

CUALIFICACIÓN PROFESIONAL: Operación de redes locales

Familia Profesional:	Informática y Comunicaciones
Nivel:	2
Código:	IFC299_2
Estado:	BOE
Publicación:	RD 545/2023
Referencia Normativa:	Orden PRE/1636/2015, RD 1201/2007

Competencia general

Instalar y mantener redes locales, asegurando la conectividad interna y hacia el exterior, así como el acceso a los recursos de la misma, mediante la instalación de los dispositivos y su 'software' y la configuración y monitorización de la red, resolviendo los problemas o incidencias que se detecten, garantizando la seguridad informática, cumpliendo la normativa aplicable medioambiental y en materia de protección de datos y propiedad intelectual e industrial.

Unidades de competencia

- UC0220_2:** INSTALAR DISPOSITIVOS DE COMUNICACIONES EN REDES LOCALES
- UC0955_2:** Mantener los procesos de comunicaciones en redes locales
- UC2688_2:** INTERCONECTAR REDES PRIVADAS Y PÚBLICAS

Entorno Profesional

Ámbito Profesional

Desarrolla su actividad profesional en el departamento de informática dedicado a la operación de redes, en entidades de naturaleza pública o privada, empresas de tamaño mediano o grande, tanto por cuenta propia como ajena, con independencia de su forma jurídica. Desarrolla su actividad dependiendo, en su caso, funcional y/o jerárquicamente de un superior. Puede tener personal a su cargo en ocasiones, por temporadas o de forma estable. En el desarrollo de la actividad profesional se aplican los principios de accesibilidad universal y diseño universal o diseño para todas las personas de acuerdo con la normativa aplicable.

Sectores Productivos

Se ubica sobre todo en el sector servicios, en el subsector de instalación y mantenimiento de redes de ordenadores y en cualquier otro sector productivo que por su tamaño y organización necesiten disponer de redes departamentales.

Ocupaciones y puestos de trabajo relevantes

Los términos de la siguiente relación de ocupaciones y puestos de trabajo se utilizan con carácter genérico y omnicomprendivo de mujeres y hombres.

- Técnicos de soporte de dispositivos de red local
- Operadores de dispositivos de red local

Formación Asociada (540 horas)

Módulos Formativos

- MF0220_2:** INSTALACIÓN DE DISPOSITIVOS DE COMUNICACIONES EN REDES LOCALES (210 horas)
- MF0955_2:** Mantenimiento de procesos de comunicaciones en redes locales (180 horas)
- MF2688_2:** INTERCONEXIÓN DE REDES PRIVADAS Y PÚBLICAS (150 horas)

UNIDAD DE COMPETENCIA 1

INSTALAR DISPOSITIVOS DE COMUNICACIONES EN REDES LOCALES

Nivel: 2
Código: UC0220_2
Estado: BOE

Realizaciones profesionales y criterios de realización

RP1: Instalar nodos en redes locales, habilitando su conectividad y el 'software' para implementar servicios de comunicaciones internas, permitiendo su acceso, tanto presencial como en remoto, para su gestión y mantenimiento, según especificaciones técnicas del fabricante para cada equipo, aplicando la planificación de la acción preventiva.

CR1.1 Los interfaces y módulos de los equipos de la red se instalan o, en su caso, se verifican para que ofrezcan las características de conectividad especificadas atendiendo a los medios de transmisión que se utilizan, la configuración física de la red en que se ubicarán y la documentación técnica del fabricante.

CR1.2 La versión de 'firmware' de los equipos de red se instala o, en su caso, se actualiza, utilizando la última versión disponible y siguiendo las instrucciones del fabricante.

CR1.3 Los equipos se instalan en el bastidor del armario ('rack') siguiendo las instrucciones del fabricante, comprobando los parámetros correspondientes a la alimentación eléctrica, sujeción mecánica y puesta a tierra, entre otros, y atendiendo a las condiciones medioambientales de temperatura y humedad.

CR1.4 Los equipos se conectan a la red eléctrica, teniendo en cuenta posibles circuitos independientes en el caso de equipos con fuente de alimentación redundante y verificando la toma de tierra.

CR1.5 Los equipos se conectan a la red de datos, conforme a los medios de transmisión que se utilizan, asegurando su funcionalidad y verificando la habilitación de su conectividad y funcionamiento, usando herramientas de monitorización al efecto, siguiendo las especificaciones de la organización y de modo que queden accesibles para su gestión remota.

CR1.6 El parte de trabajo o informe técnico de instalación se cumplimenta, utilizando el modelo o aplicación informática establecidos por la entidad responsable de la instalación, indicando ítems tales como las interconexiones realizadas, la fecha y hora de instalación y datos del técnico, entre otros, a fin de garantizar la trazabilidad de los procesos.

RP2: Configurar dispositivos, asegurando su funcionalidad en la red para su puesta en marcha y posterior gestión según los requerimientos y las especificaciones operativas suministradas por la entidad responsable de la instalación.

CR2.1 Los protocolos de los equipos, tales como encaminadores ('routers') y conmutadores ('switches'), entre otros, se configuran, a través de su interfaz específica para la gestión del equipo, en base a la topología de la red.

CR2.2 El funcionamiento de los protocolos de gestión tales como SNMP y SSH, entre otros, necesarios para la gestión remota del equipo de comunicaciones, se comprueba, previa habilitación.

CR2.3 Los protocolos asociados a las aplicaciones de red instaladas se configuran en los servidores, para soportar los servicios implementados, de acuerdo con los manuales de instalación.

CR2.4 El 'software' de cifrado se configura en los nodos de la red que se determine, previa instalación, a través de la interfaz específica, para crear redes privadas virtuales.

CR2.5 Los dispositivos de comunicaciones y su configuración se comprueban, ejecutando pruebas para asegurar la conformidad de los mismos.

CR2.6 El nodo de red se incluye en los sistemas de monitorización de la infraestructura, recogiendo sus parámetros de funcionamiento característicos tales como tramas gestionadas, ancho de banda utilizado y errores/colisiones, entre otros.

CR2.7 Los procesos de configuración y de prueba del dispositivo de comunicaciones se documentan, indicando ítems tales como los valores de los parámetros incluidos y datos del técnico, entre otros, utilizando el modelo o aplicación informática establecidos en la entidad responsable de la instalación para registrar las actividades realizadas, garantizando la trazabilidad de los procesos.

RP3: Corregir incidencias detectadas en la instalación de dispositivos de la red, diagnosticando los problemas y aplicado soluciones o, en su caso informando de ellas, según los protocolos de actuación frente a fallos predefinidos en los planes de contingencia, para garantizar la prestación de los servicios de comunicaciones.

CR3.1 Los sistemas de notificación de incidencias se revisan, comprobando posibles alarmas frente a fallos o indisponibilidad del servicio, para garantizar el correcto funcionamiento de las comunicaciones.

CR3.2 El dispositivo en el que se ha producido la incidencia se localiza, interpretando la información recibida del sistema de alarmas y la documentación técnica tal como el mapa de la red u otra, iniciando actuaciones mediante conexión remota o de manera presencial en los equipos o sistemas implicados, para identificar el problema físico y/o lógico causante del fallo.

CR3.3 El problema se diagnostica, indicando su naturaleza y origen tal como interrupción de la comunicación debido a problemas físicos y problemas de calidad de servicio, entre otros, planteando su solución, para rehabilitar los servicios interrumpidos o deteriorados a partir de los síntomas reportados por los sistemas de gestión de incidencias y las actuaciones de localización realizadas.

