



GUÍA DE EVIDENCIAS DE LA UNIDAD DE COMPETENCIA

“UC2736_3: Gestionar recursos de red y comunicaciones en la nube”

**CUALIFICACIÓN PROFESIONAL: ADMINISTRACIÓN DE
RECURSOS Y SERVICIOS EN LA NUBE**

Código: IFC820_3

NIVEL: 3

1. ESPECIFICACIONES DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA.

Dado que la evaluación de la competencia profesional se basa en la recopilación de pruebas o evidencias de competencia generadas por cada persona candidata, el referente a considerar para la valoración de estas evidencias de competencia (siempre que éstas no se obtengan por observación del desempeño en el puesto de trabajo) es el indicado en los apartados 1.1 y 1.2 de esta GEC, referente que explicita la competencia recogida en las realizaciones profesionales y criterios de realización de la UC2736_3: Gestionar recursos de red y comunicaciones en la nube.

1.1. Especificaciones de evaluación relacionadas con las dimensiones de la competencia profesional.

Las especificaciones recogidas en la GEC deben ser tenidas en cuenta por el asesor o asesora para el contraste y mejora del historial formativo de la persona candidata (especificaciones sobre el saber) e historial profesional (especificaciones sobre el saber hacer y saber estar).

Lo explicitado por la persona candidata durante el asesoramiento deberá ser contrastado por el evaluador o evaluadora, empleando para ello el referente de evaluación (UC y los criterios fijados en la correspondiente GEC) y el método que la Comisión de Evaluación determine. Estos métodos pueden ser, entre otros, la observación de la persona candidata en el puesto de trabajo, entrevistas profesionales, pruebas objetivas u otros. En el punto 2.1 de esta Guía se hace referencia a los mismos.

Este apartado comprende las especificaciones del “saber” y el “saber hacer”, que configuran las “competencias técnicas”, así como el “saber estar”, que comprende las “competencias sociales”.

a) Especificaciones relacionadas con el “saber hacer”.

La persona candidata demostrará el dominio práctico relacionado con las actividades profesionales que intervienen en Gestionar recursos de red y comunicaciones en la nube, y que se indican a continuación:

Nota: A un dígito se indican las actividades profesionales expresadas en las realizaciones profesionales de la unidad de competencia, y a dos dígitos las reflejadas en los criterios de realización.

1. Desplegar la infraestructura de red asociada a las aplicaciones de los sistemas según los requisitos de privacidad, seguridad y

disponibilidad, para permitir la conectividad entre recursos de la nube y otras instalaciones "on premises" o en otras nubes.

- 1.1 Los servicios de red para las aplicaciones de la organización se crean de forma automatizada, modificándolos, en su caso, empleando las herramientas y plataformas de nube seleccionadas como plantillas declarativas del servicio o hardware, línea de comandos (CLI), las API ("Application Programming Interface") o automatismos mediante lenguajes de programación, entre otras.
- 1.2 Las redes virtuales se configuran con los rangos de direcciones IP en las zonas de disponibilidad y/o regiones, estableciendo el rango de direccionamiento privado, gestión del direccionamiento público, puertas de enlace, cortafuegos y/o grupos de seguridad, y la delegación de subredes con otros servicios de nube definidos.
- 1.3 Las reglas de cortafuegos y/o grupos de seguridad para los recursos y destinos, se crean en función de las conexiones permitidas, habilitando el tráfico a los protocolos y puertos utilizados, incorporando las opciones de creación de registros disponibles y según las prácticas de la entidad responsable de la seguridad del proyecto.
- 1.4 La resolución de nombres se configura, asignando los parámetros de tipo clave-valor, para que las rutas entre los recursos internos y externos a la red permitan el intercambio de los paquetes entre los destinos, a través de zonas DNS privadas o públicas enlazadas con las redes virtuales definidas.
- 1.5 Los métodos de acceso privado a los recursos internos o en la nube de la red tales como "proxies", túneles VPN ("Virtual Private Network" o Red Privada Virtual), enlaces privados ("Private-public endpoints") o emparejamiento ("peering") entre redes virtuales se crean, configurando el cifrado y la seguridad de la conexión, la autenticación y autorización del usuario, así como su monitorización y registro de accesos.
- 1.6 Los recursos de inspección se crean, ubicándolos en las localizaciones de la topología de red que indique la persona responsable de la arquitectura, para registrar y analizar el tráfico a través de la red por motivos de seguridad o para la resolución de problemas.
- 1.7 El enrutado y conexión entre sistemas locales y servicios WAN de redes se establecen, asignando los parámetros relacionados con dicha tarea, para los escenarios que requieran funciones integradas de red, seguridad y enrutamiento proporcionados de manera gestionada en la nube.

