Referencial de competencias profesionales

Formacion Administración de Redes y Soporte Técnico IT

País: Spain

Profesiones cubiertas: Administrador de Redes, Técnico de Soporte IT, Especialista en Infraestructura de Red, Técnico de Administración de Sistemas

Este referencial es una certificación profesional privada, inspirada en los estándares de los referenciales de certificación franceses (metodología France Compétences). No constituye un referencial estatal.

Generado el 09/06/2026

Índice

ANEXO I Presentación sintética del marco del diploma

PRESENTACIÓN GENERAL

Nombre de la formación: Certificado de Profesionalidad en Administración de Redes y Soporte Técnico IT

Tipo de certificación: Certificado de Profesionalidad

Modalidades de formación:

Formación presencial con componentes prácticos en laboratorios de red, simuladores y entornos de producción controlados. Incluye trabajo en proyectos reales de administración de infraestructura de red y soporte técnico.

Finalidad y objetivos:

Capacitar profesionales para administrar infraestructuras de red corporativa, configurar y mantener dispositivos de switching y enrutamiento, implementar protocolos de enrutamiento dinámico, gestionar calidad de servicio, diagnosticar y resolver incidencias de conectividad, automatizar tareas de administración, coordinar con proveedores externos, documentar procedimientos técnicos, realizar auditorías de seguridad, administrar sistemas operativos de servidor, gestionar directorios activos y virtualización, prestar soporte técnico a usuarios finales, y proponer mejoras continuas en servicios IT.

Contexto profesional:

Los profesionales en Administración de Redes y Soporte Técnico IT son responsables de diseñar, implementar, mantener y optimizar infraestructuras de red en entornos corporativos. Trabajan en la configuración de dispositivos de red de capa 2 y capa 3, implementación de protocolos de enrutamiento dinámico, gestión de calidad de servicio, diagnóstico de problemas de conectividad, automatización de tareas administrativas, coordinación con proveedores de equipos, documentación técnica, auditorías de seguridad, administración de servidores, gestión de directorios y virtualización, y prestación de soporte técnico a usuarios finales. Su trabajo es fundamental para garantizar disponibilidad, rendimiento y seguridad de las redes corporativas.

Público objetivo y condiciones de acceso:

Profesionales con conocimientos previos de redes informáticas, sistemas operativos y protocolos de comunicación que deseen especializarse en administración de infraestructura de red y soporte técnico IT en entornos corporativos.

Prerrequisitos:

- Conocimientos básicos de redes informáticas y modelo OSI
- Familiaridad con sistemas operativos Windows y Linux
- Comprensión de protocolos TCP/IP y direccionamiento IP
- Experiencia previa en soporte técnico o administración de sistemas (recomendado)

Vías de acceso:

- formation_continue
- vae

ORGANIZACIÓN DE LA FORMACIÓN

Enfoque pedagógico:

La formación combina metodología teórica con práctica intensiva en laboratorios de red y simuladores de equipos profesionales. Se utiliza enfoque basado en competencias donde los participantes desarrollan habilidades mediante proyectos reales de administración de infraestructura.

- Aprendizaje basado en competencias profesionales reales del sector
- Integración de herramientas y tecnologías actuales utilizadas en entornos corporativos
- Énfasis en resolución de problemas mediante metodologías sistemáticas
- Desarrollo de habilidades de documentación y comunicación técnica
- Práctica intensiva en laboratorios con equipos profesionales
- Evaluación continua mediante proyectos y casos prácticos
- Preparación para certificaciones profesionales reconocidas en el sector

Métodos de aprendizaje:

- Clases teóricas con exposición de conceptos y protocolos de red
- Laboratorios prácticos con equipos reales de switching y enrutamiento
- Simuladores de red (Cisco Packet Tracer, GNS3) para escenarios complejos
- Proyectos de implementación de infraestructura de red
- Casos de estudio de diagnóstico y resolución de incidencias
- Ejercicios de automatización con Python y Ansible
- Sesiones de soporte técnico simulado a usuarios finales
- Auditorías técnicas de infraestructura existente
- Trabajo colaborativo en equipos de administración de red

Puntos fuertes de la formación:

- Formación integral que cubre administración de redes de capa 2 y capa 3
- Especialización en protocolos de enrutamiento dinámico (OSPF, BGP) y tecnologías avanzadas (MPLS, VPN)
- Desarrollo de competencias en diagnóstico y resolución de incidencias de red
- Capacitación en automatización de tareas mediante Python y Ansible
- Formación en soporte técnico a usuarios finales mediante múltiples canales
- Énfasis en documentación técnica, auditoría y mejora continua
- Administración de sistemas operativos de servidor (Windows Server y Linux)
- Gestión de directorios activos y virtualización con VMware
- Coordinación con proveedores externos para resolución de incidencias complejas
- Preparación para roles de administrador de redes y técnico de soporte IT en entornos corporativos

TABLA DE SÍNTESIS DE ACTIVIDADES - BLOQUES DE COMPETENCIAS - UNIDADES

Actividades	Bloques de competencias	Unidades
Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3 • Configurar y mantener switches de red gestionables • Configurar y mantener routers de red corporativos • Diseñar e implementar arquitecturas de red de capa 2 • Diseñar e implementar arquitecturas de red de capa 3 • Implementar VLANs y Spanning Tree Protocol para segmentación y redundancia	**Bloque 1 - Administración de Infraestructura de Red de Capa 2 y Capa 3** • Analizar el rendimiento de infraestructuras de red y hardware para identificar cuellos de botella y proponer mejoras técnicas • Configurar y mantener dispositivos de red (switches y routers) aplicando estándares de seguridad y disponibilidad • Diseñar arquitecturas de red de capa 2 y capa 3 considerando escalabilidad, redundancia y segmentación • Implementar y optimizar protocolos de switching avanzados (STP, VLAN) para evitar bucles y segmentar redes	**Unidad U1 Administración de Infraestructura de Red de Capa 2 y Capa 3**
Función 2: Configuración de Protocolos de Enrutamiento Dinámico y Avanzado • Configurar e implementar OSPF en infraestructuras de red • Configurar peering BGP y políticas de enrutamiento • Gestionar infraestructuras MPLS y servicios VPN	**Bloque 2 - Configuración de Protocolos de Enrutamiento Dinámico y Avanzado** • Configurar protocolos de enrutamiento dinámico (OSPF, BGP) para optimizar rutas y garantizar convergencia rápida • Administrar tecnologías avanzadas de red (MPLS, VPN) para garantizar conectividad segura en entornos corporativos	**Unidad U2 Configuración de Protocolos de Enrutamiento Dinámico y Avanzado**
Función 3: Gestión de Calidad de Servicio y Monitorización de Tráfico • Diseñar e implementar políticas de QoS • Configurar monitorización SNMP de infraestructura • Analizar flujos de tráfico con NetFlow y sFlow	**Bloque 3 - Gestión de Calidad de Servicio y Monitorización de Tráfico** • Aplicar políticas de Calidad de Servicio (QoS) para priorizar tráfico crítico y garantizar rendimiento de aplicaciones	**Unidad U3 Gestión de Calidad de Servicio y Monitorización de Tráfico**
Función 4: Diagnóstico y Resolución de Incidencias de Red y Conectividad • Diagnosticar y resolver incidencias de conectividad de red • Restablecer conectividad de red en puestos de usuario	**Bloque 4 - Diagnóstico y Resolución de Incidencias de Red y Conectividad** • Diagnosticar y resolver incidencias de conectividad de red utilizando herramientas de análisis y capturas de paquetes • Restablecer conectividad de red e Internet en puestos de usuario resolviendo problemas de Wi-Fi y VPN	**Unidad U4 Diagnóstico y Resolución de Incidencias de Red y Conectividad**
Función 5: Automatización de Tareas de Red y Sistemas • Desarrollar scripts Python para automatización de tareas de red • Crear y mantener playbooks Ansible para automatización	**Bloque 5 - Automatización de Tareas de Red y Sistemas** • Automatizar tareas de administración de red y sistemas mediante scripts y herramientas de orquestación	**Unidad U5 Automatización de Tareas de Red y Sistemas**

Actividades	Bloques de competencias	Unidades
Función 6: Gestión de Incidencias y Coordinación con Proveedores • Coordinar resolución de incidencias con proveedores externos • Gestionar casos de soporte con fabricantes de equipos • Gestionar incidencias críticas de alto impacto	**Bloque 6 - Gestión de Incidencias y Coordinación con Proveedores** • Coordinar la resolución de incidencias complejas con proveedores externos y fabricantes de equipos	**Unidad U6 Gestión de Incidencias y Coordinación con Proveedores**
Función 7: Documentación, Auditoría y Mejora Continua • Documentar procedimientos técnicos y configuraciones • Facilitar auditorías técnicas de sistemas y redes • Proponer e implementar mejoras continuas	**Bloque 7 - Documentación, Auditoría y Mejora Continua** • Documentar procedimientos técnicos, configuraciones y cambios de infraestructura para asegurar trazabilidad y continuidad • Preparar y ejecutar auditorías técnicas de sistemas y redes cumpliendo estándares de seguridad y regulatorios • Gestionar certificados digitales y provisiones de sistemas monitoreando vigencia y renovación • Proponer mejoras continuas en procesos y servicios IT realizando análisis coste-beneficio y presentando propuestas	**Unidad U7 Documentación, Auditoría y Mejora Continua**
Función 8: Administración de Sistemas Operativos y Servicios de Servidor • Administrar sistemas operativos de servidor Windows y Linux • Administrar servicios DNS y DHCP • Instalar y configurar servicios web, correo y transferencia de archivos • Implantar y administrar bases de datos en producción	**Bloque 8 - Administración de Sistemas Operativos y Servicios de Servidor** • Administrar sistemas operativos de servidor (Windows y Linux) configurando roles, servicios y actualizaciones	**Unidad U8 Administración de Sistemas Operativos y Servicios de Servidor**
Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso • Administrar Active Directory y políticas de grupo • Administrar plataformas de virtualización VMware • Administrar y configurar soluciones VPN corporativas • Administrar firewalls y gestionar certificados digitales	**Bloque 9 - Administración de Directorios, Virtualización y Seguridad de Acceso**	**Unidad U9 Administración de Directorios, Virtualización y Seguridad de Acceso**

Actividades	Bloques de competencias	Unidades
Función 10: Soporte Técnico a Usuarios Finales • Prestar soporte remoto a usuarios finales • Prestar soporte remoto por Internet y presencial • Resolver incidencias de aplicaciones y asesorar a usuarios	**Bloque 10 - Soporte Técnico a Usuarios Finales** • Prestar soporte técnico remoto a usuarios mediante teléfono, Internet y herramientas de acceso remoto • Prestar soporte técnico presencial a usuarios en puestos de trabajo diagnosticando y resolviendo problemas in situ • Resolver problemas de aplicaciones corporativas coordinando con proveedores y equipos de desarrollo • Asesorar y capacitar a usuarios en el uso de aplicaciones corporativas elaborando guías y documentación	**Unidad U10 Soporte Técnico a Usuarios Finales**
Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones • Realizar mantenimiento preventivo de equipos y sistemas • Instalar componentes de hardware en estaciones y servidores • Configurar sistemas según estándares corporativos • Diagnosticar fallos de hardware y software • Guiar a clientes en instalación de componentes de hardware	**Bloque 11 - Mantenimiento, Instalación de Hardware y Gestión de Configuraciones**	**Unidad U11 Mantenimiento, Instalación de Hardware y Gestión de Configuraciones**
Función 12: Operaciones IT, Monitorización y Gestión de Cambios • Monitorizar activamente sistemas y redes • Aplicar procedimientos ITIL de gestión de cambios y problemas • Asegurar ejecución de copias de seguridad y mantenimiento • Definir operativas de explotación y gestionar Centro de Control IT • Evaluar rendimiento de infraestructura y colaborar en proyectos	**Bloque 12 - Operaciones IT, Monitorización y Gestión de Cambios**	**Unidad U12 Operaciones IT, Monitorización y Gestión de Cambios**

Tabla de síntesis de funciones y actividades

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3
Actividad 1.1 Configurar y mantener switches de red gestionables
Actividad 1.2 Configurar y mantener routers de red corporativos
Actividad 1.3 Diseñar e implementar arquitecturas de red de capa 2
Actividad 1.4 Diseñar e implementar arquitecturas de red de capa 3
Actividad 1.5 Implementar VLANs y Spanning Tree Protocol para segmentación y redundancia
Función 2: Configuración de Protocolos de Enrutamiento Dinámico y Avanzado
Actividad 2.1 Configurar e implementar OSPF en infraestructuras de red
Actividad 2.2 Configurar peering BGP y políticas de enrutamiento
Actividad 2.3 Gestionar infraestructuras MPLS y servicios VPN
Función 3: Gestión de Calidad de Servicio y Monitorización de Tráfico
Actividad 3.1 Diseñar e implementar políticas de QoS
Actividad 3.2 Configurar monitorización SNMP de infraestructura
Actividad 3.3 Analizar flujos de tráfico con NetFlow y sFlow
Función 4: Diagnóstico y Resolución de Incidencias de Red y Conectividad
Actividad 4.1 Diagnosticar y resolver incidencias de conectividad de red
Actividad 4.2 Restablecer conectividad de red en puestos de usuario
Función 5: Automatización de Tareas de Red y Sistemas
Actividad 5.1 Desarrollar scripts Python para automatización de tareas de red
Actividad 5.2 Crear y mantener playbooks Ansible para automatización
Función 6: Gestión de Incidencias y Coordinación con Proveedores
Actividad 6.1 Coordinar resolución de incidencias con proveedores externos
Actividad 6.2 Gestionar casos de soporte con fabricantes de equipos
Actividad 6.3 Gestionar incidencias críticas de alto impacto
Función 7: Documentación, Auditoría y Mejora Continua
Actividad 7.1 Documentar procedimientos técnicos y configuraciones
Actividad 7.2 Facilitar auditorías técnicas de sistemas y redes
Actividad 7.3 Proponer e implementar mejoras continuas
Función 8: Administración de Sistemas Operativos y Servicios de Servidor
Actividad 8.1 Administrar sistemas operativos de servidor Windows y Linux
Actividad 8.2 Administrar servicios DNS y DHCP
Actividad 8.3 Instalar y configurar servicios web, correo y transferencia de archivos
Actividad 8.4 Implantar y administrar bases de datos en producción

Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso
Actividad 9.1 Administrar Active Directory y políticas de grupo
Actividad 9.2 Administrar plataformas de virtualización VMware
Actividad 9.3 Administrar y configurar soluciones VPN corporativas
Actividad 9.4 Administrar firewalls y gestionar certificados digitales
Función 10: Soporte Técnico a Usuarios Finales
Actividad 10.1 Prestar soporte remoto a usuarios finales
Actividad 10.2 Prestar soporte remoto por Internet y presencial
Actividad 10.3 Resolver incidencias de aplicaciones y asesorar a usuarios
Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones
Actividad 11.1 Realizar mantenimiento preventivo de equipos y sistemas
Actividad 11.2 Instalar componentes de hardware en estaciones y servidores
Actividad 11.3 Configurar sistemas según estándares corporativos
Actividad 11.4 Diagnosticar fallos de hardware y software
Actividad 11.5 Guiar a clientes en instalación de componentes de hardware
Función 12: Operaciones IT, Monitorización y Gestión de Cambios
Actividad 12.1 Monitorizar activamente sistemas y redes
Actividad 12.2 Aplicar procedimientos ITIL de gestión de cambios y problemas
Actividad 12.3 Asegurar ejecución de copias de seguridad y mantenimiento
Actividad 12.4 Definir operativas de explotación y gestionar Centro de Control IT
Actividad 12.5 Evaluar rendimiento de infraestructura y colaborar en proyectos

Estas áreas, desglosadas en actividades que el profesional realiza con autonomía o bajo supervisión, pueden no ejercerse todas en la entidad empleadora, especialmente en un primer empleo.

ANEXO II Marco de actividades profesionales

Contexto profesional y empleos

La Administración de Redes y Soporte Técnico IT constituye un área profesional fundamental en la transformación digital de las organizaciones. Los profesionales en este campo son responsables de diseñar, implementar, mantener y optimizar infraestructuras de red que soportan las operaciones corporativas. Su trabajo abarca desde la configuración de dispositivos de switching y enrutamiento hasta la implementación de protocolos de enrutamiento dinámico, gestión de calidad de servicio, diagnóstico de problemas de conectividad, automatización de tareas administrativas, coordinación con proveedores externos, documentación técnica, auditorías de seguridad, administración de servidores, gestión de directorios y virtualización, y prestación de soporte técnico a usuarios finales. En un contexto de transformación digital acelerada, estos profesionales son esenciales para garantizar que las redes corporativas funcionan con disponibilidad, rendimiento y seguridad óptimos, permitiendo que las organizaciones cumplan sus objetivos de negocio.

La persona titulada desempeña diferentes funciones:
– administración de infraestructura de red de capa 2 y capa 3 ;
– configuración de protocolos de enrutamiento dinámico y avanzado ;
– gestión de calidad de servicio y monitorización de tráfico ;
– diagnóstico y resolución de incidencias de red y conectividad ;
– automatización de tareas de red y sistemas ;
– gestión de incidencias y coordinación con proveedores ;
– documentación, auditoría y mejora continua ;
– administración de sistemas operativos y servicios de servidor ;
– administración de directorios, virtualización y seguridad de acceso ;
– soporte técnico a usuarios finales ;
– mantenimiento, instalación de hardware y gestión de configuraciones ;
– operaciones it, monitorización y gestión de cambios ;

Empleos relacionados

Los empleos de estos profesionales se encuentran en distintas estructuras públicas y privadas, entre ellas:
– Departamentos de Tecnología de la Información en empresas medianas y grandes ;
– Empresas de servicios de consultoría IT y sistemas integrados ;
– Proveedores de servicios de telecomunicaciones y conectividad ;
– Centros de datos y proveedores de servicios en la nube ;
– Departamentos de operaciones IT en organizaciones financieras y públicas ;
– Empresas especializadas en seguridad de redes y ciberseguridad ;
– Proveedores de servicios gestionados (MSP) de infraestructura IT ;

Los puestos reciben denominaciones diferentes según el sector. Algunos ejemplos son:
– Administrador de Redes ;
– Técnico de Administración de Redes ;
– Especialista en Infraestructura de Red ;
– Técnico de Soporte IT ;
– Administrador de Sistemas de Red ;
– Ingeniero de Redes Junior ;

– Técnico de Operaciones de Red ;
– Especialista en Conectividad Corporativa ;
– Técnico de Diagnóstico de Red ;
– Administrador de Infraestructura IT ;

Remuneración en Nivel de Entrada

Los profesionales que inician su carrera en Administración de Redes y Soporte Técnico IT en España pueden esperar una remuneración inicial entre 18.000 y 24.000 euros anuales, dependiendo de la ubicación geográfica, tamaño de la empresa, sector industrial y experiencia previa. En grandes ciudades como Madrid y Barcelona, y en sectores como finanzas y telecomunicaciones, la remuneración tiende a ser superior. Con experiencia y especialización, la remuneración puede aumentar significativamente hacia roles de ingeniero de redes o especialista senior.

Evolución profesional (3 a 5 años)

Los profesionales en Administración de Redes y Soporte Técnico IT tienen múltiples oportunidades de evolución profesional hacia roles de mayor responsabilidad y especialización. La progresión típica avanza desde técnico especializado hacia roles de liderazgo técnico, arquitectura de infraestructura y gestión de operaciones IT.

- Ingeniero de Redes - especialización en diseño y optimización de infraestructuras complejas
- Arquitecto de Infraestructura IT - diseño integral de soluciones de red y sistemas
- Especialista en Seguridad de Redes - enfoque en protección de infraestructura contra amenazas
- Especialista en Cloud Computing - administración de redes en entornos de nube pública y privada
- Líder Técnico de Operaciones IT - supervisión de equipos de administración de infraestructura
- Especialista en Automatización y DevOps - enfoque en automatización de procesos IT
- Consultor de Infraestructura IT - asesoramiento a organizaciones en diseño de redes
- Especialista en Monitorización y Observabilidad - gestión avanzada de rendimiento y disponibilidad

Continuación de estudios

Los profesionales que completen esta formación pueden continuar su desarrollo mediante certificaciones profesionales reconocidas en el sector como Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), CompTIA Network+, o especializaciones en tecnologías específicas como seguridad de redes, virtualización, cloud computing o automatización. Asimismo, pueden acceder a formaciones de nivel superior en Ingeniería de Telecomunicaciones, Máster en Administración de Sistemas de Información, o programas especializados en Arquitectura de Infraestructura IT.

ÉTICA Y DEONTOLOGÍA PROFESIONAL

La práctica profesional en Administración de Redes y Soporte Técnico IT requiere adherencia a principios éticos fundamentales que garanticen integridad, seguridad y confianza en la infraestructura IT corporativa.

- Confidencialidad de datos: Protección rigurosa de información sensible de la organización y usuarios, respetando privacidad y cumpliendo regulaciones de protección de datos
- Integridad técnica: Implementación de cambios únicamente después de validación exhaustiva, documentación completa y aprobación de autoridades competentes
- Disponibilidad de servicios: Priorización de disponibilidad y continuidad de servicios críticos, minimizando tiempo de inactividad y planificando cambios en ventanas de mantenimiento
- Seguridad de infraestructura: Implementación de controles de seguridad apropiados, cumplimiento de políticas de seguridad corporativa y estándares regulatorios

• Transparencia en comunicación: Comunicación clara y honesta con usuarios, proveedores y gestión sobre estado de sistemas, incidencias y limitaciones técnicas
• Responsabilidad profesional: Asunción de responsabilidad por decisiones técnicas, documentación de acciones realizadas y escalado apropiado de problemas complejos
• Cumplimiento normativo: Adherencia a regulaciones aplicables incluyendo protección de datos, seguridad de información y estándares de industria
• Desarrollo continuo: Actualización permanente de conocimientos y habilidades para mantener competencia técnica en tecnologías en evolución

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3

Actividad 1.1 Configurar y mantener switches de red gestionables

- Instalar y configurar switches Ethernet gestionables en entornos LAN corporativos
  - ■ Realizar la instalación física del switch en el rack o armario de red
  - ■ Configurar la dirección IP de gestión y acceso remoto (SSH, Telnet)
  - ■ Aplicar configuraciones de seguridad básicas (contraseñas, SNMP, ACLs)
- Gestionar tablas MAC, puertos troncales y configuraciones de acceso
  - ■ Configurar puertos de acceso (access ports) asignados a VLANs específicas
  - ■ Establecer puertos troncales (trunk ports) para la transmisión de múltiples VLANs
  - ■ Monitorizar y limpiar tablas MAC para evitar congestión de memoria
  - ■ Implementar port security para prevenir acceso no autorizado
- Realizar mantenimiento periódico y actualización de firmware
  - ■ Verificar la versión actual del firmware instalado
  - ■ Descargar y validar la integridad de la nueva versión de firmware
  - ■ Ejecutar la actualización en ventanas de mantenimiento programadas
  - ■ Verificar la funcionalidad del switch tras la actualización

■ Medios y recursos

- Switches Ethernet gestionables (Cisco Catalyst, HPE Aruba, etc.)
- Herramientas de acceso remoto (SSH, Telnet, consola serie)
- Software de gestión de switches (Cisco IOS, HPE Comware, etc.)
- Documentación técnica del fabricante
- Herramientas de diagnóstico (ping, traceroute, show commands)

■ Resultados esperados

- Switch configurado y operativo en la red corporativa
- Puertos correctamente asignados a VLANs y funcionales
- Firmware actualizado a la versión más reciente
- Documentación de configuración actualizada en el repositorio técnico

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3

Actividad 1.2 Configurar y mantener routers de red corporativos

- Instalar y configurar routers en entornos corporativos y de operador
  - ■ Realizar la instalación física del router en el rack de red
  - ■ Configurar interfaces de red (Ethernet, serie, etc.) con direcciones IP
  - ■ Establecer la configuración de gestión remota (SSH, SNMP)
  - ■ Aplicar políticas de seguridad básicas en el router
- Gestionar interfaces, tablas de enrutamiento y listas de control de acceso
  - ■ Configurar interfaces de red con direcciones IP y máscaras de subred
  - ■ Definir rutas estáticas o dinámicas según la topología de red
  - ■ Crear y aplicar listas de control de acceso (ACLs) para filtrado de tráfico
  - ■ Monitorizar la tabla de enrutamiento y resolver conflictos de rutas

- Actualizar firmware y documentar configuraciones
  - ■ Verificar la versión actual del firmware del router
  - ■ Descargar y validar la nueva versión de firmware
  - ■ Ejecutar la actualización en ventanas de mantenimiento
  - ■ Documentar la configuración en el repositorio técnico centralizado

■ Medios y recursos

- Routers corporativos (Cisco IOS-XE, Juniper Junos, etc.)
- Herramientas de acceso remoto (SSH, consola serie)
- Software de gestión de routers
- Documentación técnica del fabricante
- Herramientas de diagnóstico de red (ping, traceroute, show ip route)

■ Resultados esperados

- Router instalado y operativo en la infraestructura corporativa
- Interfaces configuradas y rutas establecidas correctamente
- ACLs aplicadas y validadas para el filtrado de tráfico
- Firmware actualizado y documentación técnica completa

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3

Actividad 1.3 Diseñar e implementar arquitecturas de red de capa 2

- Planificar y desplegar arquitecturas de red en capa 2 (Ethernet, switching)
  - ■ Analizar los requisitos de conectividad y ancho de banda
  - ■ Diseñar la topología de switching (árbol, malla, etc.)
  - ■ Seleccionar los switches y componentes de red adecuados
  - ■ Crear un diagrama de la arquitectura de capa 2
- Definir topologías, segmentaciones y redundancias a nivel de enlace
  - ■ Implementar redundancia mediante enlaces troncales y protocolos como STP
  - ■ Segmentar la red en VLANs según criterios de negocio
  - ■ Configurar puertos troncales para la comunicación entre switches
  - ■ Validar la topología activa y la convergencia de STP
- Documentar el diseño y validar su correcto funcionamiento
  - ■ Crear documentación detallada de la arquitectura de capa 2
  - ■ Realizar pruebas de conectividad entre segmentos de red
  - ■ Verificar la redundancia y la recuperación ante fallos
  - ■ Actualizar la documentación técnica con el diseño final

■ Medios y recursos

- Herramientas de diseño de red (Visio, Lucidchart, etc.)
- Switches gestionables de capa 2
- Herramientas de diagnóstico (ping, traceroute, show commands)
- Documentación de estándares de red corporativos
- Simuladores de red (Cisco Packet Tracer, GNS3)

■ Resultados esperados

- Arquitectura de capa 2 diseñada y documentada
- Topología de switching implementada y validada
- Redundancia y segmentación funcionando correctamente

• Documentación técnica completa y actualizada

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3

Actividad 1.4 Diseñar e implementar arquitecturas de red de capa 3

- Planificar y desplegar arquitecturas de red en capa 3 (IP, routing)
  - Analizar los requisitos de conectividad IP y enrutamiento
  - Diseñar la topología de routers y la estructura de la red
  - Seleccionar los routers y dispositivos de capa 3 adecuados
  - Crear un diagrama de la arquitectura de capa 3
- Definir esquemas de direccionamiento, subnetting y políticas de enrutamiento
  - Planificar el esquema de direccionamiento IP (público/privado)
  - Diseñar subnets y aplicar CIDR para optimizar el uso de direcciones
  - Definir políticas de enrutamiento estático o dinámico
  - Documentar el plan de direccionamiento IP
- Validar la conectividad extremo a extremo y documentar la arquitectura
  - Realizar pruebas de conectividad entre todos los segmentos de red
  - Verificar la resolución de nombres (DNS) en toda la infraestructura
  - Validar el enrutamiento de paquetes mediante traceroute
  - Documentar la arquitectura final y los parámetros de configuración

Medios y recursos

- Herramientas de diseño de red (Visio, Lucidchart, etc.)
- Routers de capa 3 (Cisco, Juniper, etc.)
- Herramientas de cálculo de subnetting (ipcalc, subnet calculators)
- Herramientas de diagnóstico (ping, traceroute, show ip route)
- Documentación de estándares de direccionamiento corporativos

Resultados esperados

- Arquitectura de capa 3 diseñada y documentada
- Esquema de direccionamiento IP implementado y validado
- Conectividad extremo a extremo verificada
- Documentación técnica completa con parámetros de configuración

Función 1: Administración de Infraestructura de Red de Capa 2 y Capa 3

Actividad 1.5 Implementar VLANs y Spanning Tree Protocol para segmentación y redundancia

- Crear y configurar VLANs en switches gestionables para aislar segmentos de red
  - Definir las VLANs según criterios de negocio y seguridad
  - Crear las VLANs en los switches gestionables
  - Asignar nombres descriptivos a cada VLAN
  - Configurar la VLAN de gestión para acceso remoto a switches
- Asignar puertos de acceso y troncales según la arquitectura definida
  - Configurar puertos de acceso (access ports) en cada VLAN
  - Establecer puertos troncales (trunk ports) entre switches
  - Configurar el protocolo de encapsulación (802.1Q)
  - Verificar la asignación de puertos mediante show commands
- Implementar y ajustar el protocolo Spanning Tree (STP/RSTP/MSTP)

- ■ Habilitar STP en todos los switches de la red
- ■ Definir el puente raíz (root bridge) para optimizar la topología
- ■ Configurar prioridades de puente para controlar la topología activa
- ■ Monitorizar la convergencia de STP y resolver anomalías

• Verificar el correcto aislamiento y comunicación entre VLANs

- ■ Realizar pruebas de conectividad dentro de cada VLAN
- ■ Verificar que no hay comunicación no autorizada entre VLANs
- ■ Validar la comunicación entre VLANs a través de routers
- ■ Documentar la configuración de VLANs y STP

■ Medios y recursos

- Switches gestionables con soporte para VLANs y STP
- Herramientas de acceso remoto (SSH, consola serie)
- Herramientas de diagnóstico (ping, show vlan, show spanning-tree)
- Documentación de estándares de VLANs corporativos
- Simuladores de red para pruebas de configuración

■ Resultados esperados

- VLANs creadas y configuradas en todos los switches
- Puertos correctamente asignados a VLANs y troncales
- STP/RSTP/MSTP implementado y convergencia verificada
- Aislamiento de VLANs validado y documentado
- Documentación técnica actualizada con configuración de VLANs

Función 2: Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Función 2: Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Actividad 2.1 Configurar e implementar OSPF en infraestructuras de red

- Configurar el protocolo OSPF en routers de la red corporativa
  - ■ Habilitar OSPF en los routers y asignar un ID de router único
  - ■ Definir las interfaces que participarán en OSPF
  - ■ Configurar el área OSPF (área 0 como backbone)
  - ■ Establecer las métricas de costo para las interfaces
- Definir áreas, costes y redistribución de rutas según la topología
  - ■ Crear áreas OSPF adicionales si es necesario (área 1, área 2, etc.)
  - ■ Configurar routers fronterizos de área (ABR) y routers fronterizos de sistema autónomo (ASBR)
  - ■ Ajustar los costes de las interfaces para optimizar el enrutamiento
  - ■ Implementar redistribución de rutas desde otros protocolos de enrutamiento
- Monitorizar la convergencia y resolver anomalías de enrutamiento
  - ■ Verificar la adyacencia OSPF entre routers vecinos
  - ■ Monitorizar la tabla de enrutamiento OSPF
  - ■ Analizar los logs de OSPF para detectar problemas de convergencia
  - ■ Resolver anomalías de enrutamiento mediante ajustes de configuración

■ Medios y recursos

- Routers con soporte para OSPF (Cisco IOS, Juniper Junos, etc.)
- Herramientas de acceso remoto (SSH, consola serie)
- Herramientas de diagnóstico (show ip ospf, show ip route ospf)
- Documentación de estándares OSPF corporativos
- Simuladores de red para pruebas de configuración OSPF

■ Resultados esperados

- OSPF configurado y operativo en todos los routers
- Áreas OSPF definidas y routers fronterizos configurados
- Convergencia OSPF verificada y optimizada
- Tabla de enrutamiento OSPF correcta y documentada
- Documentación técnica con configuración OSPF

Función 2: Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Actividad 2.2 Configurar peering BGP y políticas de enrutamiento

- Establecer sesiones BGP con proveedores de tránsito y peers de interconexión
  - ■ Configurar el número de sistema autónomo (ASN) del router local
  - ■ Establecer sesiones BGP con routers vecinos (eBGP o iBGP)
  - ■ Configurar los parámetros de sesión (timers, keepalive, hold time)
  - ■ Verificar la adyacencia BGP y el estado de las sesiones
- Definir políticas de importación y exportación de rutas mediante route-maps y filtros
  - ■ Crear route-maps para filtrar y modificar atributos de rutas
  - ■ Configurar políticas de importación (inbound) de rutas

- Configurar políticas de exportación (outbound) de rutas
- Implementar filtros de prefijos para controlar la propagación de rutas

• Supervisar la estabilidad de las sesiones y el estado de las rutas anunciadas
- Monitorizar el estado de las sesiones BGP
- Analizar las rutas anunciadas y recibidas
- Detectar y resolver problemas de convergencia BGP
- Documentar las políticas de enrutamiento BGP implementadas

■ Medios y recursos

• Routers con soporte para BGP (Cisco IOS, Juniper Junos, etc.)
• Herramientas de acceso remoto (SSH, consola serie)
• Herramientas de diagnóstico (show ip bgp, show ip bgp summary)
• Documentación de políticas BGP corporativos
• Simuladores de red para pruebas de configuración BGP

■ Resultados esperados

• Sesiones BGP establecidas y operativas
• Políticas de enrutamiento configuradas y validadas
• Rutas anunciadas y recibidas correctamente
• Estabilidad de sesiones BGP verificada
• Documentación técnica con configuración BGP

Función 2: Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Actividad 2.3 Gestionar infraestructuras MPLS y servicios VPN

• Configurar y administrar infraestructuras MPLS para la interconexión de sedes
- Habilitar MPLS en los routers de la red de núcleo
- Configurar el protocolo de distribución de etiquetas (LDP o RSVP-TE)
- Establecer los caminos de conmutación de etiquetas (LSPs)
- Verificar la distribución de etiquetas y la conmutación MPLS

• Gestionar LSPs, VRFs y servicios L2/L3 VPN sobre MPLS
- Crear y configurar funciones virtuales de enrutamiento (VRFs)
- Establecer VPN de capa 3 (L3 VPN) sobre MPLS
- Configurar servicios de capa 2 (L2 VPN) si es necesario
- Asignar clientes a VRFs y configurar las políticas de enrutamiento

• Supervisar el rendimiento y resolver incidencias en la red MPLS
- Monitorizar el estado de los LSPs y la distribución de etiquetas
- Analizar el rendimiento de los servicios VPN
- Detectar y resolver problemas de convergencia MPLS
- Documentar la configuración MPLS y los servicios VPN

■ Medios y recursos

• Routers con soporte para MPLS (Cisco IOS, Juniper Junos, etc.)
• Herramientas de acceso remoto (SSH, consola serie)
• Herramientas de diagnóstico (show mpls ldp, show mpls forwarding-table)
• Documentación de estándares MPLS corporativos
• Simuladores de red para pruebas de configuración MPLS

■ Resultados esperados

- MPLS configurado y operativo en la red de núcleo
- LSPs establecidos y funcionales
- VRFs y servicios VPN configurados y validados
- Rendimiento MPLS supervisado y optimizado
- Documentación técnica con configuración MPLS

Función 3: Gestión de Calidad de Servicio y Monitorización de Tráfico

Función 3: Gestión de Calidad de Servicio y Monitorización de Tráfico

Actividad 3.1 Diseñar e implementar políticas de QoS

- Diseñar políticas de calidad de servicio en routers y switches
  - ■ Identificar las aplicaciones críticas y sus requisitos de QoS
  - ■ Definir las clases de tráfico (voz, video, datos, etc.)
  - ■ Establecer los parámetros de QoS (ancho de banda, latencia, jitter)
  - ■ Crear un plan de implementación de QoS
- Clasificar, marcar y gestionar colas de tráfico según prioridades
  - ■ Configurar la clasificación de tráfico basada en criterios (puerto, protocolo, etc.)
  - ■ Implementar el marcado de tráfico (DSCP, CoS)
  - ■ Configurar colas de tráfico y políticas de gestión de colas
  - ■ Establecer políticas de policía y conformación de tráfico
- Verificar el cumplimiento de los parámetros de latencia y ancho de banda
  - ■ Realizar pruebas de latencia y jitter para aplicaciones críticas
  - ■ Monitorizar el ancho de banda utilizado por cada clase de tráfico
  - ■ Analizar los resultados y ajustar las políticas de QoS si es necesario
  - ■ Documentar la configuración de QoS y los resultados de las pruebas

■ Medios y recursos

- Routers y switches con soporte para QoS
- Herramientas de diagnóstico de QoS (show policy-map, show queue)
- Herramientas de prueba de rendimiento (iperf, jperf)
- Documentación de estándares QoS corporativos
- Simuladores de red para pruebas de configuración QoS

■ Resultados esperados

- Políticas de QoS diseñadas y documentadas
- Clasificación y marcado de tráfico implementados
- Colas de tráfico configuradas y funcionales
- Parámetros de latencia y ancho de banda verificados
- Documentación técnica con configuración QoS

Función 3: Gestión de Calidad de Servicio y Monitorización de Tráfico

Actividad 3.2 Configurar monitorización SNMP de infraestructura

- Configurar agentes y gestores SNMP para la monitorización de dispositivos
  - ■ Habilitar SNMP en routers, switches y servidores
  - ■ Configurar la comunidad SNMP (read-only, read-write)
  - ■ Establecer la dirección IP del gestor SNMP
  - ■ Verificar la conectividad SNMP entre agentes y gestor
- Definir traps y umbrales de alerta para la detección proactiva
  - ■ Configurar traps SNMP para eventos críticos (enlace caído, temperatura alta, etc.)
  - ■ Establecer umbrales de alerta para métricas de rendimiento

- Configurar la notificación de traps al gestor SNMP
- Definir acciones automáticas ante ciertos eventos

- Analizar los datos recogidos para anticipar problemas de capacidad
  - Recopilar datos de rendimiento de dispositivos mediante SNMP
  - Analizar tendencias de utilización de recursos
  - Identificar cuellos de botella y problemas de capacidad
  - Documentar los hallazgos y las recomendaciones

■ Medios y recursos

- Dispositivos de red con soporte para SNMP
- Gestor SNMP (Nagios, Zabbix, PRTG, etc.)
- Herramientas de diagnóstico SNMP (snmpwalk, snmpget)
- Documentación de OIDs SNMP relevantes
- Herramientas de análisis de datos (Excel, Grafana, etc.)

