CUALIFICACIÓN PROFESIONAL:
Administración de recursos y servicios en la nube

Familia Profesional:	***Informática y Comunicaciones***
Nivel:	***3***
Código:	***IFC820_3***
Estado:	***BOE***
Publicación:	***RD 546/2023***

Competencia general

Administrar el despliegue en plataformas de la nube, gestionando servicios y recursos tales como computación, red y comunicaciones entre sistemas en la nube y equipos locales, almacenamiento de información y bases de datos y automatizando los procesos en su caso, en condiciones de seguridad, cumpliendo la normativa aplicable en materia de protección de datos y propiedad intelectual e industrial y la planificación de la actividad preventiva, así como los estándares de calidad.

Unidades de competencia

UC2735_3: Gestionar recursos y servicios en la nube
UC2736_3: Gestionar recursos de red y comunicaciones en la nube
UC2737_3: Administrar recursos de computación en entornos de nube
UC2738_3: Gestionar recursos de almacenamiento y de bases de datos en la nube
UC2739_3: Desplegar servicios administrados en la nube
UC2740_3: Automatizar despliegues en la nube

Entorno Profesional

Ámbito Profesional

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

Sectores Productivos

Se ubica en el sector servicios, en el subsector de los servicios de desarrollo, instalación, mantenimiento, gestión y asistencia técnica de sistemas informáticos y telemáticos, y en cualquier sector productivo que requiera los servicios anteriores.

Ocupaciones y puestos de trabajo relevantes

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

- Administradores de infraestructuras en la nube
- Administradores de bases de datos en la nube

- Administradores de sistemas en la nube
- Técnicos de soluciones en la nube
- Administradores de operaciones en la nube

Formación Asociada (750 horas)

Módulos Formativos

MF2735_3: Gestión de recursos y servicios en la nube (120 horas)
MF2736_3: Gestión de recursos de red y comunicaciones en la nube (120 horas)
MF2737_3: Administración de recursos de computación en entornos de nube (150 horas)
MF2738_3: Gestionar recursos de almacenamiento y de bases de datos en la nube (150 horas)
MF2739_3: Despliegue de servicios administrados en la nube (90 horas)
MF2740_3: Automatización de despliegues en la nube (120 horas)

UNIDAD DE COMPETENCIA 1

Gestionar recursos y servicios en la nube

Nivel: *3*
Código: *UC2735_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Preparar los interfaces de acceso y uso, configurándolos para acceder a los servicios de la plataforma en la nube.

CR1.1 La conexión a la plataforma para el uso de interfaces gráficas se efectúa mediante un navegador, autenticándose y configurando elementos tales como el idioma, aspecto gráfico y preferencias entre otros, para acceder a los servicios de la plataforma.

CR1.2 Las interfaces de línea de comandos se instalan, previa descarga, en el entorno a utilizar, tal como en local, en un servidor o en una plataforma administrada, inicializando la interfaz, autenticándose y administrando las configuraciones almacenadas.

CR1.3 Las librerías de cliente para los lenguajes de computación a utilizar se descargan, usando los gestores de dependencias.

RP2: Establecer jerarquías de recursos para organizarlos, utilizando los niveles de organización disponibles según el proveedor utilizado, siguiendo las prácticas recomendadas por el proveedor y las directrices de la entidad que suscribe el servicio.

CR2.1 Los nodos que representan una entidad o empresa se crean, siguiendo las directrices de dicha entidad, administrando su configuración para asegurar el funcionamiento de los recursos dependientes de los mismos.

CR2.2 Los niveles intermedios de agrupación de recursos se crean, estableciendo una jerarquía en los mismos y configurando las políticas disponibles, siguiendo las directrices de la entidad respecto a la arquitectura en la planificación inicial.

CR2.3 Los contenedores de recursos de bajo nivel se crean, gestionando las configuraciones de seguridad y control de accesos, facturación y restricciones para permitir el posterior despliegue de recursos.

CR2.4 Las políticas de configuraciones comunes a todos o parte de los recursos de la entidad, tales como restricciones, parametrizaciones de seguridad o etiquetado de recursos, se implementan en cada uno de los niveles de la jerarquía, asignando parámetros, para que dichas configuraciones se hereden y apliquen automáticamente en los recursos, facilitar la gobernanza de los recursos en la nube y así mejorar la autonomía y productividad de cada individuo o grupo de trabajo.

RP3: Administrar las identidades y control de accesos, manteniendo la seguridad respecto a la autenticación y permisos y facilitando la realización de acciones de forma simple, rápida y eficiente para permitir la gestión de los recursos y servicios por las personas y programas encargados de ello de acuerdo a las indicaciones de la entidad que suscribe el servicio.

CR3.1 Las identidades para los usuarios se crean, administrándolas para permitir su autenticación en los servicios, agrupándolas en grupos y/o dominios, bien creándolas en el entorno de nube o sincronizándolos en su caso con otro entorno externo al proveedor o delegando la validación a otro entorno físico o nube, implementando las prácticas de seguridad para gestión de identidades y autenticación definidas por los responsables de seguridad tales como política de contraseñas, doble factor de autenticación, entre otras.

CR3.2 Las cuentas de servicio se crean, gestionándolas y asignándolas a cada programa o recurso que necesite una autenticación individual, aplicando el principio JIT ("Just in Time") para crearlas exactamente en el momento en que se requieran, implementando las prácticas de seguridad para gestión de credenciales definidas por los responsables de seguridad tales como políticas de creación y descarga de claves y periodos de rotación, entre otras.

CR3.3 Los roles personalizados se administran para cada caso en que no se ajusten a las operaciones previstas, por tener asignados más o menos permisos individuales de los que requiere para su actividad.

CR3.4 Los roles para cada identidad se asignan, según los principios de "mínimo privilegio" y "continuidad de negocio", para permitir acceder o administrar los recursos y aplicaciones por parte de las personas y programas encargados de ello.

CR3.5 Las configuraciones de seguridad de control de acceso se auditan para asegurar el despliegue, analizando la gestión de las identidades asignadas, roles y permisos asignados, acciones realizadas y accesos a datos, de forma periódica y en respuesta a situaciones imprevistas que lo requieran, para mantener el principio de "mínimo privilegio" y "continuidad de negocio".

CR3.6 Los secretos, credenciales, certificados, claves e información sensible en general cuyo acceso deba restringirse se almacenan, usando un repositorio de secretos, permitiendo el acceso sólo a las personas y programas que deban acceder a los mismos previa autenticación, asegurando su privacidad, centralizando su gestión y registrando sus accesos y operaciones para auditarlos posteriormente.

RP4: Configurar la facturación de los recursos desplegados, siguiendo las indicaciones contables de la empresa e imputando los costes a los centros de gastos establecidos, según directrices financieras y contables de la organización, para gestionar su pago y controlar los costes incurridos.

CR4.1 Los recursos para facilitar la gestión, control y análisis de costes entre otros, se etiquetan asignando identificadores según nomenclatura especificada por la organización.

CR4.2 Las cuentas de gasto se crean, estableciendo los términos y métodos de pago indicados por la misma, vinculando los recursos al centro de gasto asignado y asegurando que ningún problema o retraso con los pagos afecte a la continuidad de los recursos o procesos de la empresa.

CR4.3 Las previsiones de gastos se establecen según los recursos a utilizar en función de métricas como la carga, número de usuarios, datos almacenados, entre otros, usando herramientas de planificación de gastos.

CR4.4 Las alertas de gastos se configuran, estableciendo canales de notificación a los responsables y/o acciones automáticas que reaccionen a dichos eventos.

CR4.5 Los costes mensuales o diarios se verifican, analizándolos mediante las técnicas y servicios disponibles, tales como paneles de reporte interactivos o análisis a partir de los datos exportados a otro entorno o sistema, entre otros, identificando los costes relativos a cada recurso y/o aplicación en conjunto, para detectar sobrecostes y/o desviaciones del presupuesto y reportarlo al departamento responsable y aplicar reajustes en su caso.

RP5: Configurar el entorno para el posterior despliegue de recursos, administrando las cuotas de uso y habilitando las API ("Application Programming Interface") requeridas, en su caso, según los servicios a utilizar y el uso o número de recursos a desplegar previsto.

CR5.1 Los valores para cada cuota de despliegue de recursos y utilización de servicios y API se planifican, asegurándose de tener suficiente cuota disponible para el despliegue y funcionamiento de los recursos a desplegar, respetando los límites y contemplando las recomendaciones de buenas prácticas a la hora de distribuir las cuotas indicadas por el fabricante, tanto a efectos de coste como de limitaciones generales que pudieran afectar a todo el entorno de nube.

CR5.2 Las cuotas de despliegue de recursos y utilización de servicios se establecen, configurándolas una a una, ampliando o reduciendo cuando se requiera incrementar o restringir un número máximo de recursos posible en un entorno concreto, por razones tales como controlar los costes o desplegar entornos de pruebas limitados, entre otros.

CR5.3 Las API de cada servicio se habilitan para poder utilizar los servicios, deshabilitando aquellas correspondientes a servicios que no se prevean utilizar, para mantener una mayor seguridad y control de costes en cada entorno.

Contexto profesional

Medios de producción

Plataformas de nube pública o privada. Herramientas gráficas, de línea de comandos, librerías de cliente y API de la plataforma de nube. Herramientas de infraestructura como código. Conexión de red a la plataforma de nube y a infraestructuras de la nube híbrida o distribuida. Sistemas operativos. Navegadores. Compiladores, intérpretes e IDE para lenguajes de "scripting" y declarativos.

Productos y resultados

Interfaces de acceso y uso de la plataforma en la nube preparados. Jerarquías de recursos organizadas. Identidades y control de acceso administrado y seguro. Facturación de los recursos desplegados configurada. Entorno en la nube configurado para el despliegue. Cuotas de uso administradas y API habilitadas.

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 (documentación técnica del diseño del sistema a desarrollar; documentación técnica y de usuario del sistema desarrollado; normas corporativas de desarrollo de software, de pruebas, de control de calidad). Documentación técnica (Documentación técnica del proveedor; guías de buena arquitectura de los proveedores de nube; manuales de funcionamiento de los servicios en nube; manuales de funcionamiento del software empleado; documentación técnica de los interfaces de programación; documentación técnica de los kits de desarrollo (SDK) utilizados; manuales del lenguaje de programación empleado; manuales o ayudas de uso del sistema operativo; soportes técnicos para asistencia telefónica, contenidos audiovisuales, mensajería y foros, entre otros).

UNIDAD DE COMPETENCIA 2

Gestionar recursos de red y comunicaciones en la nube

Nivel: *3*
Código: *UC2736_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: 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.

CR1.1 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.

CR1.2 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.

CR1.3 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.

CR1.4 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.

CR1.5 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.

CR1.6 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.

CR1.7 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.

RP2: 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.

CR2.1 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.

CR2.2 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.

CR2.3 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.

CR2.4 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.

CR2.5 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.

CR2.6 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.

RP3: 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.

CR3.1 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.

CR3.2 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.

CR3.3 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.

CR3.4 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.

CR3.5 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.

CR3.6 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.

RP4: Configurar la seguridad de los recursos, monitorizando sus conexiones, para registrar los accesos e identificar su potencial riesgo en los sistemas.

CR4.1 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.

CR4.2 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.

CR4.3 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.

CR4.4 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.

CR4.5 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

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.

