y configurar la arquitectura hardware necesaria para la instalación del sistema de copias de seguridad.
   - Conocer arquitecturas que permiten mayor tolerancia a fallos:
     - Conocer el concepto de sistemas en cluster.
     - Diseñar e implementar la arquitectura hardware necesaria para la instalación de un cluster. Implementar la arquitectura hardware necesaria para la instalación de un cluster de base de datos.
     - Conocer el concepto de sistemas balanceados por red.

cve: BOE-A-2011-19503

4. **Diagnosticar y resolver las averías**
   - Consultar la documentación del fabricante y la documentación interna de la organización, así como al servicio de asistencia técnica del fabricante, o de terceros con los que la organización tenga contrato de mantenimiento, en busca del origen y resolución de incidentes.
   - Utilizar las herramientas de diagnóstico y documentación facilitadas por el fabricante.
   - Planificar y ejecutar la reparación acorde a la documentación del fabricante y a los procedimientos internos.
   - Planificar y ejecutar la reparación garantizando la integridad de la información, y minimizando el impacto sobre la disponibilidad de servicio:
     - Poner en marcha los mecanismos definidos en la organización para mantener el servicio mientras se procede la sustitución o reparación.
     - Sustituir o reparar el componente averiado atendiendo a las especificaciones del fabricante.
     - Verificar el correcto funcionamiento del sistema tras la sustitución de los componentes averiados.
     - Restablecer la normal explotación del servicio.
   - Conocer e interpretar adecuadamente los planes de recuperación de servicio existentes en la empresa.

UNIDAD FORMATIVA 2

Denominación: GESTIONAR EL CRECIMIENTO Y LAS CONDICIONES AMBIENTALES

Código: UF1892

Duración: 50 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP4 y la RP5.

Capacidades y criterios de evaluación

C1: Analizar y evaluar los dispositivos disponibles en el mercado para proponer implantaciones hardware que mejoren el rendimiento y las prestaciones del sistema informático.

CE1.1 Identificar, evaluar y clasificar los dispositivos hardware existentes en el mercado, según evolución y tipología, utilizando para ello catálogos comerciales, documentación técnica, revistas especializadas o cualquier otro método o soporte.

CE1.2 Identificar las partes de un sistema informático, típicamente susceptibles de provocar cuellos de botella y degradaciones de la productividad.

CE1.3 Explicar las tendencias de evolución tecnológica en los dispositivos físicos comunes de un sistema informático con objeto de proponer mejoras en el mismo.

CE1.4 En un supuesto práctico de planificación de crecimiento de un sistema correctamente caracterizado, dadas unas estimaciones de posibles aumentos de la carga de trabajo o de usuarios:

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

cve: BOE-A-2011-19503

– Documentar exhaustivamente los resultados de la evaluación del sistema sometido a nuevas cargas y proponer, de forma razonada, cambios en la configuración actual o nuevas implantaciones hardware.

C2: Aplicar procedimientos de seguridad y de acondicionamiento ambiental con el fin de garantizar la integridad del sistema y el entorno adecuado según especificaciones y requisitos de los sistemas a instalar.

CE2.1 Enumerar y describir los principales factores ambientales y del entorno a tener en cuenta en la instalación adecuada de equipos informáticos, para establecer las precauciones que puedan evitarnos o aminorar su efecto.

CE2.2 Enumerar y describir los principales factores ambientales y del entorno que pueden degradar el funcionamiento de una red de comunicaciones, para establecer las precauciones que puedan evitarlos o aminorar su efecto.

CE2.3 Interpretar las especificaciones técnicas de los dispositivos y el plan de seguridad para adecuar su instalación y ubicación física consiguiendo un óptimo rendimiento de los mismos.

CE2.4 Evaluar la instalación de la red eléctrica asegurándose que su capacidad y los equipos disponibles son los adecuados para conectar todos los dispositivos hardware y que el funcionamiento de estos sea óptimo.