CR3.4 Las incidencias que no se hayan conseguido aislar se reportan al nivel de responsabilidad superior, utilizando los canales de comunicación establecidos en la entidad responsable del mantenimiento, incluyendo el listado de los síntomas reportados por los sistemas de gestión de incidencias y la naturaleza y origen de las mismas.

CR3.5 La incidencia se subsana con las herramientas específicas, teniendo en cuenta el diagnóstico, respetando los protocolos de actuación de la entidad responsable y del fabricante, para rehabilitar los servicios interrumpidos o deteriorados.

CR3.6 La detección, diagnóstico y solución de la incidencia se documenta, utilizando el modelo o aplicación informática establecida para registrar las tareas efectuadas garantizando la trazabilidad de los procesos en el parte de incidencias.

Contexto profesional

Medios de producción

Analizadores de red. Certificadores de cableado. Herramientas manuales para trabajos eléctricos y mecánicos. Herramientas 'software' para pruebas de conectividad. Herramientas 'software' para control de inventario de elementos de red. Ordenadores, impresoras y periféricos. Sistemas operativos.

Conmutadores ('switches'), encaminadores ('routers'). Tarjetas de red. Cables y conectores. 'Software' de gestión de red. 'Software' propietario de los dispositivos de red. Herramientas ofimáticas. Mapas de la red.

Productos y resultados

Nodos de redes locales instalados. Dispositivos configurados. Incidencias detectadas en dispositivos de red solucionadas.

Información utilizada o generada

Normativa aplicable de protección medioambiental. Normativa aplicable de propiedad industrial. Normativa aplicable de protección de datos. Normativa aplicable de planificación de la acción preventiva. Mapa de la red. Inventario del 'hardware' de la organización. Órdenes y partes de trabajo. Documentación de red. Plan de seguridad. Plan de mantenimiento. Manuales de instalación de los dispositivos. Manuales de configuración de los dispositivos. Manual de calidad con normas y criterios de calidad.

UNIDAD DE COMPETENCIA 2

Mantener los procesos de comunicaciones en redes locales

Nivel: 2
Código: UC0955_2
Estado: BOE

Realizaciones profesionales y criterios de realización

RP1: Monitorizar la red local, para detectar y, en su caso, solucionar o reportar los fallos, asegurando su rendimiento en ausencia de congestión de tráfico de datos y el acceso a los servidores, según la tipología de red y siguiendo los procedimientos indicados por la entidad responsable de la misma, garantizando la calidad de servicio y la seguridad física y lógica.

CR1.1 La herramienta de monitorización seleccionada por el administrador de red se instala, configurando el servidor y la sonda local asociada a su misma máquina con los sensores, para garantizar la correcta supervisión de todos los dispositivos asociados a la red local, generando una plataforma de gestión unificada.

CR1.2 Las sondas de monitorización remota se instalan, configurándolas en los puntos de la red a supervisar, para que, mediante chequeos del tráfico de red, proporcionen información a la plataforma de gestión.

CR1.3 Los agentes del 'software' de red se instalan, comprobando su ejecución de forma continua en los nodos a gestionar, para que proporcionen a la plataforma de gestión la información recogida por sus respectivos sistemas operativos.

CR1.4 Los ficheros de registro de actividad ('log') de los diferentes servicios se recopilan, con objeto de analizar los procesos asociados a los mismos, manteniendo los recursos de almacenamiento y gestión en condiciones adecuadas de visibilidad, accesibilidad, integración y escalabilidad del proceso, para explotar los datos e identificar errores y conflictos a resolver.

CR1.5 La interfaz de la herramienta de gestión de red y los filtros de selección de alarmas y alertas se configuran, optimizando los procesos de notificación y gestión de incidencias.

RP2: Mantener los dispositivos de la red local, revisándolos de manera periódica, comprobando alarmas y solucionando incidencias con el fin de garantizar los servicios de comunicaciones dentro de los parámetros recogidos en los requisitos, siguiendo procedimientos indicados por el administrador de la red y normas de calidad del servicio establecidos en el plan de mantenimiento preventivo.

CR2.1 El mapa de la red se actualiza, lanzando tareas de descubrimiento de red desde la plataforma de gestión, para disponer de una imagen real de todos los dispositivos conectados en ella, según las especificaciones recibidas por el administrador de la red.

CR2.2 La conectividad de los dispositivos de la red, tanto activos como pasivos, se comprueba con las señales acústico-luminosas observables y la aplicación de comandos de red específicos para valorar posibles deterioros o alteraciones físicas o lógicas.

CR2.3 Las causas del comportamiento anómalo de los dispositivos de la red se identifican, para proceder a su solución, aplicando la metodología de diagnóstico establecida en el plan de

mantenimiento por el administrador de la red, utilizando herramientas 'hardware' y 'software' de diagnóstico para localizar la fuente de posibles errores y consultando la documentación técnica.

CR2.4 Las incidencias detectadas, localizadas mediante procesos de inspección o recibidas desde las herramientas de monitorización, se subsanan previo diagnóstico, mediante conexión remota o de manera presencial, poniendo en marcha las medidas para su solución, tales como el reseteo, actualización o reemplazo de dispositivos, de cableado u otras.

CR2.5 La seguridad y configuración de la red a las políticas y normas establecidas en la organización se verifican, realizando pruebas y utilizando las herramientas específicas de seguridad para la generación de alarmas.

CR2.6 Los resultados de las pruebas se documentan en el plan de mantenimiento del administrador de red y en el histórico de incidencias y averías, incluyendo los datos de las incidencias y las soluciones adoptadas, utilizando el modelo o aplicación informática establecidos en la entidad responsable del servicio para registrar las actividades realizadas, garantizando la trazabilidad de los procesos.

RP3: Actualizar los componentes 'hardware' y 'firmware' de los dispositivos de comunicaciones de la red local, usando los medios proporcionados por el fabricante, para adecuar su funcionalidad a los cambios en las tecnologías según las especificaciones y procedimientos recibidos del administrador de la red, así como la documentación técnica del fabricante.

CR3.1 El 'hardware' de los equipos de comunicaciones se actualiza parcial o totalmente, usando el medio proporcionado por el fabricante, con el fin de adaptarlo a nuevas funcionalidades.

CR3.2 El 'firmware' actualmente instalado en los equipos de comunicaciones se salvaguarda, realizando una copia de seguridad de la versión instalada, a fin de poder restaurarla en caso de fallo de la actualización.

CR3.3 El 'firmware' de los equipos de comunicaciones se actualiza, accediendo al sitio 'web' del fabricante o con la opción de búsqueda de actualizaciones, si dicha opción está disponible con el sistema operativo que gestiona cada dispositivo, para adaptarlo a nuevas funcionalidades.

CR3.4 Las configuraciones de los equipos de comunicaciones se modifican, incluyendo la parametrización que especifique el administrador de la red, para cambiarles la funcionalidad o adaptarlos a los nuevos equipos introducidos.

CR3.5 Los componentes 'hardware' y 'firmware' actualizados se verifican mediante pruebas, para asegurar su funcionalidad.

CR3.6 Las actuaciones realizadas sobre los dispositivos se documentan, utilizando el modelo o aplicación informática establecido por el administrador de la red para registrar las actividades realizadas, incluyendo las referencias de los dispositivos y la versión del 'firmware' actualizado, garantizando la trazabilidad de los procesos.