Productos y resultados

Infraestructura de la red desplegada. Servicios de proveedores de nube y aplicaciones desplegados, configurados y parametrizados. Aplicaciones publicadas disponibles. Ficheros y datos almacenados en servicios de nube. Copias de seguridad realizadas. Recursos de red desplegados y configurados. Entorno híbrido constituido. Seguridad del entorno implantada.

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).

UNIDAD DE COMPETENCIA 3

Administrar recursos de computación en entornos de nube

Nivel: *3*
Código: *UC2737_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Desplegar las instancias de computación y los grupos de cómputo para usar sus recursos, aplicando las características definidas previamente y proporcionando capacidades de autoescalado, para obtener un entorno de trabajo sobre el que configurar la capacidad de procesamiento según las necesidades del proyecto.

CR1.1 La región y la zona de disponibilidad se eligen, tras autenticarse en la plataforma de nube, usando credenciales para el proyecto especificado, interpretando las necesidades de arquitectura de la solución de la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.

CR1.2 La plantilla de ejecución de cómputo, en el caso de grupos de escalado o para definir instancias homogéneas, se crea incluyendo el tipo de instancia, sus características de CPU, memoria, reserva de recursos en la plataforma y almacenamiento.

CR1.3 La opción de computación se selecciona, eligiéndola en el listado proporcionado por el proveedor de nube y tomando el elemento cuyas características de CPU, memoria y modo de virtualización se correspondan con los criterios funcionales, económicos y operativos del proyecto, incluyendo la reserva de recursos en la plataforma, y usando plantillas para homogeneizar el proceso en caso de disponer de ellas.

CR1.4 Los recursos de computación se modifican, en su caso, en la configuración de la instancia de cómputo, analizando los requisitos de tamaño, velocidad, memoria y características especiales de replicación necesarias según el proyecto.

CR1.5 Los recursos de red se añaden, escogiéndolos de entre los disponibles para el proyecto, atendiendo a la región y zona de disponibilidad seleccionadas y teniendo en cuenta los requisitos de comunicaciones recogidos en el proyecto, seleccionando los segmentos y direccionamiento de red correspondientes a la zona o región e incluyendo la solicitud de direccionamiento público en su caso.

CR1.6 El comportamiento automatizado asociado al grupo de escalado y requerido tanto en despliegue como en la eliminación de recursos de cómputo se define, asegurando que, ante cambios de las cargas de trabajo, los recursos se crean y destruyen de la forma solicitada en la documentación del proyecto.

CR1.7 Los recursos de monitorización se añaden, seleccionando los disponibles en el proveedor de nube, bien inicialmente o bien con posterioridad al despliegue, mediante la solución de monitorización descrita en la documentación del proyecto, para supervisar el estado y rendimiento de la instancia.

CR1.8 La configuración de seguridad en la instancia se administra, recogiendo los requisitos descritos en el proyecto con el fin de garantizar exclusivamente los accesos a los puertos, protocolos y usuarios especificados en la documentación del proyecto.

CR1.9 Las etiquetas que identifiquen las instancias de computación dentro de la plataforma se crean, asignándolas de forma unívoca, indicando elementos tales como el proyecto asociado y

el rol dentro del mismo, entre otra información, de forma que sea posible en el futuro agrupar los recursos de las instancias asociadas al proyecto.

RP2: Desplegar contenedores partiendo de imágenes almacenadas en el registro al efecto ("hub"), para ejecutar aplicaciones basadas en estos recursos según las necesidades del proyecto.

CR2.1 La región y la zona de disponibilidad se eligen, tras autenticarse en la plataforma de nube usando credenciales para el proyecto especificado, interpretando las necesidades de arquitectura de la solución de la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.

CR2.2 Las imágenes requeridas para el despliegue de los componentes de las aplicaciones sobre contenedores se administran, localizándolas en un "hub", descargándolas, configurándolas interpretando la documentación técnica, creándolas en su caso y almacenándolas en un registro de imágenes, accesible con las credenciales de la plataforma.

CR2.3 Las características del despliegue del contenedor se configuran, mediante variables de entorno o ficheros de configuración que se aplican en el momento de inicio del contenedor, asegurando la asignación de recursos a cada componente descrito en la documentación del proyecto, configurando:

- Los requisitos y límites de consumo de memoria y CPU de cada uno.
- Los privilegios del usuario de ejecución del proceso principal del contenedor.
- Los requisitos de almacenamiento persistente que se pudieran demandar en el proyecto para poder proporcionar recursos de almacenamiento externos al contenedor.
- Las configuraciones de resolución de nombres de red, la integración con otros contenedores de la plataforma y los accesos que se permiten a los puertos y el protocolo.

CR2.4 Los nodos de cómputo se orquestan, configurándolos, haciendo uso de los grupos de cómputo o autoescalado junto a la orquestación de balanceo y enrutado de los contenedores en la red, para que estén controlados y gestionados, según indicaciones de la documentación del proyecto.

CR2.5 Las opciones de monitorización del estado y rendimiento de los contenedores se añaden, bien usando las disponibles en el proveedor de nube o bien posteriormente al despliegue y mediante una solución de monitorización particular descrita en la documentación del proyecto.

RP3: Desplegar la infraestructura de funciones como servicio, mediante el método seleccionado, para ejecutar componentes de aplicaciones basados en funciones desplegadas sobre cómputo, según las necesidades del proyecto.

CR3.1 La región y la zona de disponibilidad se eligen, tras autenticarse en la plataforma de nube usando credenciales para el proyecto especificado, interpretando las necesidades de arquitectura de la solución de la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.

CR3.2 Las funciones como servicio se crean, mediante uno de los métodos siguientes:

- Codificándolas en alguno de los lenguajes de programación soportados.
- Utilizando funciones existentes y publicadas en la plataforma.
- Ejecutando un contenedor de cómputo con un servicio que ejecutará la función definida.
- Desplegando aplicaciones ya preparadas por el proveedor de la nube.
- Escribiendo los ficheros de código que definen la creación dentro de la nube con las necesidades y características que permiten tener las infraestructuras de computo definidas en el proyecto.

CR3.3 Los permisos que posibilitan ejecutar la función como servicio se asocian, bien seleccionando un rol existente con los permisos, bien creando uno nuevo con las especificaciones indicadas en la documentación del proyecto.

CR3.4 Los requisitos de almacenamiento persistente para proporcionar recursos de almacenamiento externos al entorno de ejecución de la función como servicio se configuran, asignando parámetros tales como contenedores, almacenamiento, redes, máquinas virtuales, entre otros componentes de arquitectura, según las necesidades descritas en la documentación del proyecto.

CR3.5 Los recursos de monitorización y gestión de eventos se añaden a los ficheros de creación automatizada de infraestructura, incluyendo las configuraciones de dichos recursos y las etiquetas que identifiquen unívocamente los elementos descritos en la documentación del proyecto para el control del estado y rendimiento de los elementos de la arquitectura de los aplicativos.

CR3.6 El despliegue de la función como servicio se configura, garantizando la procedencia de los orígenes definidos en la documentación asociada al proyecto.

CR3.7 Las etiquetas que identifiquen las funciones como servicio dentro de la plataforma se añaden, asegurando que sean unívocas, indicando elementos tales como el proyecto asociado y el rol dentro del mismo, entre otra información, de forma que sea posible agrupar los recursos asociados al proyecto.

RP4: Preparar procedimientos y automatizaciones de "backup" de infraestructuras de cómputo en plataforma de proveedor de nube para asegurar los datos y el estado de los recursos desplegados según las necesidades del proyecto.

CR4.1 La región y la zona de disponibilidad se eligen, tras autenticarse en la plataforma de nube, usando credenciales para el proyecto especificado, interpretando las necesidades de arquitectura de la solución de la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.

CR4.2 Los planes de copias de seguridad se crean, teniendo en cuenta las directrices indicadas en el proyecto con las retenciones, frecuencias de ejecución, en las regiones y zonas en las que pudieran estar desplegados los recursos identificados en la documentación del proyecto.

CR4.3 La disponibilidad de los datos, velocidad de recuperación y retención de las copias de seguridad junto con las directrices de seguridad encriptado, meta información y duplicados a otros entornos, se configuran estableciendo las opciones de "backup", teniendo en cuenta las necesidades descritas en la documentación del proyecto, dentro de los estándares que la plataforma de la nube permite para poder usar los datos salvaguardados en distintas regiones o zonas o recuperación de "backup".

CR4.4 Los planes de seguridad establecidos se asocian a los recursos definidos en la plataforma de una de las formas siguientes:
- Usando las etiquetas asociadas a los mismos.
- Asignando los recursos de forma directa.
- Agrupando por tipo de servicio del proveedor de nube.

CR4.5 Las políticas de seguridad se crean, definiendo estándares de copias de seguridad y planificaciones en la plataforma, siguiendo las implementaciones incluidas para ella por el proveedor de nube y según la documentación del proyecto.

Contexto profesional

Medios de producción

Equipos informáticos de tipo servidor virtual en proveedores de nube. Software de servidores: contenedores. Despliegues en entornos de nube. Sistemas operativos y parámetros de configuración. Herramientas de seguridad informática y virtualización en entornos nube.

Productos y resultados

Instancias de computación, desplegadas. Contenedores desplegados. Clúster de orquestación de contenedores desplegado. Infraestructura de funciones como servicio desplegada. Infraestructura de funciones como servicio desplegada. Infraestructuras de cómputo desplegadas. Copias de seguridad de servidores y datos automatizados.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de protección de datos y propiedad intelectual e industrial; normativa aplicable de seguridad informática; Normativa aplicable sobre prevención de riesgos laborales -ergonomía-). Normas internas de trabajo (documentación de diseño del servicio y requisitos de cómputo. Normas internas de calidad y seguridad. Acuerdo de nivel de servicio -"Service level agreement" SLA-. Documentación de configuración de sistemas y servicios. Plan de pruebas e informe de fallos. Histórico de sucesos, manual de operación para recuperación ante fallos). Documentación técnica (documentación de provisión de plataformas nube. Documentación de productos software. Manuales de uso y funcionamiento de los sistemas informáticos. Manuales de instalación del software asociado a esta unidad de competencia. Manuales de administración del software asociado a esta unidad de competencia. Materiales de cursos de formación. Sistemas de ayuda del software. Soportes técnicos de asistencia. Manuales de operación de plataformas de nube).

UNIDAD DE COMPETENCIA 4

Gestionar recursos de almacenamiento y de bases de datos en la nube

Nivel: *3*
Código: *UC2738_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Seleccionar el tipo de almacenamiento para los datos del sistema según los requisitos funcionales y los criterios de durabilidad, seguridad, fiabilidad, rendimiento y coste especificados por la entidad responsable, para un almacenamiento eficiente en el entorno o proyecto.

CR1.1 Las operaciones del almacenamiento de objetos y de ficheros, tanto de bloque como en red, se comprueba que cumplen los requisitos funcionales y no funcionales del proyecto y la organización.

CR1.2 Los tipos de almacenamiento proporcionados por el proveedor seleccionado se consultan, a partir de la documentación del mismo, para verificar cuál ofrece garantías según criterios de durabilidad, fiabilidad y rendimiento especificados.

CR1.3 Los tipos de almacenamiento no disponibles en la región o regiones donde el sistema vaya a desplegarse se descartan, consultando la documentación del proveedor sobre disponibilidad geográfica.

CR1.4 El tipo de almacenamiento que resulte más económico se selecciona, consultando las tablas de precios del proveedor de nube.