CE2.5 En un supuesto práctico de instalación de equipamiento informático:

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

CE2.6 En un supuesto práctico de comprobación de la seguridad del sistema informático:

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

Contenidos

1. Gestionar el crecimiento

– Planificar las ampliaciones. Dimensionar los crecimientos futuros:
  – Extrapolar de las mediciones de la plataforma en producción.
  – Simular con modelos matemáticos las nuevas cargas previstas.
  – Evaluar si las nuevas cargas previstas son asumibles en la plataforma actual.
– Analizar el mercado en busca de las soluciones hardware que ofrece:
  – Conocer el catálogo de productos de los principales fabricantes.
  – Seleccionar el producto más adecuado.
  – Identificar correctamente los distintos tipos de hardware.
  – Conocer las orientaciones de precios.
  – Razonar la propuesta equilibrando la componente técnica y la económica.

cve: BOE-A-2011-19503

– Localizar a los prescriptores de mercado:
  – Utilizar los informes comparativos como apoyo a la elección de hardware.
  – Utilizar los informes de tendencias como apoyo a la elección de hardware.
– Ejecutar las ampliaciones garantizando la mayor disponibilidad del servicio.

2. Establecer las condiciones ambientales adecuadas

– Conocer los factores ambientales que pueden afectar al funcionamiento de la instalación:
  – Identificar los factores que afectan a los equipos informáticos.
  – Identificar los factores que afectan a las comunicaciones.
– Interpretar adecuadamente las necesidades ambientales del hardware.
  – Identificar los parámetros críticos ambientales para el correcto funcionamiento del hardware: Establecer mediciones de temperatura, humedad, y presión, y establecer mediciones de ruidos, vibraciones, y campos electromagnéticos.
  – Revisar especificaciones de los fabricantes del hardware.
  – Establecer rangos de uso de los parámetros para el equipamiento.
– Comprobar la calidad del suministro industrial:
  – Comprobar la instalación eléctrica: Comprobar que la capacidad de la instalación eléctrica cumplen con los valores esperados de consumo y comprobar conexión del equipamiento a circuitos filtrados por SAIs.
  – Comprobar la instalación de refrigeración: Revisar las especificaciones del acondicionamiento de frío y comprobar que cumple con los requerimientos de refrigeración esperados en base a las especificaciones técnicas del equipamiento hardware.
– Diseñar la ubicación de los equipos en la sala:
  – Diseñar de la distribución.
  – Elegir el emplazamiento de los diferentes equipos hardware.

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 – UF1891	70	35
Unidad formativa 2 – UF1892	50	25

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 SOFTWARE DE UN SISTEMA INFORMÁTICO.

Código: MF0485_3

Nivel de cualificación profesional: 3

cve: BOE-A-2011-19503

Asociado a la Unidad de Competencia:

UC0485_3: Instalar, configurar y administrar el software de base y de aplicación del sistema.

Duración: 210 horas

UNIDAD FORMATIVA 1

Denominación: INSTALACIÓN Y PARAMETRIZACIÓN DEL SOFTWARE

Código: UF1893

Duración: 90 horas

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

Capacidades y criterios de evaluación

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

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

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

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

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

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

CE1.6 En varios supuestos prácticos de instalación y configuración de un sistema operativo en un sistema informático:

- Instalar el software del sistema operativo documentando exhaustivamente el proceso, las incidencias ocurridas y los parámetros utilizados.
- Configurar adecuadamente los parámetros del sistema operativo referidos al sistema de memoria, indicando la organización a seguir y la utilización de técnicas avanzadas de gestión.
- Configurar adecuadamente los parámetros del sistema operativo relativos a la ejecución de tareas: planificación de trabajos, mecanismos de sincronización y asignación de recursos.
- Parametrizar adecuadamente el sistema de entrada / salida comprobando el funcionamiento óptimo de los dispositivos periféricos.
- Organizar los sistemas de ficheros creando las estructuras necesarias para el correcto funcionamiento del sistema.
- Configurar los parámetros del sistema operativo de forma que se cumplan las especificaciones del plan de seguridad del sistema.
- Verificar el funcionamiento del sistema operativo y dispositivos intervinientes en el sistema, asegurando configuración de sus controladores y la ausencia de conflictos utilizando el software de diagnóstico que fuere necesario.
- Establecer y configurar los parámetros de red del sistema operativo de forma que se aseguren y garanticen la integridad de los datos y fiabilidad del sistema siguiendo en todo momento el plan de seguridad y calidad de la organización.
- Habilitar la organización y configuración de usuarios según las necesidades y plan de seguridad de la organización.