RP4: Comprobar la seguridad lógica y física concerniente a los dispositivos de comunicaciones de la red local, para garantizar tanto las condiciones de integridad, disponibilidad, confidencialidad, control lógico del acceso y trazabilidad de los datos, como las del acceso físico a los servicios a usuarios autorizados, según las especificaciones y normas de seguridad recibidas del administrador de la red.

CR4.1 Las notificaciones de las alertas de seguridad recibidas por los canales de comunicación establecidos en las herramientas que las generan y elegidas por el administrador se atienden,

usando las opciones de la misma herramienta, para iniciar la corrección de las incidencias notificadas.

CR4.2 Los dispositivos de comunicaciones se revisan para asegurar que su acceso físico y lógico está controlado, de acuerdo con los criterios de autenticación establecidos por el administrador de la red.

CR4.3 Los ficheros de auditoría de los dispositivos de comunicaciones se recogen, analizándolos para detectar posibles accesos indebidos que afecten a la confidencialidad y/o integridad de los datos, siguiendo las indicaciones de los procedimientos de seguridad establecidos por el administrador de la red.

CR4.4 La trazabilidad de los datos en la red se comprueba, validando que se cumple con la normativa legal en relación al tratamiento de los mismos, mediante las herramientas específicas de rastreo determinadas por el administrador de la red.

CR4.5 Las actuaciones realizadas se documentan, utilizando el modelo o aplicación informática establecidos por el administrador del sistema, registrando las actividades realizadas, garantizando la propia trazabilidad de los sistemas y procesos de seguridad.

Contexto profesional

Medios de producción

Analizadores de red ('sniffers'). Certificadores de cableado. Herramientas manuales para trabajos eléctricos y mecánicos. Herramientas de diagnóstico. Herramientas 'software' para pruebas de conectividad. Herramientas 'software' de inventario de equipos de red. Ordenadores, impresoras y periféricos. Sistemas operativos. Conmutadores ('switches') y encaminadores ('routers'). Tarjetas de red. Cables y conectores. 'Software' de clientes de red. 'Software' de gestión de red. 'Software' de monitorización de red. Sondas de monitorización remota (RMON). 'Software' propietario de los dispositivos de red. Herramientas ofimáticas. Herramientas de auditoría. Mapa de la red. Herramientas de monitorización de la cobertura en redes inalámbricas. Sistemas de detección y prevención de intrusión inalámbrica (WIDS/WIPS).

Productos y resultados

Red local monitorizada. Mantenimiento de los dispositivos de la red local aplicado. Componentes 'hardware' y 'firmware' de los dispositivos de comunicaciones de la red local actualizados. Seguridad lógica y física comprobada y garantizada.

Información utilizada o generada

Normativa aplicable de protección medioambiental, de planificación de la acción preventiva y de propiedad industrial. Normativa aplicable de protección de datos. Mapas de la red. Inventario 'hardware' y de configuración de la red. Partes de trabajo. Histórico de incidencias y averías. Documentación de red. Especificaciones operativas de la organización. Manual de calidad. Plan de mantenimiento. Plan de seguridad. Manuales de instalación de los dispositivos. Manuales de configuración de los dispositivos. Manual de las herramientas de monitorización.

UNIDAD DE COMPETENCIA 3

INTERCONECTAR REDES PRIVADAS Y PÚBLICAS

Nivel: 2
Código: UC2688_2
Estado: BOE

Realizaciones profesionales y criterios de realización

RP1: Instalar los nodos de interconexión de redes públicas y privadas, comprobando parámetros y verificando su funcionamiento, para habilitar la comunicación entre ambas, siguiendo las especificaciones recibidas de la entidad responsable de la instalación y la documentación técnica del fabricante, así como aplicando la planificación de la acción preventiva en los trabajos.

CR1.1 Los requisitos de implantación del dispositivo, así como las líneas de comunicaciones con sus correspondientes interfaces se comprueban, asegurando que se cumplan las condiciones de compatibilidad, según las especificaciones recibidas y del fabricante.

CR1.2 El dispositivo se instala, comprobando los parámetros correspondientes a la alimentación eléctrica, sujeción mecánica y puesta a tierra, entre otros.

CR1.3 Los interfaces y módulos de adaptación de las líneas de comunicación se instalan, comprobando y asegurando su funcionalidad, para proceder a su conexión según los requisitos de implantación del dispositivo de comunicaciones.

CR1.4 Las líneas de comunicaciones y el dispositivo se conectan, verificando la habilitación de la conexión y su funcionamiento para asegurar la comunicación entre la red pública y privada y la prestación del servicio de comunicaciones.

CR1.5 El parte de trabajo o informe técnico de la instalación se cumplimenta, utilizando el modelo o aplicación informática establecidos por la entidad responsable de la instalación, documentando los trabajos realizados e incluyendo elementos tales como fecha de la instalación, dispositivos instalados, módulos incluidos y conexiones, entre otros, a fin de garantizar la trazabilidad de los procesos.

RP2: Configurar los protocolos de comunicaciones en los dispositivos de interconexión de red para asegurar la conectividad entre la red pública y privada, habilitando sus parámetros funcionales, según los requerimientos operativos y las especificaciones de la entidad responsable de la instalación.

CR2.1 Los equipos activos de comunicaciones se configuran, mediante su interfaz específica, habilitando los parámetros funcionales, para permitir la coexistencia e/o interconexión de redes locales a través de redes públicas.

CR2.2 Los interfaces externos de los encaminadores ('routers') se configuran, mediante las herramientas de gestión del dispositivo, habilitando su funcionalidad, empleando el 'software' del fabricante para el acceso a las redes externas, para proporcionar conectividad según los requisitos de la entidad operadora de comunicaciones.

CR2.3 Los parámetros de funcionamiento y calidad de servicio de los dispositivos de interconexión se verifican, mediante la ejecución de pruebas finales de parámetros tales como conectividad, velocidad de transmisión y latencia, que confirmen su completa operatividad.

CR2.4 Las medidas de seguridad en las comunicaciones tales como cortafuegos ('firewalls') u otros se implementan, configurando reglas de acceso y validándolas.

CR2.5 Los procesos de configuración y pruebas de los dispositivos de interconexión se documentan, utilizando el modelo o aplicación informática establecidos por la entidad responsable de la instalación, para registrar las actividades realizadas e incluyendo elementos tales como fecha de la realización, protocolos habilitados y resultado de las pruebas funcionales, entre otros, garantizando la trazabilidad de los procesos.

RP3: Mantener la conexión con la red pública, para asegurar la continuidad y calidad del servicio, gestionando las incidencias y alertas de los dispositivos de interconexión de la red privada y las reportadas por los usuarios, según los protocolos de actuación frente a fallos predefinidos en los planes de contingencia.

CR3.1 Los sistemas de alertas y alarmas se comprueban, observando la información proporcionada por las herramientas de monitorización, para asegurar la prestación de los servicios de comunicaciones.

CR3.2 Las notificaciones de incidencias por parte de los usuarios, realizadas a través del Centro de Atención al Usuario (CAU), se recogen incluyéndolas en el parte o en una aplicación 'software' de incidencias y averías, para poder realizar su seguimiento, estudio y análisis.

CR3.3 Los síntomas recogidos en el parte o notificados por los sistemas de alarmas se comprueban, utilizando la información contenida en el histórico y la documentación técnica del equipo y realizando pruebas según el procedimiento de actuación establecido por la entidad responsable, para diagnosticar y localizar la naturaleza de la incidencia.