CR1.5 Los parámetros del almacenamiento que afectan a los costes de uso del servicio, incluyendo los de almacenamiento, acceso, transferencia, operaciones de lectura y escritura, replicación, copia de respaldo y recuperación, así como cualquier otro coste específico que el proveedor haya asignado al almacenamiento escogido, se ajustan a partir de la información proporcionada por el proveedor y cumpliendo los requisitos funcionales y no funcionales de la organización.

RP2: Administrar los sistemas de almacenamiento de objetos en nube, configurando y monitorizando los mismos, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a los requisitos especificados por la persona responsable del entorno o del proyecto.

CR2.1 Los nombres de los contenedores (también conocidos como depósitos o "buckets") y de las etiquetas para metadatos se definen, teniendo en cuenta las limitaciones técnicas del proveedor de nube, para cumplir con las especificaciones del proyecto en curso y facilitar su administración.

CR2.2 La clase de almacenamiento -y en su caso, objeto- para cada contenedor se define, teniendo en cuenta los requisitos funcionales del proyecto, los patrones de acceso a los datos, las limitaciones impuestas para cada clase en el proveedor de nube, y los costes asociados de almacenamiento y de recuperación de objetos.

CR2.3 La región geográfica del almacenamiento de objetos se escoge, de entre todas las soportadas por el proveedor de nube, para asegurar que los requisitos de latencia y coste son

los más eficientes, teniendo en cuenta las restricciones de residencia de los datos especificadas en el proyecto.

CR2.4 Los parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, se configurarán mediante herramientas gráficas, y/o de línea de comandos, y/o interfaces de programación (API), y/o infraestructura como código (IaC) para garantizar el cumplimiento de los requisitos del proyecto.

CR2.5 Los parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría se configuran para garantizar de forma demostrable que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.

CR2.6 Los parámetros de acceso público, en caso de que los requisitos especifiquen acceso HTTP o HTTPS usando un dominio personalizado, se configuran utilizando en su caso un certificado SSL proporcionado por el proveedor de nube, para que los usuarios puedan acceder al contenido almacenado usando el dominio especificado.

CR2.7 Las políticas de ciclo de vida de los objetos se configuran, mediante las herramientas proporcionadas por el proveedor de nube o vía IaC, para que conforme pasa el tiempo los objetos cambien automáticamente de clase y, en su caso, se versionen o se borren, garantizando así las políticas de retención de datos especificadas en el proyecto.

CR2.8 La política de replicación y copia de seguridad de los objetos se configuran, verificándola para asegurar que, en caso de pérdida de información, esta se puede recuperar en la forma y tiempos especificados en el proyecto.

RP3: Administrar los sistemas de almacenamiento de ficheros en nube, tanto en dispositivos de bloque como en sistemas de almacenamiento en red, utilizando tanto herramientas gráficas como de línea de comandos, API ("Application Programming Interface"), y/o IaC para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a los requisitos especificados por la persona responsable del entorno o del proyecto.

CR3.1 La clase de almacenamiento se escoge, teniendo en cuenta los requisitos funcionales del proyecto, los patrones de acceso a los datos, la durabilidad de los datos, las limitaciones impuestas para cada clase en el proveedor de nube, y los costes asociados de almacenamiento y de recuperación de datos.

CR3.2 La región geográfica -y en su caso la replicación entre múltiples zonas o regiones- se escoge, para asegurar que los requisitos de latencia y coste son los más eficientes, siempre teniendo en cuenta las restricciones de residencia de los datos especificadas en el proyecto.

CR3.3 Los parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, se configurarán mediante las herramientas proporcionadas por el proveedor de nube vía IaC, para garantizar el cumplimiento de los requisitos del proyecto.

CR3.4 Los parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría se configuran para garantizar que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.

CR3.5 El montaje del dispositivo de almacenamiento o del sistema de ficheros se implementa para garantizar el acceso a los ficheros desde tantos puntos como se hayan definido en los requisitos y en modalidad de solo lectura o bien de lectura/escritura según esté establecido, realizando un desmontaje previo ordenado del dispositivo si fuera necesario.

CR3.6 Los cambios durante el ciclo de vida del dispositivo o sistema de ficheros tales como cambios de tamaño reservado, cambios en la clase de almacenamiento, modificaciones en la

configuración, desmontaje del sistema de ficheros y/o borrado, entre otros, se aplican para adaptarse a los requisitos cambiantes del proyecto.

CR3.7 Las políticas o mecanismos de replicación y copia de seguridad de los dispositivos y/o ficheros se configuran, asegurando que, en caso de pérdida accidental de la información, ésta se puede recuperar en la forma y tiempos especificados en el proyecto.

RP4: Administrar los sistemas de bases de datos, utilizando tanto herramientas gráficas como de línea de comandos, API, y/o IaC, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a los requisitos especificados por la persona responsable del entorno o del proyecto.

CR4.1 La región geográfica y, en su caso, la replicación entre múltiples zonas o regiones se escoge, para asegurar que los requisitos de latencia y coste son los más eficientes, teniendo en cuenta las restricciones de residencia de los datos especificadas en el proyecto.

CR4.2 Los parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, se configuran mediante las herramientas proporcionadas por el proveedor de nube vía IaC, para garantizar el cumplimiento de los requisitos del proyecto.

CR4.3 Los parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría se configuran para garantizar que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.

CR4.4 Los cambios durante el ciclo de vida de la BBDD tales como cambios de tamaño reservado, de capacidad de computación provisionada, de replicación de los datos, o modificaciones en la configuración, entre otros, se aplican mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD, para adaptarse a los requisitos cambiantes del proyecto.

CR4.5 Las políticas o mecanismos de replicación y copia de seguridad de la BBDD se configuran, verificándolas para asegurar que, en caso de pérdida accidental de la información, ésta se puede recuperar en la forma y tiempos especificados en el proyecto.

CR4.6 El rendimiento de las operaciones de inserción y consulta se monitoriza activamente, mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD, para detectar potenciales problemas que requieran cambiar la infraestructura, la configuración, o las aplicaciones que usan el sistema.

CR4.7 Las optimizaciones a nivel de configuración como a nivel de sugerencias de rediseño del esquema o la distribución de los datos se efectúan, para garantizar que el rendimiento y coste de las operaciones se mantiene dentro de los requisitos aceptables, siempre teniendo en cuenta sugerencias de diseño genéricas y considerando que para optimizaciones complejas se requiere la ayuda de otros perfiles especializados en BBDD.

RP5: Gestionar los datos tanto desde el exterior, como entre sistemas de almacenamiento y bases de datos soportados por el proveedor de nube, utilizando tanto herramientas gráficas, como de línea de comandos, API y/o IaC, para facilitar el flujo de información en el sistema, según los requisitos especificados por la entidad responsable del entorno o del proyecto.

CR5.1 Las opciones de transferencia y sincronización de datos se evalúan utilizando las herramientas proporcionadas por el proveedor de nube para seleccionar la mejor opción teniendo en cuenta los requisitos funcionales y de seguridad establecidos en el proyecto consultando la documentación y para los de latencia mediante una prueba de transferencia de ficheros.

CR5.2 Las tablas detalladas de precios del proveedor de nube sobre transferencia y sincronización de datos se consultan, asegurando que se están teniendo en cuenta todos los costes de uso del servicio, incluyendo los de transferencia entre diferentes zonas y/o regiones.

CR5.3 Las conexiones se configuran para permitir el flujo de datos entre origen y destino de manera segura y eficiente, utilizando las herramientas proporcionadas por el proveedor de nube.

CR5.4 El provisionado de los dispositivos, en el caso de transferencia de datos offline, se efectúa mediante el mecanismo establecido por el proveedor de nube para que se envíe el dispositivo físico entre proveedor y cliente, de cara a realizar la copia local de datos y el posterior envío al punto de destino, prestando especial atención a la seguridad y cifrado de los datos.

CR5.5 Los parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría se configuran, utilizando las herramientas proporcionadas por el proveedor de nube, para garantizar que la información transferida solo se envía entre los orígenes y destinos especificados y que nunca abandona la zona geográfica marcada en los requisitos del proyecto.

CR5.6 Los parámetros de sincronización de datos, tanto unidireccional como bidireccional, se configuran, utilizando las herramientas proporcionadas por el proveedor de nube, para que ésta se realice de forma automática y desatendida cumpliendo los requisitos de latencia marcados por la persona o entidad responsable del proyecto.

CR5.7 La importación y/o exportación de datos se completa de manera manual o supervisada, para aquellos casos en los que los requisitos no impliquen replicación periódica.

CR5.8 Los procesos de importación, exportación, y/o sincronización de datos, tanto automáticos como manuales, se monitorizan específicamente para identificar problemas de conectividad o integridad de las transferencias, observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

RP6: Administrar la infraestructura de datos de nube híbrida, utilizando tanto herramientas gráficas, como de líneas de comandos, API, y/o IaC, para permitir la interoperabilidad de la nube con otros entornos, siguiendo los criterios de patrones de acceso, seguridad, durabilidad, fiabilidad y rendimiento especificados por la entidad responsable del entorno o del proyecto.

CR6.1 La implementación de la configuración definida por el equipo de arquitectura del proyecto se verifica a partir de las instrucciones a seguir contenidas en la documentación sobre transferencia y sincronización de datos.

CR6.2 Los mecanismos avanzados entre los sistemas implicados que haya que tener en cuenta a la hora de escribir la configuración, tales como VPN o conexiones dedicadas, entre otros, se verifica que existen, consultando la documentación del proyecto sobre interconexión de redes.

CR6.3 Las conexiones se configuran, usando SSH o VPN en caso de conexión con el exterior, o usando los mecanismos de red privada proporcionados por los proveedores de nube, para permitir el flujo de datos entre origen y destino de manera segura y eficiente.

CR6.4 La visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría se configura, asignando parámetros del sistema relativos, para garantizar que la información transferida solo se envía entre los orígenes y destinos especificados y que nunca abandona la zona geográfica marcada en los requisitos del proyecto.

CR6.5 La sincronización de datos, tanto unidireccional como bidireccional, se configura, asignando parámetros para que ésta se realice de forma automática y desatendida, cumpliendo los requisitos de latencia marcados por la persona o entidad responsable del proyecto.

CR6.6 La importación y/o exportación de datos se completa de manera manual o supervisada, para aquellos casos en los que los requisitos no impliquen replicación periódica, conectándose a la infraestructura de nube y lanzando la operación.

CR6.7 Los procesos de importación, exportación, y/o sincronización de datos, tanto automáticos como manuales, se monitorizan específicamente para identificar problemas de conectividad o integridad en las transferencias, observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

RP7: Administrar los sistemas de transformación y análisis de datos (OLAP), utilizando tanto herramientas gráficas como de línea de comandos y/o API, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a los requisitos especificados por la entidad responsable del entorno o del proyecto.

CR7.1 La región geográfica y en su caso, la replicación entre múltiples zonas o regiones, se escoge para asegurar que los requisitos de latencia y coste son los más eficientes, teniendo en cuenta las restricciones de residencia de los datos especificadas en el proyecto.

CR7.2 Los parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, se configuran mediante las herramientas proporcionadas por el proveedor de nube vía IaC.

CR7.3 Los parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría se configuran, garantizando de forma demostrable que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.

CR7.4 La retención y/o particionado y/o compactación de datos definidos por el equipo de ingeniería de datos -o equivalente- se configuran, asignando los parámetros del sistema OLAP, para mantener el equilibrio entre la información disponible para análisis y el coste de almacenamiento según lo establecido por las personas responsables del proyecto.