■ Resultados esperados

- SNMP configurado en todos los dispositivos de red
- Traps y umbrales definidos y funcionales
- Alertas generadas y notificadas correctamente
- Datos de rendimiento recopilados y analizados
- Documentación técnica con configuración SNMP

Función 3: Gestión de Calidad de Servicio y Monitorización de Tráfico

Actividad 3.3 Analizar flujos de tráfico con NetFlow y sFlow

- Configurar exportadores NetFlow en routers y switches
  - Habilitar NetFlow en las interfaces de red relevantes
  - Configurar la versión de NetFlow (v5, v9, IPFIX)
  - Establecer la dirección IP y puerto del colector NetFlow
  - Verificar la exportación de flujos hacia el colector
- Configurar agentes sFlow para el muestreo de tráfico
  - Habilitar sFlow en los dispositivos de red
  - Configurar la tasa de muestreo de paquetes
  - Establecer la dirección IP y puerto del colector sFlow
  - Verificar la recopilación de datos de muestreo
- Analizar los flujos mediante colectores y herramientas de visualización
  - Recopilar datos de flujos en el colector NetFlow/sFlow
  - Visualizar los flujos de tráfico mediante herramientas especializadas
  - Identificar patrones de tráfico y aplicaciones principales
  - Detectar anomalías y comportamientos sospechosos
- Identificar patrones anómalos y elaborar informes de capacidad
  - Analizar los datos de flujos para detectar anomalías
  - Generar informes de utilización de ancho de banda
  - Identificar aplicaciones que consumen más recursos
  - Documentar los hallazgos y las recomendaciones de mejora

■ Medios y recursos

- Routers y switches con soporte para NetFlow/sFlow
- Colector NetFlow/sFlow (nfcapd, Splunk, etc.)
- Herramientas de visualización de flujos (Wireshark, SolarWinds, etc.)

- Herramientas de análisis de datos (Python, R, etc.)
- Documentación de estándares NetFlow/sFlow

■ **Resultados esperados**

- NetFlow/sFlow configurado en dispositivos de red
- Flujos de tráfico recopilados y analizados
- Patrones de tráfico identificados y documentados
- Anomalías detectadas y reportadas
- Informes de capacidad elaborados y presentados

Función 4: Diagnóstico y Resolución de Incidencias de Red y Conectividad

Función 4: Diagnóstico y Resolución de Incidencias de Red y Conectividad

Actividad 4.1 Diagnosticar y resolver incidencias de conectividad de red

- Analizar síntomas de pérdida de conectividad mediante herramientas de diagnóstico
  - ■ Recopilar información sobre la incidencia (síntomas, equipos afectados, etc.)
  - ■ Ejecutar pruebas de conectividad básicas (ping, traceroute)
  - ■ Verificar el estado de los enlaces de red y dispositivos
  - ■ Analizar los logs de dispositivos de red para detectar errores
- Identificar la causa raíz y aplicar la solución correctiva
  - ■ Realizar capturas de paquetes (tcpdump, Wireshark) si es necesario
  - ■ Analizar los paquetes capturados para identificar problemas
  - ■ Determinar si el problema es de capa 2, capa 3 u otro nivel
  - ■ Aplicar la solución correctiva (reconfiguración, reinicio, etc.)
- Documentar la incidencia y las acciones realizadas
  - ■ Registrar la incidencia en el sistema de ticketing
  - ■ Documentar los pasos de diagnóstico realizados
  - ■ Registrar la causa raíz identificada
  - ■ Documentar la solución aplicada y el resultado final

■ Medios y recursos

- Herramientas de diagnóstico de red (ping, traceroute, nslookup)
- Analizadores de paquetes (Wireshark, tcpdump)
- Herramientas de acceso remoto (SSH, consola serie)
- Documentación de topología de red
- Sistema de ticketing para registro de incidencias

■ Resultados esperados

- Causa raíz de la incidencia identificada
- Solución correctiva aplicada y validada
- Conectividad de red restablecida
- Incidencia documentada en el sistema de ticketing
- Lecciones aprendidas registradas para futuras referencias

Función 4: Diagnóstico y Resolución de Incidencias de Red y Conectividad

Actividad 4.2 Restablecer conectividad de red en puestos de usuario

- Diagnosticar problemas de conectividad de red en equipos de usuario
  - ■ Recopilar información sobre el problema (síntomas, equipos afectados)
  - ■ Verificar la configuración de red del equipo (IP, gateway, DNS)
  - ■ Ejecutar pruebas de conectividad (ping, ipconfig, ifconfig)
  - ■ Verificar el estado del adaptador de red (cableado o Wi-Fi)
- Verificar la configuración de red del equipo y los parámetros de acceso
  - ■ Revisar la configuración de IP (DHCP o estática)
  - ■ Verificar la puerta de enlace predeterminada

    - ■ Comprobar la configuración de DNS
    - ■ Validar la conectividad a los servidores DNS
  - Resolver problemas de Wi-Fi, VPN y conectividad de red
    - ■ Diagnosticar problemas de conexión Wi-Fi (señal, autenticación)
    - ■ Resolver problemas de VPN (conexión, autenticación, rutas)
    - ■ Restablecer la conexión de red mediante reinicio de adaptadores
    - ■ Aplicar configuraciones de red correctas si es necesario
  - Confirmar el restablecimiento del servicio con el usuario
    - ■ Realizar pruebas de conectividad finales (ping, acceso a Internet)
    - ■ Verificar que el usuario puede acceder a los recursos necesarios
    - ■ Documentar la solución aplicada
    - ■ Registrar la incidencia como resuelta en el sistema de ticketing

■ Medios y recursos

- Herramientas de diagnóstico de red (ping, ipconfig, ifconfig)
- Herramientas de acceso remoto (VPN, escritorio remoto)
- Documentación de configuración de red corporativa
- Herramientas de gestión de Wi-Fi
- Sistema de ticketing para registro de incidencias

■ Resultados esperados

- Problema de conectividad diagnosticado
- Configuración de red verificada y corregida
- Conectividad de red restablecida
- Usuario confirmando el acceso a recursos
- Incidencia documentada y resuelta

Función 5: Automatización de Tareas de Red y Sistemas

Función 5: Automatización de Tareas de Red y Sistemas

Actividad 5.1 Desarrollar scripts Python para automatización de tareas de red

- Desarrollar scripts en Python para automatizar configuraciones de red
  - ■ Identificar las tareas repetitivas que pueden automatizarse
  - ■ Diseñar la estructura del script y los módulos necesarios
  - ■ Utilizar librerías de Python para acceso a dispositivos (Paramiko, Netmiko)
  - ■ Implementar la lógica de configuración en el script
- Automatizar inventarios y comprobaciones de red
  - ■ Crear scripts para recopilar información de dispositivos de red
  - ■ Implementar verificaciones de configuración y estado
  - ■ Generar reportes automáticos de inventario
  - ■ Integrar los scripts con sistemas de gestión de configuración
- Integrar las automatizaciones en flujos de trabajo operativos
  - ■ Integrar los scripts en pipelines de CI/CD
  - ■ Crear interfaces de usuario para ejecutar los scripts
  - ■ Implementar logging y manejo de errores
  - ■ Documentar los scripts y su uso
- Mantener y documentar el código desarrollado
  - ■ Realizar pruebas unitarias de los scripts
  - ■ Documentar el código con comentarios y docstrings
  - ■ Mantener versiones del código en un repositorio (Git)
  - ■ Actualizar los scripts según cambios en la infraestructura

■ Medios y recursos

- Lenguaje de programación Python
- Librerías de Python (Paramiko, Netmiko, Ansible, etc.)
- Entorno de desarrollo (IDE, editor de código)
- Sistema de control de versiones (Git, GitHub)
- Documentación de APIs de dispositivos de red

■ Resultados esperados

- Scripts Python desarrollados y funcionales
- Automatización de tareas de red implementada
- Reducción de tiempo en tareas repetitivas
- Código documentado y mantenible
- Integración en flujos de trabajo operativos

Función 5: Automatización de Tareas de Red y Sistemas

Actividad 5.2 Crear y mantener playbooks Ansible para automatización

- Crear playbooks de Ansible para despliegue y configuración automatizada
  - ■ Diseñar la estructura de playbooks y roles
  - ■ Crear playbooks para configuración de dispositivos de red
  - ■ Implementar playbooks para despliegue de servidores
  - ■ Utilizar módulos de Ansible específicos para cada tarea

- Gestionar inventarios dinámicos y roles reutilizables
  - ■ Crear inventarios dinámicos desde fuentes externas
  - ■ Desarrollar roles reutilizables para tareas comunes
  - ■ Implementar variables y templates en los playbooks
  - ■ Organizar los playbooks en una estructura modular
- Integrar Ansible en pipelines de CI/CD
  - ■ Integrar Ansible con herramientas de CI/CD (Jenkins, GitLab CI)
  - ■ Crear pipelines para despliegue automatizado
  - ■ Implementar pruebas de configuración en los pipelines
  - ■ Documentar los pipelines y su uso
- Mantener y actualizar los playbooks según cambios
  - ■ Realizar pruebas de los playbooks en entornos de prueba
  - ■ Actualizar los playbooks según cambios en la infraestructura
  - ■ Documentar los playbooks y su uso
  - ■ Mantener versiones de los playbooks en un repositorio

■ Medios y recursos

- Herramienta de automatización Ansible
- Lenguaje YAML para definición de playbooks
- Sistema de control de versiones (Git, GitHub)
- Herramientas de CI/CD (Jenkins, GitLab CI, etc.)
- Documentación de módulos de Ansible

■ Resultados esperados

- Playbooks Ansible desarrollados y funcionales
- Automatización de despliegue implementada
- Inventarios dinámicos configurados
- Roles reutilizables creados
- Integración en pipelines CI/CD completada

Función 6: Gestión de Incidencias y Coordinación con Proveedores

Función 6: Gestión de Incidencias y Coordinación con Proveedores

Actividad 6.1 Coordinar resolución de incidencias con proveedores externos

- Gestionar la comunicación con proveedores de servicios
  - ■ Identificar el proveedor responsable de la incidencia
  - ■ Contactar al proveedor y reportar la incidencia
  - ■ Proporcionar información técnica detallada del problema
  - ■ Establecer un canal de comunicación para seguimiento
- Hacer seguimiento del estado de los tickets abiertos
  - ■ Registrar el ticket de incidencia con el proveedor
  - ■ Monitorizar el progreso de la resolución
  - ■ Solicitar actualizaciones periódicas al proveedor
  - ■ Documentar todas las comunicaciones en el ticket
- Escalar cuando los tiempos de resolución superen los ANS
  - ■ Monitorizar el tiempo transcurrido desde la apertura del ticket
  - ■ Comparar con los ANS definidos en el contrato
  - ■ Escalar a niveles superiores del proveedor si es necesario
  - ■ Informar a la dirección técnica sobre el incumplimiento de ANS

■ Medios y recursos

- Sistema de ticketing para registro de incidencias
- Contactos de proveedores de servicios
- Documentación de ANS con proveedores
- Herramientas de comunicación (correo, teléfono, chat)
- Plantillas de reportes de incidencias

■ Resultados esperados

- Incidencia reportada al proveedor
- Ticket abierto y en seguimiento
- Comunicación regular con el proveedor
- Escalado realizado si es necesario
- Incidencia resuelta dentro de los ANS

Función 6: Gestión de Incidencias y Coordinación con Proveedores

Actividad 6.2 Gestionar casos de soporte con fabricantes de equipos

- Abrir y gestionar casos de soporte con fabricantes
  - ■ Identificar el fabricante del equipo o software afectado
  - ■ Acceder al portal de soporte del fabricante
  - ■ Abrir un caso de soporte con descripción detallada del problema
  - ■ Proporcionar información de contacto y disponibilidad
- Proporcionar información técnica para agilizar el diagnóstico
  - ■ Recopilar logs y configuraciones del equipo afectado
  - ■ Realizar diagnósticos preliminares antes de contactar

- Proporcionar versiones de firmware y software
- Responder rápidamente a las solicitudes de información del fabricante

- Hacer seguimiento hasta la resolución definitiva
  - Monitorizar el progreso del caso de soporte
  - Solicitar actualizaciones periódicas al fabricante
  - Probar las soluciones propuestas en el entorno de producción
  - Confirmar la resolución del problema
- Documentar la solución para futuras referencias
  - Registrar la solución en la base de conocimiento
  - Documentar los pasos de resolución
  - Crear una guía de referencia rápida si es aplicable
  - Compartir la solución con el equipo técnico

Medios y recursos

- Portales de soporte de fabricantes (Cisco, HPE, etc.)
- Herramientas de diagnóstico del fabricante
- Documentación técnica del equipo
- Sistema de ticketing para registro de casos
- Base de conocimiento para documentación de soluciones

Resultados esperados

- Caso de soporte abierto con el fabricante
- Información técnica proporcionada
- Caso en seguimiento y progresando
- Solución implementada y validada
- Documentación de la solución completada

Función 6: Gestión de Incidencias y Coordinación con Proveedores

Actividad 6.3 Gestionar incidencias críticas de alto impacto

- Coordinar la respuesta ante incidencias críticas
  - Activar el plan de respuesta a incidencias críticas
  - Convocar al equipo de respuesta (war room)
  - Asignar roles y responsabilidades al equipo
  - Establecer un canal de comunicación centralizado
- Escalar y comunicar el estado a las partes interesadas
  - Informar a la dirección técnica y de negocio
  - Proporcionar actualizaciones periódicas del estado
  - Comunicar el impacto estimado en los servicios
  - Establecer expectativas realistas de resolución
- Liderar el proceso de resolución
  - Coordinar los esfuerzos de diagnóstico y resolución
  - Tomar decisiones rápidas para minimizar el impacto
  - Escalar a proveedores o fabricantes si es necesario
  - Validar la resolución antes de dar por cerrada la incidencia
- Elaborar el informe post-mortem
  - Documentar la cronología de la incidencia
  - Identificar la causa raíz del problema
  - Analizar las acciones correctivas implementadas
  - Proponer mejoras para evitar incidencias similares

■ **Medios y recursos**

- Plan de respuesta a incidencias críticas
- Herramientas de comunicación (conferencia, chat)
- Sistema de ticketing para registro de incidencias
- Documentación de procedimientos de escalado
- Plantillas de informes post-mortem

■ **Resultados esperados**

- Incidencia crítica identificada y escalada
- Equipo de respuesta activado y coordinado
- Comunicación regular con partes interesadas
- Incidencia resuelta y servicios restablecidos
- Informe post-mortem elaborado y compartido

Función 7: Documentación, Auditoría y Mejora Continua

Función 7: Documentación, Auditoría y Mejora Continua

Actividad 7.1 Documentar procedimientos técnicos y configuraciones

- Redactar documentación técnica de procedimientos
  - ■ Identificar los procedimientos críticos que requieren documentación
  - ■ Redactar guías paso a paso para cada procedimiento
  - ■ Incluir diagramas y capturas de pantalla cuando sea necesario
  - ■ Revisar la documentación para claridad y precisión
- Documentar arquitecturas y configuraciones de sistemas
  - ■ Crear diagramas de arquitectura de red y sistemas
  - ■ Documentar las configuraciones de dispositivos clave
  - ■ Incluir parámetros de configuración y justificación
  - ■ Mantener la documentación actualizada con cambios
- Organizar la documentación en repositorios accesibles
  - ■ Crear una estructura de carpetas lógica para la documentación
  - ■ Utilizar un sistema de gestión de documentos (wiki, SharePoint)
  - ■ Establecer permisos de acceso apropiados
  - ■ Facilitar la búsqueda y recuperación de documentación
- Asegurar la trazabilidad de los cambios realizados
  - ■ Mantener un registro de cambios en la documentación
  - ■ Documentar la fecha y autor de cada cambio
  - ■ Incluir justificación de los cambios realizados
  - ■ Mantener versiones anteriores para referencia histórica

■ Medios y recursos

- Herramientas de documentación (Word, Markdown, etc.)
- Sistemas de gestión de documentos (wiki, SharePoint, Confluence)
- Herramientas de diagramación (Visio, Lucidchart, Draw.io)
- Sistema de control de versiones (Git, GitHub)
- Plantillas de documentación técnica

■ Resultados esperados

- Procedimientos técnicos documentados y accesibles
- Arquitecturas y configuraciones documentadas
- Documentación organizada en repositorio centralizado
- Trazabilidad de cambios implementada
- Documentación actualizada y mantenida

Función 7: Documentación, Auditoría y Mejora Continua

Actividad 7.2 Facilitar auditorías técnicas de sistemas y redes

- Preparar información técnica requerida durante auditorías
  - ■ Identificar los requisitos de información de los auditores
  - ■ Recopilar documentación de configuraciones y procedimientos
  - ■ Preparar reportes de cumplimiento normativo
  - ■ Organizar la información de forma clara y accesible

- Acompañar a los auditores en la revisión de configuraciones
  - ■ Facilitar el acceso a sistemas y dispositivos de red
  - ■ Explicar las configuraciones y procedimientos implementados
  - ■ Responder a preguntas técnicas de los auditores
  - ■ Documentar las observaciones y hallazgos
- Implementar acciones correctivas derivadas de hallazgos
  - ■ Analizar los hallazgos de la auditoría
  - ■ Desarrollar un plan de acción para corregir deficiencias
  - ■ Implementar las acciones correctivas en el plazo establecido
  - ■ Validar que las acciones correctivas son efectivas

■ **Medios y recursos**

- Documentación técnica de sistemas y redes
- Reportes de cumplimiento normativo
- Herramientas de acceso a sistemas (SSH, consola)
- Estándares de auditoría (ISO 27001, ITIL, etc.)
- Sistema de seguimiento de acciones correctivas

■ **Resultados esperados**

- Información técnica preparada para auditoría
- Auditores acompañados en revisión de configuraciones
- Hallazgos de auditoría documentados
- Acciones correctivas implementadas
- Cumplimiento normativo validado

Función 7: Documentación, Auditoría y Mejora Continua

Actividad 7.3 Proponer e implementar mejoras continuas

- Identificar oportunidades de mejora en procesos y servicios
  - ■ Analizar los procesos operativos actuales
  - ■ Recopilar feedback del equipo técnico y usuarios
  - ■ Identificar ineficiencias y cuellos de botella
  - ■ Proponer soluciones de mejora
- Elaborar propuestas de mejora con análisis coste-beneficio
  - ■ Cuantificar los beneficios de la mejora propuesta
  - ■ Estimar los costos de implementación
  - ■ Calcular el retorno de inversión (ROI)
  - ■ Documentar la propuesta de forma clara y persuasiva
- Presentar las iniciativas a la dirección técnica
  - ■ Preparar una presentación de la propuesta de mejora
  - ■ Presentar el análisis coste-beneficio
  - ■ Responder a preguntas y objeciones
  - ■ Obtener aprobación para la implementación
- Hacer seguimiento de la implantación de mejoras
  - ■ Planificar la implementación de la mejora
  - ■ Coordinar con los equipos involucrados
  - ■ Monitorizar el progreso de la implementación
  - ■ Validar que la mejora proporciona los beneficios esperados

■ **Medios y recursos**

- Herramientas de análisis de procesos
- Herramientas de cálculo de ROI
- Herramientas de presentación (PowerPoint, etc.)
- Documentación de procesos actuales
- Feedback de usuarios y equipo técnico

■ Resultados esperados

- Oportunidades de mejora identificadas
- Propuestas de mejora documentadas con análisis coste-beneficio
- Propuestas presentadas a dirección técnica
- Mejoras aprobadas e implementadas
- Beneficios de mejoras validados y documentados

Función 8: Administración de Sistemas Operativos y Servicios de Servidor

Función 8: Administración de Sistemas Operativos y Servicios de Servidor

Actividad 8.1 Administrar sistemas operativos de servidor Windows y Linux

- Instalar y configurar sistemas operativos Windows Server
  - ■ Preparar el medio de instalación de Windows Server
  - ■ Realizar la instalación en el servidor
  - ■ Configurar parámetros básicos (nombre, IP, zona horaria)
  - ■ Aplicar actualizaciones y parches de seguridad
- Instalar y configurar sistemas operativos Linux
  - ■ Seleccionar la distribución Linux apropiada
  - ■ Realizar la instalación en el servidor
  - ■ Configurar parámetros básicos (nombre, IP, zona horaria)
  - ■ Aplicar actualizaciones y parches de seguridad
- Gestionar roles, características y actualizaciones del sistema
  - ■ Instalar roles y características según requisitos
  - ■ Configurar servicios del sistema
  - ■ Aplicar actualizaciones periódicas del SO
  - ■ Monitorizar la salud del sistema operativo
- Garantizar la estabilidad y disponibilidad del servidor
  - ■ Monitorizar el rendimiento del servidor
  - ■ Realizar mantenimiento preventivo
  - ■ Resolver problemas de estabilidad
  - ■ Documentar la configuración del servidor

■ Medios y recursos

- Medios de instalación de Windows Server y Linux
- Herramientas de gestión de servidores (Server Manager, etc.)
- Herramientas de monitorización (Nagios, Zabbix, etc.)
- Documentación de estándares de configuración
- Herramientas de diagnóstico del SO

■ Resultados esperados

- Sistemas operativos instalados y configurados
- Roles y características instalados según requisitos
- Actualizaciones aplicadas y servidor estable
- Servidor monitorizado y disponible
- Documentación de configuración completada

Función 8: Administración de Sistemas Operativos y Servicios de Servidor

Actividad 8.2 Administrar servicios DNS y DHCP

- Configurar y mantener servidores DNS internos y externos
  - ■ Instalar y configurar el servicio DNS
  - ■ Crear zonas DNS para dominios corporativos

- Configurar registros DNS (A, AAAA, MX, CNAME, etc.)
- Implementar replicación de zonas entre servidores DNS

• Gestionar zonas, registros y políticas de reenvío
- Mantener los registros DNS actualizados
- Configurar reenviadores condicionales para dominios externos
- Implementar políticas de seguridad DNS (DNSSEC)
- Monitorizar la resolución de nombres

• Configurar y gestionar servidores DHCP
- Instalar y configurar el servicio DHCP
- Crear ámbitos DHCP para subredes corporativas
- Configurar opciones DHCP (gateway, DNS, etc.)
- Implementar reservas DHCP para equipos críticos

• Diagnosticar y resolver problemas de resolución de nombres
- Utilizar herramientas de diagnóstico DNS (nslookup, dig)
- Analizar logs de DNS para detectar problemas
- Resolver conflictos de resolución de nombres
- Documentar los problemas y soluciones

■ Medios y recursos

• Servidores DNS (BIND, Windows DNS, etc.)
• Servidores DHCP (ISC DHCP, Windows DHCP, etc.)
• Herramientas de diagnóstico (nslookup, dig, ipconfig)
• Documentación de estándares DNS/DHCP corporativos
• Herramientas de monitorización de DNS/DHCP

■ Resultados esperados

• Servidores DNS configurados y operativos
• Zonas DNS creadas y registros actualizados
• Servidores DHCP configurados y asignando direcciones
• Resolución de nombres funcionando correctamente
• Documentación de configuración DNS/DHCP completada

Función 8: Administración de Sistemas Operativos y Servicios de Servidor

Actividad 8.3 Instalar y configurar servicios web, correo y transferencia de archivos

• Desplegar y configurar servidores web (Apache, Nginx)
- Instalar el servidor web en el servidor
- Configurar hosts virtuales para múltiples sitios
- Instalar y configurar certificados SSL/TLS
- Configurar reglas de acceso y seguridad

• Configurar servidores de correo electrónico
- Instalar servicios SMTP, IMAP, POP3
- Configurar dominios y buzones de correo
- Implementar políticas antispam y antivirus
- Configurar autenticación y encriptación

• Desplegar y administrar servicios FTP/SFTP
- Instalar el servicio FTP/SFTP
- Configurar usuarios y permisos de acceso
- Establecer cuotas de almacenamiento
- Implementar seguridad (SSL/TLS, autenticación)

- Garantizar la seguridad y disponibilidad de los servicios
  - ■ Monitorizar el estado de los servicios
  - ■ Aplicar actualizaciones de seguridad
  - ■ Realizar copias de seguridad de datos
  - ■ Documentar la configuración de los servicios

■ **Medios y recursos**

- Servidores web (Apache, Nginx)
- Servidores de correo (Postfix, Exim, Exchange)
- Servidores FTP/SFTP (vsftpd, OpenSSH)
- Certificados SSL/TLS
- Herramientas de monitorización de servicios

■ **Resultados esperados**

- Servidores web configurados y operativos
- Servicios de correo funcionando correctamente
- Servicios FTP/SFTP disponibles y seguros
- Certificados SSL/TLS instalados y válidos
- Documentación de configuración completada

Función 8: Administración de Sistemas Operativos y Servicios de Servidor

Actividad 8.4 Implantar y administrar bases de datos en producción

- Instalar y configurar sistemas gestores de bases de datos
  - ■ Seleccionar el SGBD apropiado (MySQL, PostgreSQL, SQL Server)
  - ■ Instalar el SGBD en el servidor
  - ■ Configurar parámetros de rendimiento y seguridad
  - ■ Aplicar actualizaciones y parches de seguridad
- Gestionar usuarios, permisos y esquemas de base de datos
  - ■ Crear usuarios de base de datos con permisos apropiados
  - ■ Crear esquemas y tablas según requisitos
  - ■ Configurar políticas de acceso y autenticación
  - ■ Implementar auditoría de acceso a datos
- Supervisar el rendimiento y realizar tareas de mantenimiento
  - ■ Monitorizar el rendimiento de la base de datos
  - ■ Optimizar índices y consultas
  - ■ Realizar mantenimiento de fragmentación
  - ■ Analizar logs de errores y alertas
- Asegurar la disponibilidad y recuperación de datos
  - ■ Implementar copias de seguridad regulares
  - ■ Configurar replicación o clustering si es necesario
  - ■ Realizar pruebas de recuperación
  - ■ Documentar procedimientos de recuperación

■ **Medios y recursos**

- Sistemas gestores de bases de datos (MySQL, PostgreSQL, SQL Server)
- Herramientas de administración de BD (phpMyAdmin, pgAdmin, SSMS)
- Herramientas de monitorización de BD (Nagios, Zabbix)
- Herramientas de backup (mysqldump, pg_dump, etc.)
- Documentación de estándares de BD corporativos

■ **Resultados esperados**

- Base de datos instalada y configurada
- Usuarios y permisos configurados
- Rendimiento de BD monitorizado y optimizado
- Copias de seguridad implementadas y probadas
- Documentación de configuración completada

Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso

Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso

Actividad 9.1 Administrar Active Directory y políticas de grupo

- Administrar el servicio de directorio Active Directory
  - ■ Instalar y configurar Active Directory
  - ■ Crear bosques y dominios según estructura corporativa
  - ■ Configurar controladores de dominio
  - ■ Implementar replicación de directorio
- Gestionar usuarios, grupos y unidades organizativas
  - ■ Crear y mantener cuentas de usuario
  - ■ Crear grupos de seguridad y distribución
  - ■ Organizar usuarios en unidades organizativas (OU)
  - ■ Implementar políticas de contraseña y expiración
- Configurar políticas de grupo (GPO) para control centralizado
  - ■ Crear GPOs para aplicar configuraciones a usuarios y equipos
  - ■ Configurar políticas de seguridad (firewall, antivirus, etc.)
  - ■ Implementar mapeo de unidades de red y impresoras
  - ■ Monitorizar la aplicación de GPOs
- Supervisar la replicación y la salud del dominio
  - ■ Monitorizar la replicación entre controladores de dominio
  - ■ Verificar la salud del dominio
  - ■ Resolver problemas de replicación
  - ■ Documentar la configuración de Active Directory

■ Medios y recursos

- Windows Server con Active Directory
- Herramientas de administración (Active Directory Users and Computers, GPMC)
- Herramientas de diagnóstico (dcdiag, repadmin)
- Documentación de estructura de dominios corporativos
- Herramientas de monitorización de AD

■ Resultados esperados

- Active Directory instalado y configurado
- Usuarios y grupos creados y organizados
- GPOs configuradas y aplicadas
- Replicación de directorio funcionando
- Documentación de configuración de AD completada

Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso

Actividad 9.2 Administrar plataformas de virtualización VMware

- Instalar y configurar plataformas VMware vSphere/ESXi
  - ■ Instalar ESXi en servidores físicos
  - ■ Configurar vCenter Server para gestión centralizada

- Crear clústeres de hosts ESXi
- Configurar almacenamiento compartido (SAN, NAS)

• Gestionar máquinas virtuales y recursos
- Crear y configurar máquinas virtuales
- Asignar recursos (CPU, memoria, disco) a VMs
- Implementar políticas de reserva de recursos
- Monitorizar el uso de recursos de VMs

• Optimizar recursos de cómputo, almacenamiento y red
- Configurar vMotion para migración de VMs
- Implementar DRS (Distributed Resource Scheduler)
- Optimizar el almacenamiento (thin provisioning, snapshots)
- Configurar redes virtuales y switches distribuidos

• Supervisar el rendimiento y realizar mantenimiento
- Monitorizar el rendimiento del entorno virtualizado
- Realizar actualizaciones de ESXi y vCenter
- Ejecutar tareas de mantenimiento preventivo
- Documentar la configuración de VMware

■ **Medios y recursos**

• Servidores físicos para ESXi
• VMware vSphere/ESXi
• VMware vCenter Server
• Almacenamiento compartido (SAN, NAS)
• Herramientas de monitorización de VMware

■ **Resultados esperados**

• Plataforma VMware instalada y configurada
• Máquinas virtuales creadas y operativas
• Recursos optimizados y distribuidos
• Rendimiento del entorno virtualizado monitorizado
• Documentación de configuración de VMware completada

Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso

Actividad 9.3 Administrar y configurar soluciones VPN corporativas

• Desplegar soluciones VPN site-to-site
- Configurar VPN IPSec entre sedes corporativas
- Establecer túneles VPN seguros
- Configurar políticas de encriptación y autenticación
- Verificar la conectividad entre sedes

• Desplegar soluciones VPN de acceso remoto
- Configurar servidores VPN para acceso remoto
- Implementar autenticación de usuarios (RADIUS, LDAP)
- Configurar asignación de direcciones IP a clientes VPN
- Implementar políticas de seguridad para acceso remoto

• Gestionar usuarios, certificados y políticas de acceso
- Crear cuentas de usuario para acceso VPN
- Generar y gestionar certificados digitales
- Configurar políticas de acceso basadas en grupos
- Implementar autenticación multifactor si es necesario

- Supervisar el rendimiento y la disponibilidad del servicio VPN
  - ■ Monitorizar conexiones VPN activas
  - ■ Analizar logs de VPN para detectar problemas
  - ■ Realizar pruebas de conectividad VPN
  - ■ Documentar la configuración de VPN

■ Medios y recursos

- Routers o servidores VPN
- Certificados digitales
- Herramientas de autenticación (RADIUS, LDAP)
- Herramientas de monitorización de VPN
- Documentación de estándares VPN corporativos

■ Resultados esperados

- Soluciones VPN site-to-site configuradas
- Acceso remoto VPN disponible para usuarios
- Usuarios y certificados gestionados
- Conectividad VPN monitorizada y disponible
- Documentación de configuración VPN completada

Función 9: Administración de Directorios, Virtualización y Seguridad de Acceso

Actividad 9.4 Administrar firewalls y gestionar certificados digitales

- Configurar y mantener firewalls perimetrales e internos
  - ■ Instalar y configurar firewalls en puntos de acceso
  - ■ Definir reglas de filtrado de tráfico
  - ■ Configurar NAT (Network Address Translation)
  - ■ Implementar políticas de seguridad basadas en zonas
- Gestionar reglas de filtrado y políticas de seguridad
  - ■ Crear reglas de entrada y salida
  - ■ Implementar listas de control de acceso (ACLs)
  - ■ Configurar inspección de estado (stateful inspection)
  - ■ Monitorizar el tráfico bloqueado
- Revisar logs y alertas para detectar intentos de acceso
  - ■ Analizar logs de firewall para detectar anomalías
  - ■ Investigar intentos de acceso no autorizado
  - ■ Implementar contramedidas contra ataques
  - ■ Documentar incidentes de seguridad
- Administrar el ciclo de vida de certificados digitales
  - ■ Generar solicitudes de certificados digitales
  - ■ Instalar certificados en dispositivos y servicios
  - ■ Monitorizar la vigencia de certificados
  - ■ Renovar certificados antes de su expiración

■ Medios y recursos

- Firewalls (Cisco ASA, Palo Alto, Fortinet, etc.)
- Herramientas de gestión de firewalls
- Autoridades de certificación (CA)
- Herramientas de monitorización de certificados
- Documentación de políticas de seguridad corporativos

■ **Resultados esperados**

- Firewalls configurados y operativos
- Reglas de filtrado implementadas y validadas
- Logs de firewall analizados y monitorizados
- Certificados digitales gestionados y renovados
- Documentación de configuración de firewall completada

Función 10: Soporte Técnico a Usuarios Finales

Función 10: Soporte Técnico a Usuarios Finales

Actividad 10.1 Prestar soporte remoto a usuarios finales

- Atender llamadas de usuarios con incidencias técnicas
  - ■ Recibir y registrar la llamada del usuario
  - ■ Recopilar información sobre el problema
  - ■ Clasificar la incidencia por prioridad
  - ■ Asignar un técnico para la resolución
- Guiar al usuario paso a paso para resolver el problema
  - ■ Explicar los pasos de forma clara y sencilla
  - ■ Verificar que el usuario sigue las instrucciones
  - ■ Adaptar las instrucciones según el nivel técnico del usuario
  - ■ Confirmar que el problema se ha resuelto
- Utilizar herramientas de acceso remoto para diagnóstico
  - ■ Solicitar permiso al usuario para acceso remoto
  - ■ Utilizar herramientas de escritorio remoto (RDP, TeamViewer)
  - ■ Diagnosticar el problema de forma remota
  - ■ Aplicar la solución sin afectar otros sistemas
- Registrar la incidencia en el sistema de ticketing
  - ■ Documentar la descripción del problema
  - ■ Registrar los pasos de diagnóstico realizados
  - ■ Documentar la solución aplicada
  - ■ Cerrar la incidencia con resultado

■ Medios y recursos

- Sistema de ticketing para registro de incidencias
- Herramientas de acceso remoto (RDP, TeamViewer, AnyDesk)
- Herramientas de diagnóstico (ping, ipconfig, etc.)
- Base de conocimiento de soluciones comunes
- Documentación de procedimientos de soporte

■ Resultados esperados

- Incidencia registrada en el sistema de ticketing
- Usuario guiado en la resolución del problema
- Problema diagnosticado y resuelto
- Incidencia documentada con solución
- Usuario satisfecho con la resolución

Función 10: Soporte Técnico a Usuarios Finales

Actividad 10.2 Prestar soporte remoto por Internet y presencial

- Utilizar herramientas de acceso remoto para resolver incidencias
  - ■ Establecer conexión remota con el equipo del usuario
  - ■ Diagnosticar problemas de software y configuración
  - ■ Resolver problemas de conectividad de red
  - ■ Validar la solución con el usuario

- Desplazarse al puesto del usuario para soporte presencial
  - ■ Planificar la visita al puesto del usuario
  - ■ Diagnosticar el problema in situ
  - ■ Aplicar la solución adecuada
  - ■ Informar al usuario del resultado
- Diagnosticar y solucionar problemas de hardware
  - ■ Identificar problemas de hardware (disco duro, memoria, etc.)
  - ■ Realizar pruebas de diagnóstico
  - ■ Sustituir componentes defectuosos si es necesario
  - ■ Verificar el funcionamiento del equipo
- Documentar las actuaciones realizadas
  - ■ Registrar la incidencia en el sistema de ticketing
  - ■ Documentar los pasos de diagnóstico
  - ■ Documentar la solución aplicada
  - ■ Registrar el tiempo invertido en la resolución

■ **Medios y recursos**

- Herramientas de acceso remoto (VPN, escritorio remoto)
- Herramientas de diagnóstico de hardware
- Componentes de reemplazo (RAM, disco duro, etc.)
- Sistema de ticketing para registro de incidencias
- Documentación de procedimientos de soporte

■ **Resultados esperados**

- Incidencia diagnosticada y resuelta
- Equipo del usuario funcionando correctamente
- Usuario satisfecho con la solución
- Incidencia documentada en el sistema
- Tiempo de resolución registrado