cve: BOE-A-2011-19503

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

CE1.7 En varios supuestos prácticos de instalación y configuración de software de aplicación en un sistema informático:
– Instalar el software de aplicación documentando exhaustivamente el proceso, las incidencias ocurridas y los parámetros utilizados.
– Configurar los parámetros del software de aplicación referidos a la utilización de recursos del sistema de forma que se minimice el impacto sobre el rendimiento del mismo.
– Configurar los parámetros del software de aplicación de forma que se cumpla las especificaciones del plan de seguridad del sistema.
– Verificar el funcionamiento del software de aplicación y dispositivos que componen el sistema, asegurando la configuración de sus controladores y la ausencia de conflictos utilizando el software de diagnóstico que fuere necesario.
– Actualizar el software de aplicación asegurando la integridad del sistema, de los datos y según el plan de seguridad de la organización.
– Documentar la configuración del software de aplicación detallando los parámetros utilizados.
– Interpretar adecuadamente el plan de seguridad de la organización para implementar las medidas especificadas en el mismo según normativa de seguridad informática.

C2: Identificar los componentes software del sistema distinguiendo sus características y detallando parámetros.
CE2.1 Analizar y enumerar los diferentes tipos de sistemas operativos precisando sus características más importantes.
CE2.2 Clasificar y describir los diferentes tipos de aplicaciones y componentes software explicando sus principales características, funciones y propósito.
CE2.3 Identificar las funciones que realiza un sistema operativo instalado en un sistema informático.
CE2.4 Explicar los requisitos legales relativos a propiedad intelectual a tener en cuenta en la instalación de software en el sistema.
CE2.5 A partir de un supuesto práctico de identificación y registro de software de un sistema informático:
– Clasificar una colección de software instalado atendiendo a diferentes criterios: propósito, idoneidad para un sistema y compatibilidad entre otros.
– Operar con herramientas de inventariado registrando de forma exhaustiva las características del software instalado.
– Comprobar el número y ubicación de licencias instaladas de aplicaciones protegidas por las leyes de propiedad intelectual para su correcto cumplimiento.
– Comprobar las aplicaciones instaladas para comprobar la no existencia de software no permitido.
– Registrar y controlar los privilegios de acceso a las aplicaciones de los usuarios según el plan de seguridad y las leyes de protección de datos vigentes.
– Documentar la instalación del software detallando los procedimientos, incidencias más frecuentes y parámetros utilizados.

cve: BOE-A-2011-19503

Contenidos

1. Software

- Conocer y comprender qué es el software, y para qué sirve.
- Distinguir software, de firmware, y de hardware.
- Identificar los diferentes tipos de software.

2. Sistemas Operativos

- Comprender la definición y utilidad de los sistemas operativos:
  - Enumerar las funciones de un sistema operativo.
  - Conocer la evolución histórica de los sistemas operativos.
  - Distinguir los diferentes componentes de un sistema operativo.
  - Comprender la gestión de procesos.
  - Distinguir los diferentes tipos de sistemas de archivos.
  - Conocer los sistemas de entrada/salida.
  - Conocer el uso de controladores para la gestión de hardware.
  - Distinguir los parámetros habituales a configurar y sus valores típicos.
  - Conocer los servicios habituales y su finalidad.
  - Conocer la utilidad de usuarios y grupos de usuarios, así como los de uso habitual.
- Identificar los distintos tipos de sistemas operativos, describiendo sus funciones y estructura.
- Clasificar los sistemas operativos:
  - Clasificar los sistemas operativos según propósito.
  - Clasificar los sistemas operativos según su grado de implantación.
  - Sistemas operativos monousuario y multiusuario.
  - Sistemas operativos monotarea y multitarea.
  - Sistemas operativos distribuidos.
  - Sistemas operativos en tiempo real.
- Conocer las políticas definidas en la organización, de aplicación en la instalación del sistema operativo.
- Instalar y parametrizar los sistemas operativos:
  - Realizar los preparativos previos a la instalación.
  - Recolectar los controladores necesarios.
  - Definir el tipo de sistema de archivo a utilizar, seleccionándolo de entre las posibles alternativas, en base a las necesidades del uso previsto.
  - Definir los valores de los parámetros habituales a configurar.
  - Instalar el sistema operativo, configurando el hardware con los controladores adecuados, que garanticen el correcto funcionamiento del sistema:
    - Instalar manualmente el sistema operativo.
    - Instalar desatendidamente el sistema operativo.
    - Instalar automáticamente el sistema operativo.
    - Clonar servidores.
    - Configurar la red.
    - Comprobar la correcta instalación del sistema operativo mediante pruebas de arranque y parada, y herramientas de diagnóstico.
    - Actualizar el sistema operativo.
- Conocer y utilizar adecuadamente las herramientas de gestión del sistema operativo, de uso habitual:
  - Conocer y utilizar las herramientas de gestión de grupos y usuarios.
  - Conocer y utilizar correctamente las herramientas de gestión de permisos del sistema de archivos.
  - Conocer y utilizar correctamente las herramientas de configuración y diagnóstico de red.

cve: BOE-A-2011-19503

- Conocer y utilizar correctamente las herramientas de gestión de servicios.
- Conocer y utilizar correctamente las herramientas de monitorización del sistemas facilitadas por el fabricante del sistema.