CR7.5 Los trabajos de carga y transformación de datos (ETL) se monitorizan validando que no existen errores en los archivos log del sistema y que el tiempo de ejecución no se degrada, para detectar posibles problemas que requieran la intervención del equipo de ingeniería de datos.

CR7.6 Las políticas o mecanismos de replicación y copia de seguridad de los datos en el sistema OLAP se configuran, verificando que, en caso de pérdida accidental de la información, ésta se puede recuperar en la forma y tiempos especificados en el proyecto.

CR7.7 El rendimiento de las operaciones y el espacio de almacenamiento ocupado se monitorizan activamente, mediante las herramientas proporcionadas por el proveedor de nube, para detectar potenciales problemas que requieran la intervención del equipo de ingeniería de datos.

CR7.8 Las optimizaciones sugeridas por el equipo de ingeniería de datos se efectúan para garantizar que el rendimiento de las operaciones se mantiene dentro de los requisitos aceptables, utilizando las herramientas proporcionadas por el proveedor de nube.

Contexto profesional

Medios de producción

Plataformas de nube pública o privada. Herramientas gráficas y de línea de comandos de la plataforma de nube. Herramientas de infraestructura como código. Conexión de red a la plataforma de nube y a infraestructuras de la nube híbrida.

Productos y resultados

Sistemas de almacenamiento en nube seleccionados. Sistemas de almacenamiento de objetos configurados y administrados. Sistemas de almacenamiento de ficheros configurados y administrados. Sistemas de bases de datos en nube seleccionados. Sistemas de bases de datos configurados y administrados. Intercambio y sincronización de datos entre los diferentes sistemas. Plataforma de nube híbrida configurada y administrada. Sistemas de análisis y transformación configurados y administrados.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de protección de datos, normativa aplicable de seguridad informática y propiedad intelectual e industrial, Normativa aplicable sobre prevención de riesgos laborales -ergonomía-). Normas internas de trabajo (documentación técnica del diseño del sistema a desarrollar; documentación técnica y de usuario del sistema desarrollado; normas corporativas de desarrollo de software, de pruebas, de control de calidad). Documentación técnica (Guías de buena arquitectura de los proveedores de nube; manuales de funcionamiento de los servicios en nube; manuales de funcionamiento del software empleado; documentación técnica de los interfaces de programación; documentación técnica de los kits de desarrollo (SDK) utilizados; manuales del lenguaje de programación empleado; manuales o ayudas de uso del sistema operativo; soportes técnicos para asistencia -telefónica, Internet, contenidos audiovisuales, mensajería y foros, entre otros-).

UNIDAD DE COMPETENCIA 5

Desplegar servicios administrados en la nube

Nivel: *3*
Código: *UC2739_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Desplegar recursos en la nube de manera automática a través de plantillas de ficheros para estandarizar el aprovisionamiento mediante infraestructura como código (IaC).

CR1.1 Los recursos a desplegar en la nube de manera conjunta, tales como tipo de servicios, arquitectura, configuración y proveedor donde realizar el despliegue, entre otros, se determinan analizando el estado final que se desea alcanzar, considerando el proveedor de nube en el que se realizará el despliegue.

CR1.2 El servicio de motor de despliegue de infraestructura como código y conectores se seleccionan, configurándolos para permitir la ejecución automática del despliegue de los recursos a aprovisionar en el proveedor de nube y verificando que se tienen los permisos requeridos para su aprovisionamiento.

CR1.3 Las plantillas y ficheros se crean, asignando valores a parámetros, referencias, variables de configuración y estado final de los recursos en la nube a desplegar.

CR1.4 Las plantillas y sintaxis de los ficheros se validan, creando el plan de despliegue con el motor de despliegue de infraestructura como código.

CR1.5 El estado de la infraestructura actual y el estado deseado final se comparan, validando los pasos y tareas que se requieren llevar a cabo tales como creación y configuración de los recursos u otros para dejar la infraestructura en el estado especificado por el usuario.

CR1.6 El plan de despliegue se ejecuta, creando y configurando los recursos en la nube de acuerdo a las plantillas y ficheros generados.

CR1.7 Los resultados de aprovisionamiento de los recursos en la nube se revisan, validando que el estado final de los recursos a desplegar en el proveedor de nube es el establecido de acuerdo a la información de las plantillas y ficheros.

CR1.8 Las plantillas y ficheros creados se documentan, incluyendo procedimientos de actualización, compartiéndolos en un repositorio de código para su utilización por otros usuarios.

RP2: Desplegar servicios de mensajería asíncrona para optimizar la transmisión y el procesamiento de los flujos de datos que se intercambian entre múltiples fuentes (publicadores) y distribuirlos a múltiples receptores (subscriptores), monitorizando los resultados.

CR2.1 El servicio de mensajería asíncrona se aprovisiona, habilitándolo en la consola, verificando que se tienen los permisos necesarios para su aprovisionamiento.

CR2.2 El servicio de mensajería asíncrona se configura, incluyendo el tema -recurso al que los publicadores envían mensajes-, subscripciones para la entrega de mensajes, tipo de entrega y parámetros de reintento y eliminación de los mensajes.

CR2.3 El proceso de almacenamiento y entrega se monitoriza, verificando que los mensajes son entregados a los suscriptores del tema.

RP3: Desplegar servicios de ejecución de trabajos por lotes para la ejecución de manera repetitiva de trabajos sin supervisión directa del usuario, monitorizando los resultados.

CR3.1 El servicio de automatización de ejecución de trabajos por lotes se aprovisiona, habilitándolo en la consola en caso necesario.

CR3.2 El trabajo por lotes a automatizar se configura con información de nombre, programación de la frecuencia de ejecución del trabajo, reintentos ante fallos, y objetivos del trabajo a ejecutar, servicio de nube a llamar o extremo HTTP, activando la planificación de la ejecución y verificando que se tienen los permisos requeridos por el servicio.

CR3.3 La ejecución del trabajo automatizado se monitoriza, validando que el trabajo se ha ejecutado según la planificación realizada y en los tiempos de ejecución requeridos en ella.

RP4: Aprovisionar servicios de integración y despliegue continuo (CI/CD) para automatizar la compilación y despliegue de código en los entornos de ejecución, monitorizando los resultados.

CR4.1 El servicio de CI/CD se aprovisiona, incluyendo repositorio de código para la compartición de versiones de código entre los desarrolladores, servicio de compilación y despliegue según el lenguaje y tecnología a utilizar y para el almacenamiento de los activos de código, compiladores o imágenes de contenedores generados.

CR4.2 Los entornos de ejecución se establecen, configurándolos de acuerdo a las estrategias y recursos de despliegue de la organización, identificando su propósito y procedimiento de actualización de las versiones a desplegar.

CR4.3 Los permisos de acceso a los servicios y plantillas de trabajos de compilación, repositorios de código, activos e imágenes y entornos de ejecución se configuran, asignando las autorizaciones para permitir su acceso.

CR4.4 Los parámetros de automatización de las tareas de compilación y despliegue y eventos de activación se configuran, bien especificando los eventos que inician la ejecución como la publicación de una nueva versión en el repositorio de código o bien, definiendo una planificación de ejecución en periodos de tiempo.

CR4.5 La ejecución y los "logs" se monitorizan, revisando los trabajos ejecutados que no hayan finalizado con éxito.

RP5: Desplegar soluciones de terceros seleccionándolas desde el "marketplace" para automatizar el despliegue de paquetes de "software".

CR5.1 El catálogo de soluciones del "marketplace" se revisa, interpretando las especificaciones de despliegue, costes estimados o manuales de fabricantes, licenciamiento y los requisitos recogidos en la documentación técnica de las soluciones.

CR5.2 La solución a desplegar del catálogo se selecciona, configurando los parámetros tales como nombre, zona y red dónde se realizará el despliegue, claves de autenticación, parámetros de capacidad de cómputo y almacenamiento según las necesidades de uso, y asignando permisos para el aprovisionamiento de los servicios a utilizar.

CR5.3 El despliegue automático de la solución se solicita desde el catálogo, monitorizando los pasos de despliegue.

CR5.4 La instalación y configuración de la solución desplegada se verifica mediante la ejecución de una serie de pruebas como la revisión de "logs" de despliegue, acceso a recursos y test de funcionamiento de la solución.

CR5.5 Los procedimientos de operación y mantenimiento de la solución se documentan, incluyendo tareas de monitorización, revisión de "logs", actualización de nuevas versiones, y borrado.

CR5.6 Los datos finales de configuración de la solución, ubicación, las URL de acceso, operación y seguridad se comprueban, verificando que quedan documentados en la plataforma.

Contexto profesional

Medios de producción

Plataformas de nube pública o privada. Herramientas gráficas y de línea de comandos proporcionados por la plataforma de nube. Herramientas de infraestructura como código, bien proporcionada por el proveedor de nube o por una tercera parte. Conexión de red a la plataforma de nube.

Productos y resultados

Recursos en la nube desplegados. Plantillas y ficheros declarativos creados. Resultados de aprovisionamiento revisados. Servicios de mensajería asíncrona desplegados y monitorizados. Servicios de ejecución de trabajos por lotes desplegados. Servicios de CI/CD desplegados. "Software" del "marketplace" desplegado.

Información utilizada o generada

Normas externas de trabajo (Normativa aplicable sobre prevención de riesgos laborales -ergonomía-; Normativa aplicable de protección de datos, propiedad intelectual e industrial). Normas internas de trabajo (documentación de diseño y aprovisionamiento de los recursos en nube; normas internas de calidad y seguridad; acuerdos de nivel de servicio -SLAs-; documentación de configuración de sistemas y servicios; plan de pruebas e informe de fallos; histórico de sucesos, manual de operación para recuperación ante fallos). Documentación técnica (documentación de servicios en la nube; documentación de provisión de plataformas nube; manuales de uso y funcionamiento de los servicios; manuales de instalación del "software" asociado a esta unidad de competencia; manuales de administración de los servicios asociados a esta unidad de competencia; materiales de cursos de formación; sistemas de ayuda de los servicios en la nube; soportes técnicos de asistencia; manuales de operación de plataformas de nube).

UNIDAD DE COMPETENCIA 6

Automatizar despliegues en la nube

Nivel: *3*
Código: *UC2740_3*
Estado: *Tramitación BOE*

Realizaciones profesionales y criterios de realización

RP1: Gestionar los repositorios de código fuente del software y de los servicios asociados a las aplicaciones de los sistemas, según las necesidades de uso, directivas de calidad y seguridad de la organización, para facilitar su mantenimiento, recuperación y permitir la trazabilidad del sistema.

CR1.1 Los orígenes de código fuente se organizan con una estructura que permite su uso de forma consistente en la organización.

CR1.2 Los parámetros del sistema que afectan a la autenticación y autorización se ajustan a las necesidades de acceso, integración con herramientas y seguridad de la organización.

CR1.3 Las modificaciones sobre el código fuente se validan, siguiendo las guías de desarrollo y los flujos de trabajo y políticas tales como aprobación, asignación o revisión, entre otras, definidas en la organización.

CR1.4 Los parámetros de calidad definidos sobre el código fuente asociado a los sistemas se miden, aplicando los estándares de calidad de la organización, para ejecutar acciones correctivas.

CR1.5 Los procesos de copia de seguridad y recuperación del código fuente, se ejecutan de forma periódica, siguiendo el resultado un proceso de validación donde se consideren las actuaciones necesarias para la optimización y la gestión de repositorios de gran tamaño.