CR3.4 La incidencia se subsana, usando las herramientas específicas, para rehabilitar los servicios interrumpidos o deteriorados.

CR3.5 Las incidencias solucionadas y alertas atendidas se registran en las aplicaciones de gestión, para su notificación al usuario, siguiendo los procedimientos establecidos por la entidad responsable de la gestión del sistema.

CR3.6 Las incidencias que no se han conseguido solucionar se reportan, informando por los canales de comunicación establecidos por la entidad responsable de la gestión del sistema al nivel de responsabilidad superior.

CR3.7 La detección, diagnóstico y solución de la incidencia se documenta, utilizando el modelo o aplicación informática establecidos por la entidad responsable de la gestión del sistema, para registrar las tareas efectuadas y los equipos reparados o reemplazados, entre otros, garantizando la trazabilidad de los procesos en el histórico de incidencias y averías.

Contexto profesional

Medios de producción

Elementos activos de red. Analizadores de cableado. Herramientas de gestión de red. Herramientas de control de líneas públicas de comunicaciones. 'Sniffers'. Herramientas manuales para trabajos eléctricos y mecánicos. Herramientas 'software' para pruebas de conectividad. Herramientas ofimáticas. Herramientas de diagnóstico. Aplicaciones de gestión de incidencias. Mapa de la red.

Productos y resultados

Nodos de interconexión de redes públicas y privadas instalados. Protocolos de comunicaciones en los dispositivos de interconexión configurados. Alertas generadas por los sistemas de monitorización de red gestionadas. Elementos de interconexión de redes públicas y privadas mantenidos y operativos.

Información utilizada o generada

Normativa aplicable de planificación de la acción preventiva. Normativa aplicable de protección de datos. Normativa aplicable de propiedad industrial. Normativa aplicable de protección medioambiental. Órdenes de trabajo. Partes de Incidencias. Guías de resolución de problemas. Informes históricos de incidencias y averías. Normas y criterios de calidad definidos por la entidad responsable del sistema y entidad operadora. Informes técnicos de puesta en servicio. Manuales de los dispositivos. Cursos de formación.

MÓDULO FORMATIVO 1

INSTALACIÓN DE DISPOSITIVOS DE COMUNICACIONES EN REDES LOCALES

Nivel:	2
Código:	MF0220_2
Asociado a la UC:	UC0220_2 - INSTALAR DISPOSITIVOS DE COMUNICACIONES EN REDES LOCALES
Duración (horas):	210
Estado:	BOE

Capacidades y criterios de evaluación

- C1:** Describir elementos de comunicaciones que conforman una red local, diferenciando sus características y funcionalidad, para identificar los componentes que constituyen el mapa físico.
- CE1.1** Explicar las topologías de una red local teniendo en cuenta las arquitecturas y tecnologías existentes.
 - CE1.2** Enumerar los elementos que pueden encontrarse en el mapa físico de una red local en función del ámbito de aplicación y las infraestructuras de red utilizadas.
 - CE1.3** Describir cada uno de los dispositivos integrantes de una red local teniendo en cuenta sus características y funcionalidades asociadas.
 - CE1.4** Identificar la normativa aplicable y la reglamentación técnica y/o estándares que afectan a la implantación de las redes locales en función de los procedimientos dados.
 - CE1.5** En un supuesto práctico de descripción de elementos de comunicaciones de una red local, diferenciando sus características y funcionalidad:
 - Elaborar su mapa físico según unas especificaciones recibidas.
 - Elaborar sus mapas lógicos según unas especificaciones recibidas.
- C2:** Aplicar procedimientos de instalación y configuración de un nodo de red local, incluyendo gestores de protocolos y otros programas que soportan servicios de comunicaciones, para su puesta en funcionamiento.
- CE2.1** Enumerar los protocolos que se configuran en un nodo de una red local teniendo en cuenta la tecnología y estándares utilizados, explicando la funcionalidad de cada uno.
 - CE2.2** Explicar el sistema de direccionamiento de un nodo que se utilizan en la red local en función de las tecnologías de red usadas.
 - CE2.3** Clasificar el cableado de interconexión de un nodo, explicando estándares, características y las técnicas de 'conectorizado'.
 - CE2.4** En un supuesto práctico de aplicación de procedimientos de instalación y configuración de un nodo de red local, incluyendo gestores de protocolos y otros programas que soportan servicios de comunicaciones:
 - Instalar interfaces y módulos de los equipos de la red o, en su caso, verificarlos para que ofrezcan las características de conectividad especificadas, atendiendo a los medios de transmisión que se utilizan, la configuración física de la red en que se ubicará y la documentación técnica del fabricante.
 - Instalar o, en su caso, actualizar la versión de 'firmware' de un equipo de red, utilizando la última versión disponible y siguiendo las instrucciones del fabricante.

- Instalar el equipo en el bastidor del armario ('rack') siguiendo las instrucciones del fabricante, comprobando los parámetros correspondientes a la alimentación eléctrica, sujeción mecánica y puesta a tierra, entre otros, y atendiendo a las condiciones medioambientales de temperatura y humedad.
- Conectar el equipo a la red eléctrica, teniendo en cuenta posibles circuitos independientes en el caso de equipos con fuente de alimentación redundante y verificando la toma de tierra.
- Conectar el equipo a la red de datos, conforme a los medios de transmisión que se utilizan, asegurando su funcionalidad y verificando la habilitación de su conectividad y funcionamiento, usando herramientas de monitorización al efecto, siguiendo las especificaciones de la organización y de modo que quede accesible para su gestión remota.
- Complimentar el parte de trabajo o informe técnico de instalación, utilizando un modelo o aplicación informática, indicando ítems tales como las interconexiones realizadas, la fecha y hora de instalación y datos del técnico entre otros, a fin de garantizar la trazabilidad de los procesos.

C3: Aplicar procedimientos de prueba y verificación de la conectividad en una red local, usando herramientas al efecto para asegurar la funcionalidad.

CE3.1 Explicar las etapas de un proceso de verificación de conectividad en una red local, describiendo las acciones de cada paso.

CE3.2 Enumerar las herramientas utilizadas para verificar la conectividad en una red local, según las tecnologías implementadas, describiendo sus características.

CE3.3 Explicar el funcionamiento operativo de las herramientas de gestión de red para comprobar el estado de los dispositivos de comunicaciones, teniendo en cuenta las especificaciones técnicas de las herramientas.

CE3.4 En un supuesto práctico de aplicación de procedimientos de prueba y verificación de la conectividad en una red local, usando herramientas al efecto para asegurar la funcionalidad:

- Monitorizar el estado de la red, para comprobar su funcionamiento, usando herramientas de verificación y gestión.
- Verificar las conexiones según una documentación o mapa de red, comprobando cada conexión autorizada y detectando conexiones no autorizadas.
- Verificar el acceso a los recursos compartidos, comprobando la disponibilidad desde los equipos autorizados y la confidencialidad desde los no autorizados.
- Documentar los procesos de prueba y verificación realizados, de acuerdo con unas especificaciones técnicas.

C4: Configurar parámetros de los protocolos de comunicaciones en los nodos para su integración en una red, usando la interfaz específica de cada equipo.

CE4.1 Identificar parámetros de unos protocolos de comunicaciones a configurar, explicando su función y su rango de valores permitido.

