Estándar de competencias profesionales

Gestionar recursos de red y comunicaciones en la nube

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP2736_3**
Estado	**BOE**
Publicación	**RD 546/2023**

Competencia profesional

Elementos de la competencia

EC1 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.

IC1.1 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.

IC1.2 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.

IC1.3 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.

IC1.4 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.

IC1.5 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.

IC1.6 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.

IC1.7 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.

EC2 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.

IC2.1 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.

IC2.2 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.

IC2.3 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.

IC2.4 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.

IC2.5 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.

IC2.6 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.

EC3 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.

IC3.1 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.

IC3.2 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.

IC3.3 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.

IC3.4 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.

IC3.5 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.

IC3.6 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.

EC4 Configurar la seguridad de los recursos, monitorizando sus conexiones, para registrar los accesos e identificar su potencial riesgo en los sistemas.

IC4.1 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.

IC4.2 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.

IC4.3 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.

IC4.4 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.

IC4.5 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.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Conexión a la red. Equipamiento informático: componentes, periféricos, cableado y equipamiento para equipos portátiles, entre otros. Sistemas operativos. Navegadores. Lenguajes de "scripting". Lenguajes estructurados para automatizaciones. Lenguajes declarativos. Utilidades y aplicaciones incorporadas a los sistemas operativos. Versiones de actualización de librerías de API de los servicios de nube. Documentación técnica asociada a los servicios de nube. Utilidades no incorporadas al sistema operativo. Herramientas de depuración. Sistemas de análisis de red. Herramientas de comunicación y colaboración en equipo. Sistemas de monitorización de redes. Sistemas operativos y parámetros de configuración. Servicios de transferencia de ficheros y conexión remota. Herramientas de copia de seguridad. Herramientas de gestión y control de cambios, incidencias y configuración. Aplicaciones de gestión de incidencias, código fuente, gestión de proyectos y comunicación/colaboración.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de protección de datos, propiedad industrial y seguridad informática, normativa aplicable de prevención de riesgos -ergonomía-). Normas internas de trabajo (guías de despliegue, instalación, configuración y actualización de los servicios de las aplicaciones desarrolladas; diseño y especificaciones de los servicios a desplegar y operar; documentación técnica y de usuario del sistema desarrollado; especificaciones de la arquitectura de referencia de servicio en nube corporativo; normas corporativas de desarrollo de software, de pruebas, de control de calidad; documentación asociada a los scripts desarrollados; documentación de las pruebas de funcionamiento de los servicios y aplicaciones desarrolladas). Documentación técnica (manuales y documentación técnica de servicios de proveedores de nube; manuales de condiciones de nivel de servicios de proveedores de nube "Service level agreement" -SLA-; manuales de funcionamiento de las herramientas de gestión del ciclo de vida del software).