CR1.6 Las dependencias externas de paquetes, librerías o integraciones se validan de forma periódica, siguiendo las prácticas definidas en la organización en los ámbitos de seguridad, soportabilidad, rendimiento, y publicación.

RP2: Modificar el código fuente de despliegue y plantillas responsables de la creación de los servicios en la nube, cumpliendo las directivas de operación, calidad y seguridad de la organización para simplificar la operación y el despliegue.

CR2.1 Los servicios requeridos para las aplicaciones de la organización se crean de forma automatizada, modificándolos, si fuera necesario, empleando las capacidades de las herramientas y plataformas de nube seleccionadas como plantillas declarativas del servicio o hardware, línea de comandos (CLI), API ("Application Programming Interface"), automatismos mediante lenguajes de programación, entre otras.

CR2.2 Los parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube se definen, considerando características propias del despliegue de las versiones de los datos de las aplicaciones, tales como creación de bases de datos, movimiento o transformación de la información y metadatos, entre otras.

CR2.3 Los parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube se definen, considerando características propias del despliegue de las versiones del software, tales como la gestión de la configuración de las aplicaciones, entre otras.

CR2.4 Los parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube se definen, considerando características propias del despliegue de las versiones del código fuente de las aplicaciones, tales como contenedores, máquinas virtuales, scripts, código binario, entre otros.

CR2.5 Los parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube se definen, considerando elementos que permitan su reutilización en distintos despliegues, tales como nombre del servicio, región geográfica, recursos asignados, permisos, confirmando que son únicos en los casos necesarios.

CR2.6 El código fuente de despliegue, plantillas declarativas del servicio o cualquier proceso responsable del despliegue se verifica que sea idempotente, siendo robusta su ejecución y proporcionando predictibilidad bajo distintas circunstancias.

RP3: Configurar los servicios de comunicación y colaboración de la organización según las necesidades de uso, directivas de comunicación y adopción de la organización, para automatizar las interacciones con los repositorios de código fuente y las herramientas de gestión de proyectos.

CR3.1 Las plataformas de comunicación y herramientas de gestión de proyectos se emplean en la organización, siguiendo la configuración con los repositorios de código fuente que permitan la recepción automática de cambios de estado y contenido.

CR3.2 Las plataformas de comunicación empleadas en la organización se determinan, según criterios de seguridad y disponibilidad, para notificar a los responsables de los sistemas afectados por métricas, alertas o reglas definidas en los repositorios de código fuente, estados de tareas, peticiones de cambios al sistema, entre otras.

CR3.3 Las plataformas de comunicación, documentación y herramientas de gestión de proyectos empleadas en la organización se configuran, conectándolas con los repositorios de código fuente, de tal modo que permitan la asignación de elementos de ambos sistemas de forma bidireccional, tales como la modificación de código fuente a tarea, resolución de errores ("bugs") a modificación de código fuente, entre otras.

RP4: Gestionar los procesos de integración y despliegue continuo (CI/CD) para configurar e implantar las versiones de las aplicaciones desarrolladas dentro del marco de las directivas de la organización sobre operación, calidad y seguridad.

CR4.1 Los fallos de ejecución, calidad, seguridad y rendimiento de las aplicaciones del sistema se resuelven mediante automatización, empleando las estrategias de pruebas de la organización e incluyendo las pruebas de diagnóstico con las herramientas integradas, proporcionando información sobre resultados y acciones a los fallos diagnosticados.

CR4.2 Las herramientas de gestión de paquetes y dependencias se instalan, configurándolas y actualizándolas, siguiendo las directrices de versionado, priorización y documentación de la organización y del fabricante de la herramienta.

CR4.3 Los parámetros del sistema que afectan a la integración con dependencias externas en el proceso de compilación del código fuente, se ajustan a las políticas de calidad, seguridad y rendimiento definidas en la organización tales como cobertura de código, pruebas de software, análisis de seguridad, dependencias de librerías, entre otras.

CR4.4 Las herramientas para la administración de la configuración del software y servicios de los sistemas desarrollados en la organización, se mantienen siguiendo la configuración deseada y definida para cada una de las aplicaciones de forma automática.

CR4.5 Los servicios responsables de la ejecución de procesos y/o compilación del software y servicios necesarios para las aplicaciones de la organización se configuran, garantizando su

disposición de uso para evitar problemas en su ejecución, manteniéndolos monitorizados para uso óptimo en seguridad, rendimiento y capacidad, como por ejemplo análisis de errores, accesos, duración, rendimiento, capacidad en compilación, entre otros.

CR4.6 Los parámetros de los servicios responsables de la ejecución de procesos y despliegue del software y servicios se ajustan a las necesidades de la organización en lo que respecta a la orquestación de flujos de aprobación, seguridad, auditoría, automatización, priorización de despliegues o correcciones críticas y configuraciones del software asociado.

CR4.7 Los parámetros de los servicios responsables de la ejecución de procesos y despliegue del software y servicios se configuran, siguiendo las características no-funcionales definidas para el tiempo de pérdida de servicio de las aplicaciones establecidas por la organización en la estrategia de despliegue, tales como "Blue/green", "canary", "ring", balanceo de carga ("traffic-splitting deployment"), despliegue incremental, entre otras.

RP5: Configurar los mecanismos de automatización del despliegue de código fuente de software y servicios, cumpliendo con el estándar definido en la organización para la monitorización, registro de las aplicaciones, recuperación, crecimiento y políticas de optimización de costes.

CR5.1 Los servicios responsables de la gestión de la configuración y/u orquestación de la infraestructura se automatizan, siguiendo los estándares y políticas de monitorización, recuperación, crecimiento y operación entre otras.

CR5.2 Los mecanismos de despliegue desarrollados se ejecutan, siguiendo validaciones del código fuente y los servicios desplegados automática o manualmente y cumpliendo con las políticas de registro de aplicaciones, gobierno, seguridad, pruebas y monitorización definidas en la organización.

CR5.3 Los mecanismos de despliegue se configuran, incorporando acciones automáticas en base a eventos o registros producidos por las aplicaciones y los servicios, permitiendo recuperar estados previos a situaciones de fallo o pérdida de servicio.

CR5.4 Los mecanismos de despliegue se configuran, incorporando acciones automáticas en base a eventos o registros producidos por las aplicaciones, usuarios y los servicios, permitiendo reducir el coste y manteniendo las políticas de la organización del servicio tales como su disponibilidad, escalabilidad, rendimiento y recuperación entre otras.

Contexto profesional

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. Herramientas de depuración. Sistemas de documentación de elementos de programación. Herramientas de comunicación y colaboración en equipo. Sistemas gestores de repositorios de código fuente. 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.

Productos y resultados

Repositorios de código fuente del software y de los servicios asociados a las aplicaciones de los sistemas disponibles. Servicios de comunicación y colaboración de la organización, configurados. Servicios de integración y despliegue continuo, gestionados. Mecanismos de automatización del despliegue de

código fuente de software y servicios configurados. Servicios en nube configurados. Scripts de despliegue, procesos interactivos y elementos reutilizables de despliegue desarrollados. Ficheros y datos almacenados en servicios de nube. Copias de seguridad y procesos de restauración establecidos.

Información utilizada o generada

Normas externas de trabajo (Normativa aplicable sobre prevención de riesgos laborales -ergonomía-; Normativa aplicable de protección de datos, propiedad intelectual e industrial). Normas internas de trabajo (guías de despliegue, instalación, configuración y actualización de los servicios de las aplicaciones desarrolladas; documentación de diseño y aprovisionamiento de los recursos en nube; diseño y especificaciones de los servicios a desplegar y operar; plan de seguridad, operación y calidad de la organización; acuerdos de nivel de servicio -SLA-; documentación de configuración de sistemas y servicios; plan de pruebas e informe de fallos; histórico de sucesos, manual de operación para recuperación ante fallos; especificaciones de la arquitectura de referencia de servicio en nube corporativo; documentación asociada a los scripts desarrollados; documentación de las pruebas de funcionamiento de los servicios de nueva y aplicaciones desarrolladas). Documentación técnica (documentación técnica asociado a los servicios de nube; manuales y documentación técnica de servicios de proveedores de nube; manuales de condiciones de nivel de servicios de proveedores de nube -SLA-; manuales de los servicios incluidos en el proveedor de nube y versión publicada; manuales de funcionamiento de las herramientas de gestión del ciclo de vida del software).

MÓDULO FORMATIVO 1

Gestión de recursos y servicios en la nube

Nivel:	*3*
Código:	*MF2735_3*
Asociado a la UC:	*UC2735_3 - Gestionar recursos y servicios en la nube*
Duración (horas):	*120*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de preparación de interfaces de acceso y uso, configurándolos para acceder a los servicios de la plataforma en la nube.

CE1.1 Describir procedimientos de conexión a plataformas en la nube para el uso de interfaces gráficas mediante un navegador, explicando cómo autenticarse y los pasos para configurar elementos tales como el idioma, aspecto gráfico y preferencias entre otros, para acceder a los servicios de la plataforma.

CE1.2 Explicar procesos de instalación de interfaces de línea de comandos, previa descarga, en el entorno a utilizar, tal como en local, en un servidor o en una plataforma administrada, describiendo los pasos a seguir para inicializar la interfaz, autenticarse y administrar las configuraciones almacenadas.

CE1.3 Detallar el proceso de descarga de librerías de cliente para los lenguajes de computación a utilizar, indicando cómo usar los gestores de dependencias.

CE1.4 En un supuesto práctico de aplicar procedimientos de preparación de interfaces de acceso y uso, configurándolos para acceder a los servicios de la plataforma en la nube:
- Efectuar una conexión a la plataforma para el uso de interfaces gráficas mediante un navegador, autenticándose y configurando elementos tales como el idioma, aspecto gráfico y preferencias entre otros, para acceder a los servicios de la plataforma.
- Instalar unas interfaces de línea de comandos, previa descarga, en el entorno a utilizar, tal como en local, en un servidor o en una plataforma administrada, inicializando la interfaz, autenticándose y administrando las configuraciones almacenadas.
- Descargar unas librerías de cliente para los lenguajes de computación a utilizar usando los gestores de dependencias.

C2: Aplicar procedimientos para establecer jerarquías de recursos y organizarlos, utilizando los niveles de organización disponibles según el proveedor utilizado, siguiendo las prácticas recomendadas por el proveedor.

CE2.1 Describir el procedimiento de creación de nodos que representan una hipotética entidad o empresa, siguiendo unas directrices y explicar cómo administrar su configuración para asegurar el funcionamiento de los recursos dependientes de los mismos.

CE2.2 Explicar cómo se definen niveles intermedios de agrupación de recursos, estableciendo una jerarquía en los mismos y configurando unas políticas en función de unas directrices respecto a la arquitectura.

CE2.3 Detallar el proceso para crear contenedores de recursos de bajo nivel, explicando cómo gestionar las configuraciones de seguridad y control de accesos, facturación y restricciones para permitir el posterior despliegue de recursos.

CE2.4 Interpretar políticas de configuraciones comunes a todos o parte de los recursos de la entidad, tales como restricciones, configuraciones de seguridad o etiquetado de los mismos, para su creación en cada uno de los niveles de la jerarquía, asignando parámetros de configuración, para que dichas configuraciones se hereden y apliquen automáticamente en los recursos y faciliten la gobernanza de los recursos en la nube y la autonomía y productividad de cada individuo o grupo de trabajo.