2. Configurar los recursos de red, asignando parámetros de balanceo y escalado horizontal y vertical, desde orígenes externos o internos, en condiciones de seguridad, para el direccionamiento y enrutado de tráfico a los recursos desplegados en la nube.

- 2.1 Los balanceadores de carga se configuran con las reglas y parámetros que permitan el tráfico hacia aplicaciones externas o internas de la organización, redireccionando y balanceando el tráfico entre destinos y permitiendo el escalado de los recursos de computación.
- 2.2 Los recursos de resolución de nombres para el intercambio automático del direccionamiento real de red o DNS (Sistema de Nombres de Dominio) se crean, indicando los parámetros tales como tipo de registro, nombre, host, entre otros, para publicar la conversión mediante URL a direcciones IP, permitiendo varias zonas y subzonas con registros internos o externos en las aplicaciones desplegadas.
- 2.3 Las opciones de caché perimetral distribuido de la nube se configuran, aportando los parámetros tales como punto de conexión, host de origen, encabezado, protocolo, entre otros, para que respondan a las peticiones desde la localización más cercana a los usuarios, permitiendo la respuesta más rápida y económica a los recursos de las aplicaciones de la organización.
- 2.4 Las opciones de traducción de direccionamiento público se establecen, utilizando los servicios del proveedor de nube, compartiendo un pequeño número de direcciones públicas entre recursos como máquinas virtuales o contenedores, sin la necesidad de utilizar una dirección para cada recurso único, permitiendo por otro lado el acceso a internet privado para las aplicaciones desplegadas.
- 2.5 El direccionamiento público y privado se establece para cada uno de los recursos de red que lo requieran, reservando direcciones IP estáticas tanto internas como externas en base a las necesidades de conectividad que tenga cada aplicación, para permitir el direccionamiento de tráfico y la estabilidad en el enrutamiento de las conexiones.
- 2.6 Los servicios de nube para el control perimetral, cortafuegos, enrutamiento y puertas de enlace se habilitan, configurando los parámetros de conectividad, protección, autorización y auditoría, siguiendo los requisitos de seguridad, acceso, supervisión y rendimiento de la organización.

3. Administrar las redes privadas físicas y virtuales de la organización mediante herramientas del proveedor de nube y de fabricantes de dispositivos de conectividad, para disponer de un entorno híbrido con conexiones privadas, directas y de alta capacidad entre los recursos locales y de nube.

- 3.1 Las redes virtuales se configuran, a través de métodos como emparejamiento de redes o redes compartidas, para permitir la conexión interna y directa entre recursos desplegados en la nube, cumpliendo los requisitos de la organización sobre conectividad y administración de las redes y su conexión.
- 3.2 Las conexiones privadas a través de túneles VPN entre las redes de instalaciones locales y redes virtuales en la nube, o entre redes virtuales en la nube en varios proveedores, se establecen utilizando

- protocolos de conexión interna, directa y segura, y cumpliendo los requisitos de conectividad de los entornos, calidad de la conexión, latencia, ancho de banda máximo permitido y costes.
- 3.3 Las conexiones directas y privadas entre redes locales y los proveedores de nube se establecen, mediante la configuración de parámetros de conexión de dispositivos físicos de la organización que permita el enrutamiento de una conexión entre el entorno nube y los equipos de la organización locales, de tal modo que se maximice el ancho de banda, se reduzca la latencia y se potencie la calidad de servicio para aquellos despliegues que requieran estas características.
 - 3.4 Las conexiones directas y de emparejamiento público de redes a través de conectividad física se establecen, permitiendo un direccionamiento de tráfico público a través de los puntos de emparejamiento disponibles para aquellas conexiones públicas cuyos requisitos de calidad de servicio, latencia o coste lo requiera así la organización.
 - 3.5 Los dispositivos de enrutamiento físicos o virtuales se definen, asignando parámetros de configuración en las redes para publicar rutas dinámicas entre las conexiones creadas y permitir la detección automática de cambios en la topología de red.
 - 3.6 Las conexiones VPN "site-to-site" o "point-to-site" se configuran, siguiendo los parámetros establecidos en la organización sobre autenticación, seguridad, cifrado, conexión y configuración de clientes VPN.

4. Configurar la seguridad de los recursos, monitorizando sus conexiones, para registrar los accesos e identificar su potencial riesgo en los sistemas.