Función 10: Soporte Técnico a Usuarios Finales

Actividad 10.3 Resolver incidencias de aplicaciones y asesorar a usuarios

- Atender y resolver incidencias de aplicaciones corporativas
  - ■ Recibir reportes de problemas con aplicaciones
  - ■ Diagnosticar problemas de funcionalidad
  - ■ Coordinar con proveedores de aplicaciones si es necesario
  - ■ Aplicar soluciones o workarounds
- Coordinar con proveedores cuando sea necesario
  - ■ Contactar al proveedor de la aplicación
  - ■ Proporcionar información técnica del problema
  - ■ Hacer seguimiento de la resolución
  - ■ Implementar la solución del proveedor
- Proporcionar formación y orientación a usuarios
  - ■ Explicar el uso correcto de la aplicación
  - ■ Resolver dudas funcionales de usuarios
  - ■ Crear guías de uso sencillas
  - ■ Fomentar la autonomía del usuario
- Documentar la solución y comunicar el resultado
  - ■ Registrar la incidencia en el sistema de ticketing

■ Documentar la solución aplicada
■ Comunicar el resultado al usuario
■ Actualizar la base de conocimiento

■ Medios y recursos

- Aplicaciones corporativas (ERP, CRM, ofimática, etc.)
- Contactos de proveedores de aplicaciones
- Sistema de ticketing para registro de incidencias
- Base de conocimiento de soluciones
- Herramientas de documentación

■ Resultados esperados

- Incidencia de aplicación diagnosticada
- Solución aplicada o workaround implementado
- Usuario capacitado en el uso de la aplicación
- Incidencia documentada y resuelta
- Base de conocimiento actualizada

Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Actividad 11.1 Realizar mantenimiento preventivo de equipos y sistemas

- Ejecutar tareas de mantenimiento programado en servidores
  - ■ Planificar ventanas de mantenimiento
  - ■ Revisar logs de errores y advertencias
  - ■ Limpiar archivos temporales y caché
  - ■ Verificar el espacio disponible en disco
- Realizar mantenimiento en equipos de red
  - ■ Revisar la temperatura de los dispositivos
  - ■ Limpiar filtros de ventilación
  - ■ Verificar la integridad de los cables
  - ■ Actualizar firmware si es necesario
- Aplicar parches de seguridad y actualizaciones
  - ■ Identificar parches de seguridad disponibles
  - ■ Planificar la aplicación de parches
  - ■ Aplicar parches en ventanas de mantenimiento
  - ■ Verificar la funcionalidad tras la aplicación
- Registrar las actuaciones realizadas
  - ■ Documentar las tareas de mantenimiento realizadas
  - ■ Registrar el estado de los equipos
  - ■ Documentar cualquier problema encontrado
  - ■ Actualizar el inventario de equipos

■ Medios y recursos

- Herramientas de monitorización de sistemas
- Herramientas de diagnóstico de hardware
- Documentación de procedimientos de mantenimiento
- Calendario de mantenimiento programado
- Sistema de registro de mantenimiento

■ Resultados esperados

- Mantenimiento preventivo ejecutado según cronograma
- Parches de seguridad aplicados
- Equipos en buen estado de funcionamiento
- Problemas potenciales identificados
- Documentación de mantenimiento actualizada

Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Actividad 11.2 Instalar componentes de hardware en estaciones y servidores

- Montar y sustituir componentes en estaciones de trabajo
  - ■ Apagar el equipo de forma segura
  - ■ Abrir la carcasa del equipo

- Instalar o sustituir componentes (RAM, disco, etc.)
- Cerrar la carcasa y encender el equipo

• Ampliar o sustituir componentes en servidores
- Seguir los procedimientos del fabricante
- Apagar el servidor de forma controlada
- Instalar o sustituir componentes
- Verificar la integridad del sistema

• Verificar el correcto reconocimiento del hardware
- Verificar que el sistema operativo reconoce el nuevo hardware
- Instalar drivers si es necesario
- Realizar pruebas de funcionamiento
- Documentar los cambios realizados

• Actualizar el inventario de equipos
- Registrar los componentes instalados
- Actualizar la configuración del equipo en el inventario
- Documentar la fecha de instalación
- Mantener un registro de cambios

■ **Medios y recursos**

• Componentes de hardware (RAM, disco duro, tarjetas de red, etc.)
• Herramientas de diagnóstico de hardware
• Documentación del fabricante
• Sistema de inventario de equipos
• Herramientas de instalación de drivers

■ **Resultados esperados**

• Componentes instalados correctamente
• Hardware reconocido por el sistema operativo
• Equipo funcionando correctamente
• Inventario actualizado
• Documentación de cambios completada

Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Actividad 11.3 Configurar sistemas según estándares corporativos

• Preparar equipos de usuario según estándares
- Instalar el sistema operativo base
- Aplicar configuraciones de red corporativas
- Instalar software base requerido
- Aplicar políticas de seguridad

• Configurar servidores según estándares
- Instalar el sistema operativo del servidor
- Aplicar configuraciones de red
- Instalar roles y servicios requeridos
- Aplicar políticas de seguridad del servidor

• Instalar y actualizar aplicaciones de software
- Instalar aplicaciones corporativas requeridas
- Configurar aplicaciones según políticas
- Aplicar actualizaciones de software
- Verificar compatibilidades

- Verificar que el sistema cumple requisitos operativos
  - Realizar pruebas de funcionalidad
  - Verificar la conectividad de red
  - Validar el acceso a recursos corporativos
  - Documentar la configuración final

Medios y recursos

- Medios de instalación de sistemas operativos
- Aplicaciones corporativas
- Documentación de estándares de configuración
- Herramientas de diagnóstico
- Sistema de gestión de configuración

Resultados esperados

- Sistema configurado según estándares corporativos
- Software base instalado y actualizado
- Políticas de seguridad aplicadas
- Sistema cumple requisitos operativos
- Documentación de configuración completada

Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Actividad 11.4 Diagnosticar fallos de hardware y software

- Identificar y analizar averías físicas en equipos
  - Recopilar información sobre el fallo
  - Realizar pruebas de diagnóstico de hardware
  - Utilizar herramientas de diagnóstico del fabricante
  - Determinar si el componente requiere reparación o sustitución
- Analizar errores y comportamientos anómalos en software
  - Revisar logs de errores del sistema operativo
  - Analizar logs de aplicaciones
  - Identificar patrones de error
  - Determinar la causa raíz del problema
- Aplicar soluciones correctivas
  - Reparar o sustituir componentes defectuosos
  - Reinstalar software si es necesario
  - Aplicar parches o actualizaciones
  - Validar que el problema se ha resuelto
- Documentar el problema y la resolución
  - Registrar la descripción del problema
  - Documentar los pasos de diagnóstico
  - Documentar la solución aplicada
  - Crear una referencia para futuros problemas similares

Medios y recursos

- Herramientas de diagnóstico de hardware (memtest, CPU-Z, etc.)
- Herramientas de análisis de logs
- Documentación técnica de equipos
- Componentes de reemplazo
- Sistema de registro de problemas

■ **Resultados esperados**

- Fallo diagnosticado y causa raíz identificada
- Solución correctiva aplicada
- Equipo o software funcionando correctamente
- Problema documentado para futuras referencias
- Base de conocimiento actualizada

Función 11: Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Actividad 11.5 Guiar a clientes en instalación de componentes de hardware

- Asistir telefónica o remotamente en instalación
  - ■ Recibir la solicitud de asistencia del cliente
  - ■ Explicar los pasos de instalación de forma clara
  - ■ Guiar al cliente paso a paso
  - ■ Responder a preguntas del cliente
- Proporcionar instrucciones claras y precisas
  - ■ Utilizar lenguaje sencillo y comprensible
  - ■ Proporcionar instrucciones paso a paso
  - ■ Incluir advertencias de seguridad
  - ■ Adaptar las instrucciones al nivel técnico del cliente
- Verificar el resultado de la instalación
  - ■ Solicitar al cliente que verifique el hardware instalado
  - ■ Guiar al cliente en pruebas de funcionamiento
  - ■ Confirmar que el hardware funciona correctamente
  - ■ Resolver problemas si es necesario
- Documentar la asistencia prestada
  - ■ Registrar la solicitud de asistencia
  - ■ Documentar los pasos de instalación realizados
  - ■ Registrar el resultado de la instalación
  - ■ Documentar cualquier problema encontrado

■ **Medios y recursos**

- Herramientas de comunicación (teléfono, chat, correo)
- Documentación de instalación de componentes
- Herramientas de acceso remoto si es necesario
- Sistema de ticketing para registro
- Plantillas de instrucciones de instalación

■ **Resultados esperados**

- Cliente guiado en instalación de hardware
- Instrucciones claras proporcionadas
- Hardware instalado correctamente
- Cliente satisfecho con la asistencia
- Asistencia documentada

Función 12: Operaciones IT, Monitorización y Gestión de Cambios

Función 12: Operaciones IT, Monitorización y Gestión de Cambios

Actividad 12.1 Monitorizar activamente sistemas y redes

- Supervisar continuamente el estado de servidores
  - ■ Configurar herramientas de monitorización (Nagios, Zabbix)
  - ■ Monitorizar CPU, memoria y disco de servidores
  - ■ Configurar alertas para umbrales críticos
  - ■ Analizar tendencias de rendimiento
- Supervisar dispositivos de red y servicios
  - ■ Monitorizar el estado de routers y switches
  - ■ Verificar la disponibilidad de servicios críticos
  - ■ Monitorizar el ancho de banda utilizado
  - ■ Detectar problemas de conectividad
- Detectar y escalar alertas antes de impacto
  - ■ Recibir y analizar alertas de monitorización
  - ■ Investigar la causa de las alertas
  - ■ Escalar problemas críticos inmediatamente
  - ■ Documentar las alertas y acciones tomadas
- Mantener actualizados los dashboards de estado
  - ■ Crear dashboards de monitorización
  - ■ Actualizar los dashboards con datos en tiempo real
  - ■ Mostrar el estado de servicios críticos
  - ■ Facilitar la visualización del estado de infraestructura

■ Medios y recursos

- Herramientas de monitorización (Nagios, Zabbix, Prometheus)
- Herramientas de visualización (Grafana, Kibana)
- Agentes de monitorización en servidores
- Herramientas SNMP para dispositivos de red
- Documentación de umbrales de alerta

■ Resultados esperados

- Monitorización configurada en infraestructura
- Alertas generadas y notificadas
- Problemas detectados proactivamente
- Dashboards de estado actualizados
- Documentación de monitorización completada

Función 12: Operaciones IT, Monitorización y Gestión de Cambios

Actividad 12.2 Aplicar procedimientos ITIL de gestión de cambios y problemas

- Registrar, evaluar y aprobar solicitudes de cambio
  - ■ Recibir solicitudes de cambio de usuarios o equipos
  - ■ Evaluar el impacto del cambio propuesto

- Obtener aprobación de cambios según procedimientos
- Planificar la implementación del cambio

- Coordinar la implementación minimizando impacto
  - Comunicar el cambio a partes interesadas
  - Ejecutar el cambio en ventana de mantenimiento
  - Monitorizar el cambio durante la implementación
  - Validar que el cambio se ha implementado correctamente
- Identificar causas raíz de incidencias recurrentes
  - Analizar incidencias recurrentes
  - Realizar análisis de causa raíz (RCA)
  - Identificar problemas subyacentes
  - Proponer soluciones definitivas
- Documentar resultados y actualizar CMDB
  - Registrar el cambio en la CMDB
  - Documentar los resultados de la implementación
  - Registrar errores conocidos
  - Actualizar la documentación técnica

Medios y recursos

- Herramienta de gestión de cambios (ServiceNow, Jira, etc.)
- CMDB (Configuration Management Database)
- Documentación de procedimientos ITIL
- Plantillas de solicitudes de cambio
- Herramientas de análisis de causa raíz

Resultados esperados

- Solicitudes de cambio registradas y evaluadas
- Cambios implementados según procedimientos
- Impacto minimizado durante implementación
- Causas raíz identificadas y documentadas
- CMDB actualizada con cambios

Función 12: Operaciones IT, Monitorización y Gestión de Cambios

Actividad 12.3 Asegurar ejecución de copias de seguridad y mantenimiento

- Planificar y supervisar trabajos de backup
  - Definir política de backup (frecuencia, retención)
  - Configurar trabajos de backup automatizados
  - Supervisar la ejecución de backups
  - Alertar sobre fallos de backup
- Verificar la integridad de las copias
  - Realizar verificaciones de integridad de backups
  - Analizar logs de backup para detectar errores
  - Validar que los datos se han copiado correctamente
  - Documentar los resultados de verificación
- Realizar pruebas de restauración periódicas
  - Planificar pruebas de restauración
  - Restaurar datos de backups en entorno de prueba
  - Validar que los datos restaurados son correctos
  - Documentar los resultados de las pruebas

- Documentar políticas y resultados de backup
  - ■ Documentar la política de backup
  - ■ Registrar los resultados de cada backup
  - ■ Mantener un registro de pruebas de restauración
  - ■ Comunicar el estado de backups a dirección

■ Medios y recursos

- Herramientas de backup (Veeam, Commvault, Bacula)
- Almacenamiento de backup (disco, cinta, nube)
- Herramientas de verificación de integridad
- Documentación de políticas de backup
- Sistema de registro de backups

■ Resultados esperados

- Política de backup definida e implementada
- Backups ejecutados según cronograma
- Integridad de backups verificada
- Pruebas de restauración realizadas exitosamente
- Documentación de backup actualizada

Función 12: Operaciones IT, Monitorización y Gestión de Cambios

Actividad 12.4 Definir operativas de explotación y gestionar Centro de Control IT

- Elaborar procedimientos operativos estándar
  - ■ Documentar procedimientos de operación diaria
  - ■ Crear guías de resolución de problemas comunes
  - ■ Definir procedimientos de escalado
  - ■ Establecer procedimientos de comunicación
- Definir métricas de seguimiento y cuadros de mando
  - ■ Identificar métricas clave de operación
  - ■ Definir objetivos de disponibilidad y rendimiento
  - ■ Crear cuadros de mando operativos
  - ■ Establecer reportes de estado
- Supervisar el cumplimiento de operativas
  - ■ Verificar que el equipo aplica las operativas
  - ■ Realizar auditorías de cumplimiento
  - ■ Identificar desviaciones y corregirlas
  - ■ Proporcionar formación cuando sea necesario
- Gestionar el Centro de Control IT
  - ■ Supervisar operaciones del centro de control
  - ■ Gestionar turnos operativos
  - ■ Coordinar procedimientos de escalado
  - ■ Elaborar informes de disponibilidad

■ Medios y recursos

- Documentación de procedimientos operativos
- Herramientas de monitorización y alertas
- Herramientas de visualización de métricas
- Sistema de ticketing para incidencias
- Herramientas de comunicación

■ **Resultados esperados**

- Procedimientos operativos documentados
- Métricas de seguimiento definidas
- Cuadros de mando operativos creados
- Cumplimiento de operativas supervisado
- Informes de disponibilidad elaborados

Función 12: Operaciones IT, Monitorización y Gestión de Cambios

Actividad 12.5 Evaluar rendimiento de infraestructura y colaborar en proyectos

- Analizar métricas de rendimiento de infraestructura
  - ■ Recopilar datos de rendimiento de servidores y red
  - ■ Analizar utilización de recursos
  - ■ Identificar cuellos de botella
  - ■ Elaborar informes de rendimiento
- Identificar cuellos de botella y proponer mejoras
  - ■ Analizar métricas para detectar problemas de capacidad
  - ■ Proponer actualizaciones de hardware
  - ■ Justificar las propuestas con datos
  - ■ Estimar el impacto de las mejoras
- Participar en proyectos de modernización
  - ■ Aportar conocimiento técnico en diseño
  - ■ Participar en pruebas de nuevos componentes
  - ■ Coordinar con otros equipos
  - ■ Documentar cambios en la infraestructura
- Coordinar con otros equipos en proyectos
  - ■ Comunicar requisitos técnicos
  - ■ Colaborar en planificación de proyectos
  - ■ Participar en reuniones de proyecto
  - ■ Asegurar integración de cambios

■ **Medios y recursos**

- Herramientas de monitorización y análisis
- Documentación de arquitectura actual
- Herramientas de cálculo de capacidad
- Documentación de estándares técnicos
- Herramientas de gestión de proyectos

■ **Resultados esperados**

- Análisis de rendimiento completado
- Cuellos de botella identificados
- Propuestas de mejora documentadas
- Participación en proyectos completada
- Documentación de cambios actualizada

ANEXO III Marco de competencias

Bloque 1 - Administración de Infraestructura de Red de Capa 2 y Capa 3

Objetivo pedagógico

Capacitar al profesional en el diseño, configuración y optimización de infraestructuras de red de capa 2 y capa 3, garantizando escalabilidad, redundancia y segmentación de la red corporativa.

Actividades

Actividad 1.1 Configurar y mantener switches de red gestionables
Actividad 1.2 Configurar y mantener routers de red corporativos
Actividad 1.3 Diseñar e implementar arquitecturas de red de capa 2
Actividad 1.4 Diseñar e implementar arquitecturas de red de capa 3
Actividad 1.5 Implementar VLANs y Spanning Tree Protocol para segmentación y redundancia

Competencias

Competencias	Indicadores
C1 - Analizar el rendimiento de infraestructuras de red y hardware para identificar cuellos de botella y proponer mejoras técnicas	Elabora informes de rendimiento que incluyen métricas de CPU, memoria, ancho de banda y latencia con recomendaciones cuantificables Identifica y documenta al menos 3 problemas de rendimiento en infraestructura con propuestas de solución justificadas
C2 - Configurar y mantener dispositivos de red (switches y routers) aplicando estándares de seguridad y disponibilidad	Configura correctamente switches y routers con VLAN, ACL y protocolos de redundancia sin interrupciones de servicio Documenta todas las configuraciones realizadas con justificación técnica de parámetros críticos
C3 - Diseñar arquitecturas de red de capa 2 y capa 3 considerando escalabilidad, redundancia y segmentación	Elabora diagramas de topología de red que incluyen esquemas de direccionamiento IP, VLAN y redundancia Justifica decisiones de diseño basadas en requisitos de disponibilidad, rendimiento y seguridad
C4 - Implementar y optimizar protocolos de switching avanzados (STP, VLAN) para evitar bucles y segmentar redes	Configura STP y VLAN con parámetros optimizados verificando ausencia de bucles mediante herramientas de diagnóstico Valida la segmentación de red mediante pruebas de conectividad entre segmentos

Saberes asociados

Conmutación de Capa 2 y Protocolos de Enlace

Fundamentos de Capa 2

- Modelo OSI y funciones de capa 2
- Tramas Ethernet y direccionamiento MAC
- Dominios de colisión y broadcast
- Puentes y switches de red

Configuración de Switches Ethernet

- Puertos de acceso y puertos troncales
- Configuración de velocidad y dúplex
- Configuración de STP en switches
- Gestión de tablas MAC y envejecimiento

VLAN y Segmentación de Red

- Conceptos de VLAN y dominios de broadcast
- Configuración de VLAN en switches
- Puertos troncales (trunk) y etiquetado 802.1Q
- Enrutamiento entre VLAN (inter-VLAN routing)

Spanning Tree Protocol (STP)

- Algoritmo de árbol de expansión
- Elección de puente raíz y puertos raíz
- Estados de puerto en STP
- Optimización de STP y RSTP

Enrutamiento de Capa 3 y Direccionamiento IP

Fundamentos de Capa 3

- Modelo OSI y funciones de capa 3
- Paquetes IP y direccionamiento lógico
- Tablas de enrutamiento y decisiones de reenvío
- Protocolos de capa 3 (IP, ICMP, ARP)

Direccionamiento IP y Subnetting

- Clases de direcciones IP y direcciones privadas
- Máscara de subred y cálculo de subredes
- Notación CIDR y agregación de rutas
- Planificación de esquemas de direccionamiento

Configuración de Routers

- Interfaces de router y configuración de IP
- Rutas estáticas y enrutamiento por defecto
- Tablas de enrutamiento y métricas
- Listas de control de acceso (ACL) básicas

Listas de Control de Acceso (ACL)

- ACL estándar y extendidas
- Filtrado de tráfico por protocolo y puerto
- Aplicación de ACL en interfaces
- Validación y depuración de ACL

Diseño y Arquitectura de Infraestructuras de Red

Principios de Diseño de Red

- Modelos jerárquicos de red (núcleo, distribución, acceso)
- Escalabilidad y crecimiento de infraestructura
- Redundancia y disponibilidad de servicios
- Segmentación de red y dominios de seguridad

Topologías de Red

- Topologías físicas y lógicas
- Topologías de malla, estrella y árbol
- Redundancia en topologías de switching
- Convergencia de topología en cambios de red

Planificación de Infraestructura

- Análisis de requisitos de red
- Capacidad y crecimiento futuro
- Consideraciones de costo y rendimiento
- Documentación de arquitectura de red

Redundancia en Switching

- Redundancia de enlaces y dispositivos
- Prevención de bucles mediante STP
- Convergencia rápida en fallos
- Validación de topología redundante

Análisis de Rendimiento e Identificación de Cuellos de Botella

Métricas de Rendimiento de Red

- Latencia, ancho de banda y jitter
- Utilización de enlaces y dispositivos
- Pérdida de paquetes y retransmisiones
- Convergencia de protocolos de enrutamiento

Herramientas de Análisis de Rendimiento

- Herramientas de monitorización de red (SNMP, NetFlow)
- Analizadores de protocolos (Wireshark, tcpdump)
- Herramientas de diagnóstico (ping, traceroute, iperf)
- Recopilación y análisis de datos de rendimiento

Identificación de Cuellos de Botella

- Análisis de utilización de enlaces
- Identificación de dispositivos saturados
- Análisis de patrones de tráfico
- Correlación de problemas de rendimiento

Propuesta de Mejoras Técnicas

- Optimización de rutas de enrutamiento
- Aumento de capacidad de enlaces
- Mejora de configuración de dispositivos
- Justificación técnica y económica de mejoras

Configuración y Mantenimiento de Dispositivos de Red

Acceso y Gestión de Dispositivos

- Acceso mediante consola, SSH y Telnet
- Autenticación y control de acceso a dispositivos
- Gestión de contraseñas y credenciales
- Backup y restauración de configuraciones

Configuración de Switches

- Configuración de puertos de acceso
- Configuración de puertos troncales
- Configuración de VLAN
- Configuración de STP y RSTP

Configuración de Routers

- Configuración de interfaces
- Configuración de rutas estáticas
- Configuración de ACL
- Configuración de enrutamiento dinámico básico

Actualización de Firmware

- Descarga de firmware de fuentes oficiales
- Planificación de actualización sin impacto
- Procedimiento de actualización de firmware
- Validación de funcionamiento post-actualización

Herramientas y Técnicas de Diagnóstico de Red

Herramientas de Diagnóstico Básicas

- Ping para verificar conectividad
- Traceroute para análisis de ruta
- Ipconfig/ifconfig para configuración de interfaz
- Arp para resolución de direcciones

Analizadores de Protocolos

- Captura de paquetes con Wireshark
- Análisis de capturas de paquetes
- Filtrado de tráfico en capturas
- Identificación de problemas mediante análisis de paquetes

Herramientas de Monitorización

- SNMP para recopilación de métricas
- NetFlow para análisis de tráfico
- Herramientas de monitorización de dispositivos
- Generación de alertas y reportes

Validación de Configuración

- Verificación de conectividad de extremo a extremo
- Validación de tablas de enrutamiento
- Verificación de VLAN y puertos troncales
- Prueba de failover y redundancia

Habilidades actitudinales

- Rigor en la recopilación y análisis de datos de rendimiento de infraestructura
- Precisión en la configuración de dispositivos sin interrupciones de servicio
- Pensamiento sistémico en el diseño de arquitecturas de red
- Validación rigurosa de configuraciones de switching y prevención de bucles

Justificación

Este bloque agrupa competencias fundamentales para la administración de la infraestructura de red física y lógica. Las competencias C1, C2, C3 y C4 comparten la finalidad común de garantizar una infraestructura de red robusta y eficiente. La coherencia funcional radica en que todas ellas abordan aspectos complementarios: análisis de rendimiento (C1), configuración de dispositivos (C2), diseño de arquitecturas (C3) y optimización de protocolos de switching (C4). Los livrables compatibles incluyen diagramas de topología, configuraciones de switches y routers, y documentación de arquitectura. Las situaciones de evaluación incluyen diseño de redes nuevas, optimización de redes existentes, resolución de problemas de conectividad y validación de redundancia.

Ubicación en la progresión

Este bloque constituye el núcleo de la formación en administración de redes, construyendo sobre conocimientos fundamentales de protocolos de red y modelos OSI. Los profesionales aprenden a diseñar y mantener infraestructuras de red que soportan las operaciones corporativas, desde la planificación inicial hasta la optimización continua. El bloque integra tanto aspectos teóricos de arquitectura de red como habilidades prácticas de configuración de dispositivos. Proporciona la base necesaria para abordar posteriormente protocolos de enrutamiento más avanzados y tecnologías especializadas. La progresión dentro del bloque avanza desde el análisis de rendimiento y configuración básica hacia el diseño integral de arquitecturas complejas.

Bloque 2 - Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Objetivo pedagógico

Desarrollar competencias en la configuración e implementación de protocolos de enrutamiento dinámico (OSPF, BGP) y tecnologías avanzadas (MPLS, VPN) para garantizar conectividad optimizada en entornos corporativos complejos.

Actividades

Actividad 2.1 Configurar e implementar OSPF en infraestructuras de red
Actividad 2.2 Configurar peering BGP y políticas de enrutamiento
Actividad 2.3 Gestionar infraestructuras MPLS y servicios VPN

Competencias

Competencias	Indicadores
C5 - Configurar protocolos de enrutamiento dinámico (OSPF, BGP) para optimizar rutas y garantizar convergencia rápida	Implementa OSPF y BGP con áreas, políticas y filtros configurados según requisitos de enrutamiento Verifica convergencia de rutas y optimización de costos mediante análisis de tablas de enrutamiento
C6 - Administrar tecnologías avanzadas de red (MPLS, VPN) para garantizar conectividad segura en entornos corporativos	Configura MPLS con LSPs y VRFs implementando VPN sobre MPLS con validación de túneles activos Documenta topología de MPLS y políticas de enrutamiento con pruebas de conectividad de extremo a extremo

Saberes asociados

Configuración de OSPF y Áreas de Enrutamiento

Fundamentos de OSPF

- Concepto de protocolo de enrutamiento dinámico interior (IGP)
- Algoritmo de estado de enlace (Dijkstra)
- Métricas de costo de OSPF
- Tipos de routers OSPF (ABR, ASBR, DR, BDR)

Configuración de OSPF

- Definición de procesos OSPF
- Configuración de interfaces OSPF
- Establecimiento de adyacencias OSPF
- Configuración de prioridades de router designado
- Ajuste de métricas de costo

Diseño de Áreas OSPF

- Concepto de áreas en OSPF
- Área de backbone (Área 0)
- Áreas estándar, stub y totalmente stub

- Planificación de jerarquía de áreas
- Optimización de propagación de rutas

Optimización de Costes de Enrutamiento

- Cálculo de métricas OSPF
- Ajuste de ancho de banda de referencia
- Manipulación de costos de enlace
- Análisis de tabla de enrutamiento
- Validación de convergencia de rutas

Configuración de BGP y Políticas de Enrutamiento

Fundamentos de BGP

- Concepto de protocolo de enrutamiento exterior (EGP)
- Sistemas autónomos (AS) y números de AS
- Peering BGP interno (iBGP) y externo (eBGP)
- Atributos de ruta BGP
- Proceso de selección de mejor ruta

Configuración de Peering BGP

- Establecimiento de sesiones BGP
- Configuración de vecinos BGP
- Intercambio de información de enrutamiento
- Validación de adyacencias BGP
- Troubleshooting de sesiones BGP

Políticas de Enrutamiento BGP

- Concepto de políticas de enrutamiento
- Route-maps para manipulación de rutas
- Filtros de prefijos
- Manipulación de atributos BGP
- Implementación de políticas de tráfico

Configuración de Route-Maps y Filtros

- Sintaxis de route-maps
- Condiciones de coincidencia (match)
- Acciones de modificación (set)
- Listas de acceso extendidas para filtrado
- Validación de aplicación de políticas

Configuración de MPLS y VPN en Entornos Corporativos

Fundamentos de MPLS

- Concepto de conmutación de etiquetas
- Etiquetas MPLS y forwarding equivalence class (FEC)
- Label switching paths (LSP)
- Ventajas de MPLS sobre enrutamiento IP tradicional
- Arquitectura de MPLS

Configuración de MPLS

- Habilitación de MPLS en interfaces
- Configuración de protocolos de distribución de etiquetas (LDP)
- Establecimiento de LSP
- Verificación de funcionamiento de MPLS
- Troubleshooting de MPLS

Gestión de LSP y VRF

- Label switched paths estáticos y dinámicos

- Routing tables virtuales (VRF)
- Separación de tráfico entre clientes
- Configuración de VRF en routers
- Validación de aislamiento de tráfico

Implementación de VPN sobre MPLS

- MPLS VPN (RFC 2547)
- Arquitectura de MPLS VPN
- Configuración de PE (Provider Edge) y CE (Customer Edge)
- Intercambio de rutas entre sitios de cliente
- Validación de conectividad de extremo a extremo

Teoría de Protocolos de Enrutamiento Dinámico

Conceptos Fundamentales de Enrutamiento

- Tabla de enrutamiento y forwarding
- Métrica de enrutamiento
- Convergencia de enrutamiento
- Bucles de enrutamiento y prevención
- Distancia administrativa

Clasificación de Protocolos de Enrutamiento

- Protocolos de vector distancia (RIP, EIGRP)
- Protocolos de estado de enlace (OSPF, IS-IS)
- Protocolos de enrutamiento exterior (BGP)
- Comparación de características
- Selección de protocolo según requisitos

Ingeniería de Tráfico

- Concepto de ingeniería de tráfico
- Manipulación de rutas para optimizar tráfico
- Load balancing entre múltiples rutas
- Priorización de rutas según requisitos
- Análisis de impacto de cambios de enrutamiento

Diagnóstico y Validación de Enrutamiento

Herramientas de Diagnóstico de Enrutamiento

- Comandos show para verificación de estado
- Análisis de tabla de enrutamiento
- Verificación de adyacencias de protocolo
- Análisis de convergencia
- Captura de paquetes de protocolo de enrutamiento

Validación de Configuración

- Verificación de sintaxis de configuración
- Validación de parámetros de protocolo
- Prueba de conectividad de extremo a extremo
- Análisis de rutas seleccionadas
- Identificación de rutas subóptimas

Troubleshooting de Enrutamiento

- Diagnóstico de problemas de convergencia
- Resolución de bucles de enrutamiento
- Análisis de pérdida de conectividad
- Identificación de problemas de configuración
- Documentación de proceso de resolución

Seguridad en Protocolos de Enrutamiento

Amenazas de Seguridad en Enrutamiento

- Ataques de falsificación de rutas
- Ataques de denegación de servicio (DoS)
- Inyección de rutas maliciosas
- Escucha de actualizaciones de enrutamiento
- Impacto de compromiso de enrutamiento

Mecanismos de Seguridad

- Autenticación de actualizaciones de enrutamiento
- Encriptación de sesiones de enrutamiento
- Filtrado de rutas
- Validación de origen de ruta (RPKI)
- Configuración de listas de acceso para enrutamiento

Habilidades actitudinales

- Validación de convergencia de rutas y comportamiento de failover
- Optimización basada en análisis de datos de tráfico
- Validación de conectividad de extremo a extremo en MPLS
- Documentación completa de configuraciones de enrutamiento

Justificación

Este bloque integra competencias especializadas en enrutamiento dinámico y tecnologías avanzadas de red. Las competencias C5 y C6 comparten el objetivo común de optimizar la conectividad entre sitios y garantizar rutas eficientes. La coherencia funcional se establece en que ambas abordan la configuración de protocolos de enrutamiento: C5 cubre protocolos IGP (OSPF) y EGP (BGP), mientras que C6 aborda tecnologías de nivel superior (MPLS, VPN). Los livrables compatibles incluyen configuraciones de routers, tablas de enrutamiento optimizadas, políticas de enrutamiento y documentación de topología. Las situaciones de evaluación incluyen implementación de OSPF en redes internas, configuración de BGP para peering externo, implementación de MPLS VPN y validación de convergencia de rutas.

Ubicación en la progresión

Este bloque representa la especialización en enrutamiento dinámico, construyendo sobre la comprensión de arquitecturas de red de capa 3 adquirida en bloques anteriores. Los profesionales avanzan desde la configuración de protocolos de enrutamiento estándar hacia la implementación de tecnologías avanzadas que permiten mayor control y optimización del tráfico. El bloque integra conceptos de ingeniería de tráfico, políticas de enrutamiento y aislamiento de tráfico mediante VRF. Proporciona las habilidades necesarias para administrar redes corporativas de múltiples sitios con requisitos complejos de conectividad y seguridad. La progresión avanza desde OSPF (protocolo interior) hacia BGP (protocolo exterior) y finalmente hacia MPLS como tecnología de transporte.

Bloque 3 - Gestión de Calidad de Servicio y Monitorización de Tráfico

Objetivo pedagógico

Capacitar en la implementación y gestión de políticas de Calidad de Servicio (QoS) para priorizar tráfico crítico y garantizar rendimiento de aplicaciones corporativas.

Actividades

Actividad 3.1 Diseñar e implementar políticas de QoS
Actividad 3.2 Configurar monitorización SNMP de infraestructura
Actividad 3.3 Analizar flujos de tráfico con NetFlow y sFlow

Competencias

Competencias	Indicadores
C7 - Aplicar políticas de Calidad de Servicio (QoS) para priorizar tráfico crítico y garantizar rendimiento de aplicaciones	Configura clasificación, marcado y colas de tráfico QoS con umbrales de ancho de banda validados Verifica mediante herramientas de análisis que el tráfico prioritario recibe el tratamiento configurado

Saberes asociados

Fundamentos de Calidad de Servicio (QoS)

Conceptos de QoS

- Definición de QoS y objetivos
- Modelos de servicio: Best Effort, IntServ, DiffServ
- Parámetros de QoS: latencia, jitter, ancho de banda, pérdida de paquetes
- Acuerdos de nivel de servicio (SLA)

Clasificación de tráfico

- Identificación de tipos de tráfico
- Criterios de clasificación: puertos, protocolos, direcciones IP
- Herramientas de clasificación de tráfico
- Mapeo de aplicaciones a clases de servicio

Marcado de tráfico

- Campos de marcado: ToS, DSCP, CoS
- Marcado en capa 2 y capa 3
- Preservación de marcas en tránsito
- Validación de marcas de tráfico

Configuración de Políticas de QoS

Configuración de QoS en dispositivos de red

- Configuración de QoS en switches Ethernet
- Configuración de QoS en routers

- Políticas de entrada y salida
- Validación de configuración de QoS

Gestión de colas de tráfico

- Algoritmos de colas: FIFO, PQ, CQ, WFQ
- Configuración de colas prioritarias
- Limitación de ancho de banda
- Gestión de congestión

Implementación de políticas de QoS

- Creación de listas de control de acceso (ACL) para clasificación
- Configuración de mapas de políticas
- Aplicación de políticas a interfaces
- Validación de aplicación de políticas

Monitorización de Tráfico de Red

Herramientas de monitorización de tráfico

- SNMP para recopilación de métricas
- NetFlow para análisis de flujos
- sFlow para muestreo de tráfico
- Analizadores de protocolos: Wireshark, tcpdump

Análisis de tráfico de red

- Identificación de patrones de tráfico
- Detección de anomalías de tráfico
- Análisis de utilización de ancho de banda
- Identificación de aplicaciones de alto consumo

Reportes de tráfico y capacidad

- Elaboración de reportes de utilización
- Análisis de tendencias de tráfico
- Predicción de necesidades de capacidad
- Presentación de datos de tráfico a stakeholders

Optimización de QoS y Rendimiento

Validación de cumplimiento de QoS

- Pruebas de priorización de tráfico
- Medición de latencia y jitter
- Validación de ancho de banda garantizado
- Pruebas de comportamiento en congestión

Ajuste de políticas de QoS

- Identificación de necesidad de ajustes
- Modificación de parámetros de QoS
- Validación de cambios en producción
- Documentación de ajustes realizados

Mejora continua de QoS

- Análisis de cumplimiento de SLA
- Identificación de oportunidades de mejora
- Propuesta de cambios basados en datos
- Implementación de mejoras de forma controlada

Protocolos de Red y Modelos de Servicio

Protocolos de transporte

- TCP y UDP
- Características de confiabilidad y latencia
- Impacto en requisitos de QoS
- Identificación de protocolos en tráfico

Aplicaciones sensibles a QoS

- Voz sobre IP (VoIP)
- Video en tiempo real
- Aplicaciones de datos críticas
- Requisitos de QoS por aplicación

Diagnóstico y Resolución de Problemas de QoS

Diagnóstico de problemas de QoS

- Identificación de problemas de latencia
- Detección de pérdida de paquetes
- Análisis de jitter en tráfico de voz
- Diagnóstico de congestión de red

Herramientas de diagnóstico de QoS

- Herramientas de medición de latencia
- Analizadores de calidad de voz
- Monitores de ancho de banda
- Herramientas de análisis de flujos

Habilidades actitudinales

- Validación de cumplimiento de requisitos de QoS
- Ajuste iterativo de políticas basado en observación
- Comunicación clara de requisitos de QoS con stakeholders

Justificación

Este bloque se dedica a la competencia especializada de QoS, que es fundamental para garantizar que aplicaciones críticas reciban el ancho de banda y prioridad necesarios. La competencia C7 aborda la clasificación, marcado y gestión de colas de tráfico. Los livrables compatibles incluyen políticas de QoS configuradas, análisis de tráfico prioritario y reportes de cumplimiento de SLA. Las situaciones de evaluación incluyen implementación de QoS en redes congestionadas, validación de priorización de tráfico de voz y video, y ajuste de políticas basado en análisis de tráfico.