CE2.5 En un supuesto práctico de aplicación de procedimientos para establecer jerarquías de recursos y organizarlos, utilizando los niveles de organización disponibles según el proveedor utilizado, siguiendo las prácticas recomendadas por el proveedor:

- Crear unos nodos que representan una entidad o empresa, siguiendo unas hipotéticas directrices de dicha entidad, administrando su configuración para asegurar el funcionamiento de los recursos dependientes de los mismos.
- Crear unos niveles intermedios de agrupación de recursos, estableciendo una jerarquía en los mismos y configurando las políticas, siguiendo unas hipotéticas directrices de la entidad respecto a la arquitectura.
- Crear unos contenedores de recursos de bajo nivel, gestionando las configuraciones de seguridad y control de accesos, facturación y restricciones para permitir el posterior despliegue de recursos.
- Implementar políticas de configuraciones comunes a todos o parte de los recursos de la entidad, tales como restricciones, configuraciones de seguridad o etiquetado de recursos, se implementan en cada uno de los niveles de la jerarquía, asignando parámetros de configuración, para que dichas configuraciones se hereden y apliquen automáticamente en los recursos y faciliten la gobernanza de los recursos en la nube y la autonomía y productividad de cada individuo o grupo de trabajo.

C3: Aplicar técnicas de administración de identidades y controles de acceso, manteniendo la seguridad respecto a la autenticación y permisos y facilitando la realización de acciones de forma simple, rápida y eficiente para permitir la gestión de los recursos y servicios por personas y programas.

CE3.1 Enumerar componentes administrativos relacionados con la gestión de identidades y controles de acceso, definiendo su utilidad y objetivos.

CE3.2 Describir procedimientos de creación y administración de identidades para los usuarios, explicando los pasos para permitir su autenticación en los servicios, agruparlas en grupos y/o dominios, bien creándolas en el entorno de nube o sincronizándolos en su caso con otro entorno externo al proveedor o delegando la validación a otro entorno físico o nube, implementando prácticas de seguridad tales como política de contraseñas y doble factor de autenticación, entre otras.

CE3.3 Explicar el proceso de creación y gestión de cuentas de servicio, aplicando el principio JIT ("Just in Time") para crearlas exactamente en el momento en que se requieran, indicando el procedimiento para asignarlas a cada programa o recurso que necesite una autenticación individual, implementando prácticas de seguridad para gestión de credenciales tales como políticas de creación y descarga de claves y periodos de rotación, entre otras.

CE3.4 Detallar procedimientos de administración de roles personalizados, explicando los pasos a aplicar para modificar permisos individuales en caso de que no se ajusten a las operaciones previstas que requiere para su actividad.

CE3.5 Definir los principios de "mínimo privilegio" y "continuidad de negocio" y su relación con la asignación de identidades a roles, para permitir acceder o administrar los recursos y aplicaciones por parte de las personas y programas encargados de ello.

CE3.6 Explicar el proceso de auditoría de configuraciones de seguridad de control de acceso detallando cómo asegurar el despliegue, analizando la gestión de las identidades asignadas, roles y permisos asignados, acciones realizadas y accesos a datos, de forma periódica y en respuesta a situaciones imprevistas que lo requieran.

CE3.7 Enumerar herramientas de repositorio de secretos, credenciales, certificados, claves e información sensible en general, para restringir su acceso, describiendo sus características para asegurar la privacidad, centralizar la gestión y registrar accesos y operaciones.

CE3.8 En un supuesto práctico de aplicación de técnicas de administración de identidades y controles de acceso, manteniendo la seguridad respecto a la autenticación y permisos y facilitando la realización de acciones de forma simple, rápida y eficiente para permitir la gestión de los recursos y servicios por personas y programas:

- Crear identidades para unos usuarios, administrándolas para permitir su autenticación en los servicios, agrupándolas en grupos y/o dominios, bien creándolas en el entorno de nube o sincronizándolos en su caso con otro entorno externo al proveedor, o delegando la validación a otro entorno físico o nube, implementando prácticas de seguridad tales como política de contraseñas, doble factor de autenticación, entre otras.
- Crear unas cuentas de servicio, gestionándolas y asignándolas a cada programa o recurso que necesite una autenticación individual, aplicando el principio JIT ("Just in Time") para crearlas exactamente en el momento en que se requieran, implementando las prácticas de seguridad para gestión de credenciales tales como políticas de creación y descarga de claves y periodos de rotación, entre otras.
- Administrar unos roles personalizados para cada caso en que no se ajusten a las operaciones previstas, por tener asignados más o menos permisos individuales de los que requiere para su actividad.
- Asignar roles para cada identidad, según los principios de "mínimo privilegio" y "continuidad de negocio", para permitir acceder o administrar los recursos y aplicaciones a unas personas y programas.
- Auditar la configuración de seguridad del control de acceso para asegurar el despliegue, analizando la gestión de las identidades asignadas, roles y permisos asignados, acciones realizadas y accesos a datos, manteniendo el principio de "mínimo privilegio" y "continuidad de negocio".
- Almacenar unos secretos, credenciales, certificados, claves e información sensible en general, usando un repositorio de secretos, permitiendo el acceso sólo a las personas y programas previa autenticación, asegurando su privacidad, centralizando su gestión y registrando sus accesos y operaciones para auditarlos posteriormente.

C4: Aplicar el proceso de configuración de la facturación de unos recursos desplegados para gestionar su pago y controlar y analizar los costes incurridos, siguiendo indicaciones contables e imputando los costes a los centros de gastos establecidos.

CE4.1 Enumerar posibilidades de identificación de recursos para facilitar la gestión, control y análisis de costes entre otros, explicando cómo etiquetarlos según esa nomenclatura.

CE4.2 Describir cuentas de gasto y sus características, tales como términos y métodos de pago indicados por la misma, explicando cómo crearlas y cómo vincular los recursos al centro de gasto asignado, asegurando que ningún problema o retraso con los pagos afecte a la continuidad de los recursos o procesos de una hipotética empresa.

CE4.3 Enumerar herramientas de planificación de gastos, explicando sus características, ventajas e inconvenientes.

CE4.4 Interpretar los criterios para establecer previsiones de gastos, según los recursos a utilizar en función de métricas como la carga, número de usuarios, datos almacenados, entre otros, usando herramientas de planificación de gastos.

CE4.5 Explicar procedimientos para configurar alertas de gastos, describiendo cómo establecer canales de notificación a los responsables y/o acciones automáticas que reaccionen a dichos eventos.

CE4.6 Describir técnicas y servicios para analizar costes, tales como paneles de reporte interactivos o análisis a partir de los datos exportados a otro entorno o sistema, entre otros, explicando cómo identificar los costes relativos a cada recurso y/o aplicación en conjunto.

CE4.7 En un supuesto práctico de aplicar el proceso de configuración de la facturación de unos recursos desplegados para gestionar su pago y controlar y analizar los costes incurridos, siguiendo indicaciones contables e imputando los costes a los centros de gastos establecidos:
- Crear unas cuentas de gasto, estableciendo los términos y métodos de pago, vinculando los recursos a un centro de gasto asignado y asegurando que ningún problema o retraso con los pagos afecte a la continuidad de los recursos o procesos de una hipotética empresa.
- Establecer unas previsiones de gastos según los recursos a utilizar en función de métricas como la carga, número de usuarios, datos almacenados, entre otros, usando herramientas de planificación de gastos.
- Configurar unas alertas de gastos, estableciendo canales de notificación a unas supuestas personas responsables y/o acciones automáticas que reaccionen a dichos eventos.
- Identificar costes relativos a cada recurso y/o aplicación en conjunto, analizando unos costes mensuales o diarios, utilizando las técnicas y servicios disponibles para ello, tales como paneles de reporte interactivos o un análisis a partir de los datos exportados a otro entorno o sistema, entre otros.

C5: Aplicar técnicas de configuración de un entorno para el posterior despliegue de recursos, administrando las cuotas de uso y habilitando las API ("Application Programming Interface") requeridas, en su caso, según los servicios a utilizar y el uso o número de recursos a desplegar.

CE5.1 Describir el procedimiento de planificación de valores para establecer cuotas de despliegue de recursos y utilización de servicios y API, explicando cómo asegurarse de tener suficiente cuota disponible tanto para el despliegue como para el funcionamiento de los recursos a desplegar.

CE5.2 Explicar el proceso de establecimiento de cuotas de despliegue de recursos y utilización de servicios, indicando los pasos para configurarlas una a una, ampliando o reduciendo cuando se requiera incrementar o restringir un número máximo de recursos posible en un entorno concreto, por razones tales como controlar los costes o desplegar entornos de pruebas limitados, entre otros.

CE5.3 Detallar el procedimiento para habilitar las API de cada servicio para poder utilizar los servicios, describiendo cómo deshabilitar aquellas correspondientes a servicios que no se prevean utilizar, para mantener una mayor seguridad y control de costes en cada entorno.

CE5.4 En un supuesto práctico de aplicación de técnicas de configuración de un entorno para el posterior despliegue de recursos, administrando las cuotas de uso y habilitando las API requeridas, en su caso, según los servicios a utilizar y el uso o número de recursos a desplegar:
- Planificar los valores para unas cuotas de despliegue de recursos y utilización de servicios y API, asegurándose de tener suficiente cuota disponible para el despliegue y funcionamiento de los recursos a desplegar.

- Establecer las cuotas de despliegue de recursos y utilización de servicios, configurándolas una a una, ampliando o reduciendo cuando se requiera incrementar o restringir un número máximo de recursos posible en un entorno concreto, por razones tales como controlar los costes o desplegar entornos de pruebas limitados, entre otros.
- Habilitar las API de cada servicio para poder utilizar los servicios, deshabilitando aquellas correspondientes a servicios que no se prevean utilizar, para mantener una mayor seguridad y control de costes en cada entorno.

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

C1 respecto a CE1.4; C2 respecto a CE2.5; C3 respecto a CE3.8; C4 respecto a CE4.7 y C5 respecto a CE5.4.

Otras Capacidades:

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.

Contenidos

1 Preparación de interfaces de acceso y uso de plataformas en la nube

Procedimientos de conexión a plataformas en la nube para el uso de interfaces gráficas. Configuración.
Procedimientos de instalación de interfaces de línea de comandos. Inicialización, autenticación y administración de configuraciones almacenadas.
Librerías de cliente para lenguajes de computación. Gestores de dependencias.

2 Establecimiento y organización de jerarquías de recursos en la nube

Creación y administración de nodos que representan una entidad o empresa.
Definición de agrupación de recursos en niveles intermedios. Jerarquía y políticas.
Creación de contenedores de recursos de bajo nivel. Gestión de configuraciones de seguridad y control de accesos, facturación y restricciones.
Políticas de configuraciones comunes a todos o parte de los recursos de la entidad. Restricciones, configuraciones de seguridad o etiquetado de recursos. Herencia de parámetros de configuración.

3 Administración de identidades y controles de acceso en la nube

Componentes administrativos relacionados con la gestión de identidades y controles de acceso.
Creación y administración de identidades para los usuarios. Grupos y/o dominios. Sincronización. Política de contraseñas y doble factor de autenticación.
Creación y gestión de cuentas de servicio. Asignación a programas o recursos. Gestión de credenciales: políticas de creación y descarga de claves y periodos de rotación, entre otras. Principio JIT ("Just in Time").

Administración de roles personalizados. Principios de "mínimo privilegio" y "continuidad de negocio".
Auditoría de configuraciones de seguridad de control de acceso.
Herramientas de repositorio de secretos, credenciales, certificados, claves e información sensible.