- 4.1 Las políticas de seguridad sobre los recursos de la nube se configuran, creando reglas que permitan identificar accesos desde los orígenes y destinos de las comunicaciones para su monitorización y control.
- 4.2 Los servicios de cortafuegos para los servicios de nube se configuran, especificando las reglas, políticas e integración de servicios de terceros definidos por la organización.
- 4.3 Las herramientas para la administración y protección de aplicaciones o servicios "web" se activan, identificando y previniendo posibles ataques y amenazas en capa 7 de comunicaciones, utilizando herramientas WAF ("Web Application Firewall") y/o IPS (Sistema de prevención de intrusos), entre otras, para minimizar los riesgos ante ataques de denegación de servicio ("Denial of Service" o DoS), evitar la fuga de datos y bloqueo de conexiones maliciosas o no deseadas.
- 4.4 Las configuraciones de seguridad para las aplicaciones de la organización se crean, incorporando los parámetros de autorización, autenticación, auditoría, entre otros, empleando los mecanismos de automatización de cada plataforma de nube, durante su provisión, tales como plantillas declarativas del servicio o hardware, línea de comandos (CLI), las API ("Application programming interface") o automatismos mediante lenguajes de programación, modificándolas en su caso,

empleando los mismos mecanismos para la automatización mencionados, permitiendo la trazabilidad, observabilidad y auditoría de los sistemas.

- 4.5 Los recursos de red y la conectividad del resto de recursos desplegados se configuran, para permitir la monitorización de su estado de salud, mediante alertas, estado de conexión, "log" y análisis del tráfico que permitan anticipar problemas o identificar incidencias en las comunicaciones y servicios.

b) Especificaciones relacionadas con el “saber”.

La persona candidata, en su caso, deberá demostrar que posee los conocimientos técnicos (conceptos y procedimientos) que dan soporte a las actividades profesionales implicadas en las realizaciones profesionales de la **UC2736_3: Gestionar recursos de red y comunicaciones en la nube**. Estos conocimientos se presentan agrupados a partir de las actividades profesionales que aparecen en cursiva y negrita:

1. Despliegue de infraestructuras de red asociadas a las aplicaciones de sistemas

- Creación y modificación automatizada de servicios de red para las aplicaciones. Herramientas: plantillas declarativas del servicio o hardware, línea de comandos (CLI), API ("Application programming interface") o automatismos mediante lenguajes de programación, entre otras.
- Direccionamiento privado y público en redes virtuales. Puertas de enlace, cortafuegos y/o grupos de seguridad. Subredes con otros servicios de nube.
- Cortafuegos. Reglas. Grupos de seguridad para los recursos y destinos. Procedimientos de habilitación del tráfico a los protocolos y puertos utilizados.
- Resolución de nombres. Parámetros clave-valor. Zonas DNS privadas o públicas. Enlace con redes virtuales.
- Acceso privado recursos internos: "proxies", túneles VPN ("Virtual Private Network" o Red Privada Virtual) o emparejamiento ("peering") entre redes virtuales. Configuración del cifrado, seguridad de la conexión, autenticación y autorización del usuario. Monitorización y registro de accesos.
- Creación de recursos de inspección de registro y análisis del tráfico. Ubicaciones en una topología de red.
- Enrutado y conexión entre sistemas locales y servicios WAN de redes. Funciones integradas de red, seguridad y enrutamiento proporcionados de manera gestionada en la nube.

2. Configuración de balanceo y escalado de recursos de red

- Configuración de balanceadores de carga. Reglas y parámetros. Tráfico hacia aplicaciones externas o internas. Escalado de los recursos de computación.
- Recursos de resolución de nombres o DNS (Sistema de Nombres de Dominio). Parámetros: tipo de registro, nombre, host, entre otros.
- Parámetros de caché perimetral distribuido de la nube. Punto de conexión, host de origen, encabezado, protocolo, entre otros. Configuración.

- Direccionamiento público y privado. Opciones de traducción. Compartición de direcciones públicas entre recursos: máquinas virtuales o contenedores. Reserva de direcciones IP estáticas internas y externas.
- Servicios de nube para el control perimetral. Cortafuegos, enrutamiento y puertas de enlace. Parámetros de conectividad, protección, autorización y auditoría. Requisitos de seguridad, acceso, supervisión y rendimiento.