Ubicación en la progresión

Este bloque representa una especialización en la optimización del rendimiento de la red mediante control granular del tráfico. Construye sobre la comprensión de arquitecturas de red y protocolos de enrutamiento, añadiendo una capa de gestión de recursos que garantiza que el tráfico crítico recibe tratamiento prioritario. Los profesionales aprenden a identificar tipos de tráfico, clasificarlos según requisitos de negocio y aplicar políticas que aseguran cumplimiento de acuerdos de nivel de servicio. El bloque integra tanto conceptos teóricos de modelos de servicio como habilidades prácticas de configuración de dispositivos de red. Proporciona herramientas para resolver problemas de rendimiento causados por congestión de red.

Bloque 4 - Diagnóstico y Resolución de Incidencias de Red y Conectividad

Objetivo pedagógico

Desarrollar competencias en diagnóstico sistemático de problemas de red y conectividad, utilizando herramientas de análisis y metodologías estructuradas para identificar causa raíz y resolver incidencias.

Actividades

Actividad 4.1 Diagnosticar y resolver incidencias de conectividad de red
Actividad 4.2 Restablecer conectividad de red en puestos de usuario

Competencias

Competencias	Indicadores
C8 - Diagnosticar y resolver incidencias de conectividad de red utilizando herramientas de análisis y capturas de paquetes	Utiliza herramientas como ping, traceroute, tcpdump y analizadores de protocolos para identificar causa raíz de problemas Documenta el proceso de diagnóstico y la solución implementada con evidencia de resolución
C17 - Restablecer conectividad de red e Internet en puestos de usuario resolviendo problemas de Wi-Fi y VPN	Diagnostica y resuelve problemas de conectividad en equipos de usuario verificando conexión exitosa Configura parámetros de red, Wi-Fi y VPN según políticas corporativas

Saberes asociados

Herramientas de Diagnóstico de Red

Herramientas de Diagnóstico Básicas

- Ping para verificación de conectividad
- Traceroute para análisis de ruta de paquetes
- Ipconfig/ifconfig para configuración de interfaces
- Netstat para análisis de conexiones activas
- Nslookup para resolución de nombres DNS

Analizadores de Protocolos

- Wireshark para captura y análisis de paquetes
- Tcpdump para captura de tráfico en línea de comandos
- Interpretación de capturas de paquetes
- Análisis de protocolos de capa 2 y 3
- Identificación de anomalías en tráfico

Herramientas de Análisis de Conectividad

- Arp para resolución de direcciones MAC
- Route para visualización de tabla de enrutamiento
- Telnet para prueba de conectividad de puertos
- Nmap para escaneo de puertos y servicios
- Mtr para análisis combinado de ruta y latencia

Protocolos de Conectividad de Red

Protocolos de Capa 2

- Ethernet y direccionamiento MAC
- VLAN y etiquetado 802.1Q
- Spanning Tree Protocol (STP)
- Link Aggregation (LAG)
- Protocolo de Resolución de Direcciones (ARP)

Protocolos de Capa 3

- IPv4 e IPv6
- Subnetting y CIDR
- Enrutamiento estático y dinámico
- ICMP para diagnóstico
- Protocolo de Control de Transmisión (TCP) y UDP

Protocolos de Acceso Remoto

- Wi-Fi (802.11) y autenticación
- VPN (Virtual Private Network)
- PPP y PPTP
- L2TP y IPSec
- Problemas comunes de conectividad remota

Metodología de Diagnóstico Sistemático

Proceso de Diagnóstico Estructurado

- Recopilación de información del problema
- Reproducción del problema
- Aislamiento de variables
- Prueba de hipótesis
- Identificación de causa raíz

Análisis de Capas OSI

- Diagnóstico de capa física
- Diagnóstico de capa de enlace
- Diagnóstico de capa de red
- Diagnóstico de capa de transporte
- Diagnóstico de capas superiores

Documentación de Diagnóstico

- Registro de síntomas iniciales
- Documentación de pasos de diagnóstico
- Captura de evidencia técnica
- Análisis de causa raíz
- Documentación de solución implementada

Conectividad de Usuario Final

Conectividad Cableada

- Ethernet y cableado estructurado
- Puertos de red en equipos
- Configuración de IP estática y DHCP
- Problemas de cable y conectores
- Validación de conectividad física

Conectividad Inalámbrica

- Redes Wi-Fi corporativas

- Autenticación 802.1X
- Problemas de señal y cobertura
- Roaming entre puntos de acceso
- Diagnóstico de problemas Wi-Fi

Conectividad Remota

- Clientes VPN
- Configuración de VPN en equipos
- Problemas de conexión VPN
- Autenticación remota
- Validación de túneles VPN

Comunicación Efectiva con Usuarios

Comunicación Técnica Adaptada

- Explicación de problemas técnicos en lenguaje simple
- Evitar jerga técnica innecesaria
- Adaptación al nivel de conocimiento del usuario
- Claridad en instrucciones paso a paso
- Confirmación de comprensión del usuario

Gestión de Expectativas

- Estimación realista de tiempo de resolución
- Comunicación de avances en diagnóstico
- Explicación de limitaciones técnicas
- Propuesta de soluciones alternativas
- Confirmación de resolución satisfactoria

Profesionalismo en Interacción

- Escucha activa de preocupaciones del usuario
- Paciencia ante usuarios frustrados
- Tono profesional y respetuoso
- Evitar culpabilización del usuario
- Seguimiento post-resolución

Gestión de Incidencias de Conectividad

Registro y Seguimiento de Incidencias

- Apertura de tickets de incidencia
- Clasificación de severidad
- Asignación de prioridad
- Seguimiento de estado
- Cierre de incidencia con documentación

Escalado de Problemas

- Identificación de problemas que requieren escalado
- Comunicación clara con niveles superiores
- Provisión de información completa para escalado
- Seguimiento de casos escalados
- Aprendizaje de resoluciones escaladas

Análisis de Incidencias Recurrentes

- Identificación de patrones de problemas
- Análisis de causa raíz de incidencias recurrentes
- Propuesta de soluciones permanentes
- Documentación de soluciones
- Capacitación de usuarios para prevención

Habilidades actitudinales

- Uso sistemático de herramientas de diagnóstico apropiadas
- Documentación completa de proceso de diagnóstico y resolución
- Comunicación clara con usuarios durante diagnóstico
- Configuración de conectividad según políticas corporativas

Justificación

Este bloque integra competencias de diagnóstico de red a nivel de infraestructura (C8) y a nivel de usuario final (C17). Ambas competencias comparten la finalidad común de restablecer conectividad mediante diagnóstico sistemático. La coherencia funcional radica en que C8 proporciona habilidades de diagnóstico profundo con herramientas avanzadas, mientras que C17 aplica estas habilidades a problemas específicos de usuarios finales. Los livrables compatibles incluyen reportes de diagnóstico, análisis de capturas de paquetes y documentación de resolución. Las situaciones de evaluación incluyen diagnóstico de problemas de conectividad de red, análisis de capturas de paquetes, resolución de problemas de Wi-Fi y VPN en puestos de usuario.

Ubicación en la progresión

Este bloque representa las habilidades esenciales de troubleshooting que permiten al profesional mantener la disponibilidad de la red. Construye sobre la comprensión de arquitecturas de red y protocolos adquirida en bloques anteriores, añadiendo metodologías sistemáticas de diagnóstico. Los profesionales aprenden a utilizar herramientas de análisis de red, interpretar datos de diagnóstico e identificar causa raíz de problemas. El bloque integra tanto diagnóstico a nivel de infraestructura como resolución de problemas de conectividad de usuarios finales. Proporciona las habilidades necesarias para responder rápidamente a incidencias y minimizar tiempo de inactividad. La progresión avanza desde herramientas básicas de diagnóstico hacia análisis profundo con capturas de paquetes.

Bloque 5 - Automatización de Tareas de Red y Sistemas

Objetivo pedagógico

Capacitar en el desarrollo de scripts y playbooks para automatizar tareas recurrentes de administración de red y sistemas, mejorando eficiencia y reduciendo errores manuales.

Actividades

Actividad 5.1 Desarrollar scripts Python para automatización de tareas de red
Actividad 5.2 Crear y mantener playbooks Ansible para automatización

Competencias

Competencias	Indicadores
C9 - Automatizar tareas de administración de red y sistemas mediante scripts y herramientas de orquestación	Desarrolla scripts en Python o playbooks en Ansible que automatizan al menos 3 tareas recurrentes de red Documenta código con comentarios explicativos y valida ejecución sin errores en entorno de prueba

Saberes asociados

Programación en Python para Automatización de Red

Fundamentos de Python

- Sintaxis y estructura de Python
- Variables, tipos de datos y operadores
- Estructuras de control (if, for, while)
- Funciones y módulos
- Manejo de excepciones

Librerías de Red en Python

- Netmiko para automatización de dispositivos Cisco
- Paramiko para conexiones SSH
- Requests para APIs REST
- Scapy para análisis de paquetes
- Napalm para abstracción de dispositivos

Desarrollo de Scripts de Automatización

- Conexión a dispositivos de red
- Envío de comandos y recopilación de salida
- Procesamiento de datos de configuración
- Generación de reportes automatizados
- Manejo de errores y validación

Orquestación con Ansible

Conceptos Fundamentales de Ansible

- Arquitectura sin agentes de Ansible
- Inventarios y variables

- Módulos de red (ios, eos, junos)
- Módulos de sistemas (command, shell, copy)
- Módulos de configuración (template, lineinfile)

Desarrollo de Playbooks

- Estructura de playbooks YAML
- Tareas y handlers
- Condicionales y bucles
- Roles y estructura modular
- Uso de variables y templates Jinja2

Integración en Pipelines CI/CD

- Integración con Jenkins
- Integración con GitLab CI
- Integración con GitHub Actions
- Control de versiones de playbooks
- Validación y testing de playbooks

Conceptos de Automatización de Red

Patrones de Automatización

- Identificación de tareas repetitivas
- Diseño de flujos de automatización
- Manejo de cambios de configuración
- Validación de cambios
- Rollback y recuperación

APIs de Dispositivos de Red

- APIs REST en dispositivos modernos
- NETCONF y YANG
- APIs propietarias de fabricantes
- Autenticación y autorización
- Manejo de respuestas y errores

Mejores Prácticas de Automatización

- Idempotencia en automatización
- Documentación de scripts
- Versionado de código
- Testing de automatización
- Seguridad en credenciales

Documentación de Código y Automatización

Documentación de Scripts

- Comentarios explicativos en código
- Docstrings en funciones
- README y guías de uso
- Ejemplos de ejecución
- Parámetros y opciones

Documentación de Playbooks

- Descripción de playbooks
- Documentación de variables
- Documentación de roles
- Ejemplos de invocación
- Requisitos y dependencias

Mantenimiento de Documentación

- Actualización con cambios de código
- Control de versiones de documentación
- Revisión de documentación
- Accesibilidad de documentación
- Archivos de cambios (changelog)

Testing y Validación de Automatización

Testing de Scripts Python

- Pruebas unitarias con unittest
- Pruebas con pytest
- Mocking de dispositivos de red
- Pruebas de integración
- Cobertura de código

Validación de Playbooks

- Sintaxis YAML
- Validación de playbooks
- Ejecución en modo dry-run
- Testing en entorno de prueba
- Validación de resultados

Entornos de Prueba

- Laboratorios virtuales
- Emuladores de dispositivos
- Contenedores para testing
- Máquinas virtuales de prueba
- Datos de prueba realistas

Habilidades actitudinales

- Validación rigurosa de scripts y playbooks antes de producción
- Documentación completa de código y automatización
- Desarrollo de código limpio y mantenible

Justificación

Este bloque se dedica a la competencia de automatización mediante Python y Ansible. La competencia C9 aborda tanto programación en Python como configuración de Ansible para automatizar tareas de red. Los livrables compatibles incluyen scripts Python funcionales, playbooks de Ansible documentados e integración en pipelines CI/CD. Las situaciones de evaluación incluyen desarrollo de scripts para backup de configuraciones, automatización de aplicación de configuraciones, recopilación de información de dispositivos y generación de reportes.

Ubicación en la progresión

Este bloque representa la evolución hacia prácticas modernas de administración de infraestructura mediante automatización. Construye sobre la comprensión de tareas de administración de red adquirida en bloques anteriores, añadiendo habilidades de programación y orquestación. Los profesionales aprenden a identificar tareas repetitivas, desarrollar scripts que las automatizan y validar ejecución sin errores. El bloque integra tanto lenguajes de programación como herramientas de orquestación especializadas en infraestructura. Proporciona las habilidades necesarias para escalar operaciones de red a entornos grandes y complejos. La progresión avanza desde scripts simples en Python hacia playbooks complejos en Ansible con integración en pipelines de entrega continua.

Bloque 6 - Gestión de Incidencias y Coordinación con Proveedores

Objetivo pedagógico

Desarrollar competencias en gestión de incidencias complejas y coordinación efectiva con proveedores externos y fabricantes de equipos para garantizar resolución oportuna.

Actividades

Actividad 6.1 Coordinar resolución de incidencias con proveedores externos
Actividad 6.2 Gestionar casos de soporte con fabricantes de equipos
Actividad 6.3 Gestionar incidencias críticas de alto impacto

Competencias

Competencias	Indicadores
C10 - Coordinar la resolución de incidencias complejas con proveedores externos y fabricantes de equipos	Abre y realiza seguimiento de casos de soporte con proveedores documentando cada interacción y estado Escala problemas apropiadamente y comunica soluciones a equipos técnicos internos

Saberes asociados

Gestión de Incidencias y Procesos de Escalado

Ciclo de vida de incidencias

- Registro y clasificación de incidencias
- Priorización según impacto y urgencia
- Asignación y seguimiento de casos
- Cierre y documentación de resolución

Criterios de escalado a proveedores

- Identificación de problemas fuera del alcance interno
- Determinación de nivel de urgencia
- Selección de proveedor apropiado
- Documentación de motivo de escalado

Procesos de soporte de proveedores

- Apertura de casos de soporte técnico
- Niveles de soporte (L1, L2, L3)
- Acuerdos de nivel de servicio (SLA)
- Seguimiento de estado de casos

Comunicación Técnica con Proveedores Externos

Comunicación técnica clara y precisa

- Descripción detallada de síntomas y comportamiento
- Documentación de pasos reproducibles

- Proporcionar información de contexto relevante
- Utilizar terminología técnica apropiada

Gestión de comunicación con múltiples proveedores

- Coordinación entre proveedores diferentes
- Seguimiento de múltiples casos simultáneamente
- Consolidación de información de múltiples fuentes
- Comunicación de estado a stakeholders internos

Documentación de interacciones con proveedores

- Registro de cada contacto y comunicación
- Documentación de información proporcionada
- Registro de soluciones sugeridas
- Archivo de evidencia técnica compartida

Análisis de Problemas Complejos y Diagnóstico Profundo

Metodología de diagnóstico estructurado

- Recopilación de información inicial del problema
- Formulación de hipótesis de causa raíz
- Prueba sistemática de hipótesis
- Validación de causa raíz identificada

Análisis de información técnica de proveedores

- Interpretación de reportes técnicos
- Análisis de logs y trazas de error
- Evaluación de recomendaciones de proveedores
- Validación de soluciones propuestas

Identificación de patrones en incidencias

- Análisis de incidencias recurrentes
- Identificación de causas comunes
- Propuesta de soluciones preventivas
- Documentación de lecciones aprendidas

Habilidades de Coordinación y Gestión de Relaciones

Coordinación efectiva con proveedores

- Establecimiento de canales de comunicación claros
- Respuesta oportuna a solicitudes de información
- Mantenimiento de comunicación regular sobre estado
- Escalado apropiado cuando es necesario

Gestión de expectativas y plazos

- Comunicación clara de plazos esperados
- Seguimiento de compromisos de proveedores
- Gestión de retrasos y cambios de cronograma
- Documentación de acuerdos de tiempo

Profesionalismo en relaciones comerciales

- Mantenimiento de tono profesional en comunicaciones
- Resolución constructiva de desacuerdos
- Reconocimiento de limitaciones de proveedores
- Construcción de relaciones de confianza a largo plazo

Documentación y Trazabilidad de Incidencias

Registro completo de incidencias

- Documentación de descripción inicial del problema
- Registro de pasos de diagnóstico realizados
- Documentación de información proporcionada a proveedores
- Registro de soluciones recibidas y implementadas

Trazabilidad de comunicaciones

- Archivo de correos y comunicaciones con proveedores
- Registro de llamadas telefónicas y reuniones
- Documentación de referencias de casos de proveedores
- Mantenimiento de cronología de eventos

Compartir conocimiento con equipo

- Documentación de soluciones para referencia futura
- Elaboración de guías basadas en casos resueltos
- Comunicación de lecciones aprendidas al equipo
- Actualización de base de conocimiento

Conocimiento Técnico de Infraestructura y Dispositivos

Conocimiento de dispositivos de red

- Características y limitaciones de switches
- Características y limitaciones de routers
- Firmware y versiones de dispositivos
- Compatibilidad entre dispositivos

Conocimiento de servicios corporativos

- Servicios de servidor críticos
- Aplicaciones corporativas comunes
- Dependencias entre servicios
- Impacto de problemas en operaciones

Conocimiento de estándares y regulaciones

- Estándares de disponibilidad corporativos
- Requisitos de cumplimiento normativo
- Políticas de seguridad de la empresa
- Procedimientos de escalado establecidos

Habilidades actitudinales

- Escalado apropiado de problemas a proveedores
- Comunicación clara y técnica con proveedores
- Documentación completa de interacciones con proveedores

Justificación

Este bloque se dedica a la competencia de coordinación con proveedores y gestión de incidencias de alto nivel. La competencia C10 aborda apertura de casos de soporte, seguimiento de incidencias y comunicación técnica con proveedores. Los livrables compatibles incluyen casos de soporte documentados, registros de comunicación con proveedores y soluciones implementadas. Las situaciones de evaluación incluyen escalado de problemas a proveedores, seguimiento de casos de soporte, coordinación de pruebas con fabricantes y documentación de soluciones.

Ubicación en la progresión

Este bloque representa la capacidad de gestionar incidencias que requieren coordinación externa, construyendo sobre habilidades de diagnóstico y resolución de problemas. Los profesionales aprenden a identificar cuándo escalar a proveedores, proporcionar información completa para facilitar resolución y mantener comunicación efectiva durante el proceso. El bloque integra procesos de gestión de incidencias con habilidades de comunicación técnica. Proporciona las herramientas necesarias para resolver problemas complejos que están fuera del alcance de la organización interna. La progresión avanza desde diagnóstico interno hacia escalado estratégico y coordinación con múltiples proveedores.

Bloque 7 - Documentación, Auditoría y Mejora Continua

Objetivo pedagógico

Capacitar en la documentación de infraestructura, preparación de auditorías, gestión de certificados y propuesta de mejoras continuas para garantizar trazabilidad, cumplimiento normativo y optimización de servicios.

Actividades

Actividad 7.1 Documentar procedimientos técnicos y configuraciones
Actividad 7.2 Facilitar auditorías técnicas de sistemas y redes
Actividad 7.3 Proponer e implementar mejoras continuas

Competencias

Competencias	Indicadores
C11 - Documentar procedimientos técnicos, configuraciones y cambios de infraestructura para asegurar trazabilidad y continuidad	Elabora documentación técnica clara que incluye procedimientos paso a paso, diagramas y justificación de cambios Mantiene registro de control de cambios con versiones, fechas y responsables identificados
C12 - Preparar y ejecutar auditorías técnicas de sistemas y redes cumpliendo estándares de seguridad y regulatorios	Recopila información técnica requerida para auditorías y prepara evidencia de cumplimiento de estándares Implementa acciones correctivas identificadas en auditorías con seguimiento de cierre
C13 - Gestionar certificados digitales y provisiones de sistemas monitoreando vigencia y renovación	Mantiene inventario de certificados digitales con fechas de vencimiento y realiza renovaciones antes de expiración Automatiza o documenta proceso de provisión de sistemas con checklist de configuración completado
C19 - Proponer mejoras continuas en procesos y servicios IT realizando análisis coste-beneficio y presentando propuestas	Identifica oportunidades de mejora en procesos IT y elabora propuestas con análisis de impacto y ROI Presenta propuestas a stakeholders con datos cuantitativos y justificación técnica

Saberes asociados

Documentación Técnica de Infraestructura

Procedimientos de Documentación

- Estructura de documentación técnica
- Plantillas de procedimientos
- Estándares de nomenclatura
- Control de versiones de documentación
- Actualización de documentación

Documentación de Configuraciones

- Registro de cambios de configuración
- Documentación de parámetros de dispositivos

- Diagramas de topología de red
- Inventarios de infraestructura
- Mapeo de servicios y dependencias

Trazabilidad y Auditoría

- Registro de cambios realizados
- Justificación de decisiones técnicas
- Historial de modificaciones
- Evidencia de cumplimiento
- Cadena de custodia de documentación

Auditoría Técnica y Cumplimiento Normativo

Estándares de Seguridad y Regulatorios

- Normativas de seguridad de información
- Estándares ISO 27001 y 27002
- Regulaciones de protección de datos
- Requisitos de cumplimiento sectorial
- Marcos de gobernanza IT

Procesos de Auditoría

- Planificación de auditorías
- Recopilación de evidencia
- Evaluación de conformidad
- Identificación de no conformidades
- Elaboración de reportes de auditoría

Gestión de Certificados Digitales

- Ciclo de vida de certificados SSL/TLS
- Monitorización de vigencia
- Renovación de certificados
- Gestión de cadenas de certificados
- Revocación de certificados

Mejora Continua y Optimización

Identificación de Oportunidades de Mejora

- Análisis de métricas de rendimiento
- Identificación de cuellos de botella
- Evaluación de eficiencia operativa
- Análisis de incidencias recurrentes
- Benchmarking con mejores prácticas

Análisis Coste-Beneficio

- Cálculo de costos de inversión
- Estimación de beneficios operativos
- Análisis de retorno de inversión (ROI)
- Evaluación de riesgos de cambio
- Presentación de propuestas ejecutivas

Implementación de Mejoras

- Planificación de cambios
- Validación de mejoras
- Medición de impacto
- Documentación de lecciones aprendidas
- Escalado de mejoras exitosas

Herramientas y Técnicas de Auditoría

Herramientas de Evaluación de Seguridad

- Escáneres de vulnerabilidades
- Herramientas de análisis de configuración
- Validadores de cumplimiento
- Herramientas de auditoría de acceso
- Analizadores de políticas de seguridad

Técnicas de Recopilación de Evidencia

- Entrevistas con stakeholders
- Revisión de logs y registros
- Inspección de configuraciones
- Pruebas de controles de seguridad
- Validación de procedimientos

Comunicación con Stakeholders y Presentación de Resultados

Comunicación de Hallazgos de Auditoría

- Presentación de no conformidades
- Explicación de riesgos identificados
- Recomendaciones de remediación
- Comunicación de urgencia de acciones
- Seguimiento de planes de acción

Presentación de Propuestas de Mejora

- Justificación técnica de propuestas
- Presentación de análisis coste-beneficio
- Comunicación de impacto esperado
- Respuesta a objeciones
- Obtención de aprobación ejecutiva

Rigor y Profesionalismo

- Precisión en recopilación de datos
- Objetividad en evaluación
- Integridad en reportes
- Confidencialidad de información sensible
- Cumplimiento de plazos de auditoría

Gestión de Cambios y Control de Configuración

Procesos de Gestión de Cambios

- Solicitud de cambios (RFC)
- Evaluación de impacto de cambios
- Planificación de implementación
- Validación post-cambio
- Documentación de cambios realizados

Control de Configuración

- Línea base de configuración
- Gestión de versiones
- Auditoría de configuración
- Detección de cambios no autorizados
- Recuperación de configuración anterior

Habilidades actitudinales

- Documentación completa y clara de procedimientos y cambios
- Mantenimiento de documentación actualizada
- Preparación proactiva para auditorías
- Monitorización proactiva de vigencia de certificados
- Identificación y presentación de mejoras basadas en datos

Justificación

Este bloque agrupa competencias transversales de documentación, auditoría y mejora continua. Las competencias C11, C12, C13 y C19 comparten la finalidad común de garantizar que la infraestructura está documentada, cumple estándares regulatorios y se mejora continuamente. La coherencia funcional radica en que todas ellas abordan aspectos de gobernanza: C11 documenta procedimientos y cambios, C12 prepara auditorías, C13 gestiona certificados, y C19 propone mejoras. Los livrables compatibles incluyen documentación técnica, reportes de auditoría, inventarios de certificados y propuestas de mejora. Las situaciones de evaluación incluyen elaboración de documentación de procedimientos, preparación para auditorías de seguridad, gestión de renovación de certificados y presentación de propuestas de mejora.

Ubicación en la progresión

Este bloque representa las prácticas de gobernanza y mejora continua que aseguran la sostenibilidad y conformidad de la infraestructura IT. Construye sobre todas las competencias técnicas anteriores, añadiendo procesos de documentación, auditoría y mejora. Los profesionales aprenden a documentar decisiones técnicas, preparar evidencia de cumplimiento normativo, gestionar ciclo de vida de certificados y proponer mejoras basadas en datos. El bloque integra tanto procesos de gobernanza como habilidades de comunicación con stakeholders. Proporciona las herramientas necesarias para demostrar conformidad regulatoria y justificar inversiones en mejora. La progresión avanza desde documentación básica hacia auditorías complejas y propuestas estratégicas de mejora.

Bloque 8 - Administración de Sistemas Operativos y Servicios de Servidor

Objetivo pedagógico

Desarrollar competencias en administración de sistemas operativos de servidor (Windows Server y Linux) incluyendo configuración de roles, servicios y aplicación de actualizaciones de seguridad.

Actividades

Actividad 8.1 Administrar sistemas operativos de servidor Windows y Linux
Actividad 8.2 Administrar servicios DNS y DHCP
Actividad 8.3 Instalar y configurar servicios web, correo y transferencia de archivos
Actividad 8.4 Implantar y administrar bases de datos en producción

Competencias

Competencias	Indicadores
C20 - Administrar sistemas operativos de servidor (Windows y Linux) configurando roles, servicios y actualizaciones	Instala y configura Windows Server y Linux con roles y servicios requeridos según especificaciones Aplica actualizaciones de seguridad y parches de forma planificada documentando cambios

Saberes asociados

Sistemas Operativos de Servidor

Windows Server

- Instalación y configuración inicial de Windows Server
- Roles y características de Windows Server
- Servicios de directorio y autenticación
- Gestión de usuarios y grupos locales
- Configuración de red y TCP/IP
- Gestión de discos y almacenamiento
- Actualizaciones de seguridad y parches

Linux

- Instalación de distribuciones Linux (CentOS, Ubuntu, Debian)
- Estructura de directorios y sistema de archivos
- Gestión de usuarios y permisos
- Configuración de red en Linux
- Gestión de paquetes y actualizaciones
- Servicios y demonios en Linux
- Línea de comandos y scripts básicos

Roles y Servicios de Servidor

Configuración de Roles en Windows Server

- Instalación de roles mediante Server Manager
- Configuración de servicios de red
- Gestión de características adicionales
- Validación de roles instalados
- Documentación de configuración de roles

Servicios en Linux

- Instalación de servicios mediante gestor de paquetes
- Configuración de servicios del sistema
- Gestión de demonios y servicios
- Validación de servicios activos
- Documentación de servicios configurados

Actualizaciones y Parches de Seguridad

Gestión de Actualizaciones en Windows

- Descarga de actualizaciones de fuentes oficiales
- Planificación de ventanas de mantenimiento
- Instalación de parches de seguridad
- Validación de funcionamiento post-actualización
- Rollback en caso de problemas

Gestión de Actualizaciones en Linux

- Actualización de paquetes del sistema
- Aplicación de parches de seguridad
- Gestión de dependencias
- Validación de servicios después de actualización
- Planificación de mantenimiento

Documentación y Trazabilidad de Configuración

Documentación de Servidores

- Registro de roles y características instalados
- Documentación de configuración de servicios
- Inventario de servidores
- Registro de cambios realizados
- Mantenimiento de documentación actualizada

Trazabilidad de Cambios

- Registro de fecha y hora de cambios
- Documentación de usuario que realizó cambio
- Justificación de cambios realizados
- Registro de impacto de cambios
- Auditoría de cambios

Planificación y Validación de Cambios

Planificación de Cambios sin Impacto

- Identificación de ventanas de mantenimiento
- Evaluación de impacto de cambios
- Realización de backup antes de cambios
- Comunicación de cambios a stakeholders
- Plan de rollback

Validación de Cambios

- Prueba en entorno de prueba antes de producción
- Validación de funcionamiento esperado

- Verificación de servicios críticos
- Confirmación de cambio exitoso
- Documentación de resultados

Herramientas de Administración de Servidores

Herramientas de Windows Server

- Server Manager para gestión centralizada
- PowerShell para administración automatizada
- Event Viewer para análisis de eventos
- Performance Monitor para monitorización
- Disk Management para gestión de almacenamiento

Herramientas de Linux

- Línea de comandos y shell scripting
- Gestores de paquetes (apt, yum, dnf)
- Herramientas de monitorización (top, htop, iostat)
- Logs del sistema (/var/log)
- Herramientas de diagnóstico de red

Habilidades actitudinales

- Planificación de cambios sin impacto en servicios
- Documentación completa de configuración de servidores
- Aplicación de actualizaciones de forma segura y planificada

Justificación

Este bloque se dedica a la competencia de administración de sistemas operativos de servidor. La competencia C20 aborda instalación, configuración de roles y características, y gestión de actualizaciones en Windows Server y Linux. Los livrables compatibles incluyen servidores configurados según especificaciones, documentación de roles instalados e inventario de servidores. Las situaciones de evaluación incluyen instalación de Windows Server con roles específicos, instalación de Linux con servicios requeridos, aplicación de actualizaciones de seguridad y validación de configuración.

Ubicación en la progresión

Este bloque representa las habilidades fundamentales de administración de servidores que soportan toda la infraestructura IT. Construye sobre conocimientos de sistemas operativos y servicios de red, proporcionando habilidades prácticas de instalación y configuración. Los profesionales aprenden a instalar sistemas operativos, configurar roles y servicios según requisitos, y mantener servidores actualizados con parches de seguridad. El bloque integra tanto aspectos de Windows Server como Linux, permitiendo administración de entornos heterogéneos. Proporciona la base necesaria para administrar servicios especializados como web, correo y bases de datos. La progresión avanza desde instalación básica hacia configuración compleja de roles y servicios.

Bloque 9 - Administración de Directorios, Virtualización y Seguridad de Acceso

Objetivo pedagógico

Capacitar en la administración de Active Directory, gestión de virtualización VMware y configuración de políticas de seguridad para garantizar control de acceso y optimización de recursos.

Actividades

Actividad 9.1 Administrar Active Directory y políticas de grupo
Actividad 9.2 Administrar plataformas de virtualización VMware
Actividad 9.3 Administrar y configurar soluciones VPN corporativas
Actividad 9.4 Administrar firewalls y gestionar certificados digitales

Competencias

Competencias	Indicadores

Saberes asociados

Administración de Active Directory y Directorios LDAP

Estructura y Componentes de Active Directory

- Dominios, árboles y bosques
- Unidades Organizativas (OU)
- Objetos de usuario, grupo y equipo
- Esquema de Active Directory
- Catálogo Global

Gestión de Usuarios y Grupos

- Creación y modificación de cuentas de usuario
- Gestión de grupos de seguridad y distribución
- Asignación de permisos y derechos de usuario
- Gestión de perfiles de usuario
- Delegación de administración

Políticas de Grupo (GPO)

- Creación y vinculación de GPO
- Políticas de contraseña y bloqueo de cuenta
- Políticas de software y actualizaciones
- Políticas de seguridad local
- Filtrado de GPO y WMI

Replicación y Sincronización de Directorios

- Replicación de Active Directory
- Sitios y subredes
- Sincronización de directorios con sistemas externos

- Herramientas de sincronización de directorios

Virtualización con VMware vSphere

Arquitectura de VMware vSphere

- Componentes de vSphere: ESXi, vCenter, vSAN
- Máquinas virtuales y plantillas
- Almacenamiento virtual (datastores)
- Redes virtuales y switches distribuidos

Administración de Máquinas Virtuales

- Creación y clonación de máquinas virtuales
- Configuración de recursos (CPU, memoria, disco)
- Snapshots y recuperación de máquinas virtuales
- Migración de máquinas virtuales (vMotion)
- Gestión del ciclo de vida de máquinas virtuales

Optimización de Recursos Virtuales

- Monitorización de utilización de recursos
- Balanceo de carga entre hosts
- Reserva y límite de recursos
- Ajuste de configuración de máquinas virtuales
- Análisis de capacidad y planificación

Alta Disponibilidad y Recuperación ante Desastres

- Clustering con vSphere HA
- Replicación de máquinas virtuales
- Planes de recuperación ante desastres
- Backup y restauración de máquinas virtuales

Control de Acceso y Políticas de Seguridad

Autenticación y Autorización

- Métodos de autenticación (contraseña, multifactor, biométrica)
- Modelos de autorización (RBAC, ABAC)
- Integración de autenticación con directorios
- Gestión de credenciales y secretos

Políticas de Contraseña y Seguridad de Acceso

- Requisitos de complejidad de contraseña
- Políticas de expiración y cambio de contraseña
- Bloqueo de cuenta por intentos fallidos
- Auditoría de intentos de acceso
- Gestión de acceso privilegiado (PAM)

Control de Acceso a Recursos

- Permisos de archivo y carpeta
- Listas de control de acceso (ACL)
- Permisos de impresora y dispositivos
- Acceso a aplicaciones corporativas
- Auditoría de acceso a recursos

Cumplimiento Normativo y Auditoría de Seguridad

- Estándares de seguridad (ISO 27001, NIST)
- Regulaciones de protección de datos (RGPD, LOPD)
- Auditoría de políticas de seguridad
- Reportes de cumplimiento normativo
- Gestión de riesgos de seguridad

Integración de Directorios y Sincronización de Identidades

Sincronización de Directorios

- Sincronización de Active Directory con Azure AD
- Sincronización con sistemas LDAP externos
- Herramientas de sincronización (Azure AD Connect, DirSync)
- Resolución de conflictos de sincronización
- Monitorización de sincronización

Gestión de Identidades Federadas

- Federación de identidades entre dominios
- Confianzas de dominio
- Single Sign-On (SSO)
- Integración con proveedores de identidad externos

Provisión y Desprovisión de Usuarios

- Procesos de onboarding de usuarios
- Automatización de provisión de cuentas
- Procesos de offboarding y desprovisión
- Auditoría de ciclo de vida de usuarios

Implementación de Políticas de Seguridad y Conformidad

Políticas de Seguridad Corporativa

- Políticas de uso aceptable
- Políticas de acceso remoto y VPN
- Políticas de dispositivos móviles
- Políticas de cifrado de datos
- Políticas de auditoría y logging

Implementación de Controles de Seguridad

- Controles de acceso físico
- Controles de acceso lógico
- Cifrado de datos en tránsito y en reposo
- Auditoría y logging de eventos de seguridad
- Detección y prevención de intrusiones

Gestión de Incidentes de Seguridad

- Detección de incidentes de seguridad
- Respuesta a incidentes
- Análisis forense
- Documentación de incidentes
- Mejora continua basada en incidentes

Monitorización y Auditoría de Directorios y Acceso

Monitorización de Active Directory

- Monitorización de replicación de AD
- Alertas de cambios en objetos de directorio
- Monitorización de rendimiento de AD
- Herramientas de monitorización de AD

Auditoría de Acceso y Cambios

- Auditoría de cambios en directorios
- Auditoría de intentos de acceso
- Auditoría de cambios en políticas de seguridad
- Análisis de logs de auditoría

- Reportes de auditoría

Monitorización de Máquinas Virtuales

- Monitorización de rendimiento de máquinas virtuales
- Alertas de utilización de recursos
- Monitorización de disponibilidad
- Análisis de tendencias de capacidad

Habilidades actitudinales

- Diseño de estructura de directorios lógica y escalable
- Implementación de políticas de seguridad mediante GPO
- Optimización de recursos virtuales

Justificación

Este bloque agrupa competencias de administración de directorios y virtualización. Las competencias C31 (Active Directory) y C30 (VMware) comparten la finalidad común de proporcionar infraestructura de soporte para servicios corporativos. La coherencia funcional radica en que ambas abordan aspectos de gestión centralizada: C31 gestiona usuarios y políticas de acceso, mientras que C30 gestiona recursos virtuales. Los livrables compatibles incluyen estructura de Active Directory configurada, políticas de grupo implementadas, máquinas virtuales optimizadas y documentación de infraestructura. Las situaciones de evaluación incluyen creación de estructura de OU, implementación de GPO, gestión de máquinas virtuales y optimización de recursos virtuales.