4 Configuración de la facturación de recursos desplegados en la nube

Cuentas de gasto. Términos y métodos de pago. Creación y vinculación de los recursos al centro de gasto asignado.
Criterios para establecer previsiones de gastos. Métricas: carga, número de usuarios, datos almacenados, entre otros. Herramientas de planificación de gastos.
Alertas de gastos. Establecimiento de canales de notificación y acciones automática ante eventos.
Técnicas y servicios para analizar costes. Paneles de reporte interactivos. Análisis a partir de los datos exportados.

5 Configuración de entornos para el despliegue de recursos en la nube

Establecimiento de cuotas de despliegue de recursos y utilización de servicios y API. ("Application Programming Interface"). Planificación. Incremento o restricción del número máximo de recursos en un entorno.
Procedimiento de habilitación y deshabilitación de API de cada servicio.

Parámetros de contexto de la formación

Espacios e instalaciones

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

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

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

MÓDULO FORMATIVO 2

Gestión de recursos de red y comunicaciones en la nube

Nivel: *3*
Código: *MF2736_3*
Asociado a la UC: *UC2736_3 - Gestionar recursos de red y comunicaciones en la nube*
Duración (horas): *120*
Estado: *Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de despliegue de una infraestructura de red asociada a las aplicaciones de unos sistemas, configurando la privacidad, seguridad y disponibilidad, para permitir la conectividad entre recursos de la nube y otras instalaciones "on premises" o en otras nubes.

CE1.1 Describir el proceso de creación automatizada o modificación de unos servicios de red para las aplicaciones, explicando cómo usar para ello unas 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.

CE1.2 Explicar el procedimiento de establecimiento como redes virtuales de un rango de direccionamiento privado, gestión del direccionamiento público, puertas de enlace, cortafuegos y/o grupos de seguridad, y de la delegación de subredes con otros servicios de nube, indicando los pasos a seguir para configurarlas con los rangos de direcciones IP en las zonas de disponibilidad y/o regiones.

CE1.3 Interpretar reglas de cortafuegos y/o los parámetros de creación de grupos de seguridad para los recursos y destinos, describiendo su configuración en función de las conexiones permitidas y cómo habilitar el tráfico a los protocolos y puertos utilizados, incorporando las opciones de creación de registros disponibles.

CE1.4 Determinar parámetros de tipo clave-valor que se deben asignar para la resolución de nombres explicando el proceso de configuración 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 previamente.

CE1.5 Especificar 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, describiendo cómo se crean mediante configuración del cifrado y la seguridad de la conexión, la autenticación y autorización del usuario, así como su monitorización y registro de accesos.

CE1.6 Describir el procedimiento de creación de unos recursos de inspección, explicando los pasos para ubicarlos en las localizaciones de una topología de red, para registrar y analizar el tráfico a través de la red por motivos de seguridad o para la resolución de problemas.

CE1.7 Explicar el proceso de enrutado y conexión entre sistemas locales y servicios WAN de redes, indicando cómo 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.

CE1.8 En un supuesto práctico de aplicación de procedimientos de despliegue de una infraestructura de red asociada a las aplicaciones de unos sistemas, configurando la privacidad, seguridad y disponibilidad, para permitir la conectividad entre recursos de la nube y otras instalaciones "on premises" o en otras nubes:
- Configurar unas 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.
- Crear unas 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 criterios de seguridad.
- 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 unos destinos, a través de zonas DNS privadas o públicas enlazadas con las redes virtuales definidas.
- Crear unos 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.
- Crear unos 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 por motivos de seguridad o para la resolución de problemas.
- 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.

C2: Aplicar técnicas de configuración de 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.

CE2.1 Explicar técnicas de configuración de balanceadores de carga, indicando cómo se incluyen reglas y parámetros que permitan el tráfico hacia aplicaciones externas o internas de la organización, redireccionando y balanceando el tráfico entre unos destinos y permitiendo el escalado de los recursos de computación.

CE2.2 Describir el proceso de creación de recursos de resolución de nombres para el intercambio automático del direccionamiento real de red o DNS (Sistema de Nombres de Dominio), explicando 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.

CE2.3 Enumerar parámetros de caché perimetral distribuido de la nube tales como punto de conexión, host de origen, encabezado, protocolo, entre otros, indicando cómo se configuran 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.

CE2.4 Detallar las opciones de traducción de direccionamiento público, describiendo cómo se establecen, utilizando los servicios de un 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 emplear el acceso a internet privado para las aplicaciones desplegadas.

CE2.5 Explicar los mecanismos de establecimiento de direccionamiento público y privado para cada uno de los recursos de red que lo requieran, indicando el proceso para reservar 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.

CE2.6 Interpretar los parámetros de conectividad, protección, autorización y auditoría, siguiendo los requisitos de seguridad, acceso, supervisión y rendimiento para habilitar servicios de nube para el control perimetral, cortafuegos, enrutamiento y puertas de enlace, detallando cómo configurarlos.

CE2.7 En un supuesto práctico de aplicación de técnicas de configuración de recursos de red, asignando parámetros de balanceo y escalado horizontal y vertical, desde orígenes externos, en condiciones de seguridad, para el direccionamiento y enrutado de tráfico a los recursos desplegados en la nube:

- Configurar unos balanceadores de carga con las reglas y parámetros que permitan el tráfico hacia aplicaciones externas o internas de una hipotética organización, redireccionando y balanceando el tráfico a los destinos y permitiendo el escalado de los recursos de computación.
- Crear unos 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.
- Configurar unas 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 la localización más cercana a los usuarios, permitiendo la respuesta más rápida y económica a los recursos de las aplicaciones.
- Establecer opciones de traducción de direccionamiento público, utilizando los servicios del proveedor de nube, compartiendo un pequeño número de direcciones públicas entre varios recursos como máquinas virtuales o contenedores, sin la necesidad de utilizar una dirección para cada recurso único, permitiendo emplear por otro lado el acceso a internet privado para las aplicaciones desplegadas.
- 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.
- Habilitar servicios de nube para el control perimetral, cortafuegos, enrutamiento y puertas de enlace, configurando los parámetros de conectividad, protección, autorización y auditoría, siguiendo criterios de seguridad, acceso, supervisión y rendimiento.

C3: Aplicar técnicas de administración de redes privadas físicas y virtuales mediante herramientas de un 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.

CE3.1 Describir métodos tales como emparejamiento de redes o redes compartidas, para permitir la conexión interna y directa entre recursos desplegados en la nube y configurar redes virtuales, en función de unos requisitos sobre conectividad y administración de las redes y su conexión.

CE3.2 Explicar el mecanismo para establecer 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, indicando cómo utilizar 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.

CE3.3 Describir el proceso de configuración de parámetros de conexión de dispositivos físicos que permita el enrutamiento de una conexión entre el entorno nube y los equipos locales, de tal modo que se maximice el ancho de banda, se reduzca la latencia y se potencie la calidad de servicio para establecer conexiones directas y privadas entre redes locales y los proveedores de nube.

CE3.4 Detallar el procedimiento para establecer conexiones directas y de emparejamiento público de redes a través de conectividad física, explicando cómo permitir un direccionamiento de tráfico público a través de unos puntos de emparejamiento para conexiones públicas cuyos requisitos de calidad de servicio, latencia o coste se soliciten previamente.

CE3.5 Interpretar parámetros de configuración para definir dispositivos de enrutamiento físicos o virtuales en redes, publicando rutas dinámicas entre unas conexiones creadas y permitiendo la detección automática de cambios en la topología de red.

CE3.6 Determinar parámetros sobre autenticación, seguridad, cifrado, conexión y configuración de clientes VPN, explicando su uso para configurar conexiones VPN "site-to-site" o "point-to-site".

CE3.7 En un supuesto práctico de aplicación de técnicas de administración de redes privadas físicas y virtuales mediante herramientas de un 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:

- Configurar unas 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 unos requisitos sobre conectividad y administración de las redes y su conexión.
- Establecer unas 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 unos requisitos de conectividad de los entornos, calidad de la conexión, latencia, ancho de banda máximo permitido y costes.
- Establecer unas 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.
- Establecer unas 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 conexiones públicas bajo ciertos requisitos de calidad de servicio, latencia o coste.
- Definir unos 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.
- Configurar unas conexiones VPN "site-to-site" o "point-to-site", siguiendo unos parámetros sobre autenticación, seguridad, cifrado, conexión y configuración de clientes VPN.

C4: Aplicar procedimientos de configuración de la seguridad de unos recursos, monitorizando sus conexiones, para registrar los accesos e identificar su potencial riesgo en los sistemas.

CE4.1 Describir reglas que permitan identificar accesos desde los orígenes y destinos de las comunicaciones para su monitorización y control, explicando su configuración.

CE4.2 Detallar reglas, políticas e integración de servicios de terceros para configurar cortafuegos para los servicios de nube, explicando los pasos para su parametrización.

CE4.3 Enumerar herramientas WAF ("Web Application Firewall") y/o IPS (Sistema de prevención de intrusos), entre otras explicando su uso para la administración y protección de aplicaciones o servicios "web", describiendo el proceso de activación, para identificar y prevenir posibles ataques y amenazas en capa 7 de comunicaciones, 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.

CE4.4 Interpretar parámetros de autorización, autenticación, auditoría, entre otros, para crear o modificar unas configuraciones de seguridad para las aplicaciones de la organización, empleando los mecanismos de automatización de una 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, permitiendo la trazabilidad, observabilidad y auditoría de los sistemas.

CE4.5 Explicar el procedimiento de configuración de la monitorización de unos recursos de red y la conectividad del resto de recursos desplegados, describiendo cómo añadir alertas que muestren el estado de conexión, "log" y análisis del tráfico que permitan anticipar problemas o identificar incidencias en las comunicaciones y servicios.

CE4.6 En un supuesto práctico de aplicar procedimientos de configuración de la seguridad de unos recursos, monitorizando sus conexiones, para registrar los accesos e identificar su potencial riesgo en los sistemas:

- Configurar unas políticas de seguridad sobre los recursos de una nube, creando reglas que permitan identificar accesos desde los orígenes y destinos de las comunicaciones para su monitorización y control.
- Configurar unos servicios de cortafuegos para los servicios de nube, especificando unas reglas, políticas e integración de servicios de terceros definidos.
- Activar unas 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.
- Crear unas configuraciones de seguridad para aplicaciones, incorporando los parámetros de autorización, autenticación, auditoría, entre otros, empleando los mecanismos de automatización de esa 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.
- Configurar la monitorización de unos recursos de red y la conectividad del resto de recursos desplegados, para comprobar mediante alertas su estado de salud, estado de conexión, "log" y análisis del tráfico que permitan anticipar problemas o identificar incidencias en las comunicaciones y servicios.

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

C1 respecto a CE1.8; C2 respecto a CE2.7; C3 respecto a CE3.7 y C4 respecto a CE4.6.

Otras Capacidades:

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.

Contenidos

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.

Parámetros de contexto de la formación

Espacios e instalaciones

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

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

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

MÓDULO FORMATIVO 3

Administración de recursos de computación en entornos de nube

Nivel:	*3*
Código:	*MF2737_3*
Asociado a la UC:	*UC2737_3 - Administrar recursos de computación en entornos de nube*
Duración (horas):	*150*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar técnicas de despliegue de instancias de computación y grupos de cómputo para usar unos recursos, aplicando las características definidas previamente y proporcionando capacidades de autoescalado, para obtener un entorno de trabajo sobre el que configurar la capacidad de procesamiento según unas necesidades.