- Securizar el sistema atendiendo a las normas definidas:
  - Establecer la configuración inicial de usuarios y grupos.
  - Configurar los permisos en el sistema de archivos.
  - Configurar los permisos en el registro de configuraciones.
  - Establecer los permisos en la configuración de red.
  - Revisar y desinstalar o deshabilitar los servicios innecesarios.
- Documentar la instalación:
  - Registrar el proceso y las incidencias habidas, así como las medidas adoptadas para su resolución.
  - Detallar los valores de los parámetros establecidos.

3. Software de aplicación

- Distinguir entre los distintos tipos de software de aplicación atendiendo a su uso:
  - Conocer los distintos paquetes ofimáticos de uso habitual.
  - Distinguir las distintas funcionalidades que son capaces de prestar las herramientas colaborativas.
  - Conocer la necesidad de servicio que cubre el software ERP.
  - Conocer la necesidad de servicio que cubre el software CRM.
- Conocer las políticas definidas en la organización, de aplicación en la elección e instalación del software de aplicación:
  - Comprobar la autorización de la instalación.
  - Utilizar adecuadamente las listas de aplicaciones permitidas.
  - Registrar la instalación realizada.
- Instalar el software de aplicación, atendiendo a las recomendaciones del fabricante, y a las normas de seguridad de la organización:
  - Comprobar los requisitos del software de manera previa a la instalación.
  - Seguir las instrucciones de instalación dadas por el fabricante.
  - Actualizar el software de aplicación.
- Comprobar el correcto funcionamiento del software de aplicación.
- Desplegar masiva y desatendidamente software de aplicación.

4. Automatizaciones

- Conocer los diferentes lenguajes de programación de uso habitual para la automatización de tareas:
  - Distinguir el entorno nativo de cada lenguaje de programación.
- Utilizar un editor adecuado para el desarrollo del código.
- Desarrollar pequeños scripts para la ejecución de tareas de mantenimiento:
  - Conocer los diferentes lenguajes de programación de uso más común utilizables en cada sistema operativo.
  - Conocer los comandos y estructuras de los lenguajes de scripting.
  - Utilizar adecuadamente la documentación de consulta de los lenguajes de scripting, para facilitar la correcta escritura del código.
  - Programar scripts para la ejecución de tareas de mantenimiento.
- Seleccionar el lenguaje de programación más adecuado en función de los requisitos de la tarea a automatizar y del sistema operativo sobre el que se deba ejecutar.
- Configurar la ejecución automática de la tarea en el sistema operativo:
  - Establecer el horario y frecuencia más adecuados.
  - Configurar la ejecución en el sistema comprobando su correcta ejecución, y resultados.
- Utilizar herramientas de automatización.

cve: BOE-A-2011-19503

5. Inventario de sw

- Identificar los motivos de la necesidad de inventariar.
- Seleccionar adecuadamente los parámetros a inventariar en un sistema.
- Gestionar las licencias:
  - Inventariar las licencias compradas.
  - Inventariar las licencias instaladas.
  - Realizar un plan de compra de licencias en base al crecimiento estimado y los modelos de licenciamiento del software utilizado.
- Gestionar herramientas de inventariado:
  - Utilizar adecuadamente herramientas de inventario para extraer informes de licencias en uso, y de licencias compradas.
  - Mantener al día el inventario.
  - Utilizar herramientas de inventariado automático.
- Inventariar la configuración base y de aplicación.
- Actualizar la lista de aplicaciones permitidas por usuario.

UNIDAD FORMATIVA 2

Denominación: MANTENIMIENTO DEL SOFTWARE

Código: UF1894

Duración: 70 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP2, RP4 y la RP5.

Capacidades y criterios de evaluación

C1: Planificar el soporte a los usuarios asegurando la máxima disponibilidad y la documentación de las tareas correspondientes.

CE1.1 Definir los objetivos de un plan de asistencia técnica y de soporte a usuarios.