CE4.2 Interpretar las especificaciones de una configuración de protocolos de comunicaciones determinada, teniendo en cuenta las necesidades de integración del nodo en la red y la implementación de los servicios correspondientes.

CE4.3 Describir el procedimiento a seguir para aplicar una configuración predeterminada a un nodo de red, explicándolo paso a paso.

CE4.4 Identificar los parámetros de configuración de los protocolos con características de seguridad de transmisión y cifrado, diferenciando los que afectan a la seguridad.

CE4.5 En un supuesto práctico de configuración de parámetros de protocolos de comunicaciones en los nodos para su integración en una red, usando la interfaz específica de cada equipo:

- Configurar la gestión de protocolo en equipos, tales como encaminadores ('routers') y conmutadores ('switches'), entre otros, a través de su interfaz específica para la gestión del equipo, en base a la topología de la red.
- Comprobar el funcionamiento de los protocolos de gestión tales como SNMP y SSH, entre otros, necesarios para la gestión remota del equipo de comunicaciones, previa habilitación.
- Configurar protocolos asociados a las aplicaciones de red instaladas en los servidores, para soportar los servicios implementados, de acuerdo con los manuales de instalación.
- Configurar el 'software' de cifrado en los nodos de la red que se determine en el supuesto, previa instalación, a través del interfaz específico, para crear redes privadas virtuales.
- Comprobar los dispositivos de comunicaciones y su configuración, ejecutando pruebas para asegurar la conformidad de la misma.
- Incluir el nodo de red en los sistemas de monitorización de la infraestructura, recogiendo sus parámetros de funcionamiento característicos tales como tramas gestionadas, ancho de banda utilizado y errores/colisiones, entre otros.
- Documentar los procesos de configuración y de prueba del dispositivo de comunicaciones, indicando ítems tales como los valores de los parámetros incluidos y datos del técnico entre otros, utilizando un modelo o aplicación informática y garantizando la trazabilidad de los procesos.

C5: Aplicar procedimientos de corrección de las incidencias detectadas en la instalación de elementos de comunicaciones concretos, aplicando soluciones para asegurar su funcionalidad.

CE5.1 Clasificar incidencias que se producen en los elementos de comunicaciones de las redes locales, según las tecnologías de comunicaciones empleadas y los elementos involucrados con ellas, explicándolas.

CE5.2 Describir procedimientos para la detección de incidencias de los elementos de comunicaciones de la red local usando herramientas y explicando los pasos a seguir.

CE5.3 Describir las técnicas y herramientas que se utilizan para aislar y diagnosticar las causas que han producido una incidencia reportada en la red, explicándolas.

CE5.4 Explicar los procedimientos sistemáticos de resolución de incidencias de los elementos de comunicaciones de la red local, en función de los diagnósticos.

CE5.5 En un supuesto práctico de aplicación de procedimientos de corrección de las incidencias detectadas en la instalación de elementos de comunicaciones concretos, aplicando soluciones para asegurar su funcionalidad:

- Revisar los sistemas de notificación de incidencias, comprobando posibles alarmas frente a fallos o indisponibilidad del servicio, para garantizar el correcto funcionamiento de las comunicaciones.
- Localizar el dispositivo en el que se ha producido la incidencia, interpretando la información recibida del sistema de alarmas y la documentación técnica tal como el mapa de la red u otra, iniciando actuaciones mediante conexión remota o de manera presencial en los equipos o sistemas implicados, para identificar el problema físico y/o lógico causante del fallo.
- Diagnosticar el problema, indicando su naturaleza y origen tal como interrupción de la comunicación debido a problemas físicos y problemas de calidad de servicio, entre otros, planteando su solución, para rehabilitar los servicios interrumpidos o deteriorados a partir de los síntomas reportados por los sistemas de gestión de incidencias y las actuaciones de localización realizadas.
- Subsancar la incidencia con las herramientas específicas, teniendo en cuenta el diagnóstico, respetando los protocolos del fabricante, para rehabilitar los servicios interrumpidos o deteriorados.

- Documentar la detección, diagnóstico y solución de la incidencia, utilizando un modelo o aplicación informática, para registrar las tareas efectuadas garantizando la trazabilidad de los procesos en el parte de incidencias.

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

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

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.

Finalizar el trabajo atendiendo a criterios de idoneidad, economía y eficacia.

Adaptarse a situaciones o contextos nuevos.

Respetar los procedimientos y normas internas de la organización.

Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.

Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Redes locales

Características. Topologías. Arquitecturas.

Infraestructura y elementos de una red local.

Mapas físicos y lógicos de una red.

Normativa aplicable, reglamentación técnica y estándares que afectan a la implantación de redes locales.

2 Transmisión de datos

Datos y señales.

Unidades de medida.

Efectos no deseados: atenuación, distorsión y ruido, entre otros.

Medios de transmisión: medios guiados y no guiados.

Sistemas de Cableado estructurado

Sistemas de comunicaciones inalámbricas.

Comunicación a través de redes: interfaces y protocolos.

3 Protocolos de redes locales

Protocolos de control de enlace lógico. Protocolos de acceso al medio: protocolos de contienda y de paso de testigo, entre otros. Direcciones físicas. Dirección MAC.

Protocolos ARP y RARP

Protocolo de red IP. Direccionamiento lógico. DHCP.

Protocolos de encaminamiento (RIP y OSPF, entre otros).

4 Equipos de transmisión e interconexión de red

Tipos de dispositivos según sus funciones: conmutadores ('switches'), encaminadores ('routers') y cortafuegos ('firewalls'), entre otros.

Otros dispositivos: puntos de acceso, centralitas, equipos con acceso remoto a una red privada virtual (VPN) y sistemas de detección de intrusos en redes inalámbricas, entre otros.

5 Procedimientos de instalación y verificación de elementos de conectividad de redes locales

Instalación física y mecánica de equipos: armarios ('racks'), fijaciones, distribución de cableado y condiciones ambientales, entre otros.

Procedimientos de verificación de alimentación, puesta a tierra y procedimientos de seguridad asociados.

Elementos auxiliares: sistemas de alimentación ininterrumpida, aire acondicionado y baterías, entre otros.

Normativa de seguridad en instalaciones de equipos electrónicos.

Herramientas de verificación de elementos de conectividad de redes locales.

Procedimientos sistemáticos de verificación y prueba de elementos de conectividad de redes locales.

6 Procedimientos de configuración y pruebas de protocolos de comunicaciones en nodos de redes locales

Parámetros de los protocolos de comunicaciones.

Parámetros de configuración y servicios en los equipos de red.

Procedimientos sistemáticos de configuración de los protocolos de comunicaciones más habituales en nodos de redes locales.

Pruebas funcionales de unidad y sistema.

Herramientas de gestión remota: características funcionales y de operación.

7 Detección y diagnóstico de incidencias en la instalación de dispositivos de redes locales

Incidencias en dispositivos de red: clasificaciones según su tipología.

Herramientas de monitorización para la localización y notificación de incidencias.

Herramientas de diagnóstico de dispositivos de comunicaciones en redes locales.

Procesos de gestión de incidencias en redes locales.

Parte de incidencias y averías.

Parámetros de contexto de la formación

Espacios e instalaciones

Los espacios e instalaciones darán respuesta, en forma de aula, aula-taller, taller de prácticas, laboratorio o espacio singular, a las necesidades formativas, de acuerdo con el Contexto Profesional establecido en la Unidad de Competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos, salud laboral, accesibilidad universal y protección medioambiental.