Ubicación en la progresión

Este bloque representa la infraestructura de soporte que permite la administración centralizada de usuarios y recursos en entornos corporativos. Construye sobre conocimientos de sistemas operativos de servidor, añadiendo capacidades de gestión centralizada y virtualización. Los profesionales aprenden a diseñar estructura de directorios, implementar políticas de grupo para garantizar conformidad de seguridad, y administrar máquinas virtuales para optimizar utilización de recursos. El bloque integra tanto aspectos de seguridad de acceso como optimización de infraestructura. Proporciona las herramientas necesarias para escalar administración de usuarios y recursos a entornos grandes. La progresión avanza desde gestión básica de usuarios hacia implementación compleja de políticas de grupo y optimización de virtualización.

Bloque 10 - Soporte Técnico a Usuarios Finales

Objetivo pedagógico

Desarrollar competencias en prestación de soporte técnico a usuarios finales mediante múltiples canales, incluyendo soporte remoto, presencial, resolución de problemas de aplicaciones y capacitación.

Actividades

Actividad 10.1 Prestar soporte remoto a usuarios finales
Actividad 10.2 Prestar soporte remoto por Internet y presencial
Actividad 10.3 Resolver incidencias de aplicaciones y asesorar a usuarios

Competencias

Competencias	Indicadores
C14 - Prestar soporte técnico remoto a usuarios mediante teléfono, Internet y herramientas de acceso remoto	Resuelve incidencias de usuarios documentando problema, pasos de diagnóstico y solución en sistema de tickets Comunica de forma clara instrucciones técnicas adaptadas al nivel de conocimiento del usuario
C15 - Prestar soporte técnico presencial a usuarios en puestos de trabajo diagnosticando y resolviendo problemas in situ	Realiza diagnóstico de problemas en equipos de usuario identificando causa raíz y aplicando solución Documenta incidencia con descripción de problema, acciones realizadas y resultado final
C16 - Resolver problemas de aplicaciones corporativas coordinando con proveedores y equipos de desarrollo	Diagnostica problemas de aplicaciones diferenciando entre problemas de software, red o infraestructura Coordina con proveedores de aplicaciones y documenta soluciones implementadas
C18 - Asesorar y capacitar a usuarios en el uso de aplicaciones corporativas elaborando guías y documentación	Elabora guías de usuario claras con capturas de pantalla e instrucciones paso a paso Imparte sesiones de capacitación documentando asistencia y temas cubiertos

Saberes asociados

Soporte Técnico Remoto

Herramientas de Acceso Remoto

- Configuración de software de acceso remoto (TeamViewer, AnyDesk, RDP)
- Conexión segura a equipos de usuarios
- Transferencia de archivos remota
- Sesiones de soporte documentadas

Comunicación Telefónica Técnica

- Descripción clara de problemas por teléfono
- Guía paso a paso de usuarios no técnicos
- Confirmación de resolución con usuario
- Documentación de llamadas de soporte

Diagnóstico Remoto de Problemas

- Recopilación de información del problema
- Pruebas de conectividad remota
- Análisis de logs de sistema remoto
- Identificación de causa raíz sin acceso físico

Soporte Técnico Presencial

Diagnóstico In Situ

- Inspección física de equipos
- Pruebas de hardware en puesto de usuario
- Diagnóstico de conectividad local
- Identificación de problemas de configuración

Resolución de Problemas de Conectividad

- Diagnóstico de problemas de Wi-Fi
- Resolución de problemas de VPN
- Configuración de conexión de red
- Validación de conectividad a servicios corporativos

Interacción Profesional con Usuarios

- Presentación profesional
- Escucha activa de problemas del usuario
- Explicación clara de soluciones
- Confirmación de satisfacción del usuario

Resolución de Problemas de Aplicaciones Corporativas

Diagnóstico de Problemas de Aplicaciones

- Identificación de errores de aplicación
- Análisis de logs de aplicación
- Diferenciación entre problemas de aplicación y sistema
- Recopilación de información para escalado a desarrolladores

Coordinación con Proveedores de Aplicaciones

- Comunicación técnica con soporte de proveedor
- Escalado de problemas complejos
- Seguimiento de casos de soporte
- Implementación de soluciones proporcionadas

Resolución de Problemas Comunes

- Problemas de autenticación en aplicaciones
- Errores de conectividad a bases de datos
- Problemas de rendimiento de aplicaciones
- Incompatibilidades de versiones

Capacitación y Asesoramiento a Usuarios

Elaboración de Documentación de Usuario

- Creación de guías paso a paso
- Documentación de procedimientos comunes
- Elaboración de manuales de usuario
- Uso de capturas de pantalla y videos

Impartición de Sesiones de Capacitación

- Adaptación de contenido al nivel del usuario
- Uso de ejemplos relevantes
- Respuesta a preguntas de usuarios

- Evaluación de comprensión

Asesoramiento en Uso de Aplicaciones

- Explicación de funcionalidades de aplicaciones
- Mejores prácticas de uso
- Resolución de dudas de usuarios
- Seguimiento post-capacitación

Gestión de Incidencias de Usuario

Registro y Documentación de Incidencias

- Creación de tickets de soporte
- Descripción clara del problema
- Asignación de prioridad
- Documentación de pasos de resolución

Seguimiento de Incidencias

- Actualización de estado de incidencias
- Comunicación con usuario sobre progreso
- Escalado cuando sea necesario
- Cierre de incidencias con confirmación

Análisis de Incidencias Recurrentes

- Identificación de patrones de problemas
- Propuesta de soluciones preventivas
- Documentación de soluciones permanentes
- Capacitación preventiva de usuarios

Habilidades Blandas para Soporte Técnico

Comunicación Efectiva

- Adaptación del lenguaje al nivel técnico del usuario
- Escucha activa de preocupaciones
- Explicación clara sin jerga innecesaria
- Confirmación de comprensión

Profesionalismo y Empatía

- Presentación profesional
- Trato respetuoso a usuarios
- Paciencia ante usuarios frustrados
- Reconocimiento de impacto del problema en usuario

Gestión de Expectativas

- Comunicación clara de tiempos de resolución
- Actualización regular sobre progreso
- Explicación de limitaciones técnicas
- Propuesta de soluciones alternativas

Habilidades actitudinales

- Comunicación clara adaptada al nivel técnico del usuario
- Documentación completa de incidencias de usuario
- Profesionalismo en interacción con usuarios
- Capacitación efectiva de usuarios

Justificación

Este bloque agrupa competencias de soporte técnico a usuarios finales. Las competencias C14, C15, C16 y C18 comparten la finalidad común de resolver problemas de usuarios y mejorar su productividad. La coherencia funcional radica en que todas ellas abordan interacción con usuarios: C14 proporciona soporte remoto, C15 proporciona soporte presencial, C16 resuelve problemas de aplicaciones, y C18 capacita usuarios. Los livrables compatibles incluyen incidencias resueltas, guías de usuario elaboradas y usuarios capacitados. Las situaciones de evaluación incluyen resolución de incidencias de usuarios, diagnóstico in situ, resolución de problemas de aplicaciones y impartición de sesiones de capacitación.

Ubicación en la progresión

Este bloque representa la interfaz entre la infraestructura técnica y los usuarios finales, proporcionando soporte que garantiza productividad. Construye sobre conocimientos técnicos de diagnóstico y resolución de problemas, añadiendo habilidades de comunicación y capacitación. Los profesionales aprenden a diagnosticar problemas de usuarios, resolverlos mediante múltiples canales, y capacitar usuarios para evitar problemas futuros. El bloque integra tanto habilidades técnicas como habilidades blandas de comunicación. Proporciona las herramientas necesarias para mantener satisfacción de usuarios y reducir incidencias recurrentes. La progresión avanza desde soporte remoto básico hacia resolución compleja de problemas y capacitación estratégica.

Bloque 11 - Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Objetivo pedagógico

Capacitar en la configuración de sistemas informáticos, aplicación de políticas de seguridad y asistencia en instalación de componentes de hardware para garantizar funcionamiento esperado.

Actividades

Actividad 11.1 Realizar mantenimiento preventivo de equipos y sistemas
Actividad 11.2 Instalar componentes de hardware en estaciones y servidores
Actividad 11.3 Configurar sistemas según estándares corporativos
Actividad 11.4 Diagnosticar fallos de hardware y software
Actividad 11.5 Guiar a clientes en instalación de componentes de hardware

Competencias

Competencias	Indicadores

Saberes asociados

Componentes de Hardware y Arquitectura de Sistemas

Componentes de Hardware

- Procesadores y memoria RAM
- Discos duros y SSD
- Tarjetas de red y adaptadores
- Fuentes de alimentación
- Sistemas de refrigeración

Arquitectura de Sistemas Informáticos

- Arquitectura x86 y x64
- Buses de datos y protocolos de comunicación
- BIOS y UEFI
- Particionamiento de discos
- Sistemas de archivos

Instalación y Ensamblaje de Hardware

- Procedimientos de instalación segura
- Gestión de componentes sensibles a electricidad estática
- Verificación de compatibilidad de componentes
- Pruebas de funcionamiento post-instalación

Configuración de Sistemas Operativos

Instalación de Sistemas Operativos

- Instalación de Windows 10/11

- Instalación de Windows Server
- Instalación de distribuciones Linux
- Configuración de arranque y particiones
- Instalación de drivers de dispositivos

Configuración Inicial de Sistemas

- Configuración de red (IP, DNS, DHCP)
- Configuración de nombre de equipo
- Configuración de zona horaria y localización
- Instalación de actualizaciones de sistema
- Configuración de almacenamiento

Aplicación de Políticas de Seguridad

- Configuración de firewall local
- Configuración de antivirus
- Aplicación de políticas de contraseña
- Configuración de control de acceso
- Auditoría de permisos de archivos

Políticas de Seguridad Corporativa

Estándares de Seguridad Corporativa

- Políticas de contraseña corporativas
- Políticas de cifrado de datos
- Políticas de acceso a recursos
- Políticas de auditoría y registro
- Cumplimiento normativo (RGPD, ISO 27001)

Configuración de Seguridad en Sistemas

- Desactivación de servicios innecesarios
- Configuración de permisos de archivos
- Configuración de acceso remoto seguro
- Implementación de autenticación multifactor
- Gestión de certificados digitales

Documentación de Configuración de Seguridad

- Registro de políticas aplicadas
- Documentación de cambios de seguridad
- Trazabilidad de configuraciones
- Auditoría de cumplimiento

Diagnóstico y Validación de Hardware

Herramientas de Diagnóstico de Hardware

- Herramientas de prueba de memoria (Memtest86)
- Herramientas de diagnóstico de disco (SMART, chkdsk)
- Herramientas de monitorización de temperatura
- Herramientas de prueba de procesador
- Herramientas de diagnóstico de red

Validación de Funcionamiento

- Pruebas de arranque del sistema
- Pruebas de rendimiento de hardware
- Validación de conectividad de red
- Pruebas de almacenamiento
- Validación de periféricos

Resolución de Problemas de Hardware

- Diagnóstico de fallos de arranque
- Resolución de problemas de memoria
- Resolución de problemas de disco
- Resolución de problemas de conectividad
- Identificación de componentes defectuosos

Comunicación y Asistencia al Usuario

Comunicación Técnica Clara

- Explicación de procedimientos técnicos en lenguaje comprensible
- Adaptación del nivel de detalle al conocimiento del usuario
- Uso de ejemplos relevantes
- Confirmación de comprensión del usuario

Asistencia en Instalación de Hardware

- Instrucciones paso a paso para instalación
- Respuesta a preguntas del usuario
- Validación de instalación correcta
- Seguimiento post-instalación

Profesionalismo y Actitud de Servicio

- Presentación profesional
- Trato respetuoso con usuarios
- Escucha activa de preocupaciones
- Disponibilidad para seguimiento

Documentación y Estándares de Configuración

Documentación de Configuración

- Registro de configuraciones aplicadas
- Documentación de especificaciones de hardware
- Documentación de políticas de seguridad aplicadas
- Registro de cambios realizados
- Trazabilidad de instalaciones

Estándares Corporativos de Configuración

- Imágenes estándar de sistemas operativos
- Configuraciones base corporativas
- Políticas de nomenclatura de equipos
- Estándares de particionamiento
- Estándares de instalación de software

Gestión de Inventario de Hardware

- Registro de equipos instalados
- Seguimiento de números de serie
- Documentación de especificaciones técnicas
- Registro de garantías y soporte
- Actualización de inventario

Habilidades actitudinales

- Configuración precisa según especificaciones corporativas
- Comunicación clara de instrucciones de instalación
- Documentación de asistencia en instalación

Justificación

Este bloque agrupa competencias de configuración de sistemas y soporte en instalación de hardware. Las competencias C28 y C29 comparten la finalidad común de preparar sistemas para funcionamiento operativo. La coherencia funcional radica en que ambas abordan aspectos de preparación de sistemas: C28 configura sistemas operativos y aplica políticas de seguridad, mientras que C29 asiste en instalación de componentes. Los livrables compatibles incluyen sistemas configurados según especificaciones, políticas de seguridad aplicadas y usuarios asistidos en instalación. Las situaciones de evaluación incluyen configuración de sistemas nuevos, aplicación de políticas de seguridad y asistencia en instalación de hardware.

Ubicación en la progresión

Este bloque representa las actividades de preparación y mantenimiento de sistemas que garantizan funcionamiento correcto. Construye sobre conocimientos de sistemas operativos y configuración de red, proporcionando habilidades prácticas de preparación de sistemas. Los profesionales aprenden a configurar sistemas según especificaciones corporativas, aplicar políticas de seguridad y asistir usuarios en instalación de hardware. El bloque integra tanto aspectos técnicos de configuración como habilidades de comunicación con usuarios. Proporciona las herramientas necesarias para garantizar que nuevos sistemas funcionan correctamente desde el inicio. La progresión avanza desde configuración básica hacia aplicación compleja de políticas de seguridad.

Bloque 12 - Operaciones IT, Monitorización y Gestión de Cambios

Objetivo pedagógico

Desarrollar competencias en administración de servicios de servidor especializados, monitorización de infraestructura y gestión de incidencias críticas para garantizar disponibilidad y rendimiento operativo.

Actividades

Actividad 12.1 Monitorizar activamente sistemas y redes
Actividad 12.2 Aplicar procedimientos ITIL de gestión de cambios y problemas
Actividad 12.3 Asegurar ejecución de copias de seguridad y mantenimiento
Actividad 12.4 Definir operativas de explotación y gestionar Centro de Control IT
Actividad 12.5 Evaluar rendimiento de infraestructura y colaborar en proyectos

Competencias

Competencias	Indicadores

Saberes asociados

Operaciones IT y Gestión de Servicios

Ciclo de vida de servicios IT

- Fases de operación de servicios
- Gestión de disponibilidad de servicios
- Gestión de continuidad de servicios
- Métricas de nivel de servicio (SLA)

Procesos de gestión de cambios

- Evaluación de impacto de cambios
- Planificación de ventanas de mantenimiento
- Procedimientos de rollback
- Documentación de cambios

Gestión de incidencias críticas

- Escalado de incidencias
- Comunicación de estado
- Resolución de problemas de alto impacto
- Documentación de lecciones aprendidas

Monitorización y Análisis de Infraestructura

Herramientas de monitorización de red

- SNMP (Simple Network Management Protocol)
- NetFlow y sFlow para análisis de tráfico
- Herramientas de monitorización centralizada

- Configuración de alertas y umbrales

Análisis de capacidad y rendimiento

- Recopilación de métricas de rendimiento
- Análisis de tendencias de tráfico
- Identificación de cuellos de botella
- Planificación de capacidad

Métricas de disponibilidad y rendimiento

- Tiempo de actividad (uptime)
- Latencia y jitter
- Pérdida de paquetes
- Utilización de ancho de banda

Servicios de Servidor Especializados

Servicios web y aplicaciones

- Instalación y configuración de servidores web (Apache, IIS, Nginx)
- Gestión de certificados SSL/TLS
- Configuración de virtual hosts
- Optimización de rendimiento de aplicaciones web

Servicios de correo electrónico

- Instalación y configuración de servidores de correo
- Gestión de buzones de usuario
- Configuración de políticas de retención
- Monitorización de colas de correo

Servicios de transferencia de archivos

- Configuración de servidores FTP/SFTP
- Gestión de permisos de acceso
- Monitorización de transferencias
- Seguridad en transferencia de archivos

Administración de bases de datos

- Instalación y configuración de SGBD
- Gestión de copias de seguridad
- Monitorización de rendimiento de bases de datos
- Optimización de consultas

Gestión de Cambios y Configuración

Procedimientos de cambio controlado

- Solicitud de cambio (RFC)
- Evaluación de riesgo de cambios
- Aprobación de cambios
- Implementación controlada de cambios

Gestión de configuración

- Inventario de configuración
- Línea base de configuración
- Control de versiones de configuración
- Auditoría de configuración

Planificación de mantenimiento

- Ventanas de mantenimiento programado
- Comunicación de mantenimiento a usuarios
- Validación post-cambio

- Documentación de cambios realizados

Herramientas Avanzadas de Diagnóstico y Análisis

Análisis de paquetes y tráfico

- Captura de paquetes con tcpdump/Wireshark
- Análisis de protocolos de red
- Identificación de anomalías en tráfico
- Análisis de flujos NetFlow/sFlow

Herramientas de monitorización avanzada

- Configuración de SNMP en dispositivos
- Recopilación de métricas SNMP
- Generación de alertas automáticas
- Dashboards de monitorización

Diagnóstico de rendimiento

- Medición de latencia y jitter
- Análisis de pérdida de paquetes
- Evaluación de utilización de recursos
- Identificación de cuellos de botella

Postura Profesional en Operaciones IT

Responsabilidad en operaciones críticas

- Conciencia de impacto de cambios en usuarios
- Planificación cuidadosa de cambios
- Validación exhaustiva antes de producción
- Documentación completa de acciones

Respuesta a incidencias críticas

- Identificación rápida de problemas críticos
- Escalado apropiado de incidencias
- Comunicación clara durante crisis
- Análisis de causa raíz post-incidencia

Mejora continua de operaciones

- Análisis de tendencias de incidencias
- Identificación de mejoras preventivas
- Implementación de automatización
- Compartir conocimiento con equipo

Habilidades actitudinales

- Instalación y configuración correcta de servicios especializados
- Monitorización proactiva de infraestructura
- Análisis de tráfico para optimización de capacidad
- Respuesta rápida a incidencias críticas

Justificación

Este bloque agrupa competencias de operaciones IT, servicios de servidor y monitorización. Las competencias C33-C40 comparten la finalidad común de garantizar disponibilidad y rendimiento de infraestructura. La coherencia funcional radica en que todas ellas abordan aspectos operativos: C33-C35 administran servicios especializados (web, correo, FTP), C36 administra bases de datos, C37-C39 monitorean infraestructura, y C40 gestiona incidencias críticas. Los livrables compatibles incluyen servicios

configurados, monitorización implementada, reportes de capacidad y incidencias críticas resueltas. Las situaciones de evaluación incluyen instalación de servicios web, configuración de correo, monitorización con SNMP/NetFlow, análisis de tráfico y gestión de incidencias de alto impacto.

Ubicación en la progresión

Este bloque representa la especialización en operaciones IT que garantiza disponibilidad continua de servicios corporativos. Construye sobre conocimientos de administración de servidores, añadiendo capacidades de monitorización avanzada y gestión de incidencias críticas. Los profesionales aprenden a administrar servicios especializados, implementar monitorización proactiva y responder rápidamente a incidencias de alto impacto. El bloque integra tanto administración de servicios como análisis de tráfico y monitorización de rendimiento. Proporciona las herramientas necesarias para mantener disponibilidad de servicios críticos y cumplir SLA. La progresión avanza desde administración básica de servicios hacia monitorización avanzada y gestión de incidencias críticas.

ANEXO IV Marco de evaluación

ANEXO IV a. Exenciones de unidades

Posesión de certificación CCNA (Cisco Certified Network Associate) válida, exentos de realizar la unidad U1.

Posesión de certificación CCNP (Cisco Certified Network Professional) válida, exentos de realizar la unidad U2.

Experiencia profesional demostrada de al menos 3 años en administración de redes corporativas, exentos de realizar la unidad U1.

Experiencia profesional demostrada de al menos 2 años en soporte técnico IT, exentos de realizar la unidad U4.

Posesión de certificación CompTIA Security+ válida, exentos de realizar la unidad U7.

Posesión de certificación Microsoft Certified: Windows Server Administrator Associate válida, exentos de realizar la unidad U8.

Posesión de certificación VMware Certified Associate (VCA) válida, exentos de realizar la unidad U9.

ANEXO IV b. Reglamento de examen

Pruebas	Unidad	Coef.	Forma	Duración
E1 Evaluación de Administración de Infraestructura de Red de Capa 2 y Capa 3	**U1**	**2**	Prueba práctica única	3h
E2 Evaluación de Configuración de Protocolos de Enrutamiento Dinámico y Avanzado	**U2**	**2**	Prueba práctica única	3h
E3 Evaluación de Gestión de Calidad de Servicio y Monitorización de Tráfico	**U3**	**1**	Prueba práctica única	2h
E4 Evaluación de Diagnóstico y Resolución de Incidencias de Red y Conectividad	**U4**	**2**	Prueba práctica única	2h30
E5 Evaluación de Automatización de Tareas de Red y Sistemas	**U5**	**1**	Prueba práctica única	2h
E6 Evaluación de Gestión de Incidencias y Coordinación con Proveedores	**U6**	**1**	Prueba oral única	1h
E7 Evaluación de Documentación, Auditoría y Mejora Continua	**U7**	**2**	Prueba escrita única	2h
E8 Evaluación de Administración de Sistemas Operativos y Servicios de Servidor	**U8**	**2**	Prueba práctica única	2h30
E9 Evaluación de Administración de Directorios, Virtualización y Seguridad de Acceso	**U9**	**2**	Prueba práctica única	2h30
E10 Evaluación de Soporte Técnico a Usuarios Finales	**U10**	**2**	Prueba oral única	1h30
E11 Evaluación de Mantenimiento, Instalación de Hardware y Gestión de Configuraciones	**U11**	**1**	Prueba práctica única	2h
E12 Evaluación de Operaciones IT, Monitorización y Gestión de Cambios	**U12**	**2**	Prueba práctica única	3h

*Pruebas optativas: solo se tienen en cuenta los puntos por encima de la media.

ANEXO IV c. Definición de las pruebas

E1 : Evaluación de Administración de Infraestructura de Red de Capa 2 y Capa 3

Finalidades de la prueba

Evaluar la capacidad del candidato para analizar rendimiento de infraestructura, configurar dispositivos de red, diseñar arquitecturas de capa 2 y capa 3, e implementar protocolos de switching avanzados.

Contenido de la prueba

Análisis de rendimiento de infraestructura de red; Evaluación de hardware y dispositivos de red; Configuración de switches Ethernet y gestión de VLAN; Configuración de routers y tablas de enrutamiento; Diseño de arquitecturas de capa 2 con redundancia; Diseño de arquitecturas de capa 3 con subnetting y CIDR; Implementación de Spanning Tree Protocol (STP); Prevención de bucles de red; Elaboración de informes técnicos de infraestructura.

Competencias evaluadas

C1 - Analizar el rendimiento de infraestructuras de red y hardware para identificar cuellos de botella y proponer mejoras técnicas

C2 - Configurar y mantener dispositivos de red (switches y routers) aplicando estándares de seguridad y disponibilidad

C3 - Diseñar arquitecturas de red de capa 2 y capa 3 considerando escalabilidad, redundancia y segmentación

C4 - Implementar y optimizar protocolos de switching avanzados (STP, VLAN) para evitar bucles y segmentar redes

Criterios de evaluación

- Análisis preciso de métricas de rendimiento de infraestructura con identificación correcta de cuellos de botella
- Configuración correcta de switches con VLAN y puertos troncales sin interrupciones de servicio
- Configuración correcta de routers con tablas de enrutamiento y listas de control de acceso (ACL)
- Diseño de arquitecturas de capa 2 escalables con redundancia mediante STP
- Diseño de arquitecturas de capa 3 con esquemas de direccionamiento IP y subnetting correcto
- Validación de ausencia de bucles mediante herramientas de diagnóstico
- Documentación completa de topología y configuraciones realizadas
- Elaboración de informes técnicos con recomendaciones de mejora

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica en laboratorio de red con configuración de dispositivos reales o simulados

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica en laboratorio de red

Vae : Prueba práctica única — Demostración práctica de competencias en entorno de laboratorio

Reglas específicas

- El candidato debe demostrar capacidad de configurar dispositivos sin interrupciones de servicio
- Se requiere validación de configuraciones mediante herramientas de diagnóstico
- La documentación de topología y configuraciones es obligatoria
- Se evalúa tanto el proceso de diseño como el resultado final

E2 : Evaluación de Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Finalidades de la prueba

Evaluar la capacidad del candidato para configurar protocolos de enrutamiento dinámico (OSPF, BGP) y tecnologías avanzadas (MPLS, VPN) en entornos corporativos complejos.

Contenido de la prueba

Configuración de OSPF con definición de áreas y optimización de costes; Configuración de BGP con gestión de políticas de enrutamiento; Configuración de route-maps y filtros de enrutamiento; Configuración de MPLS y LSPs; Gestión de VRFs para aislamiento de tráfico; Implementación de VPN sobre MPLS; Validación de convergencia de rutas; Análisis de tablas de enrutamiento; Optimización de comportamiento de failover.

Competencias evaluadas

C5 - Configurar protocolos de enrutamiento dinámico (OSPF, BGP) para optimizar rutas y garantizar convergencia rápida

C6 - Administrar tecnologías avanzadas de red (MPLS, VPN) para garantizar conectividad segura en entornos corporativos

Criterios de evaluación

- Configuración correcta de OSPF con múltiples áreas y optimización de costes de enlace
- Configuración correcta de BGP con políticas de enrutamiento y route-maps
- Implementación correcta de MPLS con LSPs activos y funcionales
- Configuración correcta de VRFs para aislamiento de tráfico en VPN
- Validación de convergencia de rutas en escenarios de cambio de topología
- Prueba de failover y recuperación con comportamiento esperado
- Análisis correcto de tablas de enrutamiento para identificar rutas subóptimas
- Documentación completa de configuraciones de enrutamiento con justificación técnica

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica en laboratorio de red con configuración de routers

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica en laboratorio de red

Vae : Prueba práctica única — Demostración práctica de competencias en entorno de laboratorio

Reglas específicas

- Se requiere validación de convergencia de rutas mediante herramientas de diagnóstico
- La prueba de failover es obligatoria para demostrar comportamiento correcto
- Se evalúa la optimización de costes de enrutamiento basada en análisis de tráfico

• La documentación de políticas de enrutamiento es obligatoria

E3 : Evaluación de Gestión de Calidad de Servicio y Monitorización de Tráfico

Finalidades de la prueba

Evaluar la capacidad del candidato para implementar y gestionar políticas de Calidad de Servicio (QoS) que garanticen priorización de tráfico crítico y rendimiento de aplicaciones.

Contenido de la prueba

Configuración de QoS en dispositivos de red; Clasificación y marcado de tráfico (DSCP, CoS); Gestión de colas de tráfico (FIFO, PQ, CQ, WFQ); Implementación de políticas de QoS basadas en aplicaciones; Monitorización de cumplimiento de QoS; Validación de priorización de tráfico; Análisis de impacto de QoS en rendimiento; Ajuste iterativo de políticas de QoS.

Competencias evaluadas

C7 - Aplicar políticas de Calidad de Servicio (QoS) para priorizar tráfico crítico y garantizar rendimiento de aplicaciones

Criterios de evaluación

• Configuración correcta de políticas de QoS con clasificación y marcado de tráfico
• Implementación correcta de colas de tráfico con priorización apropiada
• Validación de que tráfico prioritario recibe tratamiento configurado
• Prueba de escenarios de congestión con comportamiento esperado de QoS
• Monitorización correcta de cumplimiento de requisitos de QoS
• Análisis de métricas de latencia y jitter para validar rendimiento
• Documentación de políticas de QoS con justificación técnica
• Ajuste iterativo de políticas basado en observación de comportamiento

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica en laboratorio de red con configuración de QoS

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica en laboratorio de red

Vae : Prueba práctica única — Demostración práctica de competencias en entorno de laboratorio

Reglas específicas

• Se requiere validación de priorización de tráfico mediante herramientas de monitorización
• La prueba de escenarios de congestión es obligatoria
• Se evalúa la capacidad de ajuste iterativo de políticas basado en datos
• La documentación de políticas de QoS es obligatoria

E4 : Evaluación de Diagnóstico y Resolución de Incidencias de Red y Conectividad

Finalidades de la prueba

Evaluar la capacidad del candidato para diagnosticar sistemáticamente problemas de red y conectividad, utilizando herramientas de análisis y metodologías estructuradas para identificar causa raíz.

Contenido de la prueba

Diagnóstico de conectividad de red mediante herramientas (ping, traceroute, ipconfig, ifconfig); Uso de analizadores de protocolos (Wireshark, tcpdump); Análisis de capturas de paquetes; Diagnóstico de problemas de Wi-Fi; Diagnóstico de problemas de VPN; Diagnóstico de problemas de conectividad de usuarios; Documentación de proceso de diagnóstico; Identificación de causa raíz; Resolución de incidencias de conectividad.

Competencias evaluadas

C8 - Diagnosticar y resolver incidencias de conectividad de red utilizando herramientas de análisis y capturas de paquetes

C17 - Restablecer conectividad de red e Internet en puestos de usuario resolviendo problemas de Wi-Fi y VPN

Criterios de evaluación

- Selección apropiada de herramientas de diagnóstico para cada tipo de problema
- Uso correcto de herramientas de diagnóstico (ping, traceroute, ipconfig, Wireshark)
- Análisis correcto de capturas de paquetes para identificar problemas
- Identificación correcta de causa raíz de problemas de conectividad
- Resolución efectiva de problemas de Wi-Fi y VPN
- Documentación completa de proceso de diagnóstico y pasos realizados
- Comunicación clara con usuarios durante diagnóstico
- Validación de resolución antes de cerrar incidencia

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica con escenarios de problemas de conectividad a resolver

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica con escenarios de problemas de conectividad

Vae : Prueba práctica única — Demostración práctica de diagnóstico de problemas reales

Reglas específicas

- Se requiere uso de múltiples herramientas para validar hallazgos
- La documentación del proceso de diagnóstico es obligatoria
- Se evalúa la capacidad de identificar causa raíz, no solo síntomas
- Se requiere validación de resolución antes de cerrar incidencia

E5 : Evaluación de Automatización de Tareas de Red y Sistemas

Finalidades de la prueba

Evaluar la capacidad del candidato para desarrollar scripts y playbooks que automatizan tareas recurrentes de administración de red y sistemas.

Contenido de la prueba

Programación en Python para automatización de tareas de red; Desarrollo de scripts para recopilación de información de dispositivos; Desarrollo de scripts para backup de configuraciones; Configuración de Ansible para automatización; Desarrollo de playbooks de Ansible; Integración de automatización en pipelines CI/CD; Documentación de código y automatización; Validación de scripts y playbooks antes de producción.

Competencias evaluadas

C9 - Automatizar tareas de administración de red y sistemas mediante scripts y herramientas de orquestación

Criterios de evaluación

- Desarrollo de scripts Python funcionales para automatización de tareas de red
- Desarrollo de playbooks Ansible correctos y funcionales
- Documentación completa de código con comentarios explicativos
- Prueba de scripts y playbooks en entorno de prueba antes de producción
- Validación de ejecución sin errores y resultados esperados
- Integración de automatización en pipelines CI/CD
- Código limpio y mantenible con convenciones de nomenclatura
- Documentación de propósito, parámetros y ejemplos de uso

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica con desarrollo de scripts y playbooks

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica con desarrollo de scripts y playbooks

Vae : Prueba práctica única — Demostración práctica de scripts y playbooks desarrollados

Reglas específicas

- Se requiere prueba en entorno de prueba antes de producción
- La documentación de código es obligatoria
- Se evalúa la calidad del código además de funcionalidad
- Se requiere validación de resultados esperados

E6 : Evaluación de Gestión de Incidencias y Coordinación con Proveedores

Finalidades de la prueba

Evaluar la capacidad del candidato para gestionar incidencias complejas y coordinar efectivamente con proveedores externos para garantizar resolución oportuna.

Contenido de la prueba

Apertura de casos de soporte con proveedores; Escalado apropiado de problemas; Comunicación técnica con proveedores; Seguimiento de casos de soporte; Coordinación de pruebas con fabricantes;

Documentación de interacciones con proveedores; Gestión de información de contacto de proveedores; Registro de soluciones recibidas; Compartir conocimiento con equipo.

Competencias evaluadas

C10 - Coordinar la resolución de incidencias complejas con proveedores externos y fabricantes de equipos

Criterios de evaluación

- Identificación correcta de cuándo escalar a proveedor
- Apertura de casos de soporte con información completa y clara
- Comunicación técnica clara y precisa con proveedores
- Respuesta oportuna a solicitudes de información de proveedores
- Seguimiento regular del estado de casos de soporte
- Documentación completa de interacciones con proveedores
- Coordinación efectiva de pruebas con fabricantes
- Compartir soluciones recibidas con equipo interno

Forma de evaluación

Vía escolar pública o privada concertada : Prueba oral única — Evaluación mediante presentación de casos de escalado y coordinación con proveedores

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba oral única — Evaluación mediante presentación de casos de escalado

Vae : Prueba oral única — Presentación de experiencia en coordinación con proveedores

Reglas específicas

- Se requiere documentación de casos de escalado
- Se evalúa la comunicación técnica con proveedores
- Se requiere seguimiento regular de casos
- Se evalúa la capacidad de compartir conocimiento con equipo

E7 : Evaluación de Documentación, Auditoría y Mejora Continua

Finalidades de la prueba

Evaluar la capacidad del candidato para documentar infraestructura, preparar auditorías, gestionar certificados y proponer mejoras continuas.

Contenido de la prueba

Documentación de procedimientos técnicos; Documentación de configuraciones de infraestructura; Documentación de cambios realizados; Mantenimiento de documentación actualizada; Preparación de auditorías técnicas; Verificación de cumplimiento de estándares; Gestión de inventario de certificados digitales; Monitorización de vigencia de certificados; Renovación de certificados; Identificación de oportunidades de mejora; Análisis coste-beneficio de mejoras; Presentación de propuestas de mejora.

Competencias evaluadas

C11 - Documentar procedimientos técnicos, configuraciones y cambios de infraestructura para asegurar trazabilidad y continuidad

C12 - Preparar y ejecutar auditorías técnicas de sistemas y redes cumpliendo estándares de seguridad y regulatorios

C13 - Gestionar certificados digitales y provisiones de sistemas monitoreando vigencia y renovación

C19 - Proponer mejoras continuas en procesos y servicios IT realizando análisis coste-beneficio y presentando propuestas

Criterios de evaluación

- Documentación completa y clara de procedimientos técnicos
- Documentación detallada de configuraciones de infraestructura
- Registro de todos los cambios realizados con suficiente detalle
- Mantenimiento de documentación actualizada y accesible
- Preparación proactiva para auditorías técnicas
- Identificación correcta de requisitos de cumplimiento normativo
- Mantenimiento de inventario actualizado de certificados
- Monitorización proactiva de vigencia de certificados
- Renovación de certificados antes de expiración
- Identificación regular de oportunidades de mejora
- Análisis coste-beneficio claro de propuestas de mejora
- Presentación efectiva de propuestas a stakeholders

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Evaluación mediante elaboración de documentación y propuestas de mejora

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba escrita única — Evaluación mediante elaboración de documentación

Vae : Prueba escrita única — Presentación de documentación y propuestas de mejora realizadas

Reglas específicas

- Se requiere documentación completa de procedimientos y cambios
- Se evalúa la capacidad de mantener documentación actualizada
- Se requiere preparación proactiva para auditorías
- Se evalúa la calidad del análisis coste-beneficio de mejoras

E8 : Evaluación de Administración de Sistemas Operativos y Servicios de Servidor

Finalidades de la prueba

Evaluar la capacidad del candidato para administrar sistemas operativos de servidor (Windows Server y Linux) incluyendo configuración de roles, servicios y actualizaciones.

Contenido de la prueba

Instalación de Windows Server y Linux; Configuración de roles y características en Windows Server; Instalación de servicios en Linux; Configuración de servicios de servidor; Gestión de usuarios y grupos; Aplicación de actualizaciones de seguridad; Planificación de cambios sin impacto en servicios; Backup y recuperación de servidores; Documentación de configuración de servidores; Mantenimiento de inventario de servidores.

Competencias evaluadas

C20 - Administrar sistemas operativos de servidor (Windows y Linux) configurando roles, servicios y actualizaciones

Criterios de evaluación

- Instalación correcta de Windows Server y Linux según especificaciones
- Configuración correcta de roles y características en Windows Server
- Instalación correcta de servicios en Linux
- Configuración correcta de servicios de servidor
- Gestión correcta de usuarios y grupos
- Aplicación correcta de actualizaciones de seguridad
- Planificación de cambios en ventanas de mantenimiento
- Realización de backup antes de cambios
- Validación de cambios antes de aplicar en producción
- Documentación completa de configuración de servidores
- Mantenimiento de inventario actualizado de servidores
- Validación de funcionamiento después de actualización

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica con instalación y configuración de servidores

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica con instalación y configuración de servidores

Vae : Prueba práctica única — Demostración práctica de administración de servidores

Reglas específicas

- Se requiere instalación correcta de sistemas operativos
- Se evalúa la configuración de roles y servicios
- Se requiere planificación de cambios sin impacto en servicios
- Se evalúa la documentación de configuración de servidores

E9 : Evaluación de Administración de Directorios, Virtualización y Seguridad de Acceso

Finalidades de la prueba

Evaluar la capacidad del candidato para administrar Active Directory, gestionar virtualización VMware y configurar políticas de seguridad.