CE1.2 Explicar las ventajas y características principales de las técnicas de asistencia remota a los usuarios a través de los servicios y herramientas disponibles en el sistema.

CE1.3 Enumerar y describir los problemas más comunes relativos a la implantación de software en puestos de usuario.

CE1.4 Enumerar y describir los problemas más comunes relativos a dispositivos hardware y de red en puestos de usuario.

CE1.5 Establecer procedimientos de instalación, configuración y mantenimiento de software de base y aplicación en puestos de usuario.

CE1.6 En varios supuestos prácticos de planificación de soporte a los usuarios en un sistema debidamente caracterizado:

- Fijar procedimientos de asistencia basados en la anotación sistemática de los problemas detectados al personal de apoyo.
- Documentar exhaustivamente los problemas más comunes relativos a los recursos software del sistema.
- Documentar exhaustivamente los problemas más comunes relativos a los recursos hardware del sistema.
- Planificar el entrenamiento para la adaptación del personal a las herramientas de trabajo.
- Configurar y operar adecuadamente con herramientas de asistencia remota de usuarios.

C2: Analizar el sistema mediante técnicas de simulación y modelado para optimizar el rendimiento.

CE2.1 Definir el concepto de simulación explicando las ventajas de utilización de esta técnica así como sus posibles aplicaciones en diferentes ámbitos.

cve: BOE-A-2011-19503

CE2.2 Explicar la necesidad de representación de sistemas a través de modelos para su posterior estudio.
CE2.3 Identificar y caracterizar adecuadamente los pasos a seguir para realizar la simulación de un sistema.
CE2.4 En un supuesto práctico de simulación de un sistema informático debidamente caracterizado:
- Formular los objetivos a alcanzar a través de la simulación del sistema.
- Analizar las características del sistema y construir un modelo del mismo utilizando herramientas de modelado disponibles.
- Construir un modelo de simulación según los objetivos definidos y el modelo obtenido, utilizando las herramientas de simulación disponibles.
- Ejecutar el modelo de simulación documentando exhaustivamente los datos obtenidos.
- Analizar los resultados de la simulación extrayendo los puntos de mal funcionamiento o problemáticos del sistema.
- Ajustar la configuración del sistema para solucionar los problemas detectados y optimizar el rendimiento.
- Documentar los procesos de simulación detallando los objetivos, modelos y resultados obtenidos.

Contenidos

1. Planes de mantenimiento
- Conocer la utilidad y funciones de los planes de mantenimiento:
  - Mantener actualizado el software.
  - Gestionar el antivirus.
  - Formar a los usuarios en las labores de mantenimiento que deben realizar.
  - Optimizar el sistema de archivos.
- Diseñar, desarrollar y documentar el plan de mantenimiento:
  - Diseñar los mantenimientos proactivos.
  - Documentar los mantenimientos reactivos.
- Gestionar los problemas frecuentes:
  - Localizar y documentar los problemas frecuentes.
  - Resolver los casos de problemas frecuentes.
  - Dotar a los usuarios de medios para solucionar por sus propios medios los problemas frecuentes.
  - Atajar la causa raíz de los problemas frecuentes.
- Utilizar el conocimiento adquirido con la experiencia:
  - Consultar las bases de datos de conocimiento acorde con las normas establecidas en la organización.
  - Actualizar las base de datos de conocimiento con nueva información derivada de las actividades de mantenimiento.
- Atender al usuario:
  - Registrar las solicitudes de los usuarios, estableciendo una correcta priorización en su resolución.
  - Informar al usuario del estado de resolución de su solicitud y del tiempo estimado de resolución de la misma.
  - Formar al usuario en los procedimientos y canales adecuados para la solicitud de servicio y notificación de incidente, así como en las posibles soluciones a aplicar ante la aparición de problemas frecuentes.
- Actualizar el sistema, manteniéndolo al día en las versiones adecuadas a las funcionalidades requeridas por las necesidades, y a los requisitos de seguridad del sistema:
  - Actualizar el sistema operativo.
  - Actualizar las aplicaciones.

cve: BOE-A-2011-19503

- Parchear el sistema operativo.
- Parchear las aplicaciones.