3. Administración de redes privadas físicas y virtuales

- Emparejamiento de redes o redes compartidas.
- Establecimiento de conexiones privadas a través de túneles VPN entre las redes físicas y virtuales o entre redes virtuales de varios proveedores. Protocolos de conexión interna, directa y segura. Calidad de la conexión, latencia, ancho de banda y costes.
- Enrutamiento de conexiones entre el entorno nube y equipos locales.
- Conexiones directas y de emparejamiento público de redes a través de conectividad física. Puntos de emparejamiento para conexiones públicas. Requisitos de calidad de servicio, latencia y/o coste.
- Dispositivos de enrutamiento físicos o virtuales en redes. Configuración. Rutas dinámicas. Detección automática de cambios en la topología de red.
- Autenticación, seguridad, cifrado, conexión y configuración de clientes VPN. Conexiones VPN "site-to-site" o "point-to-site".

4. Configuración y monitorización de la seguridad de recursos en nube

- Monitorización y control de accesos a la nube. Definición y configuración de reglas.
- Cortafuegos en la nube. Reglas, políticas e integración de servicios de terceros.
- Herramientas WAF ("Web Application Firewall"). Herramientas IPS (Sistema de prevención de intrusos). Otras herramientas para administración y protección de aplicaciones o servicios "web". Prevención de ataques y amenazas en capa 7 de comunicaciones.
- Configuraciones de seguridad para las aplicaciones. Parámetros de autorización, autenticación, auditoría, entre otros. Mecanismos de automatización de plataforma de nube: plantillas declarativas del servicio o hardware, línea de comandos (CLI), las API ("Application programming interface") o automatismos mediante lenguajes de programación.
- Configuración de la monitorización de recursos de red y conectividad de recursos desplegados. Alertas del estado de conexión, "log" y análisis del tráfico.

c) Especificaciones relacionadas con el "saber estar".

La persona candidata debe demostrar la posesión de actitudes de comportamiento en el trabajo y formas de actuar e interactuar, según las siguientes especificaciones:

- Responsabilizarse del trabajo que desarrolla y del cumplimiento de los objetivos.
- Demostrar cierto grado de autonomía en la resolución de contingencias relacionadas con su actividad.

- Comunicarse eficazmente con las personas adecuadas en cada momento, respetando los canales establecidos en la organización.
- Mantener una actitud asertiva, empática y conciliadora con las personas demostrando cordialidad y amabilidad en el trato.
- Adaptarse a la organización, a sus cambios organizativos y tecnológicos, así como a situaciones o contextos nuevos.
- Aplicar de forma efectiva el principio de igualdad de trato y no discriminación en las condiciones de trabajo entre mujeres y hombres.

1.2. Situaciones profesionales de evaluación y criterios de evaluación.

La situación profesional de evaluación define el contexto profesional en el que se tiene que desarrollar la misma. Esta situación permite al evaluador o evaluadora obtener evidencias de competencia de la persona candidata que incluyen, básicamente, todo el contexto profesional de la Unidad de Competencia implicada.

Así mismo, la situación profesional de evaluación se sustenta en actividades profesionales que permiten inferir competencia profesional respecto a la práctica totalidad de realizaciones profesionales de la Unidad de Competencia.

Por último, indicar que la situación profesional de evaluación define un contexto abierto y flexible, que puede ser completado por las CC.AA., cuando éstas decidan aplicar una prueba profesional a las personas candidatas.

En el caso de la “UC2736_3: Gestionar recursos de red y comunicaciones en la nube”, se tiene una situación profesional de evaluación y se concreta en los siguientes términos:

1.2.1. Situación profesional de evaluación.

a) Descripción de la situación profesional de evaluación.

1.

Condiciones adicionales:

b) Criterios de evaluación asociados a la situación de evaluación.

Cada criterio de evaluación está formado por un criterio de mérito significativo, así como por los indicadores y escalas de desempeño competente asociados a cada uno de dichos criterios.

En la situación profesional de evaluación, los criterios de evaluación se especifican en el cuadro siguiente:

<i>Criterios de mérito</i>	<i>Indicadores de desempeño competente</i>
	-
<i>Cumplimiento del tiempo asignado, considerando el que emplearía un o una profesional competente.</i>	
<i>El desempeño competente requiere el cumplimiento, en todos los criterios de mérito, de la normativa aplicable en materia de prevención de riesgos laborales, protección medioambiental</i>	

No existen escalas

2. MÉTODOS DE EVALUACIÓN DE LA UNIDAD DE COMPETENCIA Y ORIENTACIONES PARA LAS COMISIONES DE EVALUACIÓN Y EVALUADORES/AS.

La selección de métodos de evaluación que deben realizar las Comisiones de Evaluación será específica para cada persona candidata, y dependerá fundamentalmente de tres factores: nivel de cualificación de la unidad de competencia, características personales de la persona candidata y evidencias de competencia indirectas aportadas por la misma.