Contenido de la prueba

Instalación y configuración de Active Directory; Creación de estructura de unidades organizativas (OU); Gestión de usuarios y grupos en Active Directory; Implementación de políticas de grupo (GPO); Configuración de políticas de contraseña; Implementación de restricciones de acceso; Instalación de VMware vSphere; Creación y gestión de máquinas virtuales; Configuración de recursos virtuales; Monitorización de utilización de recursos; Optimización de máquinas virtuales.

Competencias evaluadas

Criterios de evaluación

- Instalación correcta de Active Directory
- Creación de estructura de OU lógica y escalable
- Gestión correcta de usuarios y grupos
- Implementación correcta de políticas de grupo (GPO)
- Configuración correcta de políticas de contraseña
- Implementación correcta de restricciones de acceso
- Validación de aplicación de políticas
- Instalación correcta de VMware vSphere
- Creación correcta de máquinas virtuales
- Configuración correcta de recursos virtuales
- Monitorización de utilización de recursos
- Optimización de máquinas virtuales basada en demanda

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica con configuración de Active Directory y VMware

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica con configuración de Active Directory y VMware

Vae : Prueba práctica única — Demostración práctica de administración de directorios y virtualización

Reglas específicas

- Se requiere creación de estructura de OU lógica
- Se evalúa la implementación de políticas de grupo
- Se requiere configuración correcta de máquinas virtuales
- Se evalúa la optimización de recursos virtuales

E10 : Evaluación de Soporte Técnico a Usuarios Finales

Finalidades de la prueba

Evaluar la capacidad del candidato para prestar soporte técnico a usuarios finales mediante múltiples canales incluyendo soporte remoto, presencial y capacitación.

Contenido de la prueba

Soporte técnico remoto mediante teléfono e Internet; Soporte técnico presencial en puestos de trabajo; Diagnóstico de problemas de usuarios; Resolución de problemas de aplicaciones corporativas; Coordinación con proveedores de aplicaciones; Capacitación de usuarios en aplicaciones corporativas; Elaboración de guías de usuario; Documentación de incidencias de usuario; Comunicación clara con usuarios; Profesionalismo en interacción con usuarios.

Competencias evaluadas

C14 - Prestar soporte técnico remoto a usuarios mediante teléfono, Internet y herramientas de acceso remoto

C15 - Prestar soporte técnico presencial a usuarios en puestos de trabajo diagnosticando y resolviendo problemas in situ

C16 - Resolver problemas de aplicaciones corporativas coordinando con proveedores y equipos de desarrollo

C18 - Asesorar y capacitar a usuarios en el uso de aplicaciones corporativas elaborando guías y documentación

Criterios de evaluación

- Prestación de soporte remoto efectivo mediante teléfono e Internet
- Prestación de soporte presencial con diagnóstico in situ
- Diagnóstico correcto de problemas de usuarios
- Resolución efectiva de problemas de aplicaciones corporativas
- Coordinación efectiva con proveedores de aplicaciones
- Capacitación clara y efectiva de usuarios
- Elaboración de guías de usuario comprensibles
- Documentación completa de incidencias de usuario
- Comunicación clara adaptada al nivel técnico del usuario
- Profesionalismo en apariencia y trato con usuarios
- Paciencia y respeto en interacción con usuarios
- Proporcionar soluciones sin condescendencia

Forma de evaluación

Vía escolar pública o privada concertada : Prueba oral única — Evaluación mediante simulación de soporte a usuarios y presentación de casos

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba oral única — Evaluación mediante simulación de soporte a usuarios

Vae : Prueba oral única — Presentación de experiencia en soporte a usuarios finales

Reglas específicas

- Se requiere demostración de habilidades de comunicación con usuarios
- Se evalúa la capacidad de diagnóstico de problemas de usuarios
- Se requiere documentación de incidencias de usuario
- Se evalúa la capacidad de capacitación de usuarios

E11 : Evaluación de Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Finalidades de la prueba

Evaluar la capacidad del candidato para configurar sistemas informáticos, aplicar políticas de seguridad y asistir en instalación de componentes de hardware.

Contenido de la prueba

Configuración de sistemas informáticos según especificaciones corporativas; Aplicación de políticas de seguridad en sistemas; Asistencia en instalación de componentes de hardware; Comunicación clara de

instrucciones de instalación; Documentación de asistencia en instalación; Validación de funcionamiento de sistemas; Gestión de configuraciones de sistemas; Mantenimiento de inventario de sistemas.

Competencias evaluadas

Criterios de evaluación

- Configuración correcta de sistemas según especificaciones corporativas
- Aplicación correcta de políticas de seguridad
- Asistencia efectiva en instalación de hardware
- Comunicación clara de instrucciones de instalación
- Documentación completa de asistencia en instalación
- Validación de funcionamiento de sistemas
- Gestión correcta de configuraciones de sistemas
- Mantenimiento de inventario actualizado de sistemas

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica con configuración de sistemas e instalación de hardware

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica con configuración de sistemas

Vae : Prueba práctica única — Demostración práctica de configuración de sistemas

Reglas específicas

- Se requiere configuración según especificaciones corporativas
- Se evalúa la aplicación de políticas de seguridad
- Se requiere documentación de asistencia en instalación
- Se evalúa la comunicación clara con usuarios

E12 : Evaluación de Operaciones IT, Monitorización y Gestión de Cambios

Finalidades de la prueba

Evaluar la capacidad del candidato para administrar servicios de servidor especializados, monitorizar infraestructura y gestionar incidencias críticas.

Contenido de la prueba

Instalación y configuración de servicios web (Apache, IIS); Instalación y configuración de servicios de correo; Instalación y configuración de servicios FTP; Administración de bases de datos; Configuración de monitorización con SNMP; Configuración de análisis de tráfico con NetFlow/sFlow; Análisis de flujos de tráfico; Elaboración de reportes de capacidad; Identificación de problemas antes de impacto en usuarios; Respuesta rápida a incidencias críticas; Escalado apropiado de incidencias; Documentación de resolución de incidencias.

Competencias evaluadas

Criterios de evaluación

- Instalación correcta de servicios web (Apache, IIS)
- Instalación correcta de servicios de correo
- Instalación correcta de servicios FTP
- Administración correcta de bases de datos
- Configuración correcta de monitorización con SNMP
- Configuración correcta de análisis de tráfico con NetFlow/sFlow
- Análisis correcto de flujos de tráfico
- Elaboración de reportes de capacidad precisos
- Identificación proactiva de problemas
- Respuesta rápida a incidencias críticas
- Escalado apropiado de incidencias
- Documentación completa de resolución de incidencias

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Evaluación práctica con instalación de servicios y configuración de monitorización

Aprendizaje : Evaluación continua — Evaluación continua mediante situaciones de trabajo en empresa

Formación continua : Prueba práctica única — Evaluación práctica con instalación de servicios y monitorización

Vae : Prueba práctica única — Demostración práctica de administración de servicios y monitorización

Reglas específicas

- Se requiere instalación correcta de servicios especializados
- Se evalúa la configuración de monitorización proactiva
- Se requiere análisis de tráfico para optimización de capacidad
- Se evalúa la respuesta rápida a incidencias críticas

ANEXO IV d. Dispositivo de evaluación detallado por bloque

Este anexo describe, para cada bloque de competencias, el dispositivo de evaluación detallado: indicadores SMART por misión profesional, situaciones de evaluación (simulaciones, estudios de caso), pruebas esperadas (producciones documentales, acciones observables, elementos reflexivos), criterios de éxito agrupados en siete familias, y el umbral de validación del bloque. Este dispositivo constituye la referencia para evaluadores y tribunales.

Bloque 1 - Administración de Infraestructura de Red de Capa 2 y Capa 3

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Número de métricas de rendimiento recopiladas y analizadas por informe técnico Porcentaje de mejoras propuestas implementadas dentro de 3 meses Reducción de latencia o aumento de ancho de banda logrado tras implementación de mejoras Tiempo promedio de análisis desde recopilación de datos hasta presentación de informe
M02 — Configurar y mantener switches de red	Número de switches configurados sin interrupciones de servicio Porcentaje de puertos troncales funcionando correctamente tras configuración Tiempo de convergencia de STP tras cambios de topología Número de actualizaciones de firmware completadas exitosamente
M03 — Configurar y mantener routers de red	Número de routers configurados con rutas estáticas y ACL Porcentaje de rutas en tabla de enrutamiento alcanzables Tiempo de convergencia de rutas tras cambios de topología Número de ACL implementadas sin bloqueo de tráfico legítimo
M04 — Diseñar y administrar redes de capa 2	Número de arquitecturas de capa 2 diseñadas según requisitos Porcentaje de topologías que cumplen requisitos de redundancia Tiempo de convergencia de STP en topología diseñada Número de VLAN implementadas correctamente en arquitectura
M05 — Diseñar y administrar redes de capa 3	Número de esquemas de direccionamiento IP diseñados Porcentaje de subredes planificadas sin solapamiento Eficiencia de utilización de espacio de direcciones IP Número de routers configurados según esquema de direccionamiento
M06 — Implementar VLANs para segmentar la red	Número de VLAN configuradas en switches Porcentaje de puertos asignados correctamente a VLAN Número de puertos troncales funcionando correctamente Tiempo de convergencia de enrutamiento entre VLAN

Misión	Indicadores SMART
M07 — Configurar STP para evitar bucles de red	Número de topologías de switching sin bucles detectados Tiempo de convergencia de STP tras fallo de enlace Porcentaje de puertos en estado de reenvío tras convergencia Número de cambios de topología gestionados sin interrupciones

Situaciones de evaluación

Análisis de Rendimiento de Infraestructura de Red Existente

Contexto : Se requiere analizar el rendimiento de una infraestructura de red corporativa existente que soporta 500 usuarios distribuidos en 3 sitios. La red presenta problemas ocasionales de latencia en aplicaciones críticas. El profesional debe recopilar métricas de rendimiento, identificar cuellos de botella y proponer mejoras técnicas justificadas.

Restricciones : Análisis sin interrupciones de servicio, utilización de herramientas de monitorización disponibles, documentación de todas las métricas recopiladas, propuestas de mejora con análisis coste-beneficio

Producciones esperadas :

- Informe de análisis de rendimiento con métricas de latencia, ancho de banda y utilización
- Identificación de cuellos de botella con evidencia técnica
- Propuestas de mejora con justificación técnica y económica
- Diagrama de topología actual con anotaciones de problemas identificados

Competencias evaluadas : C1

Configuración de Switches y Puertos Troncales en Red Corporativa

Contexto : Se requiere configurar 5 switches de acceso en una red corporativa para implementar segmentación mediante VLAN. Los switches deben conectarse a un switch de distribución mediante puertos troncales. Se deben aplicar estándares de seguridad corporativos incluyendo control de acceso a puertos de gestión.

Restricciones : Configuración sin interrupciones de servicio, aplicación de estándares de seguridad corporativos, documentación de todas las configuraciones, validación de conectividad de extremo a extremo

Producciones esperadas :

- Configuración de switches con VLAN y puertos troncales
- Documentación de configuración de cada switch
- Validación de conectividad entre VLAN
- Diagrama de topología de switching implementada

Competencias evaluadas : C2, C4

Diseño de Arquitectura de Red de Capa 2 y Capa 3 para Nueva Sucursal

Contexto : Se requiere diseñar una infraestructura de red completa para una nueva sucursal corporativa con 200 usuarios. El diseño debe considerar escalabilidad para crecimiento futuro, redundancia de enlaces críticos, segmentación mediante VLAN y enrutamiento eficiente. Se deben documentar decisiones de diseño y justificar con requisitos de negocio.

Restricciones : Diseño escalable para crecimiento futuro, redundancia en componentes críticos, segmentación de red por departamento, documentación completa de arquitectura, consideración de costos

Producciones esperadas :

- Diagrama de arquitectura de red de capa 2 y capa 3
- Esquema de direccionamiento IP con subnetting
- Plan de VLAN con asignación de puertos
- Documento de justificación de decisiones de diseño
- Especificación de equipos requeridos

Competencias evaluadas : C3, C4

Optimización de Topología de Switching con STP para Prevención de Bucles

Contexto : Se requiere optimizar una topología de switching existente que presenta bucles de red causados por conexiones redundantes. Se debe implementar y optimizar Spanning Tree Protocol para prevenir bucles manteniendo redundancia. Se deben validar tiempos de convergencia y documentar topología resultante.

Restricciones : Prevención de bucles sin perder redundancia, optimización de tiempos de convergencia, validación mediante herramientas de diagnóstico, documentación de topología de STP

Producciones esperadas :

- Configuración de STP en switches
- Diagrama de árbol de expansión resultante
- Validación de ausencia de bucles
- Medición de tiempos de convergencia
- Documentación de puentes raíz y puertos raíz

Competencias evaluadas : C4

Diagnóstico y Resolución de Problema de Conectividad de Red

Contexto : Se reporta que un departamento de 50 usuarios no tiene conectividad a servidores corporativos. El profesional debe diagnosticar el problema utilizando herramientas de análisis, identificar causa raíz y resolver la incidencia. Se deben documentar todos los pasos de diagnóstico y la solución implementada.

Restricciones : Diagnóstico sistemático con herramientas apropiadas, identificación de causa raíz, resolución sin impacto en otros usuarios, documentación completa de proceso

Producciones esperadas :

- Registro de diagnóstico con pasos realizados
- Análisis de capturas de paquetes si es necesario
- Identificación de causa raíz con evidencia técnica
- Solución implementada y validada
- Informe de cierre de incidencia

Competencias evaluadas : C1, C2, C3

Pruebas esperadas

■ **Pruebas documentales**

- Informe de análisis de rendimiento de infraestructura con métricas y propuestas de mejora
- Configuraciones de switches y routers documentadas con comentarios explicativos
- Diagrama de arquitectura de red de capa 2 y capa 3 con topología física y lógica
- Esquema de direccionamiento IP con cálculo de subredes y CIDR
- Plan de VLAN con asignación de puertos y puertos troncales
- Documentación de STP con árbol de expansión y puertos raíz
- Registros de diagnóstico de incidencias con pasos realizados y soluciones
- Especificación de equipos de red con justificación técnica

■ Pruebas de acción (en campo)

- Configuración de switches Ethernet con VLAN y puertos troncales
- Configuración de routers con interfaces, rutas estáticas y ACL
- Implementación de STP para prevención de bucles
- Recopilación de métricas de rendimiento mediante herramientas de monitorización
- Análisis de capturas de paquetes para diagnóstico de problemas
- Validación de conectividad de extremo a extremo
- Prueba de failover y convergencia de topología
- Actualización de firmware de dispositivos de red

■ Pruebas reflexivas

- Análisis de decisiones de diseño de arquitectura y justificación con requisitos de negocio
- Reflexión sobre trade-offs entre redundancia, costo y complejidad
- Evaluación de impacto de cambios de configuración en usuarios
- Análisis de causa raíz de problemas de conectividad
- Revisión de efectividad de propuestas de mejora implementadas
- Identificación de lecciones aprendidas en diagnóstico de incidencias
- Evaluación de escalabilidad de arquitectura diseñada
- Análisis de convergencia de STP en diferentes escenarios de fallo

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Configuraciones de dispositivos cumplen estándares de seguridad corporativos y mejores prácticas de la industria	Verificación de aplicación de políticas de seguridad, control de acceso a dispositivos, y cumplimiento de estándares documentados
Qualité	Arquitecturas de red diseñadas son escalables, redundantes y optimizadas para rendimiento	Validación de topología sin bucles, convergencia de STP < 30 segundos, utilización de enlaces < 80%, documentación completa
Comunicación	Documentación técnica es clara, completa y permite reproducción de configuraciones por otros profesionales	Revisión de documentación por pares, capacidad de otro profesional de reproducir configuración, claridad de diagramas

Familia	Definición	Ponderación
Pertinence	Propuestas de mejora son técnicamente justificadas y alineadas con requisitos de negocio	Análisis coste-beneficio de propuestas, alineación con objetivos de negocio, validación de impacto técnico
Traçabilité	Todos los cambios de configuración están documentados con fecha, autor, justificación y resultado	Registro completo de cambios, documentación de antes/después, trazabilidad de decisiones técnicas
Cohérence	Diseños de red mantienen coherencia entre capa 2 y capa 3, con segmentación consistente	Validación de alineación entre VLAN y subredes, consistencia de políticas de seguridad, coherencia de topología
Posture	Profesional demuestra rigor en validación de configuraciones, precisión en análisis de rendimiento y pensamiento sistémico en diseño	Validación de ausencia de bucles mediante múltiples herramientas, análisis de rendimiento con múltiples fuentes de datos, consideración de impacto sistémico

Umbral de validación : Promedio ≥ 10/20

Bloque 2 - Configuración de Protocolos de Enrutamiento Dinámico y Avanzado

Indicadores de desempeño por misión

Misión	Indicadores SMART
M08 — Implantar protocolos de routing dinámico con OSPF	Porcentaje de routers con OSPF configurado correctamente según especificaciones de diseño Tiempo de convergencia de OSPF ante cambios de topología (objetivo: < 5 segundos) Número de rutas óptimas en tabla de enrutamiento versus rutas subóptimas Disponibilidad de conectividad entre áreas OSPF (objetivo: > 99.9%)
M09 — Configurar peering y políticas con BGP	Número de sesiones BGP activas versus configuradas Tiempo de convergencia de BGP ante cambios de ruta (objetivo: < 30 segundos) Porcentaje de rutas filtradas correctamente según políticas de enrutamiento Número de incidentes de ruta incorrecta detectados y corregidos
M10 — Gestionar redes MPLS en entornos corporativos	Número de LSP activos y funcionales en infraestructura MPLS Porcentaje de tráfico de VPN aislado correctamente entre clientes Tiempo de establecimiento de nuevo LSP (objetivo: < 2 minutos) Disponibilidad de conectividad de extremo a extremo en MPLS VPN (objetivo: > 99.95%)

Situaciones de evaluación

Implementación de OSPF en Red Corporativa Multi-Área

Contexto : Una empresa con múltiples sedes requiere implementar OSPF para optimizar enrutamiento entre sus oficinas. La red actual utiliza enrutamiento estático y necesita convergencia automática ante cambios de topología. Se requiere diseñar una estructura de áreas OSPF que refleje la geografía de la empresa y optimizar costos de enrutamiento.

Restricciones : Minimizar impacto en tráfico existente, mantener disponibilidad de servicios críticos durante implementación, documentar todas las configuraciones realizadas, validar convergencia en escenarios de fallo simulado

Producciones esperadas :

- Diagrama de topología OSPF con áreas definidas
- Configuración de OSPF en todos los routers
- Tabla de enrutamiento optimizada con rutas OSPF
- Documentación de parámetros OSPF configurados
- Reporte de validación de convergencia
- Plan de rollback en caso de problemas

Competencias evaluadas : C5

Configuración de BGP para Peering Externo con Proveedores

Contexto : Una empresa necesita establecer conectividad con múltiples proveedores de Internet mediante BGP. Se requiere configurar peering eBGP, implementar políticas de enrutamiento para controlar qué rutas se aceptan y anuncian, y validar que el tráfico sigue rutas óptimas según políticas de la empresa.

Restricciones : Implementar filtros de prefijos para seguridad, aplicar políticas de preferencia de ruta, documentar todas las políticas de enrutamiento, validar que no se anuncian rutas privadas al exterior

Producciones esperadas :

- Configuración de sesiones BGP con proveedores
- Route-maps para implementación de políticas
- Listas de acceso para filtrado de prefijos
- Tabla de enrutamiento BGP con rutas óptimas
- Documentación de políticas de enrutamiento
- Reporte de validación de peering BGP

Competencias evaluadas : C5

Implementación de MPLS VPN para Conectividad Segura entre Sedes

Contexto : Una empresa multinacional requiere implementar MPLS VPN para conectar de forma segura sus múltiples sedes a través de una red de proveedor. Se requiere configurar PE y CE, establecer LSP, crear VRF para separar tráfico de diferentes clientes internos, y validar aislamiento de tráfico entre sedes.

Restricciones : Garantizar aislamiento completo de tráfico entre VRF, validar conectividad de extremo a extremo, documentar topología de MPLS VPN, implementar redundancia de LSP para alta disponibilidad

Producciones esperadas :

- Configuración de PE y CE para MPLS VPN
- Definición de VRF en routers PE
- LSP configurados y validados
- Tabla de enrutamiento de VRF con rutas correctas
- Documentación de topología MPLS VPN
- Reporte de validación de aislamiento de tráfico

Competencias evaluadas : C6

Optimización de Costos de Enrutamiento en OSPF Existente

Contexto : Una empresa tiene OSPF implementado pero experimenta problemas de enrutamiento subóptimo. Se requiere analizar la tabla de enrutamiento actual, identificar rutas que no siguen caminos óptimos, ajustar costos de enlace para optimizar enrutamiento, y validar que la convergencia se mantiene rápida.

Restricciones : Realizar cambios de forma incremental, validar impacto de cada cambio, mantener disponibilidad de servicios durante optimización, documentar justificación de cada cambio de costo

Producciones esperadas :

- Análisis de tabla de enrutamiento actual
- Identificación de rutas subóptimas
- Propuesta de ajustes de costo con justificación
- Configuración de nuevos costos de enlace
- Tabla de enrutamiento optimizada
- Reporte de validación de convergencia post-optimización

Competencias evaluadas : C5

Diagnóstico y Resolución de Problema de Convergencia en BGP

Contexto : Una empresa experimenta problemas de convergencia lenta en BGP cuando cambia la topología de red. Se requiere diagnosticar la causa del problema, analizar configuración de BGP, identificar si es problema de timers, políticas o configuración de vecinos, y resolver el problema.

Restricciones : Utilizar herramientas de diagnóstico apropiadas, documentar todos los pasos de diagnóstico, validar resolución del problema, minimizar impacto en tráfico durante diagnóstico

Producciones esperadas :

- Análisis de configuración BGP
- Captura de paquetes BGP durante cambio de topología
- Identificación de causa raíz del problema
- Cambios de configuración realizados
- Validación de convergencia mejorada
- Documentación de problema y solución

Competencias evaluadas : C5

Pruebas esperadas

■ Pruebas documentales

- Configuraciones de OSPF documentadas con parámetros críticos
- Configuraciones de BGP con políticas de enrutamiento
- Configuraciones de MPLS y VRF
- Diagramas de topología de enrutamiento
- Tablas de enrutamiento capturadas y analizadas
- Documentación de route-maps y filtros
- Reportes de validación de convergencia
- Documentación de políticas de enrutamiento
- Planes de implementación y rollback
- Registros de cambios de configuración

■ Pruebas de acción (en campo)

- Configuración de procesos OSPF en routers
- Definición de áreas OSPF y parámetros de costo
- Establecimiento de sesiones BGP con vecinos
- Implementación de route-maps para políticas de enrutamiento
- Configuración de filtros de prefijos
- Habilitación de MPLS en interfaces
- Configuración de VRF para aislamiento de tráfico
- Establecimiento de LSP en MPLS
- Validación de adyacencias de protocolo
- Prueba de conectividad de extremo a extremo
- Análisis de tabla de enrutamiento
- Ajuste de parámetros de convergencia

■ Pruebas reflexivas

- Análisis de decisiones de diseño de áreas OSPF
- Justificación de selección de costos de enrutamiento
- Evaluación de impacto de políticas BGP en tráfico
- Reflexión sobre trade-offs entre convergencia y estabilidad

• Análisis de lecciones aprendidas en implementación
• Evaluación de efectividad de políticas de enrutamiento
• Reflexión sobre mejoras futuras en diseño de enrutamiento
• Análisis de problemas encontrados y soluciones aplicadas
• Evaluación de cumplimiento de requisitos de negocio
• Reflexión sobre impacto de cambios en rendimiento de red

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Configuración de protocolos de enrutamiento cumple con estándares RFC y mejores prácticas de la industria	Verificación de parámetros configurados contra RFC 2328 (OSPF), RFC 4271 (BGP), RFC 3031 (MPLS)
Qualité	Convergencia de enrutamiento es rápida y estable ante cambios de topología	Tiempo de convergencia < 5 segundos para OSPF, < 30 segundos para BGP, ausencia de bucles de enrutamiento
Comunicación	Documentación de configuraciones es clara, completa y permite reproducción por otros administradores	Documentación incluye diagrama de topología, parámetros configurados, justificación de decisiones, plan de rollback
Pertinence	Rutas seleccionadas son óptimas según métricas de costo y políticas de enrutamiento definidas	Análisis de tabla de enrutamiento confirma que rutas seleccionadas son óptimas, ausencia de rutas subóptimas
Traçabilité	Todos los cambios de configuración están documentados con fecha, autor, justificación y resultado	Registro de cambios completo, documentación de antes/después, validación de impacto de cambios
Cohérence	Configuración de enrutamiento es coherente entre todos los routers y refleja arquitectura de red diseñada	Verificación de que todos los routers tienen configuración consistente, tabla de enrutamiento refleja topología diseñada
Posture	Profesional demuestra rigor en validación de configuraciones y documentación de decisiones técnicas	Validación de convergencia en escenarios de fallo, documentación de justificación de parámetros, prueba de conectividad de extremo a extremo

Umbral de validación : Promedio ≥ 10/20

Bloque 3 - Gestión de Calidad de Servicio y Monitorización de Tráfico

Indicadores de desempeño por misión

Misión	Indicadores SMART
M11 — Aplicar políticas de QoS para priorizar tráfico de red	Porcentaje de tráfico crítico que recibe priorización configurada (objetivo: 100%) Latencia promedio de tráfico de voz medida en ms (objetivo: <150ms) Jitter máximo en tráfico de video en tiempo real (objetivo: <50ms) Cumplimiento de SLA de ancho de banda garantizado (objetivo: ≥99%)
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Número de cuellos de botella identificados mediante análisis de tráfico Reducción de latencia después de implementar QoS (objetivo: >20%) Mejora en utilización de ancho de banda (objetivo: >15%) Número de recomendaciones de mejora presentadas basadas en análisis

Situaciones de evaluación

Implementación de QoS en red congestionada

Contexto : Una empresa con 500 usuarios experimenta problemas de latencia en aplicaciones de voz y video. La red corporativa tiene enlaces de 1Gbps saturados durante horas pico. Se requiere implementar QoS para priorizar tráfico crítico sin afectar otros servicios.

Restricciones : Cambios deben realizarse sin interrumpir servicios en producción. Debe validarse cumplimiento de SLA de 150ms de latencia para VoIP. Documentación de políticas debe ser completa.

Producciones esperadas :

- Análisis de tráfico actual identificando tipos de aplicaciones y consumo de ancho de banda
- Propuesta de clasificación de tráfico con clases de servicio definidas
- Configuración de QoS en switches y routers con ACL y mapas de políticas
- Plan de implementación por fases minimizando impacto en usuarios
- Validación de cumplimiento de requisitos de QoS con mediciones de latencia y jitter
- Documentación de políticas de QoS implementadas

Competencias evaluadas : C7

Análisis de tráfico y propuesta de mejoras de rendimiento

Contexto : Se requiere analizar patrones de tráfico en una red corporativa para identificar cuellos de botella y proponer mejoras. La empresa tiene múltiples sitios con enlaces WAN de capacidad limitada.

Restricciones : Análisis debe basarse en datos reales de NetFlow o sFlow. Propuestas deben incluir análisis coste-beneficio. Debe identificarse impacto de cambios en SLA.

Producciones esperadas :

- Configuración de herramientas de monitorización de tráfico (NetFlow, sFlow)
- Recopilación de datos de tráfico durante período representativo (mínimo 1 semana)
- Análisis de patrones de tráfico identificando aplicaciones principales
- Identificación de cuellos de botella y anomalías de tráfico
- Propuestas de mejora con análisis coste-beneficio
- Reportes de tráfico con visualizaciones de utilización de ancho de banda

Competencias evaluadas : C1, C7

Validación y ajuste de políticas de QoS en producción

Contexto : Se han implementado políticas de QoS en la red corporativa pero se observan desviaciones en cumplimiento de SLA. Se requiere validar configuración, identificar problemas y realizar ajustes.

Restricciones : Validación debe realizarse sin interrumpir servicios. Ajustes deben ser incrementales y validables. Debe documentarse cada cambio realizado.

Producciones esperadas :

- Plan de validación de políticas de QoS
- Pruebas de priorización de tráfico en diferentes escenarios de congestión
- Mediciones de latencia, jitter y pérdida de paquetes
- Identificación de desviaciones respecto a configuración esperada
- Propuestas de ajuste con justificación técnica
- Implementación de ajustes de forma controlada
- Validación de mejora después de ajustes
- Documentación de cambios realizados

Competencias evaluadas : C7

Diagnóstico de problemas de rendimiento de aplicaciones críticas

Contexto : Usuarios reportan problemas de rendimiento en aplicación de voz corporativa. Se requiere diagnosticar si el problema es de QoS, ancho de banda, latencia o configuración de red.

Restricciones : Diagnóstico debe realizarse sin afectar usuarios. Debe utilizarse múltiples herramientas para validar hallazgos. Causa raíz debe identificarse claramente.

Producciones esperadas :

- Recopilación de información de usuarios sobre síntomas
- Análisis de tráfico de VoIP con herramientas especializadas
- Medición de latencia, jitter y pérdida de paquetes en ruta de VoIP
- Análisis de configuración de QoS en dispositivos de red
- Análisis de utilización de ancho de banda en enlaces críticos
- Identificación de causa raíz del problema
- Propuesta de solución con justificación técnica
- Documentación de diagnóstico y resolución

Competencias evaluadas : C7, C1

Comunicación de requisitos de QoS con stakeholders de negocio

Contexto : Se requiere presentar a directivos de negocio el impacto de QoS en rendimiento de aplicaciones críticas y justificar inversión en mejoras de infraestructura.

Restricciones : Presentación debe ser comprensible para audiencia no técnica. Debe incluir datos de cumplimiento de SLA. Debe presentarse análisis coste-beneficio de propuestas.

Producciones esperadas :

- Análisis de requisitos de QoS por aplicación crítica
- Datos de cumplimiento actual de SLA
- Visualizaciones de impacto de QoS en rendimiento de aplicaciones
- Propuestas de mejora con análisis coste-beneficio
- Presentación ejecutiva con recomendaciones
- Documentación de requisitos de QoS en lenguaje de negocio

Competencias evaluadas : C7

Pruebas esperadas

■ Pruebas documentales

- Políticas de QoS documentadas con clasificación de tráfico definida
- Configuraciones de dispositivos de red con QoS implementado
- Reportes de análisis de tráfico con identificación de patrones
- Reportes de validación de cumplimiento de SLA
- Documentación de cambios realizados en políticas de QoS
- Propuestas de mejora con análisis coste-beneficio
- Diagramas de topología de red con políticas de QoS indicadas
- Registros de monitorización de tráfico y métricas de QoS

■ Pruebas de acción (en campo)

- Configuración de clasificación de tráfico en switches y routers
- Implementación de marcado de tráfico (DSCP, CoS)
- Configuración de colas prioritarias y limitación de ancho de banda
- Aplicación de políticas de QoS a interfaces de red
- Validación de priorización de tráfico mediante pruebas
- Ajuste iterativo de parámetros de QoS basado en observación
- Recopilación de datos de tráfico mediante herramientas de monitorización
- Análisis de flujos de tráfico para identificar anomalías

■ Pruebas reflexivas

- Análisis de cumplimiento de requisitos de QoS versus configuración implementada
- Evaluación de efectividad de políticas de QoS en resolución de problemas de rendimiento
- Reflexión sobre impacto de cambios de QoS en experiencia de usuarios
- Análisis de lecciones aprendidas en implementación de QoS
- Evaluación de necesidad de ajustes basada en datos de monitorización
- Reflexión sobre comunicación de requisitos técnicos a stakeholders de negocio
- Análisis de oportunidades de mejora continua en políticas de QoS

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Las políticas de QoS implementadas cumplen con estándares corporativos de priorización de tráfico	100% de políticas de QoS alineadas con estándares definidos, validadas mediante auditoría de configuración
Qualité	La configuración de QoS garantiza cumplimiento de requisitos de latencia, jitter y ancho de banda para aplicaciones críticas	Latencia <150ms para VoIP, jitter <50ms para video, ancho de banda garantizado ≥99% del tiempo
Comunicación	Los requisitos de QoS se comunican claramente a stakeholders técnicos y de negocio en lenguaje apropiado	Documentación de requisitos comprensible para audiencia técnica y ejecutiva, presentaciones con datos visuales claros
Pertinence	Las políticas de QoS se basan en análisis de tráfico real y requisitos de negocio identificados	Políticas justificadas mediante datos de análisis de tráfico, alineadas con requisitos de SLA de aplicaciones críticas
Traçabilité	Todos los cambios de QoS están documentados con justificación técnica y resultados de validación	Documentación completa de cada cambio, registros de validación, trazabilidad de decisiones técnicas
Cohérence	Las políticas de QoS son coherentes en toda la infraestructura de red y no generan conflictos entre dispositivos	Validación de consistencia de políticas en switches y routers, ausencia de conflictos de configuración
Posture	El profesional demuestra rigor en validación de QoS, ajuste iterativo basado en observación y comunicación clara con stakeholders	Validación exhaustiva de cumplimiento de requisitos, documentación de proceso de ajuste, comunicación efectiva de resultados

Umbral de validación : Promedio ≥ 10/20

Bloque 4 - Diagnóstico y Resolución de Incidencias de Red y Conectividad

Indicadores de desempeño por misión

Misión	Indicadores SMART
M12 — Diagnosticar y resolver incidencias de conectividad de red	Porcentaje de incidencias de conectividad resueltas en primera línea sin escalado Tiempo promedio de diagnóstico desde apertura de incidencia hasta identificación de causa raíz Número de herramientas de diagnóstico utilizadas correctamente por incidencia Tasa de incidencias resueltas correctamente en primer intento sin reapertura
M15 — Coordinar la resolución de incidencias con proveedores externos	Tiempo de respuesta a incidencias de conectividad crítica Porcentaje de incidencias escaladas a proveedores con documentación completa Tiempo promedio de resolución de incidencias escaladas Satisfacción del usuario con proceso de diagnóstico y resolución

Situaciones de evaluación

Diagnóstico de Problema de Conectividad de Red en Puesto de Usuario

Contexto : Un usuario reporta que no puede acceder a Internet ni a recursos de red corporativa. El equipo está conectado por cable Ethernet a un puerto de switch. Se requiere diagnosticar si el problema es de configuración de IP, conectividad física, DHCP o enrutamiento.

Restricciones : Disponibilidad limitada del usuario para pruebas. No se puede interrumpir servicio de otros usuarios en el switch. Se debe completar diagnóstico en máximo 30 minutos.

Producciones esperadas :

- Registro de síntomas iniciales reportados por usuario
- Documentación de pasos de diagnóstico realizados (ping, ipconfig, traceroute)
- Captura de pantalla o salida de comandos de diagnóstico
- Identificación clara de causa raíz del problema
- Solución implementada y validada
- Confirmación de resolución con usuario
- Cierre de incidencia con documentación completa

Competencias evaluadas : C8, C17

Análisis de Captura de Paquetes para Identificar Problema de Conectividad

Contexto : Se ha capturado tráfico de red de un usuario que reporta conectividad intermitente. Se requiere analizar la captura con Wireshark para identificar si el problema es de pérdida de paquetes, latencia excesiva, problemas de DNS, o configuración de red.

Restricciones : Captura de paquetes contiene tráfico de múltiples usuarios. Se debe analizar sin comprometer privacidad de datos. Análisis debe completarse en máximo 45 minutos.

Producciones esperadas :

- Apertura de captura de paquetes en Wireshark
- Filtrado de tráfico relevante al problema
- Análisis de protocolos de capa 2, 3 y 4
- Identificación de anomalías en tráfico
- Gráficos de análisis de flujos
- Conclusiones sobre causa raíz
- Recomendaciones de resolución

Competencias evaluadas : C8

Resolución de Problema de Conectividad Wi-Fi en Puesto de Usuario

Contexto : Un usuario reporta que su equipo portátil no puede conectarse a la red Wi-Fi corporativa. Otros usuarios en la misma área pueden conectarse sin problemas. Se requiere diagnosticar si el problema es de configuración de Wi-Fi, autenticación, driver de red, o cobertura de señal.

Restricciones : Usuario necesita conectarse urgentemente para trabajar. No se puede desconectar otros usuarios. Se debe completar diagnóstico en máximo 20 minutos.

Producciones esperadas :

- Verificación de disponibilidad de redes Wi-Fi visibles
- Prueba de conexión a red Wi-Fi corporativa
- Análisis de configuración de seguridad Wi-Fi
- Verificación de driver de adaptador Wi-Fi
- Prueba de autenticación 802.1X
- Análisis de intensidad de señal
- Solución implementada (reconexión, actualización de driver, etc.)
- Validación de conectividad y acceso a recursos

Competencias evaluadas : C17

Diagnóstico de Problema de Conectividad VPN de Usuario Remoto

Contexto : Un usuario remoto reporta que no puede conectarse a la VPN corporativa. Otros usuarios remotos pueden conectarse sin problemas. Se requiere diagnosticar si el problema es de configuración de cliente VPN, credenciales, firewall, o conectividad de Internet.

Restricciones : Usuario está trabajando desde ubicación remota sin acceso a soporte presencial. Diagnóstico debe realizarse por teléfono o chat. Se debe completar en máximo 30 minutos.