2. Optimización del uso de los recursos

- Comprobar la adecuación del rendimiento del sistema a las necesidades de la organización:
  - Seleccionar los parámetros a medir para comprobar el rendimiento del sistema.
  - Establecer la monitorización necesaria para medir el rendimiento del sistema.
  - Representar gráficamente el rendimiento del sistema, interpretándolo, y estableciendo la adecuación o no a las necesidades de la organización.
  - Proponer las mejoras necesarias para el incremento del rendimiento.
- Utilizar las herramientas de modelado para predecir el rendimiento del sistema en base a las previsiones de incremento de carga del sistema.
- Realizar pruebas de carga para comprobar la escalabilidad del sistema y su adecuación a las necesidades presentes y futuras de la organización:
  - Seleccionar las herramientas adecuadas para la realización de las pruebas de carga en función de los servicios a prestar.
  - Diseñar e implementar el plan de pruebas de carga.
  - Realizar las pruebas de carga sin provocar problemas de disponibilidad de servicio en el sistema en producción.
  - Representar e interpretar el resultado de las pruebas de carga.

UNIDAD FORMATIVA 3

Denominación: AUDITORÍAS Y CONTINUIDAD DE NEGOCIO

Código: UF1895

Duración: 50 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP6 y la RP7.

Capacidades y criterios de evaluación

C1: Analizar y definir las políticas de realización de copias de respaldo y de recuperación de datos en función de las especificaciones de seguridad.

CE1.1 Clasificar los diferentes tipos de sistemas de copias de respaldo, basándose en el soporte empleado, en la topología o arquitectura y sistemas soportados (fichero, partición de disco y base de datos entre otros).

CE1.2 Describir los niveles de copias de respaldo explicando las diferencias entre ellos.

CE1.3 Asociar la política de realización de copias a los sistemas implicados, justificando las decisiones y cumpliendo la normativa vigente en materia de protección de datos de carácter personal.

CE1.4 A partir de un supuesto práctico en el que se da un escenario de sistemas de almacenamiento de información en el plan de explotación de una organización:

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

cve: BOE-A-2011-19503

– Verificar que las copias de respaldo reciben el mismo nivel de seguridad que los archivos originales.

C2: Aplicar procedimientos de auditoría utilizando técnicas y herramientas adecuadas para garantizar los parámetros de funcionamiento del sistema informático.

CE2.1 Enumerar y explicar los objetivos a cumplir con la habilitación de auditorías del sistema.

CE2.2 Clasificar según prioridad, los eventos del sistema y de las aplicaciones susceptibles de ser auditados para el mantenimiento del óptimo funcionamiento del sistema.

CE2.3 Determinar, para cada evento detectado, la necesidad de llevar a cabo acciones correctivas, estableciendo las mismas en caso afirmativo.

CE2.4 En un supuesto práctico de aplicación de procedimientos de auditoría en un sistema debidamente caracterizado:

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

Contenidos

1. Copias de respaldo

– Tipificar los datos según sus necesidades de copia.
– Diferenciar los distintos tipos de copias, distinguiendo las diferencias entre copias completas, incrementales, y diferenciales, así como las ventajas e inconvenientes de cada una de ellas, y las combinaciones más habituales de las mismas.
– Establecer correctamente los periodos de retención acordes con las normas de seguridad de la empresa, con las necesidades según el tipo de datos, y con la legislación vigente.
– Dimensionar las copias de seguridad:
  – Establecer el tamaño de copia completa acorde con los datos a copiar y la ocupación estimada en el dispositivo de copias.
  – Establecer el tamaño de las copias en función del tiempo, acorde con la política de copias a utilizar.
– Establecer la política de copias de la organización:
  – Definir el plan de copias indicando cada tipo de copia a realizar, la hora de programación, la ventana de copia, el periodo de retención.
  – Revisar la adecuación de la política de copias a las normas de la organización, así como a la legalidad vigente.
– Proponer los dispositivos de copia y soportes más adecuados en base a las necesidades de la organización:
  – Conocer las distintas alternativas posibles para los dispositivos de copia.

cve: BOE-A-2011-19503

- Razonar la mejor adecuación de cada alternativa a las necesidades de la organización.
- Realizar las copias de seguridad según los procedimientos y políticas vigentes en la organización:
  - Implementar y configurar las copias de seguridad.
  - Programar y ejecutar las copias de seguridad.
  - Verificar las copias de seguridad mediante restauraciones, documentando los tiempos de restauración y el resultado obtenido.
- Gestionar el ciclo de vida de los soportes:
  - Salvaguardar los soportes de copia, manteniéndolos en condiciones óptimas para su conservación.
  - Externalizar las copias.
  - Destruir los soportes tras su ciclo de vida útil de manera acorde con las normas de seguridad de la empresa, garantizando la imposibilidad de extracción de información de los mismos.
- Documentación de planes de recuperación:
  - Diseñar los pasos a seguir para la completa restauración de un sistema en producción.
  - Documentar las restauraciones a realizar para el restablecimiento de un sistema en producción, tras un problema mayor.

