PROCEDIMIENTO DE EVALUACIÓN Y ACREDITACIÓN DE LAS COMPETENCIAS PROFESIONALES

CUESTIONARIO DE AUTOEVALUACIÓN PARA LAS TRABAJADORAS Y TRABAJADORES

ESTÁNDAR DE COMPETENCIAS PROFESIONALES "ECP2736_3: Gestionar recursos de red y comunicaciones en la nube"

LEA ATENTAMENTE LAS INSTRUCCIONES

Conteste a este cuestionario de **FORMA SINCERA**. La información recogida en él tiene CARÁCTER RESERVADO, al estar protegida por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Su resultado servirá solamente para ayudarle, ORIENTÁNDOLE en qué medida posee la competencia profesional del "ECP2736_3: Gestionar recursos de red y comunicaciones en la nube".

No se preocupe, con independencia del resultado de esta autoevaluación, Ud. TIENE DERECHO A PARTICIPAR EN EL PROCEDIMIENTO DE EVALUACIÓN, siempre que cumpla los requisitos de la convocatoria.

Nombre y apellidos del trabajador/a: NIF:	Firma:
Nombre y apellidos del asesor/a: NIF:	Firma:

INSTRUCCIONES CUMPLIMENTACIÓN DEL CUESTIONARIO:

Las actividades profesionales aparecen ordenadas en bloques desde el número 1 en adelante. Cada uno de los bloques agrupa una serie de actividades más simples (subactividades) numeradas con 1.1., 1.2.,..., en adelante.

Lea atentamente la actividad profesional con que comienza cada bloque y a continuación las subactividades que agrupa. Marque con una cruz, en los cuadrados disponibles, el indicador de autoevaluación que considere más ajustado a su grado de dominio de cada una de ellas. Dichos indicadores son los siguientes:

1. No sé hacerlo.
2. Lo puedo hacer con ayuda.
3. Lo puedo hacer sin necesitar ayuda.
4. Lo puedo hacer sin necesitar ayuda, e incluso podría formar a otro trabajador o trabajadora.

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.1: Crear los servicios de red para las aplicaciones de la organización 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: Configurar las redes virtuales 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: Crear las reglas de cortafuegos y/o grupos de seguridad para los recursos y destinos, 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: Configurar la resolución de nombres, 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: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
1.5: Crear 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, 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: Crear los recursos de inspección, 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: Establecer el enrutado y conexión entre sistemas locales y servicios WAN de redes, 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
2.1: Configurar los balanceadores de carga 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: Crear los recursos de resolución de nombres para el intercambio automático del direccionamiento real de red o DNS (Sistema de Nombres de Dominio), 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: Configurar las opciones de caché perimetral distribuido de la nube, aportando los parámetros tales como punto de conexión, host de origen, encabezado, protocolo, entre otros, para que respondan a las peticiones desde	☐	☐	☐	☐

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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
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: Establecer las opciones de traducción de direccionamiento público, 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: Establecer el direccionamiento público y privado 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: Habilitar los servicios de nube para el control perimetral, cortafuegos, enrutamiento y puertas de enlace, 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.1: Configurar las redes virtuales, 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: Establecer 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, 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: 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
3.3: Establecer las conexiones directas y privadas entre redes locales y los proveedores de nube, 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: Establecer las conexiones directas y de emparejamiento público de redes a través de conectividad física, 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: Definir los dispositivos de enrutamiento físicos o virtuales, 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: Configurar las conexiones VPN "site-to-site" o "point-to-site", 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.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.1: Configurar las políticas de seguridad sobre los recursos de la nube, creando reglas que permitan identificar accesos desde los orígenes y destinos de las comunicaciones para su monitorización y control.	☐	☐	☐	☐
4.2: Configurar los servicios de cortafuegos para los servicios de nube, especificando las reglas, políticas e integración de servicios de terceros definidos por la organización.	☐	☐	☐	☐

4: Configurar la seguridad de los recursos, monitorizando sus conexiones, para registrar los accesos e identificar su potencial riesgo en los sistemas.	INDICADORES DE AUTOEVALUACIÓN			
	1	2	3	4
4.3: Activar las herramientas para la administración y protección de aplicaciones o servicios "web", 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: Crear las configuraciones de seguridad para las aplicaciones de la organización, 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: Configurar los recursos de red y la conectividad del resto de recursos desplegados, 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.	☐	☐	☐	☐