Producciones esperadas :

- Recopilación de información sobre error reportado
- Guía paso a paso para verificación de configuración VPN
- Instrucciones para prueba de conectividad de Internet
- Verificación de credenciales de usuario
- Análisis de logs de cliente VPN
- Prueba de conexión VPN con instrucciones del usuario
- Solución implementada (reconexión, actualización de cliente, etc.)
- Confirmación de acceso a recursos corporativos

Competencias evaluadas : C8, C17

Diagnóstico de Problema de Conectividad de Red en Infraestructura

Contexto : Se reporta que un departamento completo ha perdido conectividad de red. Se requiere diagnosticar si el problema es de switch, router, enlace WAN, o configuración de VLAN. Se necesita restaurar conectividad rápidamente.

Restricciones : Múltiples usuarios afectados. Se requiere diagnóstico rápido y escalado si es necesario. Se debe documentar completamente para análisis posterior.

Producciones esperadas :

- Verificación de estado de dispositivos de red (switch, router)
- Análisis de tabla de enrutamiento
- Verificación de configuración de VLAN
- Prueba de conectividad entre dispositivos de red
- Análisis de logs de dispositivos de red
- Identificación de punto de fallo
- Escalado a proveedor si es necesario
- Documentación de causa raíz y solución

Competencias evaluadas : C8

Pruebas esperadas

■ Pruebas documentales

- Registro de incidencia con descripción detallada del problema
- Documentación de pasos de diagnóstico realizados
- Capturas de pantalla de salida de comandos de diagnóstico
- Análisis de captura de paquetes con conclusiones
- Identificación documentada de causa raíz
- Descripción de solución implementada
- Confirmación de resolución con usuario
- Cierre de incidencia con lecciones aprendidas

■ Pruebas de acción (en campo)

- Ejecución de comandos de diagnóstico (ping, traceroute, ipconfig, netstat)
- Captura de tráfico de red con Wireshark o tcpdump
- Análisis de configuración de interfaces de red
- Verificación de tabla de enrutamiento
- Prueba de conectividad a servicios específicos
- Implementación de solución (reconexión, reconfiguración, etc.)
- Validación de resolución con usuario
- Escalado a nivel superior si es necesario

■ **Pruebas reflexivas**

- Análisis de efectividad de herramientas de diagnóstico utilizadas
- Reflexión sobre metodología de diagnóstico aplicada
- Identificación de mejoras en proceso de diagnóstico
- Análisis de tiempo invertido en diagnóstico
- Evaluación de comunicación con usuario
- Reflexión sobre causa raíz identificada
- Análisis de solución implementada y su efectividad
- Identificación de patrones en problemas similares

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Diagnóstico realizado siguiendo metodología estructurada de capa OSI	Documentación de diagnóstico incluye análisis de al menos 3 capas OSI relevantes al problema
Qualité	Identificación correcta de causa raíz del problema de conectividad	Causa raíz identificada es validada por resolución exitosa del problema sin reapertura de incidencia
Qualité	Utilización apropiada de herramientas de diagnóstico	Se utilizan al menos 2 herramientas diferentes y apropiadas para el tipo de problema
Comunicación	Comunicación clara con usuario durante diagnóstico	Usuario comprende pasos de diagnóstico y puede reproducirlos. Confirmación de resolución obtenida antes de cierre
Traçabilité	Documentación completa de proceso de diagnóstico y resolución	Incidencia contiene registro de síntomas, pasos de diagnóstico, causa raíz, solución y validación
Pertinence	Solución implementada resuelve el problema sin crear nuevos problemas	Incidencia no se reabre. Usuario confirma acceso a recursos necesarios. No hay reportes de problemas secundarios
Posture	Profesionalismo y paciencia en interacción con usuario	Usuario reporta satisfacción con proceso de diagnóstico. Comunicación es respetuosa y sin culpabilización

Umbral de validación : Promedio ≥ 10/20

Bloque 5 - Automatización de Tareas de Red y Sistemas

Indicadores de desempeño por misión

Misión	Indicadores SMART
M13 — Automatizar tareas de red mediante scripts Python	Número de scripts Python desarrollados y validados en entorno de prueba antes de producción Porcentaje de tareas automatizadas que se ejecutan sin errores en primera ejecución Tiempo reducido en ejecución de tareas manuales comparado con automatización Cobertura de documentación de scripts (comentarios, docstrings, README)
M14 — Automatizar tareas de red y sistemas con Ansible	Número de playbooks de Ansible desarrollados y validados Porcentaje de playbooks que se ejecutan correctamente en entorno de producción Tiempo de ejecución de playbooks comparado con configuración manual Número de playbooks integrados en pipelines CI/CD

Situaciones de evaluación

Desarrollo de Script Python para Backup de Configuraciones

Contexto : En una empresa con 50 dispositivos de red (switches y routers Cisco), se requiere automatizar el backup diario de configuraciones. Actualmente se realiza manualmente conectando a cada dispositivo, lo que consume 2 horas diarias. Se solicita desarrollar un script Python que se ejecute automáticamente cada noche.

Restricciones : El script debe conectarse a múltiples dispositivos usando SSH, manejar errores de conexión, almacenar configuraciones con timestamp, generar reporte de ejecución, y documentar el código de forma clara.

Producciones esperadas :

- Script Python funcional que realiza backup de configuraciones
- Documentación del script con parámetros requeridos y ejemplos de uso
- Reporte de ejecución mostrando dispositivos procesados y errores
- Código comentado con explicación de funciones principales

Competencias evaluadas : C9

Creación de Playbook Ansible para Aplicación de Configuraciones

Contexto : Se requiere aplicar la misma configuración de VLAN a 30 switches de red de forma simultánea. Actualmente se realiza manualmente en cada switch, lo que toma 4 horas. Se solicita desarrollar un playbook de Ansible que aplique la configuración de forma idempotente y genere reporte de cambios.

Restricciones : El playbook debe ser idempotente (ejecutable múltiples veces sin cambios), manejar dispositivos con diferentes versiones de IOS, generar reporte de cambios realizados, incluir validación de configuración aplicada, y estar documentado.

Producciones esperadas :

- Playbook Ansible funcional que aplica configuraciones de VLAN
- Documentación del playbook con variables requeridas
- Reporte de ejecución mostrando cambios realizados en cada dispositivo
- Validación de configuración aplicada correctamente

Competencias evaluadas : C9

Automatización de Recopilación de Información de Dispositivos

Contexto : Se requiere recopilar información de rendimiento (CPU, memoria, interfaces activas) de 100 dispositivos de red diariamente para análisis de capacidad. Actualmente se realiza mediante comandos manuales. Se solicita desarrollar un script que recopile información, la procese y genere reportes en formato CSV.

Restricciones : El script debe conectarse a múltiples dispositivos, procesar salida de comandos, manejar variaciones de formato, almacenar datos en CSV, generar gráficos de tendencias, y estar documentado con ejemplos.

Producciones esperadas :

- Script Python que recopila información de dispositivos
- Archivo CSV con datos de rendimiento recopilados
- Reporte de análisis de capacidad con gráficos
- Documentación de script con guía de uso

Competencias evaluadas : C9

Integración de Playbook Ansible en Pipeline CI/CD

Contexto : Se requiere integrar playbooks de Ansible en un pipeline de entrega continua (Jenkins) para aplicar cambios de configuración de forma automática cuando se realiza commit en repositorio Git. Se solicita configurar pipeline que valide, pruebe y aplique playbooks.

Restricciones : El pipeline debe validar sintaxis YAML, ejecutar playbooks en entorno de prueba, generar reporte de cambios, aplicar en producción solo si pruebas son exitosas, y mantener registro de todas las ejecuciones.

Producciones esperadas :

- Pipeline CI/CD configurado en Jenkins
- Playbooks validados y probados automáticamente
- Reporte de ejecuciones del pipeline
- Documentación de proceso de integración

Competencias evaluadas : C9

Desarrollo de Script para Validación de Configuraciones

Contexto : Se requiere validar que todas las configuraciones de red cumplen con estándares corporativos (nombres de dispositivos, configuración de NTP, configuración de logging). Actualmente se realiza mediante revisión manual. Se solicita desarrollar script que valide automáticamente y genere reporte de cumplimiento.

Restricciones : El script debe conectarse a dispositivos, validar múltiples parámetros de configuración, generar reporte de cumplimiento, identificar desviaciones, sugerir correcciones, y estar documentado.

Producciones esperadas :

- Script Python que valida configuraciones
- Reporte de cumplimiento de estándares
- Lista de desviaciones encontradas
- Sugerencias de correcciones

Competencias evaluadas : C9

Pruebas esperadas

■ Pruebas documentales

- Scripts Python con comentarios explicativos y docstrings
- Playbooks de Ansible documentados con descripción de variables
- README con guía de uso de scripts y playbooks
- Documentación de APIs utilizadas
- Ejemplos de ejecución de scripts
- Reportes de validación de scripts en entorno de prueba
- Changelog de versiones de scripts y playbooks
- Documentación de integración en pipelines CI/CD

■ Pruebas de acción (en campo)

- Ejecución de scripts Python en entorno de prueba sin errores
- Ejecución de playbooks de Ansible con validación de resultados
- Validación de idempotencia de playbooks
- Ejecución de scripts en entorno de producción con monitorización
- Aplicación de cambios de configuración mediante automatización
- Recopilación de datos mediante scripts automatizados
- Generación de reportes automatizados
- Integración de playbooks en pipelines CI/CD

■ Pruebas reflexivas

- Análisis de errores encontrados durante ejecución de scripts
- Evaluación de mejoras en eficiencia tras automatización
- Reflexión sobre idempotencia de playbooks
- Análisis de impacto de automatización en operaciones
- Evaluación de mantenibilidad de código desarrollado
- Reflexión sobre seguridad en manejo de credenciales
- Análisis de cobertura de documentación
- Evaluación de validación de cambios antes de producción

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	El script o playbook cumple con estándares de codificación y convenciones de nomenclatura establecidas	Revisión de código verifica cumplimiento de estándares; documentación incluye referencias a estándares aplicados
Qualité	El código está documentado con comentarios explicativos, docstrings y ejemplos de uso	Mínimo 80% de funciones tienen docstrings; scripts incluyen comentarios en secciones complejas; README proporciona ejemplos claros
Comunicación	La documentación es clara y accesible para otros administradores que necesiten mantener o ejecutar el código	Documentación incluye propósito, parámetros, ejemplos; lenguaje es claro y evita jerga innecesaria
Pertinence	El script o playbook resuelve el problema específico identificado y automatiza tareas repetitivas	Script ejecuta tareas identificadas correctamente; reduce tiempo de ejecución manual en al menos 50%
Cohérence	El código mantiene consistencia en estructura, estilo y patrones de implementación	Revisión de código verifica consistencia; funciones similares utilizan patrones similares
Traçabilité	El script o playbook genera registros de ejecución que permiten auditar cambios realizados	Logs incluyen timestamp, dispositivos procesados, cambios realizados, errores encontrados
Posture	El desarrollador valida scripts en entorno de prueba antes de producción y maneja errores de forma robusta	Evidencia de testing en entorno de prueba; manejo de excepciones en código; validación de resultados antes de aplicar cambios

Umbral de validación : Promedio ≥ 10/20

Bloque 6 - Gestión de Incidencias y Coordinación con Proveedores

Indicadores de desempeño por misión

Misión	Indicadores SMART
M15 — Coordinar la resolución de incidencias con proveedores externos	Porcentaje de incidencias escaladas a proveedores que se resuelven dentro del SLA acordado Tiempo promedio de respuesta a solicitudes de información de proveedores Número de casos de soporte abiertos simultáneamente y estado de cada uno Tasa de resolución de incidencias complejas mediante coordinación con proveedores

Situaciones de evaluación

Escalado de Incidencia Crítica de Hardware a Fabricante

Contexto : Un switch de red crítico presenta fallos intermitentes de puertos que afectan a múltiples usuarios. El diagnóstico interno ha identificado que el problema persiste después de reiniciar el dispositivo y actualizar firmware. Se requiere escalar a soporte técnico del fabricante para obtener reemplazo o reparación.

Restricciones : El dispositivo está en producción y debe mantenerse operativo. El tiempo de respuesta del fabricante es de 4 horas. Se requiere documentación completa del problema para acelerar resolución.

Producciones esperadas :

- Caso de soporte abierto con descripción técnica detallada del problema
- Documentación de pasos de diagnóstico realizados y resultados
- Información de contexto incluyendo modelo, versión de firmware y configuración
- Plan de mitigación mientras se resuelve el problema con el fabricante
- Registro de comunicaciones y seguimiento del caso

Competencias evaluadas : C10

Coordinación de Resolución de Problema de Aplicación Corporativa

Contexto : Una aplicación corporativa crítica presenta errores intermitentes que afectan productividad de usuarios. El problema requiere coordinación entre el equipo interno de IT, el proveedor de la aplicación y el equipo de desarrollo. Se necesita recopilar información de múltiples fuentes para identificar causa raíz.

Restricciones : La aplicación es crítica para operaciones. El proveedor requiere información específica de logs y configuración. El equipo de desarrollo necesita acceso a datos de error para análisis. Se requiere mantener comunicación regular con usuarios afectados.

Producciones esperadas :

- Recopilación sistemática de logs de aplicación y errores
- Documentación de pasos reproducibles del problema
- Comunicación clara con proveedor describiendo síntomas y contexto
- Coordinación de acceso a sistemas entre proveedor y equipo interno
- Seguimiento de caso con documentación de avances y soluciones propuestas

Competencias evaluadas : C10

Gestión de Múltiples Casos de Soporte Simultáneos

Contexto : El equipo está gestionando tres casos de soporte simultáneamente con diferentes proveedores: un problema de conectividad de red con el ISP, un problema de rendimiento de base de datos con el proveedor de software, y un problema de hardware con el fabricante de servidores. Cada caso requiere seguimiento regular y comunicación de estado.

Restricciones : Cada proveedor tiene diferentes canales de comunicación y tiempos de respuesta. Se requiere mantener registro actualizado del estado de cada caso. Los usuarios internos necesitan actualizaciones regulares sobre progreso. Se requiere priorizar casos según impacto en operaciones.

Producciones esperadas :

- Sistema de seguimiento de casos con estado actualizado de cada uno
- Registro de comunicaciones con cada proveedor
- Documentación de información proporcionada a cada proveedor
- Reportes de estado para stakeholders internos
- Análisis de progreso y identificación de cuellos de botella

Competencias evaluadas : C10

Resolución de Problema Recurrente mediante Análisis con Proveedor

Contexto : Se ha identificado que un problema de conectividad de red se repite cada mes aproximadamente. El problema afecta a un segmento específico de la red y se resuelve temporalmente reiniciando dispositivos. Se requiere trabajar con el proveedor de equipos de red para identificar causa raíz permanente.

Restricciones : El problema es intermitente y difícil de reproducir. Se requiere recopilar datos de múltiples incidencias para identificar patrón. El proveedor necesita acceso a logs y configuración de dispositivos. Se requiere documentar cada ocurrencia para análisis.

Producciones esperadas :

- Análisis de incidencias recurrentes identificando patrones comunes
- Recopilación de logs y datos técnicos de múltiples ocurrencias
- Comunicación con proveedor presentando análisis de patrón
- Propuesta de soluciones permanentes basadas en análisis
- Documentación de lecciones aprendidas y medidas preventivas

Competencias evaluadas : C10

Comunicación de Requisitos Técnicos Complejos a Proveedor Externo

Contexto : La empresa requiere implementar una solución de conectividad especial que requiere configuración personalizada de equipos de red. Se necesita comunicar requisitos técnicos detallados al proveedor de equipos para que proporcione configuración apropiada. La solución debe cumplir con requisitos de seguridad y rendimiento específicos.

Restricciones : Los requisitos son complejos y requieren explicación técnica clara. El proveedor necesita información suficiente para proporcionar solución apropiada. Se requiere validar que la solución propuesta cumple con requisitos. Se requiere documentación clara de acuerdos.

Producciones esperadas :

- Documento de requisitos técnicos detallados y claros
- Diagramas de arquitectura mostrando configuración requerida
- Especificación de parámetros técnicos y restricciones
- Comunicación clara con proveedor explicando requisitos
- Validación de solución propuesta contra requisitos
- Documentación de acuerdos y compromisos

Competencias evaluadas : C10

Pruebas esperadas

■ Pruebas documentales

- Casos de soporte abiertos con descripción técnica detallada
- Registros de comunicaciones con proveedores (correos, llamadas, reuniones)
- Documentación de información técnica proporcionada a proveedores
- Reportes de estado de casos de soporte
- Análisis de incidencias recurrentes y patrones identificados
- Documentación de soluciones recibidas de proveedores
- Registros de seguimiento de casos con cronología de eventos
- Guías y procedimientos basados en casos resueltos

■ Pruebas de acción (en campo)

- Apertura de casos de soporte con proveedores incluyendo información técnica completa
- Respuesta oportuna a solicitudes de información de proveedores
- Seguimiento regular del estado de casos de soporte
- Coordinación de acceso a sistemas entre proveedores y equipo interno
- Implementación de soluciones proporcionadas por proveedores
- Validación de resoluciones antes de cierre de casos
- Comunicación de estado a stakeholders internos
- Documentación de lecciones aprendidas en base de conocimiento

■ Pruebas reflexivas

- Análisis de efectividad de comunicación con proveedores
- Evaluación de tiempo de resolución versus SLA acordado
- Reflexión sobre criterios de escalado utilizados
- Análisis de patrones en incidencias recurrentes
- Evaluación de calidad de información proporcionada a proveedores
- Reflexión sobre coordinación entre múltiples proveedores
- Análisis de lecciones aprendidas de casos resueltos
- Evaluación de mejoras en procesos de escalado

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Escalado a proveedores se realiza siguiendo procedimientos establecidos de la empresa	100% de escalados documentan motivo, proveedor seleccionado y criterios de escalado aplicados
Qualité	Información técnica proporcionada a proveedores es completa, precisa y suficiente para diagnóstico	Proveedores confirman que información recibida es suficiente en 90% de casos sin solicitar información adicional
Comunicación	Comunicación con proveedores es clara, técnica y profesional	Proveedores reportan que comunicación es clara y comprensible en 95% de interacciones

Familia	Definición	Ponderación
Traçabilité	Todas las interacciones con proveedores están documentadas y trazables	100% de casos de soporte tienen registro completo de comunicaciones y acciones realizadas
Cohérence	Seguimiento de casos de soporte es consistente y coordinado entre múltiples proveedores	Información de estado es consistente entre registros internos y confirmaciones de proveedores en 100% de casos
Pertinence	Escalado a proveedores se realiza en momento apropiado cuando problema está fuera del alcance interno	Análisis de casos muestra que 95% de escalados fueron realizados en momento apropiado según criterios técnicos
Posture	Profesionalismo y colaboración en relaciones con proveedores externos	Proveedores reportan relación profesional y colaborativa en evaluaciones de satisfacción

Umbral de validación : Promedio ≥ 10/20

Bloque 7 - Documentación, Auditoría y Mejora Continua

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Porcentaje de informes técnicos que incluyen análisis de rendimiento con métricas cuantificables Número de mejoras propuestas implementadas basadas en análisis de rendimiento Tiempo promedio de elaboración de informes técnicos de evaluación de hardware Tasa de precisión de predicciones de cuellos de botella identificados en informes
M12 — Diagnosticar y resolver incidencias de conectividad de red	Porcentaje de incidencias de conectividad documentadas con análisis de causa raíz Tiempo promedio de diagnóstico desde apertura de incidencia hasta identificación de causa Número de incidencias resueltas sin escalado a proveedores Tasa de recurrencia de incidencias similares después de resolución
M13 — Automatizar tareas de red mediante scripts Python	Porcentaje de scripts documentados con ejemplos de uso y parámetros Número de tareas automatizadas que reducen tiempo manual de administración Tasa de ejecución exitosa de scripts en producción sin errores Tiempo ahorrado mensual mediante automatización de tareas recurrentes
M14 — Automatizar tareas de red y sistemas con Ansible	Porcentaje de playbooks documentados con descripción de objetivos y parámetros Número de playbooks integrados en pipelines CI/CD Tasa de ejecución exitosa de playbooks en entornos de producción Reducción de tiempo de implementación de cambios mediante automatización
M15 — Coordinar la resolución de incidencias con proveedores externos	Tiempo promedio de respuesta a solicitudes de información de proveedores Porcentaje de casos escalados a proveedores con documentación completa Número de casos resueltos por proveedores en primer contacto Tasa de satisfacción con resoluciones proporcionadas por proveedores

Situaciones de evaluación

Elaboración de Documentación de Procedimientos Técnicos

Contexto : Se requiere documentar un procedimiento completo de configuración de switches VLAN en la infraestructura corporativa. El procedimiento debe ser suficientemente detallado para que otro técnico pueda reproducirlo sin supervisión, incluyendo pasos de validación y rollback.

Restricciones : La documentación debe cumplir con plantillas corporativas, incluir diagramas de topología, parámetros de configuración específicos, y justificación de decisiones técnicas. Debe estar disponible en repositorio de documentación centralizado.

Producciones esperadas :

- Documento de procedimiento con estructura clara y pasos numerados
- Diagramas de topología antes y después de cambios
- Parámetros de configuración específicos con valores
- Procedimiento de validación y pruebas
- Procedimiento de rollback en caso de problemas
- Justificación de decisiones técnicas tomadas

Competencias evaluadas : C11

Preparación y Ejecución de Auditoría de Seguridad de Red

Contexto : Se debe realizar una auditoría técnica de seguridad de la infraestructura de red corporativa para verificar cumplimiento con estándares ISO 27001 y políticas internas. La auditoría debe evaluar configuraciones de seguridad, acceso a dispositivos, y aplicación de parches de seguridad.

Restricciones : La auditoría debe realizarse sin interrumpir servicios en producción, debe documentar evidencia de cumplimiento e incumplimiento, y debe elaborar reporte ejecutivo con recomendaciones priorizadas.

Producciones esperadas :

- Plan de auditoría con alcance y metodología
- Checklist de evaluación de conformidad
- Evidencia recopilada de cumplimiento de controles
- Identificación de no conformidades con severidad
- Reporte de auditoría con hallazgos y recomendaciones
- Plan de remediación con plazos y responsables

Competencias evaluadas : C12

Gestión de Ciclo de Vida de Certificados Digitales

Contexto : Se debe administrar el ciclo de vida completo de certificados SSL/TLS en la infraestructura corporativa, incluyendo monitorización de vigencia, renovación proactiva y gestión de cadenas de certificados. Se requiere mantener inventario actualizado y alertas de vencimiento.

Restricciones : Los certificados deben renovarse antes de expiración para evitar interrupciones de servicio. Se debe mantener documentación de certificados instalados, proveedores de certificación y procedimientos de renovación.

Producciones esperadas :

- Inventario actualizado de certificados con fechas de vencimiento
- Procedimiento de monitorización de vigencia de certificados
- Alertas configuradas para vencimientos próximos
- Solicitudes de renovación enviadas a proveedores con anticipación
- Certificados renovados instalados en dispositivos
- Documentación de cadenas de certificados y validación

Competencias evaluadas : C13

Análisis y Presentación de Propuesta de Mejora de Infraestructura

Contexto : Se ha identificado que la infraestructura de red actual tiene limitaciones de capacidad que afectan rendimiento de aplicaciones críticas. Se debe elaborar propuesta de mejora que incluya análisis técnico, estimación de costos, beneficios esperados y plan de implementación.

Restricciones : La propuesta debe incluir análisis coste-beneficio detallado, comparación de alternativas técnicas, estimación de retorno de inversión, y plan de implementación con mínimo impacto en servicios. Debe ser presentada a stakeholders ejecutivos.

Producciones esperadas :

- Análisis técnico de limitaciones actuales con métricas
- Comparación de soluciones técnicas alternativas
- Estimación de costos de inversión y operación
- Cálculo de beneficios esperados (rendimiento, disponibilidad, seguridad)
- Análisis de retorno de inversión (ROI) y período de amortización
- Plan de implementación con fases y cronograma
- Presentación ejecutiva con recomendación

Competencias evaluadas : C19

Documentación y Validación de Cambios de Configuración de Red

Contexto : Se ha implementado un cambio importante en la configuración de enrutamiento OSPF para optimizar rutas en la red corporativa. Se requiere documentar completamente el cambio, validar que funciona correctamente, y mantener trazabilidad de la modificación.

Restricciones : La documentación debe incluir configuración anterior y nueva, justificación del cambio, pasos de implementación, validación de convergencia, y plan de rollback. Debe registrarse en sistema de gestión de cambios corporativo.

Producciones esperadas :

- Solicitud de cambio (RFC) completamente documentada
- Comparación de configuración anterior y nueva
- Justificación técnica del cambio con análisis de impacto
- Procedimiento de implementación paso a paso
- Validación de convergencia de rutas después del cambio
- Documentación de tabla de enrutamiento resultante
- Registro de cambio en sistema de gestión de cambios

Competencias evaluadas : C11

Pruebas esperadas

■ Pruebas documentales

- Documentación técnica de procedimientos con estructura clara y pasos detallados
- Reportes de auditoría con hallazgos, evidencia y recomendaciones
- Inventario de certificados digitales con fechas de vencimiento
- Propuestas de mejora con análisis coste-beneficio y ROI
- Registros de cambios en sistema de gestión de cambios
- Diagramas de topología de red actualizados
- Políticas de seguridad documentadas y validadas
- Planes de remediación de no conformidades
- Evidencia de cumplimiento de estándares regulatorios

■ Pruebas de acción (en campo)

- Elaboración de documentación de procedimientos técnicos
- Ejecución de auditorías técnicas de seguridad
- Monitorización proactiva de vigencia de certificados
- Renovación de certificados antes de vencimiento
- Implementación de cambios documentados en sistema de gestión
- Validación de configuraciones después de cambios
- Identificación de oportunidades de mejora mediante análisis de datos
- Presentación de propuestas de mejora a stakeholders
- Seguimiento de planes de remediación de auditorías

■ **Pruebas reflexivas**

- Análisis de efectividad de procedimientos documentados
- Evaluación de conformidad con estándares de seguridad
- Reflexión sobre lecciones aprendidas de auditorías
- Análisis de impacto de mejoras implementadas
- Evaluación de precisión de estimaciones coste-beneficio
- Revisión de procesos de gestión de cambios
- Análisis de recurrencia de no conformidades
- Evaluación de eficiencia de automatización implementada
- Reflexión sobre mejoras en procesos de documentación

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Documentación técnica cumple con plantillas corporativas y estándares de nomenclatura establecidos	100% de documentación elaborada sigue estructura y formato corporativo
Qualité	Procedimientos documentados son suficientemente detallados para reproducción sin supervisión	Otro técnico puede ejecutar procedimiento sin necesidad de aclaraciones adicionales
Traçabilité	Todos los cambios de infraestructura están registrados en sistema de gestión de cambios con justificación	100% de cambios implementados tienen RFC completada con documentación de antes/después
Comunicación	Reportes de auditoría comunican hallazgos de forma clara a stakeholders técnicos y ejecutivos	Stakeholders comprenden hallazgos y recomendaciones sin necesidad de aclaraciones
Pertinence	Propuestas de mejora están basadas en análisis de datos y métricas de infraestructura	Cada propuesta incluye análisis cuantitativo de problema actual y beneficios esperados
Cohérence	Auditorías técnicas evalúan conformidad con estándares de seguridad y políticas corporativas de forma consistente	Criterios de evaluación aplicados uniformemente en todas las auditorías realizadas
Posture	Profesionalismo en recopilación de evidencia, objetividad en evaluación y confidencialidad de información sensible	Auditorías realizadas sin sesgos, evidencia documentada objetivamente, información sensible protegida

Umbral de validación : Promedio ≥ 10/20

Bloque 8 - Administración de Sistemas Operativos y Servicios de Servidor

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Porcentaje de métricas de rendimiento recopiladas correctamente según especificaciones Número de cuellos de botella identificados y documentados en informe técnico Precisión de recomendaciones de mejora validadas con múltiples fuentes de datos Tiempo de elaboración de informe técnico desde recopilación de datos

Situaciones de evaluación

Instalación y Configuración de Windows Server con Roles Específicos

Contexto : Se requiere instalar un nuevo servidor Windows Server 2019 en el centro de datos corporativo con roles de Active Directory, DNS y DHCP para soportar la infraestructura de red de la empresa. El servidor debe estar completamente configurado, documentado y validado antes de pasar a producción.

Restricciones : Debe realizarse en ventana de mantenimiento sin impacto en servicios existentes. Requiere backup de configuración antes de cambios. Debe cumplir con políticas de seguridad corporativas. Documentación completa obligatoria.

Producciones esperadas :

- Servidor Windows Server instalado y configurado con roles requeridos
- Documentación de roles y características instalados
- Validación de funcionamiento de servicios
- Registro de cambios realizados con fecha y usuario
- Plan de rollback documentado

Competencias evaluadas : C20

Instalación de Linux con Servicios de Servidor

Contexto : Se requiere instalar un servidor Linux (CentOS/Ubuntu) que actuará como servidor web y de aplicaciones. El servidor debe estar configurado con servicios específicos, actualizaciones de seguridad aplicadas y completamente documentado.

Restricciones : Instalación en entorno de prueba antes de producción. Debe cumplir con estándares de seguridad corporativos. Requiere documentación de servicios instalados. Validación de funcionamiento obligatoria.

Producciones esperadas :

- Servidor Linux instalado con servicios requeridos
- Documentación de servicios configurados
- Validación de servicios activos y funcionando
- Registro de cambios de configuración
- Documentación de acceso y credenciales

Competencias evaluadas : C20

Aplicación de Actualizaciones de Seguridad en Servidores de Producción

Contexto : Se han publicado parches de seguridad críticos para Windows Server y Linux. Se requiere planificar e implementar actualizaciones en servidores de producción minimizando impacto en servicios. Debe incluir validación post-actualización y documentación completa.

Restricciones : Planificación en ventana de mantenimiento. Backup obligatorio antes de actualización. Validación de servicios críticos después de actualización. Rollback plan documentado. Comunicación a stakeholders.

Producciones esperadas :

- Plan de actualización documentado con ventana de mantenimiento
- Backup de configuración realizado
- Actualizaciones aplicadas correctamente
- Validación de funcionamiento post-actualización
- Documentación de cambios y resultados
- Registro de incidencias si las hay

Competencias evaluadas : C20

Diagnóstico y Resolución de Problema de Servicio en Servidor

Contexto : Un servicio crítico en servidor Windows Server o Linux ha dejado de funcionar. Se requiere diagnosticar el problema, identificar causa raíz y resolver sin impacto en otros servicios. Incluye análisis de logs, validación de configuración y documentación de solución.

Restricciones : Diagnóstico sin interrumpir otros servicios. Documentación completa de pasos realizados. Validación de solución antes de cierre. Comunicación con usuarios afectados. Registro de incidencia.

Producciones esperadas :

- Análisis de logs del sistema
- Identificación de causa raíz del problema
- Solución implementada y validada
- Documentación de pasos de diagnóstico
- Registro de incidencia con resolución
- Comunicación a usuarios sobre resolución

Competencias evaluadas : C20

Documentación Completa de Infraestructura de Servidores

Contexto : Se requiere elaborar documentación completa de la infraestructura de servidores incluyendo inventario, roles instalados, servicios configurados, políticas de seguridad aplicadas y procedimientos de mantenimiento. Esta documentación debe ser clara, actualizada y accesible para el equipo de operaciones.

Restricciones : Documentación debe ser clara y comprensible. Debe incluir diagramas de arquitectura. Requiere validación de precisión. Debe mantenerse actualizada. Acceso controlado según políticas de seguridad.

Producciones esperadas :

- Inventario completo de servidores
- Documentación de roles y servicios por servidor
- Diagramas de arquitectura de infraestructura
- Procedimientos de mantenimiento documentados
- Políticas de seguridad aplicadas documentadas
- Registro de cambios históricos
- Guía de troubleshooting para problemas comunes

Competencias evaluadas : C20

Pruebas esperadas

■ Pruebas documentales

- Documentación de roles y características instalados en servidores
- Registros de cambios de configuración con fecha, usuario y justificación
- Documentación de servicios configurados y validados
- Planes de actualización y rollback
- Registros de incidencias resueltas
- Inventario actualizado de servidores
- Procedimientos de mantenimiento documentados
- Reportes de validación post-cambio

■ Pruebas de acción (en campo)

- Instalación de sistemas operativos de servidor
- Configuración de roles y características en Windows Server
- Instalación y configuración de servicios en Linux
- Aplicación de actualizaciones de seguridad
- Validación de funcionamiento de servicios
- Diagnóstico de problemas de servicios
- Realización de backup antes de cambios
- Ejecución de planes de rollback si es necesario

■ Pruebas reflexivas

- Análisis de impacto de cambios en infraestructura
- Evaluación de riesgos de actualizaciones
- Reflexión sobre mejoras en procedimientos de mantenimiento
- Análisis de causa raíz de problemas de servicios
- Evaluación de efectividad de documentación
- Identificación de oportunidades de automatización
- Análisis de lecciones aprendidas de incidencias
- Evaluación de cumplimiento de políticas de seguridad

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Cumplimiento de políticas de seguridad corporativas en configuración de servidores	Verificación de que todas las configuraciones cumplen con políticas documentadas; auditoría de configuración de seguridad
Qualité	Calidad técnica de instalación y configuración de sistemas operativos	Validación de funcionamiento correcto de servicios; ausencia de errores en logs; rendimiento dentro de parámetros esperados

Familia	Definición	Ponderación
Comunicación	Documentación clara y completa de configuraciones y cambios realizados	Documentación incluye suficiente detalle para reproducción; lenguaje claro y preciso; accesible para equipo de operaciones
Pertinence	Relevancia de configuraciones respecto a requisitos de negocio	Configuraciones cumplen con requisitos especificados; servicios instalados son necesarios; no hay servicios innecesarios
Traçabilité	Trazabilidad completa de cambios y configuraciones realizadas	Registro de fecha, hora, usuario y justificación de cada cambio; documentación de antes y después; auditoría de cambios
Cohérence	Coherencia de configuraciones con arquitectura de infraestructura	Configuraciones alineadas con estándares corporativos; consistencia entre servidores similares; integración correcta con infraestructura existente
Posture	Profesionalismo en planificación y ejecución de cambios	Planificación cuidadosa de cambios; comunicación proactiva a stakeholders; validación rigurosa antes de producción; documentación completa

Umbral de validación : Promedio ≥ 10/20

Bloque 9 - Administración de Directorios, Virtualización y Seguridad de Acceso

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Porcentaje de mejoras de hardware implementadas que reducen tiempo de respuesta en más del 15% Número de informes técnicos de evaluación de rendimiento elaborados con análisis de datos de al menos 3 fuentes Tiempo promedio de identificación de cuellos de botella de hardware: máximo 2 horas desde solicitud
M02 — Configurar y mantener switches de red	Número de switches configurados correctamente sin interrupciones de servicio Porcentaje de VLAN implementadas que cumplen especificaciones de segmentación requeridas Tiempo de actualización de firmware completado dentro de ventana de mantenimiento planificada
M03 — Configurar y mantener routers de red	Número de routers configurados con tablas de enrutamiento optimizadas Porcentaje de ACL implementadas que cumplen políticas de seguridad corporativa Tiempo de convergencia de rutas después de cambios de topología: máximo 30 segundos
M04 — Diseñar y administrar redes de capa 2	Número de arquitecturas de capa 2 diseñadas que cumplen requisitos de escalabilidad Porcentaje de topologías con redundancia implementada correctamente Tiempo de recuperación ante fallo de switch: máximo 5 segundos
M05 — Diseñar y administrar redes de capa 3	Número de esquemas de direccionamiento IP diseñados que optimizan utilización de espacio de direcciones Porcentaje de subnetting implementado correctamente según CIDR Documentación de arquitectura de capa 3 completada con diagramas y especificaciones
M06 — Implementar VLANs para segmentar la red	Número de VLAN configuradas que segmentan correctamente la red según requisitos Porcentaje de puertos troncales configurados sin bucles de red Tiempo de implementación de nueva VLAN: máximo 1 hora
M07 — Configurar STP para evitar bucles de red	Número de topologías de switching con STP configurado correctamente Porcentaje de bucles de red prevenidos mediante STP Tiempo de convergencia de STP después de cambio de topología: máximo 30 segundos
M08 — Implantar protocolos de routing dinámico con OSPF	Número de áreas OSPF diseñadas que optimizan convergencia Porcentaje de costes de enrutamiento optimizados según análisis de tráfico Tiempo de convergencia OSPF después de fallo de enlace: máximo 10 segundos

Misión	Indicadores SMART
M09 — Configurar peering y políticas con BGP	Número de peerings BGP configurados correctamente con vecinos externos Porcentaje de políticas de enrutamiento implementadas que cumplen requisitos de negocio Tiempo de propagación de cambios de ruta BGP: máximo 5 minutos
M10 — Gestionar redes MPLS en entornos corporativos	Número de LSP MPLS configurados con redundancia Porcentaje de VPN sobre MPLS implementadas con aislamiento de tráfico verificado Tiempo de recuperación ante fallo de LSP: máximo 50 milisegundos
M11 — Aplicar políticas de QoS para priorizar tráfico de red	Número de políticas QoS implementadas que priorizan tráfico crítico Porcentaje de tráfico prioritario que recibe tratamiento configurado Reducción de latencia de tráfico crítico: mínimo 20% después de implementación
M12 — Diagnosticar y resolver incidencias de conectividad de red	Porcentaje de incidencias de conectividad resueltas en primera línea Tiempo promedio de diagnóstico de problema: máximo 30 minutos Número de capturas de paquetes analizadas correctamente para identificar causa raíz
M13 — Automatizar tareas de red mediante scripts Python	Número de scripts Python desarrollados que automatizan tareas de red Porcentaje de scripts que funcionan sin errores en entorno de producción Documentación de código completada con ejemplos de uso
M14 — Automatizar tareas de red y sistemas con Ansible	Número de playbooks Ansible desarrollados que automatizan tareas de red y sistemas Porcentaje de playbooks integrados en pipelines CI/CD Tiempo de ejecución de playbooks: máximo 5 minutos para tareas estándar
M15 — Coordinar la resolución de incidencias con proveedores externos	Número de casos de soporte escalados a proveedores con información completa Tiempo promedio de respuesta a solicitudes de información de proveedor: máximo 4 horas Porcentaje de incidencias resueltas con coordinación de proveedor: mínimo 80%

Situaciones de evaluación

Diseño e Implementación de Estructura de Active Directory

Contexto : Una empresa con 500 usuarios distribuidos en 5 departamentos (Ventas, Finanzas, IT, Recursos Humanos, Operaciones) requiere implementar una estructura de Active Directory que permita gestión centralizada de usuarios, aplicación de políticas de grupo diferenciadas por departamento y delegación de administración a responsables de cada área.