2. Legislación vigente

- Conocer las Leyes vigentes relacionadas con el tratamiento de datos:
  - Legislación vigente en materia de protección de datos de carácter personal.
  - Legislación vigente en materia de comercio electrónico.
  - Legislación vigente en materia de protección de la propiedad intelectual.
- Enumerar los puntos principales a tener en cuenta.

3. Alternativas a las copias

- Distinguir entre salvaguarda de datos, y disponibilidad del servicio.
- Enumerar las alternativas para garantizar la disponibilidad del servicio:
  - Diseñar alternativas en cluster.
  - Diseñar alternativas basadas en almacenamiento externo.
  - Diseñar alternativas basadas en copias de imágenes.
- Indicar ventajas e inconvenientes de las alternativas para garantizar la disponibilidad del servicio sobre las copias de seguridad.

4. Planes de auditoría

- Describir los objetivos de los planes de auditoría:
  - Distinguir entre las auditorías por su tipo y aplicación (de rendimiento, de seguridad, de mejora continua, de optimización de uso)
- Describir el perfil del auditor.
- Auditar el sistema:
  - Diseñar el plan de auditoría.
  - Utilizar herramientas de auditoría.
  - Documentar el resultado de la auditoría.

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 – UF1893	90	45
Unidad formativa 2 – UF1894	70	35
Unidad formativa 3 – UF1895	50	30

cve: BOE-A-2011-19503

Secuencia:

Para acceder a las unidades formativas 2 y 3 debe haberse superado la unidad formativa 1.

Las unidades formativas 2 y 3 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.

MÓDULO FORMATIVO 3

Denominación: SEGURIDAD EN EQUIPOS INFORMÁTICOS

Código: MF0486_3

Nivel de cualificación profesional: 3

Asociado a la Unidad de Competencia:

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.

cve: BOE-A-2011-19503

– 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.
– 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

cve: BOE-A-2011-19503

– 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

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 más 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 más 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

cve: BOE-A-2011-19503

- 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
- 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.

cve: BOE-A-2011-19503

MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES DE GESTIÓN DE SISTEMAS INFORMÁTICOS

Código: MP0398

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Identificar los componentes hardware del sistema distinguiendo sus características y detallando parámetros y procedimientos de instalación.

CE1.1 Detallar las características técnicas y procedimientos de instalación y configuración de los componentes hardware de un sistema informático según especificaciones de funcionalidades dadas.

CE1.2 Definir y clasificar los diferentes tipos de dispositivos periféricos atendiendo a su propósito, describiendo las diferentes técnicas utilizadas para realizar la comunicación con los mismos y las tecnologías disponibles en controladores de entrada/salida.

CE1.3 Identificar y clasificar los diferentes dispositivos físicos disponibles para conectar el sistema a través de una red de comunicaciones.

C2: Aplicar procedimientos de seguridad y de acondicionamiento ambiental con el fin de garantizar la integridad del sistema y el entorno adecuado según especificaciones y requisitos de los sistemas a instalar.

CE2.1 Interpretar las especificaciones técnicas de los dispositivos y el plan de seguridad para adecuar su instalación y ubicación física consiguiendo un óptimo rendimiento de los mismos.

CE2.2 Evaluar la instalación de la red eléctrica asegurándose que su capacidad y los equipos disponibles son los adecuados para conectar todos los dispositivos hardware y que el funcionamiento de estos sea óptimo.

C3: Planificar el soporte a los usuarios asegurando la máxima disponibilidad y la documentación de las tareas correspondientes.

CE3.1 Definir los objetivos de un plan de asistencia técnica y de soporte a usuarios.

CE3.2 Enumerar y describir los problemas más comunes relativos a la implantación de software en puestos de usuario.

CE3.3 Enumerar y describir los problemas más comunes relativos a dispositivos hardware y de red en puestos de usuario.

CE3.4 Establecer procedimientos de instalación, configuración y mantenimiento de software de base y aplicación en puestos de usuario.