2.1. Métodos de evaluación y criterios generales de elección.

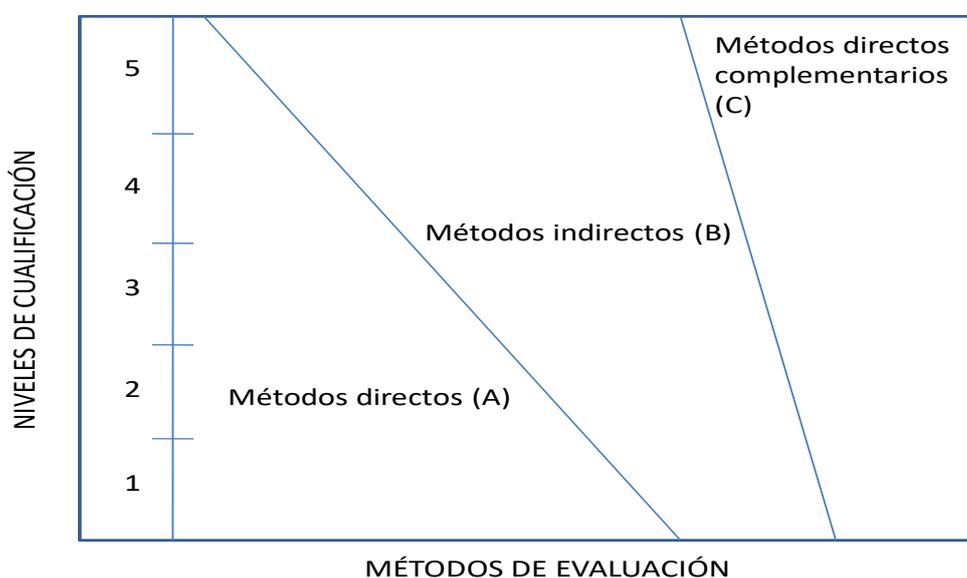
Los métodos que pueden ser empleados en la evaluación de la competencia profesional adquirida por las personas a través de la experiencia laboral, y vías no formales de formación son los que a continuación se relacionan:

- a) **Métodos indirectos:** Consisten en la valoración del historial profesional y formativo de la persona candidata; así como en la valoración de muestras sobre productos de su trabajo o de proyectos realizados.

Proporcionan evidencias de competencia inferidas de actividades realizadas en el pasado.

b) **Métodos directos:** Proporcionan evidencias de competencia en el mismo momento de realizar la evaluación. Los métodos directos susceptibles de ser utilizados son los siguientes:

- Observación en el puesto de trabajo (A).
- Observación de una situación de trabajo simulada (A).
- Pruebas de competencia profesional basadas en las situaciones profesionales de evaluación (C).
- Pruebas de habilidades (C).
- Ejecución de un proyecto (C).
- Entrevista profesional estructurada (C).
- Preguntas orales (C).
- Pruebas objetivas (C).



Fuente: Leonard Mertens (elaboración propia)

Como puede observarse en la figura anterior, en un proceso de evaluación que debe ser integrado (“holístico”), uno de los criterios de elección depende del nivel de cualificación de la UC. Como puede

observarse, a menor nivel, deben priorizarse los métodos de observación en una situación de trabajo real o simulada, mientras que, a niveles superiores, debe priorizarse la utilización de métodos indirectos acompañados de entrevista profesional estructurada.

La consideración de las características personales de la persona candidata, debe basarse en el principio de equidad. Así, por este principio, debe priorizarse la selección de aquellos métodos de carácter complementario que faciliten la generación de evidencias válidas. En este orden de ideas, nunca debe aplicarse una prueba de conocimientos de carácter escrito a una persona candidata a la que se le aprecien dificultades de expresión escrita, ya sea por razones basadas en el desarrollo de las competencias básicas o factores de integración cultural, entre otras. Una conversación profesional que genere confianza sería el método adecuado.

Por último, indicar que las evidencias de competencia indirectas debidamente contrastadas y valoradas, pueden incidir decisivamente, en cada caso particular, en la elección de otros métodos de evaluación para obtener evidencias de competencia complementarias.

2.2. Orientaciones para las Comisiones de Evaluación y Evaluadores.

- a) Cuando la persona candidata justifique sólo formación formal y no tenga experiencia en el proceso de Gestionar recursos de red y comunicaciones en la nube, se le someterá, al menos, a una prueba profesional de evaluación y a una entrevista profesional estructurada sobre la dimensión relacionada con el "saber" y "saber estar" de la competencia profesional.