- Taller de 4 m² por alumno o alumna.

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la instalación de dispositivos de comunicaciones en redes locales, que se acreditará mediante una de las dos formas siguientes:

- Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.

- Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.

2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 2

Mantenimiento de procesos de comunicaciones en redes locales

Nivel:	2
Código:	MF0955_2
Asociado a la UC:	UC0955_2 - Mantener los procesos de comunicaciones en redes locales
Duración (horas):	180
Estado:	BOE

Capacidades y criterios de evaluación

C1: Aplicar técnicas y procedimientos de monitorización de una red local, usando herramientas al efecto, para detectar incidencias.

CE1.1 Identificar parámetros que detectan el rendimiento de una red local, teniendo en cuenta su arquitectura y la tecnología de red de soporte.

CE1.2 Enumerar las herramientas 'hardware' y 'software' utilizadas en la monitorización de una red local, teniendo en cuenta sus especificaciones técnicas.

CE1.3 Describir las funciones y propiedades de las herramientas de gestión utilizadas para funciones tales como obtener información del tráfico, establecer el mapa de la red y detectar y aislar causas de incidencias, entre otros, siguiendo las especificaciones de las propias herramientas.

CE1.4 Explicar el proceso a seguir para monitorizar el tráfico de una red local en función de las topologías y protocolos de red implementados.

CE1.5 Identificar las notificaciones de alarma que informan sobre incidencias y comportamientos anómalos, diferenciando sus orígenes y explicando la información que proporcionan.

CE1.6 En un supuesto práctico de aplicación de técnicas y procedimientos de monitorización de los procesos de comunicación de una red local, usando herramientas al efecto:

- Instalar una herramienta de monitorización, configurando el servidor central y la sonda local asociada a su misma máquina con los sensores, para garantizar la correcta supervisión de todos los dispositivos asociados a la red local, generando una plataforma de gestión unificada.

- Instalar las sondas de monitorización remota, configurándolas en los puntos de la red a supervisar, para que, mediante chequeos del tráfico de red, proporcionen información a la plataforma de gestión.

- Instalar los agentes del 'software' de red, comprobando su ejecución de forma continua en los nodos a gestionar, para que proporcionen a la plataforma de gestión la información recogida por sus respectivos sistemas operativos.

- Recopilar los ficheros de registro de actividad ('log') de los diferentes servicios, con objeto de analizar los procesos asociados a los mismos, manteniendo los recursos de almacenamiento y gestión en condiciones adecuadas de visibilidad, accesibilidad, integración y escalabilidad del proceso, para explotar los datos e identificar errores y conflictos a resolver.

- Configurar la interfaz de la herramienta de gestión de red y los filtros de selección de alarmas y alertas, optimizando los procesos de notificación y gestión de incidencias.

C2: Aplicar técnicas de mantenimiento de una red local, resolviendo las incidencias detectadas, previa identificación de comportamientos anómalos en los

dispositivos que la forman y previo diagnóstico del problema, para asegurar su funcionalidad.

CE2.1 Describir procedimientos de resolución de incidencias en una red local, previa localización y diagnóstico, a partir de las alarmas de monitorización e histórico de incidencias y averías, entre otros.

CE2.2 Describir los procedimientos de documentación de las acciones correctivas realizadas, explicando su estructura y contenido.

CE2.3 En un supuesto práctico de aplicación de técnicas de mantenimiento de una red local, previa identificación de los comportamientos anómalos en los dispositivos que la forman y previo diagnóstico del problema:

- Actualizar el mapa de la red, lanzando procesos de descubrimiento de red desde la plataforma de gestión, para disponer una imagen real de todos los dispositivos conectados en ella.
- Comprobar la conectividad de los dispositivos de la red, tanto activos como pasivos, con las señales acústico-luminosas observables y la aplicación de comandos de red específicos para valorar posibles deterioros o alteraciones físicas o lógicas.
- Identificar las causas del comportamiento anómalo de los dispositivos de la red, para proceder a su solución, aplicando una metodología de diagnóstico, utilizando herramientas 'hardware' y 'software' de diagnóstico para localizar la fuente de posibles errores y consultando la documentación técnica.
- Subsanan las deficiencias detectadas, localizadas mediante procesos de inspección o recibidas desde las herramientas de monitorización, poniendo en marcha las medidas para su solución, tales como la sustitución de un conector u otras.
- Verificar la seguridad y configuración de la red, realizando pruebas y utilizando las herramientas específicas de seguridad para la generación de alarmas.
- Documentar los resultados de las pruebas, incluyendo los datos de las incidencias y las soluciones adoptadas, utilizando un modelo o aplicación informática, para registrar las actividades realizadas, garantizando la trazabilidad de los procesos.

C3: Aplicar procesos de actualización del 'hardware' y 'software' de los dispositivos de comunicaciones, usando los medios proporcionados por el fabricante, para asegurar su integridad y fiabilidad.

CE3.1 Enumerar los componentes actualizables de los dispositivos de comunicaciones, describiendo sus características.

CE3.2 Identificar los parámetros de compatibilidad de los componentes a actualizar para asegurar la efectividad en los procesos, según especificaciones técnicas de dichos componentes.

CE3.3 Describir los pasos a seguir para la actualización del 'software' de dispositivos de comunicaciones, detallando las acciones realizadas en cada paso y las herramientas 'software' utilizadas.

CE3.4 En un supuesto práctico de actualización del 'hardware' y 'software' de unos dispositivos de comunicaciones, usando los medios proporcionados por el fabricante:

- Actualizar parcial o totalmente el 'hardware' de un equipo de comunicaciones, usando el medio proporcionado por el fabricante, con el fin de adaptarlo a nuevas funcionalidades.
- Salvaguardar el 'firmware' actualmente instalado en los equipos de comunicaciones, realizando una copia de seguridad de la versión instalada, a fin de poder restaurarla en caso de fallo de la actualización.
- Actualizar el 'firmware' de los equipos de comunicaciones, accediendo al sitio 'web' del fabricante o mediante la opción de búsqueda de actualizaciones si está disponible con el sistema operativo que gestiona cada dispositivo, para adaptarlo a nuevas funcionalidades.

- Modificar las configuraciones de los equipos de comunicaciones, incluyendo una parametrización, para cambiarles la funcionalidad o adaptarlos a los nuevos equipos introducidos.
- Los componentes 'hardware' y 'firmware' actualizados se verifican mediante pruebas, para asegurar su funcionalidad.
- Las actuaciones realizadas sobre los dispositivos se documentan, utilizando un modelo o aplicación informática para registrar las actividades realizadas, incluyendo las referencias de los dispositivos y la versión del 'firmware' actualizado, garantizando la trazabilidad de los procesos.

C4: Aplicar procedimientos de mantenimiento de la seguridad lógica y física concerniente a los dispositivos de comunicaciones de una red local, identificando alertas e incidencias y solucionándolas, para garantizar tanto las condiciones de integridad, disponibilidad, confidencialidad, control lógico del acceso y trazabilidad de los datos, como las del acceso físico a los servicios a usuarios autorizados, según las especificaciones.

CE4.1 Describir las funciones relativas a seguridad física y lógica de una herramienta de gestión de red según las especificaciones, de la propia herramienta y las arquitecturas y tecnologías de red implementadas.

CE4.2 Identificar alertas de seguridad relativas a seguridad física y lógica que pueden aparecer en una red local, describiendo sus características, orígenes y la información que proporcionan, explicando los mecanismos de la propia herramienta para que se muestren, según sus especificaciones técnicas.