Restricciones : Debe minimizar tiempo de implementación, garantizar que no se interrumpa servicio actual, aplicar políticas de contraseña corporativas, implementar auditoría de cambios, documentar estructura de OU y políticas de grupo.

Producciones esperadas :

- Diagrama de estructura de OU reflejando organización de empresa
- Especificación de políticas de grupo por departamento
- Documentación de delegación de administración
- Configuración de auditoría de cambios en Active Directory
- Plan de migración de usuarios existentes

Competencias evaluadas : C31

Configuración de Políticas de Seguridad mediante GPO

Contexto : Empresa requiere implementar políticas de seguridad corporativas mediante Políticas de Grupo incluyendo: requisitos de contraseña complejos, bloqueo de cuenta después de 5 intentos fallidos, expiración de contraseña cada 90 días, restricción de acceso a aplicaciones sensibles, auditoría de intentos de acceso fallidos.

Restricciones : Políticas deben aplicarse a todos los usuarios excepto administradores, debe permitir excepciones para cuentas de servicio, debe validarse aplicación de políticas en múltiples equipos, debe documentarse cada política implementada.

Producciones esperadas :

- Políticas de Grupo creadas y vinculadas a OU apropiadas
- Validación de aplicación de políticas en equipos cliente
- Documentación de políticas de seguridad implementadas
- Reportes de cumplimiento de políticas
- Plan de auditoría de políticas de seguridad

Competencias evaluadas : C31

Administración de Máquinas Virtuales en VMware vSphere

Contexto : Centro de datos corporativo con 50 máquinas virtuales ejecutando aplicaciones críticas requiere optimización de recursos, implementación de alta disponibilidad, gestión de snapshots para recuperación ante desastres y monitorización de utilización de recursos.

Restricciones : Debe minimizar tiempo de inactividad durante cambios, debe garantizar que máquinas virtuales críticas tengan recursos suficientes, debe implementar alertas de utilización de recursos, debe documentar configuración de máquinas virtuales.

Producciones esperadas :

- Inventario de máquinas virtuales con especificación de recursos
- Configuración de clustering HA para máquinas virtuales críticas
- Plan de snapshots y recuperación ante desastres
- Monitorización de utilización de recursos implementada
- Documentación de configuración de máquinas virtuales

Competencias evaluadas : C30

Implementación de Control de Acceso a Recursos Corporativos

Contexto : Empresa requiere implementar control granular de acceso a recursos compartidos incluyendo: carpetas de departamento, impresoras especializadas, aplicaciones corporativas y bases de datos. Diferentes roles requieren diferentes niveles de acceso.

Restricciones : Debe aplicarse principio de menor privilegio, debe permitir auditoría de acceso, debe documentarse matriz de permisos, debe validarse que usuarios tienen acceso correcto, debe implementarse revisión periódica de permisos.

Producciones esperadas :

- Matriz de control de acceso por rol y recurso
- Configuración de ACL en recursos compartidos
- Documentación de permisos asignados
- Reportes de auditoría de acceso
- Plan de revisión periódica de permisos

Competencias evaluadas : C31

Sincronización de Directorios y Gestión de Identidades Federadas

Contexto : Empresa con oficinas en múltiples países requiere sincronizar Active Directory local con Azure AD para permitir acceso a aplicaciones en nube, implementar Single Sign-On y gestionar identidades federadas con proveedores de identidad externos.

Restricciones : Debe garantizar sincronización bidireccional de cambios, debe resolver conflictos de sincronización, debe implementar auditoría de cambios de identidad, debe documentarse configuración de sincronización, debe validarse acceso a aplicaciones en nube.

Producciones esperadas :

- Configuración de Azure AD Connect para sincronización
- Especificación de reglas de sincronización
- Configuración de Single Sign-On
- Documentación de sincronización de directorios
- Reportes de auditoría de cambios de identidad

Competencias evaluadas : C31

Pruebas esperadas

■ Pruebas documentales

- Diagrama de estructura de Active Directory con OU y relaciones
- Especificación de Políticas de Grupo implementadas
- Documentación de delegación de administración
- Matriz de control de acceso a recursos
- Configuración de máquinas virtuales en VMware
- Plan de sincronización de directorios
- Reportes de auditoría de acceso y cambios
- Documentación de políticas de seguridad corporativa
- Inventario de máquinas virtuales con especificaciones
- Plan de recuperación ante desastres

■ Pruebas de acción (en campo)

- Crear estructura de OU en Active Directory reflejando organización
- Implementar Políticas de Grupo para seguridad de contraseña

• Configurar delegación de administración a responsables de departamento
• Crear máquinas virtuales en VMware con recursos apropiados
• Configurar clustering HA para máquinas virtuales críticas
• Implementar sincronización de Active Directory con Azure AD
• Configurar control de acceso a recursos compartidos
• Implementar auditoría de cambios en Active Directory
• Configurar monitorización de máquinas virtuales
• Validar aplicación de políticas de seguridad en equipos cliente

■ **Pruebas reflexivas**

• Análisis de estructura de OU diseñada: ¿refleja organización actual?, ¿permite crecimiento futuro?
• Evaluación de políticas de seguridad: ¿son suficientemente restrictivas?, ¿permiten operación normal?
• Revisión de configuración de máquinas virtuales: ¿tienen recursos suficientes?, ¿hay desperdicio de recursos?
• Análisis de matriz de control de acceso: ¿cumple principio de menor privilegio?, ¿hay accesos innecesarios?
• Evaluación de sincronización de directorios: ¿funciona bidireccional?, ¿hay conflictos frecuentes?
• Revisión de auditoría de cambios: ¿se registran todos los cambios?, ¿hay cambios no autorizados?
• Análisis de plan de recuperación ante desastres: ¿es realista?, ¿se ha probado?
• Evaluación de monitorización: ¿se detectan problemas a tiempo?, ¿hay alertas falsas?

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Estructura de Active Directory cumple con políticas de seguridad corporativa y estándares regulatorios (RGPD, LOPD)	Auditoría de cumplimiento verifica que todas las políticas de grupo están implementadas correctamente
Qualité	Configuración de directorios y máquinas virtuales es precisa y completa sin errores de sintaxis	Validación técnica confirma que todas las configuraciones funcionan sin errores
Comunicación	Documentación de estructura de directorios y políticas es clara, completa y accesible a equipo de administración	Documentación incluye diagramas, especificaciones y ejemplos que permiten comprensión clara
Pertinence	Estructura de directorios y políticas de seguridad son apropiadas para tamaño y complejidad de organización	Estructura permite gestión eficiente de usuarios y aplicación de políticas diferenciadas por departamento
Traçabilité	Todos los cambios en directorios, máquinas virtuales y políticas de seguridad están documentados y auditados	Logs de auditoría registran quién realizó cambios, cuándo y qué cambios se realizaron
Cohérence	Políticas de seguridad, control de acceso y configuración de máquinas virtuales son coherentes y complementarias	Revisión de configuración verifica que no hay conflictos entre políticas y que todas trabajan juntas
Posture	Profesional demuestra rigor en validación de configuraciones, documentación completa y comunicación clara con stakeholders	Validación de configuraciones antes de implementación, documentación actualizada y comunicación regular de estado

Umbral de validación : Promedio ≥ 10/20

Bloque 10 - Soporte Técnico a Usuarios Finales

Indicadores de desempeño por misión

Misión	Indicadores SMART
M12 — Diagnosticar y resolver incidencias de conectividad de red	Porcentaje de incidencias de conectividad resueltas en primera llamada Tiempo promedio de resolución de incidencias de red Número de escalados a proveedores externos Tasa de satisfacción de usuarios con soporte remoto
M15 — Coordinar la resolución de incidencias con proveedores externos	Tiempo promedio de respuesta a escalados de proveedores Porcentaje de casos resueltos sin escalado adicional Número de interacciones con proveedores por incidencia Tasa de resolución de problemas complejos

Situaciones de evaluación

Resolución de Incidencia de Conectividad de Usuario Remota

Contexto : Un usuario reporta que no puede conectarse a la red corporativa desde su casa. El usuario no tiene conocimientos técnicos y está frustrado porque necesita acceder a aplicaciones críticas para su trabajo. Debe diagnosticar el problema mediante soporte remoto, identificar si es problema de Wi-Fi, VPN o configuración de red, y resolver la incidencia.

Restricciones : Debe utilizar herramientas de acceso remoto seguro, no puede reiniciar el equipo sin avisar al usuario, debe mantener comunicación clara durante todo el proceso, debe documentar todos los pasos realizados

Producciones esperadas :

- Ticket de soporte completamente documentado con descripción del problema inicial
- Registro de pasos de diagnóstico realizados
- Identificación clara de causa raíz
- Solución implementada y validada
- Confirmación de resolución con usuario
- Documentación de configuración final

Competencias evaluadas : C14, C17

Soporte Presencial para Problema de Hardware en Puesto de Usuario

Contexto : Un usuario reporta que su equipo no enciende. Debe acudir al puesto de trabajo, diagnosticar el problema (puede ser problema de alimentación, conexión, hardware defectuoso), resolver si es posible o escalar a mantenimiento de hardware. El usuario está presente y necesita explicación clara de qué está pasando.

Restricciones : Debe presentarse profesionalmente, debe explicar el problema de forma comprensible para usuario no técnico, debe documentar hallazgos, debe proporcionar estimación de tiempo de resolución

Producciones esperadas :

- Inspección física documentada del equipo
- Diagnóstico claro del problema
- Explicación al usuario de causa y solución
- Resolución implementada o escalado documentado
- Confirmación de funcionamiento
- Referencia de incidencia proporcionada al usuario

Competencias evaluadas : C15, C17

Resolución de Problema de Aplicación Corporativa con Escalado a Proveedor

Contexto : Un usuario reporta error en aplicación de gestión de proyectos que impide crear nuevas tareas. El error es específico de la aplicación y requiere coordinación con proveedor de software. Debe diagnosticar el problema, recopilar información técnica, escalar a proveedor y comunicar solución al usuario.

Restricciones : Debe recopilar información técnica completa para proveedor, debe mantener comunicación regular con usuario sobre progreso, debe documentar todas las interacciones con proveedor, debe validar que solución resuelve problema del usuario

Producciones esperadas :

- Diagnóstico inicial documentado
- Información técnica recopilada para proveedor
- Caso de soporte abierto con proveedor
- Registro de comunicaciones con proveedor
- Solución implementada
- Validación con usuario
- Documentación de resolución final

Competencias evaluadas : C16, C10

Capacitación de Usuario en Nueva Aplicación Corporativa

Contexto : La empresa ha implementado nueva aplicación de gestión de recursos humanos. Debe impartir sesión de capacitación a grupo de usuarios de diferentes niveles técnicos, explicar funcionalidades principales, responder preguntas y proporcionar documentación de referencia.

Restricciones : Debe adaptar nivel de detalle al conocimiento de cada usuario, debe utilizar ejemplos relevantes a su trabajo, debe proporcionar documentación escrita, debe evaluar comprensión, debe estar disponible para preguntas post-capacitación

Producciones esperadas :

- Guía de usuario elaborada
- Presentación de capacitación preparada
- Documentación de procedimientos comunes
- Registro de asistencia a capacitación
- Respuestas a preguntas de usuarios
- Información de contacto para seguimiento

Competencias evaluadas : C18

Análisis de Incidencias Recurrentes y Propuesta de Solución Preventiva

Contexto : Ha identificado que múltiples usuarios reportan problemas similares de desconexión de Wi-Fi en horarios específicos. Debe analizar patrón de incidencias, identificar causa raíz, proponer solución preventiva (puede ser reconfiguración de red, capacitación de usuarios, o mejora de infraestructura), y documentar recomendación.

Restricciones : Debe analizar datos de al menos 5 incidencias similares, debe identificar patrón común, debe proponer solución basada en análisis, debe documentar análisis y recomendación, debe presentar propuesta a equipo técnico

Producciones esperadas :

- Análisis de incidencias recurrentes
- Identificación de patrón común
- Causa raíz identificada
- Propuesta de solución preventiva
- Documentación de análisis
- Presentación de recomendación
- Plan de implementación

Competencias evaluadas : C14, C15, C18

Pruebas esperadas

■ Pruebas documentales

- Tickets de soporte completamente documentados con descripción de problema, pasos de diagnóstico y solución
- Guías de usuario elaboradas para aplicaciones corporativas
- Registros de sesiones de capacitación impartidas
- Documentación de procedimientos de resolución de problemas comunes
- Análisis de incidencias recurrentes con identificación de patrones
- Reportes de satisfacción de usuarios con soporte técnico
- Registros de comunicación con proveedores de aplicaciones
- Manuales de usuario para nuevas aplicaciones

■ Pruebas de acción (en campo)

- Resolución de incidencias de usuarios mediante soporte remoto
- Diagnóstico in situ de problemas en puestos de trabajo
- Configuración de conectividad de usuarios (Wi-Fi, VPN)
- Resolución de problemas de aplicaciones corporativas
- Escalado de problemas complejos a proveedores
- Impartición de sesiones de capacitación a usuarios
- Seguimiento de incidencias hasta cierre
- Validación de soluciones con usuarios

■ **Pruebas reflexivas**

- Análisis de causas raíz de problemas recurrentes
- Evaluación de efectividad de soluciones implementadas
- Reflexión sobre comunicación con usuarios no técnicos
- Análisis de patrones de incidencias para mejora preventiva
- Evaluación de satisfacción de usuarios con soporte
- Identificación de necesidades de capacitación adicional
- Análisis de tiempos de resolución y oportunidades de mejora
- Reflexión sobre coordinación con proveedores externos

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Cumplimiento de políticas corporativas de seguridad en acceso remoto y configuración de conectividad	Verificación de que todas las configuraciones de usuario cumplen políticas de seguridad corporativa, auditoría de acceso remoto realizado
Qualité	Resolución completa y duradera de problemas de usuarios sin recurrencia	Porcentaje de incidencias que no reaparecen en 30 días posteriores a resolución, tasa de satisfacción de usuarios con solución
Comunicación	Comunicación clara y adaptada al nivel técnico del usuario durante diagnóstico y resolución	Evaluación de claridad de explicaciones, confirmación de comprensión del usuario, feedback de usuario sobre comunicación
Pertinence	Identificación correcta de causa raíz y propuesta de solución apropiada al problema	Análisis de diagnóstico realizado, validación de que solución resuelve problema identificado, ausencia de soluciones temporales innecesarias
Traçabilité	Documentación completa de todos los pasos de diagnóstico, resolución y comunicación con usuario	Ticket de soporte con descripción clara, registro de pasos realizados, documentación de solución implementada

Familia	Definición	Ponderación
Posture	Profesionalismo, empatía y paciencia en interacción con usuarios, especialmente en situaciones de frustración	Evaluación de profesionalismo en comunicación, feedback de usuario sobre trato recibido, capacidad de mantener calma ante usuarios frustrados
Cohérence	Coherencia entre diagnóstico realizado, solución propuesta y resultado final obtenido	Validación de que solución implementada corresponde a causa raíz identificada, confirmación de que problema está realmente resuelto

Umbral de validación : Promedio ≥ 10/20

Bloque 11 - Mantenimiento, Instalación de Hardware y Gestión de Configuraciones

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Porcentaje de sistemas configurados según especificaciones corporativas en primer intento Tiempo promedio de configuración de sistema desde instalación de SO hasta aplicación de políticas de seguridad Número de incidencias de configuración reportadas post-instalación Cumplimiento de estándares de seguridad corporativa en sistemas configurados

Situaciones de evaluación

Instalación y Configuración de Estación de Trabajo Corporativa

Contexto : Se requiere preparar una estación de trabajo nueva para un usuario corporativo. El sistema debe instalarse con el sistema operativo estándar, configurarse con políticas de seguridad corporativas, conectarse a la red corporativa y validarse antes de entrega al usuario.

Restricciones : Debe completarse en máximo 2 horas, respetando estándares corporativos de configuración, aplicando todas las políticas de seguridad requeridas, sin interrumpir servicios de red existentes

Producciones esperadas :

- Sistema operativo instalado y actualizado
- Configuración de red completada (IP, DNS, nombre de equipo)
- Políticas de seguridad corporativas aplicadas (firewall, antivirus, contraseña)
- Acceso a recursos corporativos validado
- Documentación de configuración completada
- Validación de funcionamiento de hardware completada

Competencias evaluadas : C28, C29

Asistencia en Instalación de Componentes de Hardware

Contexto : Un usuario requiere asistencia para instalar una tarjeta de red adicional o memoria RAM en su estación de trabajo. Se debe proporcionar instrucciones claras, asistencia durante la instalación, validación de funcionamiento y documentación de cambios.

Restricciones : Debe minimizarse tiempo de inactividad del usuario, respetarse procedimientos de seguridad electrostática, validarse funcionamiento post-instalación, documentarse cambios realizados

Producciones esperadas :

- Instrucciones claras proporcionadas al usuario
- Componentes instalados correctamente
- Validación de funcionamiento del componente
- Documentación de hardware instalado
- Confirmación de satisfacción del usuario

Competencias evaluadas : C29

Diagnóstico y Resolución de Problema de Hardware en Estación de Trabajo

Contexto : Una estación de trabajo presenta problemas de rendimiento o no arranca correctamente. Se debe diagnosticar el problema utilizando herramientas apropiadas, identificar componente defectuoso, resolver problema o escalar a proveedor, y documentar resolución.

Restricciones : Debe utilizarse metodología sistemática de diagnóstico, documentarse todos los pasos realizados, minimizarse tiempo de inactividad del usuario, validarse resolución antes de cierre

Producciones esperadas :

- Diagnóstico sistemático realizado
- Herramientas de diagnóstico utilizadas apropiadamente
- Causa raíz identificada
- Solución implementada o escalada documentada
- Validación de funcionamiento completada
- Reporte de incidencia documentado

Competencias evaluadas : C28, C29

Aplicación de Políticas de Seguridad en Lote de Sistemas Nuevos

Contexto : Se requiere preparar un lote de 10-20 sistemas nuevos aplicando configuración estándar corporativa, políticas de seguridad y validación de funcionamiento. Se debe optimizar proceso para eficiencia manteniendo calidad.

Restricciones : Debe aplicarse configuración idéntica en todos los sistemas, respetarse estándares corporativos, documentarse cada sistema, validarse cumplimiento de políticas de seguridad

Producciones esperadas :

- Configuración estándar aplicada en todos los sistemas
- Políticas de seguridad corporativas implementadas
- Validación de funcionamiento completada en cada sistema
- Documentación de configuración de cada sistema
- Inventario de hardware actualizado
- Reporte de cumplimiento de estándares

Competencias evaluadas : C28, C29

Validación de Configuración y Cumplimiento de Estándares

Contexto : Se requiere validar que un sistema configurado cumple con todos los estándares corporativos de seguridad, configuración y funcionamiento. Se debe realizar auditoría de configuración, verificar políticas aplicadas y documentar hallazgos.

Restricciones : Debe utilizarse checklist de validación corporativa, documentarse cada verificación realizada, identificarse desviaciones de estándares, proponer correcciones necesarias

Producciones esperadas :

- Checklist de validación completado
- Verificación de políticas de seguridad
- Verificación de configuración de red
- Verificación de funcionamiento de hardware
- Identificación de desviaciones de estándares
- Reporte de validación documentado

Competencias evaluadas : C28, C29

Pruebas esperadas

■ **Pruebas documentales**

- Documentación de configuración de sistema completada con especificaciones técnicas
- Registro de políticas de seguridad aplicadas en sistema
- Inventario de hardware actualizado con especificaciones de componentes instalados
- Checklist de validación de configuración completado
- Reporte de diagnóstico de hardware con resultados de pruebas
- Documentación de cambios de hardware realizados
- Registro de cumplimiento de estándares corporativos
- Evidencia de aplicación de políticas de seguridad (capturas de pantalla de configuración)

■ **Pruebas de acción (en campo)**

- Instalación de sistema operativo en estación de trabajo nueva
- Configuración de parámetros de red (IP, DNS, nombre de equipo)
- Aplicación de políticas de seguridad corporativas (firewall, antivirus, contraseña)
- Instalación de drivers de dispositivos
- Instalación de actualizaciones de sistema operativo
- Validación de conectividad de red corporativa
- Asistencia en instalación de componentes de hardware
- Diagnóstico de problemas de hardware utilizando herramientas apropiadas
- Resolución de problemas identificados
- Validación de funcionamiento post-instalación o reparación

■ **Pruebas reflexivas**

- Análisis de desviaciones de estándares corporativos en configuración
- Evaluación de eficiencia de proceso de configuración
- Reflexión sobre problemas encontrados durante instalación y lecciones aprendidas
- Análisis de causas raíz de problemas de hardware
- Evaluación de claridad de comunicación con usuario durante asistencia
- Reflexión sobre mejoras en procedimientos de instalación
- Análisis de cumplimiento de políticas de seguridad aplicadas
- Evaluación de documentación completada para trazabilidad

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Sistema configurado cumple con todos los estándares corporativos de seguridad, configuración y funcionamiento	Checklist de validación corporativa completado al 100% sin desviaciones
Qualité	Configuración de sistema es precisa, completa y sin errores que afecten funcionamiento	Cero incidencias de configuración reportadas post-instalación en período de 30 días
Comunicación	Comunicación clara con usuario durante asistencia en instalación de hardware, explicando procedimientos en lenguaje comprensible	Usuario confirma comprensión de procedimientos y se siente asistido durante proceso

Familia	Definición	Ponderación
Traçabilité	Documentación completa de configuración, cambios y validaciones realizadas para asegurar trazabilidad	Documentación de configuración incluye especificaciones técnicas, políticas aplicadas, cambios realizados y resultados de validación
Pertinence	Selección apropiada de herramientas de diagnóstico y procedimientos según tipo de problema identificado	Herramientas utilizadas son apropiadas para diagnóstico realizado y permiten identificar causa raíz
Posture	Profesionalismo en interacción con usuario, presentación profesional y actitud de servicio durante asistencia	Usuario reporta satisfacción con profesionalismo y disponibilidad del técnico
Cohérence	Configuración de sistema es coherente con arquitectura corporativa, políticas de seguridad y estándares técnicos	Sistema configurado se integra correctamente con infraestructura corporativa sin conflictos de configuración

Umbral de validación : Promedio ≥ 10/20

Bloque 12 - Operaciones IT, Monitorización y Gestión de Cambios

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Evaluar el rendimiento del hardware y proponer mejoras	Número de métricas de rendimiento recopiladas y analizadas por mes Porcentaje de mejoras propuestas implementadas dentro de 30 días Reducción de tiempo de respuesta a incidencias de rendimiento Número de informes técnicos de análisis de rendimiento elaborados
M12 — Diagnosticar y resolver incidencias de conectividad de red	Tiempo medio de resolución de incidencias de conectividad Porcentaje de incidencias resueltas en primer contacto Número de herramientas de diagnóstico utilizadas por incidencia Tasa de precisión en identificación de causa raíz
M15 — Coordinar la resolución de incidencias con proveedores externos	Tiempo medio de respuesta a escalados de proveedores Porcentaje de incidencias resueltas con coordinación de proveedores Número de casos de soporte abiertos y cerrados por mes Tasa de satisfacción con resolución de proveedores

Situaciones de evaluación

Implementación de Monitorización SNMP en Infraestructura de Red

Contexto : Una empresa corporativa requiere implementar monitorización proactiva de su infraestructura de red para detectar problemas antes de que afecten a usuarios. Se debe configurar SNMP en switches y routers, establecer umbrales de alerta y crear dashboards de monitorización.

Restricciones : Debe realizarse sin interrumpir servicios en producción. Debe cumplir con políticas de seguridad de la empresa. Debe documentarse completamente la configuración realizada.

Producciones esperadas :

- Configuración SNMP implementada en dispositivos de red
- Umbrales de alerta definidos y validados
- Dashboard de monitorización funcional
- Documentación de configuración SNMP
- Procedimiento de respuesta a alertas

Competencias evaluadas : C1, C33, C37

Análisis de Tráfico y Planificación de Capacidad

Contexto : Se detecta congestión en enlaces de red durante horas pico. Se requiere analizar tráfico con NetFlow/sFlow, identificar aplicaciones que consumen más ancho de banda y proponer mejoras de capacidad.

Restricciones : Análisis debe realizarse sin impactar rendimiento de red. Debe utilizarse herramientas de análisis de tráfico apropiadas. Propuestas deben incluir análisis coste-beneficio.

Producciones esperadas :

- Reporte de análisis de tráfico con gráficos
- Identificación de aplicaciones de alto consumo
- Propuesta de mejora de capacidad con justificación
- Estimación de costo de mejora
- Cronograma de implementación

Competencias evaluadas : C1, C37, C38

Gestión de Cambio Controlado en Producción

Contexto : Se requiere actualizar firmware de switches de core en horario de mantenimiento. Se debe planificar cambio, evaluar riesgo, comunicar a usuarios, ejecutar cambio con validación y documentar.

Restricciones : Cambio debe realizarse en ventana de mantenimiento aprobada. Debe minimizarse impacto en usuarios. Debe existir plan de rollback. Debe documentarse completamente.

Producciones esperadas :

- Solicitud de cambio (RFC) completa
- Evaluación de impacto de cambio
- Plan de implementación con pasos detallados
- Plan de rollback
- Comunicación a usuarios
- Validación post-cambio
- Documentación de cambio realizado

Competencias evaluadas : C34, C35, C11

Respuesta a Incidencia Crítica de Disponibilidad

Contexto : Se reporta caída de servicio crítico que afecta a 500+ usuarios. Se requiere identificar causa raíz rápidamente, escalar si es necesario, comunicar estado regularmente y resolver incidencia.

Restricciones : Tiempo de respuesta crítico. Debe comunicarse estado cada 15 minutos. Debe escalarse a proveedores si es necesario. Debe documentarse completamente.

Producciones esperadas :

- Diagnóstico inicial de problema
- Identificación de causa raíz
- Escalado a proveedores si es necesario
- Comunicaciones de estado a usuarios
- Resolución de incidencia
- Reporte post-incidencia con lecciones aprendidas

Competencias evaluadas : C8, C10, C36, C40

Instalación y Configuración de Servicio Web en Producción

Contexto : Se requiere instalar nuevo servidor web para aplicación corporativa. Se debe instalar software, configurar certificados SSL, optimizar rendimiento y validar funcionamiento.

Restricciones : Debe cumplir con estándares de seguridad corporativos. Debe documentarse completamente. Debe validarse antes de poner en producción.

Producciones esperadas :

- Servidor web instalado y configurado
- Certificados SSL/TLS configurados
- Configuración de virtual hosts
- Optimización de rendimiento realizada
- Validación de funcionamiento
- Documentación de configuración

Competencias evaluadas : C33, C13, C11

Pruebas esperadas

■ Pruebas documentales

- Reportes de análisis de rendimiento de infraestructura
- Configuraciones SNMP documentadas
- Dashboards de monitorización implementados
- Reportes de análisis de tráfico con NetFlow/sFlow
- Solicitudes de cambio (RFC) completadas
- Planes de implementación de cambios
- Documentación de procedimientos de operación
- Reportes post-incidencia con análisis de causa raíz
- Inventario de configuración actualizado
- Documentación de servicios de servidor instalados

■ Pruebas de acción (en campo)

- Configurar SNMP en dispositivos de red
- Establecer umbrales de alerta en herramientas de monitorización
- Crear dashboards de monitorización
- Analizar tráfico con NetFlow/sFlow
- Elaborar reportes de capacidad
- Ejecutar cambios controlados en producción
- Validar cambios post-implementación
- Responder a incidencias críticas
- Escalar problemas a proveedores
- Instalar y configurar servicios de servidor

■ Pruebas reflexivas

- Reflexión sobre impacto de cambios en usuarios
- Análisis de causa raíz de incidencias
- Identificación de mejoras preventivas
- Evaluación de efectividad de monitorización
- Análisis de tendencias de incidencias
- Revisión de procedimientos de operación
- Lecciones aprendidas de incidencias críticas

• Mejora continua de procesos de operación

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Cambios implementados cumplen con políticas de gestión de cambios corporativas	100% de cambios documentados en RFC, evaluados por comité de cambios y aprobados antes de implementación
Qualité	Monitorización implementada detecta problemas antes de impacto en usuarios	Tiempo medio de detección de problema < 5 minutos, tasa de alertas falsas < 5%
Comunicación	Comunicación clara de estado durante incidencias críticas	Actualizaciones de estado proporcionadas cada 15 minutos durante incidencias, usuarios informados de resolución
Pertinence	Análisis de tráfico identifica aplicaciones críticas y cuellos de botella reales	Propuestas de mejora basadas en datos de tráfico, validadas con stakeholders de negocio
Traçabilité	Documentación completa de cambios, configuraciones y procedimientos	100% de cambios documentados, configuraciones registradas en inventario, procedimientos disponibles para equipo
Posture	Responsabilidad en operaciones críticas con planificación cuidadosa	Todos los cambios planificados con evaluación de riesgo, validación pre-producción, plan de rollback
Cohérence	Operaciones IT alineadas con objetivos de disponibilidad y rendimiento	Cumplimiento de SLA > 99%, tiempo medio de resolución de incidencias < 2 horas

Umbral de validación : Promedio >= 10/20

ANEXO VI Glosario y terminología

Este glosario presenta la terminología del referencial. Los términos siguientes deben utilizarse sistemáticamente en la enseñanza y la evaluación.

1. Términos profesionales obligatorios

- Active Directory
- Administración de Redes
- Análisis de Tráfico
- Auditoría Técnica
- Automatización de Tareas
- Base de Datos
- BGP
- Capa 2
- Capa 3
- Certificados Digitales
- Diagnóstico de Conectividad
- Documentación Técnica
- Gestión de Incidencias
- Infraestructura de Red
- Linux
- Mejora Continua
- Monitorización de Infraestructura
- MPLS
- NetFlow
- OSPF
- QoS
- Router
- Servidor de Correo
- Servidor Web
- sFlow
- SNMP
- Soporte Presencial
- Soporte Remoto
- Soporte Técnico IT
- Spanning Tree Protocol (STP)
- Switch
- Virtualización
- VLAN
- VMware vSphere
- Windows Server

2. Sinónimos normalizados (forma canónica en negrita)

- Análisis de Flujos → **NetFlow**
- Asistencia Directa → **Soporte Presencial**
- Asistencia Remota → **Soporte Remoto**
- Automatización de Administración → **Automatización de Tareas**

- Calidad de Servicio → **QoS**
- Certificados SSL/TLS → **Certificados Digitales**
- Conmutación de Etiquetas → **MPLS**
- Conmutador → **Switch**
- Diagnóstico de Red → **Diagnóstico de Conectividad**
- Directorio Activo → **Active Directory**
- Encaminador → **Router**
- Enrutamiento Dinámico → **OSPF**
- Enrutamiento entre Sistemas Autónomos → **BGP**
- Evaluación de Cumplimiento → **Auditoría Técnica**
- Examen de Flujos de Datos → **Análisis de Tráfico**
- Gestión de Dispositivos de Red → **SNMP**
- Gestión de Problemas → **Gestión de Incidencias**
- Muestreo de Tráfico → **sFlow**
- Máquinas Virtuales → **Virtualización**
- Plataforma de Virtualización → **VMware vSphere**
- Procedimientos Técnicos → **Documentación Técnica**
- Protocolo de Árbol de Expansión → **Spanning Tree Protocol (STP)**
- Red Virtual → **VLAN**
- Sistema Operativo de Servidor Windows → **Windows Server**
- Sistema Operativo Linux → **Linux**
- Supervisión de Infraestructura → **Monitorización de Infraestructura**

3. Glosario de términos

Término	Definición
Active Directory	Servicio de directorio de Windows Server que gestiona usuarios, grupos, equipos y políticas de seguridad en entornos corporativos centralizados.
Administración de Redes	Conjunto de actividades de planificación, configuración, monitorización y mantenimiento de infraestructuras de red para garantizar disponibilidad, rendimiento y seguridad.
Análisis de Tráfico	Examen detallado de flujos de datos en red para identificar patrones, anomalías, cuellos de botella y optimizar utilización de ancho de banda.
Auditoría Técnica	Evaluación sistemática de sistemas y redes para verificar cumplimiento de estándares de seguridad, regulatorios y de mejores prácticas.
Automatización de Tareas	Uso de scripts, playbooks y herramientas de orquestación para ejecutar automáticamente tareas repetitivas de administración de red y sistemas.
BGP	Protocolo de enrutamiento dinámico de capa 3 utilizado en Internet y redes corporativas para intercambiar información de enrutamiento entre sistemas autónomos.
Capa 2	Nivel de enlace de datos del modelo OSI que gestiona conmutación, VLAN, STP y comunicación entre dispositivos en la misma red local.

Término	Definición
Capa 3	Nivel de red del modelo OSI que gestiona enrutamiento, direccionamiento IP, subnetting y comunicación entre redes diferentes.
Certificados Digitales	Documentos criptográficos que autentican identidad de servidores y usuarios en comunicaciones seguras, requiriendo gestión de vigencia y renovación.
Diagnóstico de Conectividad	Proceso de identificación de problemas de red utilizando herramientas como ping, traceroute, tcpdump y analizadores de protocolos para determinar causa raíz.
Documentación Técnica	Registro detallado de procedimientos, configuraciones, cambios y decisiones técnicas que asegura trazabilidad, continuidad y conocimiento compartido.
Gestión de Incidencias	Proceso estructurado de registro, seguimiento, diagnóstico y resolución de problemas técnicos con documentación de acciones y cierre de casos.
Infraestructura de Red	Conjunto de dispositivos, protocolos y servicios que conforman la red corporativa incluyendo switches, routers, servidores y sistemas de conectividad.
Linux	Sistema operativo de código abierto utilizado en servidores para ejecutar servicios web, correo, base de datos y aplicaciones corporativas.
Monitorización de Infraestructura	Supervisión continua de dispositivos, servicios y recursos de red mediante herramientas que recopilan métricas y generan alertas ante desviaciones.
MPLS	Tecnología de conmutación de etiquetas que optimiza enrutamiento y permite crear redes privadas virtuales (VPN) en infraestructuras de operadores.
NetFlow	Tecnología de análisis de tráfico que captura información de flujos de datos permitiendo elaborar informes de capacidad y detectar patrones de uso.
OSPF	Protocolo de enrutamiento dinámico de capa 3 que calcula rutas óptimas basadas en costos de enlace permitiendo convergencia rápida ante cambios de topología.
QoS	Conjunto de técnicas de clasificación, marcado y gestión de colas de tráfico que garantizan prioridad y ancho de banda para aplicaciones críticas.
Router	Dispositivo de capa 3 que interconecta redes diferentes enrutando paquetes de datos según tablas de enrutamiento y políticas configuradas.
sFlow	Protocolo de muestreo de tráfico que proporciona visibilidad de flujos de datos en switches y routers para análisis de anomalías y capacidad.
SNMP	Protocolo de gestión de red que permite monitorizar dispositivos de red recopilando métricas, definiendo umbrales y generando alertas de anomalías.

Término	Definición
Soporte Presencial	Prestación de asistencia técnica directa en el puesto de trabajo del usuario realizando diagnóstico in situ y resolución de problemas.
Soporte Remoto	Prestación de asistencia técnica a usuarios o sistemas desde ubicación remota utilizando herramientas de acceso remoto, teléfono o Internet.
Soporte Técnico IT	Prestación de asistencia técnica a usuarios finales y sistemas para resolver incidencias, diagnosticar problemas y garantizar continuidad operativa.
Spanning Tree Protocol (STP)	Protocolo de capa 2 que previene bucles de red en topologías redundantes seleccionando un árbol de expansión activo entre múltiples caminos.
Switch	Dispositivo de red de capa 2 que interconecta equipos en una red local mediante puertos Ethernet, permitiendo comunicación directa entre dispositivos.
Virtualización	Tecnología que permite ejecutar múltiples sistemas operativos y aplicaciones en un único servidor físico mediante máquinas virtuales aisladas.
VLAN	Red de área local virtual que segmenta lógicamente una red física en múltiples dominios de broadcast independientes para mejorar seguridad y rendimiento.
VMware vSphere	Plataforma de virtualización empresarial que permite crear, gestionar y optimizar máquinas virtuales en infraestructuras de servidor.
Windows Server	Sistema operativo de servidor de Microsoft que proporciona servicios de directorio, web, correo, base de datos y administración centralizada de redes.