C4: Analizar y definir las políticas de realización de copias de respaldo y de recuperación de datos en función de las especificaciones de seguridad.

CE4.1 Clasificar los diferentes tipos de sistemas de copias de respaldo, basándose en el soporte empleado, en la topología o arquitectura y sistemas soportados (fichero, partición de disco y base de datos entre otros).

CE4.2 Describir los niveles de copias de respaldo explicando las diferencias entre ellos.

CE4.3 Asociar la política de realización de copias a los sistemas implicados, justificando las decisiones y cumpliendo la normativa vigente en materia de protección de datos de carácter personal.

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

cve: BOE-A-2011-19503

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.
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. Puesta en producción de nuevos sistemas
- Revisión de la documentación de instalación de sistemas y sugerir posibles mejoras sobre la misma.
- Instalación de servidores de manera acorde a las normas de la organización.
- Instalación de software de aplicación sobre los servidores.
- Desinstalación los servicios en desuso.
- Establecimiento la seguridad a nivel de servidor sobre los servidores instalados.
- Diseño y configurar la monitorización de los sistemas instalados.
- Configuración de la auditoría del sistema acorde a las normas de la organización.
- Inventario de los nuevos sistemas puestos en producción.
- Configuración de copias de seguridad de los sistemas instalados.

2. Monitorización y rendimiento de sistemas
- Revisión de la documentación de monitorización de rendimiento y capacidad de los sistemas en producción.
- Revisión de la documentación de monitorización de consumo eléctrico y medioambiental de los sistemas en producción.
- Revisión de la documentación de auditoría de los sistemas en producción.
- Comportamiento de los sistemas en producción en base a las cargas de trabajo futuras esperadas.

3. Atender a los usuarios
- Revisión de la documentación de soporte a usuarios corporativos.
- Atención a los usuarios corporativos.
- Mejoras a los procedimientos y documentación de atención a usuarios.

4. Copias de seguridad y restauración de servicio
- Revisión de la documentación de copias de seguridad de la organización.
- Procedimientos de recuperación de servidores de producción sobre equipos de pruebas, y documentar los resultados, proponiendo mejoras sobre dichos procedimientos y/o sobre las políticas de copias.

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.

cve: BOE-A-2011-19503

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	Experiencia profesional requerida en el ámbito de la unidad de competencia
MF0484_3: Administración hardware de un 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
MF0485_3: Administración software de un 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
MF0486_3: Seguridad en 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.	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
Aula técnica informática	45	60

Espacio Formativo	M1	M2	M3
Aula de gestión	X	X	X
Aula técnica informática	X	X	X

Espacio Formativo	Equipamiento
Aula de gestión	– Equipos audiovisuales – PCs instalados en red, cañón con proyección e internet – Software específico de la especialidad – 2 Pizarras para escribir con rotulador – Rotafolios – Material de aula – Mesa y silla para formador – Mesas y sillas para alumnos
Aula técnica informática	– Racks – Acondicionamiento de frío – SAIs – Servidores instalados en red – Equipos de almacenamiento externo – Dispositivos de copia de seguridad – Software de copia de seguridad – Software de monitorización – Conexión con la red del aula de gestión – Conexión a Internet

cve: BOE-A-2011-19503

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 XII

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Administración y programación en sistemas de planificación de recursos empresariales y de gestión de relaciones con clientes.

Código: IFCT0610

Familia profesional: Informática y Comunicaciones

Área profesional: Sistemas y Telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC363_3 Administración y programación en sistemas de planificación de recursos empresariales y de gestión de relaciones con clientes. (RD 1701/2007, de 14 de diciembre)

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

UC1213_3: Instalar y configurar sistemas de planificación de recursos empresariales y de gestión de relaciones con clientes.
UC1214_3: Administrar sistemas de planificación de recursos empresariales y de gestión de relaciones con clientes.
UC1215_3: Realizar y mantener componentes software en un sistema de planificación de recursos empresariales y de gestión de relaciones con clientes.

Competencia general:

Realizar los procesos de instalación, configuración y administración en sistemas de planificación de recursos empresariales y de gestión de relaciones con los clientes (sistemas ERP-CRM: Enterprise Resource Planning – Customer Relationship Management), realizando las adecuaciones necesarias mediante la programación de componentes software, siguiendo especificaciones de diseño, con el fin de soportar las reglas de negocio de la organización, y asegurando su funcionamiento dentro de los parámetros organizativos de la empresa.

cve: BOE-A-2011-19503