CE4.3 Explicar procedimientos de localización del componente y causas disparan una alerta de seguridad en una herramienta de gestión, usando los mecanismos de la propia herramienta, para comprobar los elementos de la red afectados.

CE4.4 Localizar la ubicación de los ficheros de auditoría de un dispositivo de red, describiendo los campos que lo forman y su finalidad.

CE4.5 Describir herramientas de rastreo para comprobar la trazabilidad de los datos, explicando sus características.

CE4.6 En un supuesto práctico, de aplicación de procedimientos de mantenimiento de la seguridad lógica y física concerniente a los dispositivos de comunicaciones de una red local, identificando alertas y solucionándolas:

- Atender notificaciones de las alertas de seguridad recibidas en las herramientas que las generan, usando las opciones de la misma herramienta, para iniciar la corrección de las incidencias notificadas.
- Revisar los dispositivos de comunicaciones, para asegurar que su acceso físico y lógico está controlado de acuerdo con unos criterios de autenticación.
- Recoger los ficheros de auditoría de los dispositivos de comunicaciones, analizándolos para detectar posibles accesos indebidos que afecten a la confidencialidad y/o integridad de los datos.
- Comprobar la trazabilidad de los datos en la red, validando que se cumple con la normativa legal en relación al tratamiento de los mismos, mediante unas herramientas específicas de rastreo.
- Documentar las actuaciones realizadas, utilizando un modelo o aplicación informática, registrando las actividades realizadas, garantizando la propia trazabilidad de los sistemas y procesos de seguridad.

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

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

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.

Finalizar el trabajo atendiendo a criterios de idoneidad, economía y eficacia.

Adaptarse a situaciones o contextos nuevos.

Respetar los procedimientos y normas internas de la organización.

Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.

Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Monitorización de redes locales

Herramientas 'hardware' y 'software' para monitorización de redes locales. Parámetros de detección del rendimiento. Sondas de monitorización remota y detección de intrusos.

Procedimientos de monitorización del tráfico de una red local.

Notificaciones de alarma. Clasificación.

Herramientas de gestión de red.

Herramientas de documentación del mapa de red.

2 Procedimientos de mantenimiento en redes locales

Mantenimiento preventivo y mantenimiento correctivo de redes locales.

Procedimientos de diagnóstico y resolución de incidencias. Analizadores lógicos y analizadores de cableado. Clasificaciones de incidencias según tipología física y lógica.

Herramientas de gestión de incidencias.

Procedimientos de documentación de incidencias. Histórico de incidencias y averías.

3 Procedimientos de actualización de dispositivos de comunicaciones en redes locales

Componentes actualizables de los dispositivos de comunicaciones. Parámetros de compatibilidad.

Procedimientos de actualización del 'software' de dispositivos de comunicaciones.

4 Seguridad física y lógica en redes locales

Funciones de seguridad física y lógica en herramientas de gestión.

Alertas relativas a la seguridad física y lógica.

Mecanismos de comprobación y diagnóstico en herramientas de gestión.

Ficheros de auditoría de los dispositivos de red.

Herramientas de rastreo y trazabilidad de los datos

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Taller de 4 m² por alumno o alumna.
- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con el mantenimiento de los procesos de comunicaciones en redes locales, que se acreditará mediante una de las dos formas siguientes:
 - Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
 - Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.

MÓDULO FORMATIVO 3

INTERCONEXIÓN DE REDES PRIVADAS Y PÚBLICAS

Nivel:	2
Código:	MF2688_2
Asociado a la UC:	UC2688_2 - INTERCONECTAR REDES PRIVADAS Y PÚBLICAS
Duración (horas):	150
Estado:	BOE

Capacidades y criterios de evaluación

- C1:** Identificar dispositivos para la interconexión de redes públicas y privadas, explicando sus características, según estándares de las tecnologías de comunicaciones.
- CE1.1** Identificar dispositivos de interconexión entre redes privadas y redes públicas, explicando sus características y funcionalidades, tales como tecnologías y arquitecturas de comunicaciones utilizadas, entre otras.
 - CE1.2** Enumerar las tecnologías empleadas en la interconexión de redes, describiendo sus características, en función de sus especificaciones técnicas.
 - CE1.3** Identificar los servicios de conexión, explicando su interrelación y la forma de habilitarlos y configurarlos en los equipos de la red local para la prestación de servicios de comunicaciones, según las tecnologías utilizadas.
 - CE1.4** Identificar los servicios de interconexión que soportan los proveedores de servicios de comunicaciones a los que se conecta la red privada, evaluando su adecuación en función de las especificaciones funcionales que se deben atender.
- C2:** Aplicar procedimientos de instalación y verificación de dispositivos para la interconexión de redes privadas y públicas siguiendo especificaciones dadas y comprobando su funcionalidad.
- CE2.1** Identificar los parámetros de los servicios de interconexión con la red pública según las características del propio servicio y del dispositivo de interconexión, explicando su objetivo.
 - CE2.2** Identificar, en la normativa de calidad aplicable, los requerimientos correspondientes a la interconexión con la red pública, explicando los pasos a seguir para su aplicación.
 - CE2.3** Describir los interfaces que se utilizan en la conexión de redes privadas a redes públicas, en función de la tipología de las redes utilizadas tales como dispositivos de conexión, líneas de comunicaciones y medios de transmisión empleados, entre otros.
 - CE2.4** Explicar las normativas de seguridad aplicables a la instalación de dispositivos de interconexión de redes privadas y públicas y las condiciones físicas ambientales de la propia instalación, describiéndolas.
 - CE2.5** En un supuesto práctico de instalación y verificación de un dispositivo de interconexión de redes privadas y públicas, siguiendo especificaciones dadas y comprobando su funcionalidad:
 - Comprobar los requisitos de implantación de un dispositivo, así como las líneas de comunicaciones con sus correspondientes interfaces, asegurando que se cumplan las condiciones de compatibilidad, según las especificaciones recibidas y del fabricante.

- Instalar el dispositivo, comprobando los parámetros correspondientes a la alimentación eléctrica, sujeción mecánica y puesta a tierra, entre otros, utilizando herramientas manuales de instalación y siguiendo la normativa aplicable de seguridad y recomendaciones del fabricante.
- Instalar los interfaces y módulos de adaptación de las líneas de comunicación, comprobando y asegurando su funcionalidad, para proceder a su conexión según los requisitos de implantación del dispositivo de comunicaciones.
- Implementar medidas de seguridad en el dispositivo, tales como cortafuegos ('firewalls'), configurando reglas de acceso y validándolas.
- Conectar las líneas de comunicaciones y el dispositivo, verificando la habilitación de la conexión y su funcionamiento para asegurar la comunicación entre la red pública y privada y la prestación del servicio de comunicaciones.
- Complimentar el parte de trabajo o informe técnico de la instalación, utilizando un modelo o aplicación informática, documentando los trabajos realizados e incluyendo elementos tales como fecha de la instalación, dispositivos instalados, módulos incluidos y conexiones, entre otros, a fin de garantizar la trazabilidad de los procesos.

C3: Aplicar procedimientos de configuración de protocolos y parámetros de interconexión de un dispositivo de interconexión entre redes privadas y públicas, asegurando su funcionalidad en la red y en función de los objetivos y especificaciones, para su puesta en marcha.

CE3.1 Identificar parámetros de configuración y gestión de interconexión de redes privadas virtuales, en dispositivos de interconexión, explicando sus funciones.

CE3.2 Clasificar los protocolos utilizados en un dispositivo de interconexión entre redes privadas y públicas, según sus funciones e identificando los servicios que soportan.

CE3.3 Describir procedimientos y herramientas utilizadas para implantar configuraciones en dispositivos de interconexión de redes privadas con redes públicas, explicando los pasos a seguir para que se soporten los servicios de comunicaciones.

CE3.4 Explicar funciones y valores de cada uno de los parámetros que intervienen en la configuración de un dispositivo de enlace, según especificaciones técnicas del dispositivo.

CE3.5 En un supuesto práctico de aplicación de procedimientos de configuración de protocolos y parámetros en un dispositivo de interconexión entre redes privadas y públicas, asegurando su funcionalidad en la red y en función de los objetivos y especificaciones:

- Configurar un equipo activo de comunicaciones, mediante su interfaz específica, habilitando los parámetros funcionales, para permitir la coexistencia e/o interconexión de redes locales a través de redes públicas.
- Configurar los interfaces externos del encaminador ('router'), mediante las herramientas de gestión del dispositivo, habilitando su funcionalidad, empleando el 'software' del fabricante para el acceso a las redes externas, para proporcionar conectividad según las indicaciones de la entidad operadora de comunicaciones.
- Verificar los parámetros de funcionamiento y calidad de servicio del dispositivo de interconexión, mediante la ejecución de pruebas finales que confirmen su completa operatividad.
- Documentar los procesos de configuración y pruebas del dispositivo de interconexión, utilizando un modelo o aplicación informática, para registrar las actividades realizadas e incluyendo elementos tales como fecha de la realización, protocolos habilitados y resultado de las pruebas funcionales, entre otros, garantizando la trazabilidad de los procesos.

C4: Aplicar procedimientos de monitorización y verificación del funcionamiento de un equipo de interconexión con redes externas mediante herramientas 'software' específicas para la detección de incidencias.

CE4.1 Identificar funcionalidades y procedimientos de utilización de herramientas y aplicaciones de supervisión y monitorización, en función de las características de un equipo de interconexión.

CE4.2 Explicar procedimientos de operación de las herramientas de monitorización, en función del equipo de interconexión a monitorizar.

CE4.3 Seleccionar herramientas de monitorización en función de la prueba a realizar y explicar la forma de conectarlas siguiendo unas especificaciones dadas.

CE4.4 Describir procedimientos de monitorización para asegurar la prestación de los servicios, explicando los pasos a seguir.

CE4.5 En un supuesto práctico de monitorización y verificación del funcionamiento de un equipo de interconexión con redes externas mediante herramientas 'software' específicas para la detección de incidencias:

- Seleccionar una herramienta de monitorización, en función del objetivo que se desea comprobar o verificar.
- Conectar la herramienta al equipo y configurarla, estableciendo los parámetros al efecto.
- Monitorizar el equipo usando la herramienta, para detectar congestiones de tráfico y anomalías en el servicio.
- Documentar las actividades realizadas y los resultados obtenidos, utilizando un modelo o aplicación informática para su registro, describiendo las características de las anomalías detectadas, entre otros.

C5: Aplicar técnicas de resolución de las incidencias detectadas en un dispositivo de interconexión de redes privadas y públicas, en función del diagnóstico, para el mantenimiento de la funcionalidad de la interconexión.

CE5.1 Describir incidencias que se producen en dispositivos de interconexión de las redes privadas con las redes públicas de comunicaciones, según informaciones recibidas de herramientas de notificación u otros medios.

CE5.2 Identificar procedimientos y herramientas empleados para la detección de incidencias, en función de los dispositivos de interconexión de redes privadas y públicas.

CE5.3 Describir técnicas y herramientas que se utilizan para aislar y diagnosticar las causas que producen incidencias, en dispositivos de interconexión de redes privadas y públicas.

CE5.4 Explicar procedimientos sistemáticos de resolución de incidencias, en función de los diagnósticos alcanzados.

CE5.5 En un supuesto práctico de aplicación de técnicas de resolución de incidencias en dispositivos de interconexión con disfunciones simuladas, en función del diagnóstico:

- Dictaminar la naturaleza de una incidencia, comprobando y estudiando los síntomas recogidos en el parte de incidencias o aplicación de monitorización, realizando pruebas para localizar la ubicación de la misma, utilizando la información contenida en un histórico y en la documentación técnica del equipo.
- Subsancar la incidencia usando las herramientas específicas, para rehabilitar los servicios interrumpidos o deteriorados.
- Registrar la solución de la incidencia y la alerta atendida en una aplicación de gestión, para su notificación a un hipotético usuario.
- Documentar la detección, diagnóstico y solución de la incidencia, utilizando un modelo o aplicación informática para registrar las tareas efectuadas, recogiendo elementos tales como

incidencias detectadas, soluciones introducidas y equipos reparados o reemplazados, entre otros.

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

C2 respecto a CE2.5; C3 respecto a CE3.5; C4 respecto a CE4.5 y C5 respecto a CE5.5.

Otras Capacidades:

Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.

Finalizar el trabajo atendiendo a criterios de idoneidad, economía y eficacia.

Adaptarse a situaciones o contextos nuevos.

Respetar los procedimientos y normas internas de la organización.

Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.

Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

Contenidos

1 Interconexión de redes

Dispositivos de interconexión de redes. Arquitectura, características, funcionalidades y tecnologías.
Conceptos de encaminamiento: segmentación de redes, algoritmos de encaminamiento.

2 Dispositivos de interconexión de redes

Interfaces de un dispositivo de interconexión de redes. Clasificación.
Servicios de interconexión de redes. Características y perfiles.

3 Protocolos de interconexión de redes

Pila de protocolos TCP/IP.

Mecanismos de acceso a servicios: enmascaramiento y redirección de puertos. Filtrado de paquetes.

Cifrado.

Redes Privadas Virtuales ('Virtual Private Networks' - VPN).

Protocolos de encaminamiento (RIP y OSPF, entre otros).

4 Procedimientos de instalación y prueba de dispositivos de interconexión de redes

Normativas de seguridad física y eléctrica aplicables a los dispositivos de interconexión de redes.
Procedimientos y herramientas de carga de configuración en dispositivos de interconexión de redes. Protocolos y parámetros.

5 Procedimientos de monitorización en dispositivos de interconexión de redes

Herramientas de monitorización en dispositivos de interconexión de redes.

Procedimientos sistemáticos de monitorización de equipos de interconexión de redes.

6 Procedimientos de diagnóstico de averías en dispositivos de interconexión de redes

Tipos de incidencias en la interconexión de redes públicas y privadas.

Herramientas de diagnóstico y notificación de incidencias en dispositivos de interconexión de redes.

Procedimientos de gestión de incidencias.

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Taller de 4 m² por alumno o alumna.
- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

1. Dominio de los conocimientos y las técnicas relacionados con la interconexión de redes privadas y públicas, que se acreditará mediante una de las dos formas siguientes:
 - Formación académica de nivel 2 (Marco Español de Cualificaciones para la Educación Superior) o de otras de superior nivel relacionadas con el campo profesional.
 - Experiencia profesional de un mínimo de 2 años en el campo de las competencias relacionadas con este módulo formativo.
2. Competencia pedagógica acreditada de acuerdo con lo que establezcan las Administraciones competentes.