CE1.1 Describir el proceso de elección y configuración de una región y zona de disponibilidad, explicando los pasos para autenticarse en la plataforma de nube usando credenciales para el proyecto especificado e interpretar las necesidades de arquitectura, tales como alta disponibilidad, localización de la plataforma o requisitos de red.

CE1.2 Clasificar tipos de instancia, describiendo sus características.

CE1.3 Explicar el procedimiento de creación de una plantilla de ejecución de cómputo, en el caso de grupos de escalado o para definir instancias homogéneas, detallando cómo incluir el tipo de instancia, sus características de CPU, memoria, reserva de recursos en la plataforma y almacenamiento.

CE1.4 Enumerar opciones de computación, describiendo cómo elegirla en el listado proporcionado por un proveedor de nube y tomar el elemento cuyas características de CPU, memoria y modo de virtualización se correspondan con los criterios funcionales, económicos y operativos del proyecto, incluyendo la reserva de recursos en la plataforma, y usando plantillas para homogeneizar el proceso en caso de disponer de ellas.

CE1.5 Describir recursos de computación, indicando los pasos para modificarlos, en su caso, en la configuración de la instancia de cómputo, analizando los requisitos de tamaño, velocidad, memoria y características especiales de replicación necesarias según el proyecto.

CE1.6 Explicar el procedimiento para añadir recursos de red, describiendo cómo escogerlos de entre los disponibles para el proyecto, atendiendo a la región y zona de disponibilidad seleccionadas y teniendo en cuenta los requisitos de comunicaciones recogidos en el proyecto, indicando los pasos para seleccionar los segmentos y direccionamiento de red correspondientes a una zona o región e incluir la solicitud de direccionamiento público en su caso.

CE1.7 Detallar el proceso de definición del comportamiento automatizado asociado al grupo de escalado y requerido tanto en despliegue como en la eliminación de recursos de cómputo, explicando cómo asegurar que, ante cambios de las cargas de trabajo, los recursos se crean y destruyen de una forma solicitada.

CE1.8 Clasificar recursos de monitorización para supervisar el estado y rendimiento de una instancia, explicando sus características y el proceso para añadirlos seleccionándolos en un proveedor de nube, bien inicialmente o bien con posterioridad al despliegue.

CE1.9 Describir procedimientos de administración de la configuración de seguridad en una instancia, indicando cómo garantizar exclusivamente los accesos usando unos puertos y protocolos y a ciertos usuarios especificados.

CE1.10 Explicar técnicas de etiquetado para identificar unas instancias de computación dentro de la plataforma, de modo que se asignen de forma unívoca e indicando elementos tales como el proyecto asociado y el rol dentro del mismo, entre otra información, para que sea posible en el futuro agrupar los recursos de las instancias asociadas al proyecto.

CE1.11 En un supuesto práctico de aplicación de técnicas de despliegue de instancias de computación y grupos de cómputo para usar unos recursos, aplicando las características definidas previamente y proporcionando capacidades de autoescalado, para obtener un entorno de trabajo sobre el que configurar la capacidad de procesamiento según unas necesidades:

- Elegir una región y zona de disponibilidad, tras autenticarse en la plataforma de nube usando unas credenciales, interpretando unas necesidades de arquitectura, tales como alta disponibilidad, localización de la plataforma o requisitos de red.
- Crear una plantilla de ejecución de cómputo, en el caso de grupos de escalado o para definir instancias homogéneas, incluyendo el tipo de instancia, sus características de CPU, memoria, reserva de recursos en la plataforma y almacenamiento.
- Seleccionar una opción de computación, eligiéndola en el listado proporcionado por un proveedor de nube y tomando el elemento cuyas características de CPU, memoria y modo de virtualización se correspondan con unos criterios funcionales, económicos y operativos, incluyendo la reserva de recursos en la plataforma, y usando plantillas para homogeneizar el proceso en caso de disponer de ellas.
- Modificar recursos de computación, en su caso, en la configuración de la instancia de cómputo, analizando unos requisitos de tamaño, velocidad, memoria y características especiales de replicación.
- Añadir unos recursos de red, escogiéndolos de entre unos disponibles, atendiendo a la región y zona de disponibilidad seleccionadas y teniendo en cuenta unos requisitos de comunicaciones, seleccionando los segmentos y direccionamiento de red correspondientes a la zona o región elegidas previamente e incluyendo la solicitud de direccionamiento público en su caso.
- Definir un comportamiento automatizado asociado al grupo de escalado y requerido tanto en despliegue como en la eliminación de recursos de cómputo, asegurando que, ante cambios de las cargas de trabajo, los recursos se crean y destruyen de una forma solicitada.
- Añadir unos recursos de monitorización, seleccionando los disponibles en el proveedor de nube, bien inicialmente o bien con posterioridad al despliegue para supervisar el estado y rendimiento de la instancia.
- Administrar la configuración de seguridad en la instancia, garantizando exclusivamente los accesos a unos puertos, protocolos y usuarios.
- Crear etiquetas que identifiquen las instancias de computación dentro de una plataforma, asignándolas de forma unívoca, indicando elementos tales como un proyecto asociado y rol dentro del mismo, entre otra información, de forma que sea posible en el futuro agrupar los recursos de las instancias asociadas a un proyecto.

C2: Aplicar técnicas de despliegue de contenedores, partiendo de imágenes almacenadas en un registro al efecto ("hub"), para ejecutar aplicaciones basadas en estos recursos según unas necesidades.

CE2.1 Describir los procesos de administración de imágenes para el despliegue de los componentes de las aplicaciones sobre contenedores, indicando cómo localizarlas en un "hub",

cómo descargarlas, configurarlas, interpretando la documentación técnica, crearlas en su caso y almacenarlas en un registro de imágenes, accesible con las credenciales de la plataforma.

CE2.2 Detallar las características del despliegue de un contenedor, indicando cómo se configuran, mediante variables de entorno o ficheros de configuración que se aplican en el momento de inicio del contenedor, asegurando la asignación de recursos a cada componente descrito en la documentación del proyecto.

CE2.3 Explicar el procedimiento de orquestación de nodos de cómputo, describiendo los pasos para configurarlos, haciendo uso de los grupos de cómputo o autoescalado junto a la orquestación de balanceo y enrutado de los contenedores en la red, para que estén controlados y gestionados.

CE2.4 Enumerar opciones de monitorización del estado y rendimiento de los contenedores, explicando cómo se añaden, bien usando las disponibles en el proveedor de nube o bien posteriormente al despliegue y mediante una solución de monitorización particular.

CE2.5 En un supuesto práctico de aplicación de técnicas de despliegue de contenedores, partiendo de imágenes almacenadas en un registro al efecto ("hub"), para ejecutar aplicaciones basadas en estos recursos según unas necesidades:

- Elegir una región y zona de disponibilidad, tras autenticarse en una plataforma de nube, usando credenciales, interpretando las necesidades de arquitectura de la solución en la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.
- Administrar unas imágenes para el despliegue de los componentes de las aplicaciones sobre contenedores, localizándolas en un "hub", descargándolas, configurándolas interpretando la documentación técnica, creándolas en su caso y almacenándolas en un registro de imágenes, accesible con las credenciales de la plataforma.
- Configurar características del despliegue del contenedor, mediante variables de entorno o ficheros de configuración que se aplican en el momento de inicio del contenedor, asegurando la asignación de recursos a cada componente y parametrizando: requisitos y límites de consumo de memoria y CPU de cada uno; privilegios del usuario de ejecución del proceso principal del contenedor; requisitos de almacenamiento persistente que se pudieran demandar para poder proporcionar recursos de almacenamiento externos al contenedor; configuraciones de resolución de nombres de red, la integración con otros contenedores de la plataforma y los accesos que se permiten a los puertos y el protocolo.
- Orquestar nodos de cómputo, configurándolos, haciendo uso de los grupos de cómputo o autoescalado junto a la orquestación de balanceo y enrutado de los contenedores en la red, para que estén controlados y gestionados.
- Añadir unas opciones de monitorización del estado y rendimiento de los contenedores, bien usando las disponibles en el proveedor de nube o bien posteriormente al despliegue y mediante una solución de monitorización particular.

C3: Aplicar técnicas de despliegue de la infraestructura de funciones como servicio, mediante el método seleccionado, para ejecutar componentes de aplicaciones basados en funciones desplegadas sobre cómputo.

CE3.1 Describir el proceso de creación de funciones como servicio, mediante uno de los métodos siguientes:

- Codificación en alguno de los lenguajes de programación soportados.
- Utilización de funciones existentes y publicadas en la plataforma.
- Ejecución de un contenedor de cómputo con un servicio que lanzará la función definida.
- Despliegue de aplicaciones ya preparadas por el proveedor de la nube.

- Escritura de ficheros de código que definen la creación dentro de la nube con las necesidades y características que permiten tener las infraestructuras de cómputo.

CE3.2 Explicar el proceso de asociación de permisos que posibilitan ejecutar la función como servicio, bien seleccionando un rol existente con los permisos, bien creando uno nuevo.

CE3.3 Enumerar requisitos de almacenamiento persistente para proporcionar recursos de almacenamiento externos al entorno de ejecución de la función como servicio, describiendo la manera de configurarlos asignando parámetros tales como contenedores, almacenamiento, redes, máquinas virtuales, entre otros componentes de arquitectura, en función de las necesidades.

CE3.4 Describir cómo se añaden los recursos de monitorización y gestión de eventos a los ficheros de creación automatizada de infraestructura, explicando las configuraciones de dichos recursos y las etiquetas que identifiquen unívocamente los elementos para el control del estado y rendimiento de los elementos de la arquitectura de los aplicativos.

CE3.5 Detallar el proceso de configuración del despliegue de la función como servicio, indicando cómo garantizar la procedencia de unos orígenes definidos.

CE3.6 Enumerar técnicas de etiquetado para identificar las funciones como servicio dentro de la plataforma, indicando cómo garantizar que sean unívocas, mediante la inclusión en ellas de elementos tales como el proyecto asociado y el rol dentro del mismo, entre otra información, de forma que sea posible agrupar los recursos asociados al proyecto.

CE3.7 En un supuesto práctico de aplicación de técnicas de despliegue de la infraestructura de funciones como servicio, mediante el método seleccionado, para ejecutar componentes de aplicaciones basados en funciones desplegadas sobre cómputo:

- Elegir una región y zona de disponibilidad, tras autenticarse en una plataforma de nube, usando credenciales, interpretando las necesidades de arquitectura de la solución en la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.
- Crear funciones como servicio, mediante uno de los métodos siguientes: codificándolas en alguno de los lenguajes de programación soportados; utilizando funciones existentes y publicadas en la plataforma; ejecutando un contenedor de cómputo con un servicio que ejecutará la función definida; desplegando aplicaciones ya preparadas por el proveedor de la nube; escribiendo los ficheros de código que definen la creación dentro de la nube con las necesidades y características que permiten tener unas infraestructuras de computo.
- Asociar permisos que posibiliten ejecutar la función como servicio, bien seleccionando un rol existente con los permisos, bien creando uno nuevo.
- Configurar requisitos de almacenamiento persistente para proporcionar recursos de almacenamiento externos al entorno de ejecución de la función como servicio, asignando parámetros tales como contenedores, almacenamiento, redes, máquinas virtuales, entre otros componentes de arquitectura, según unas necesidades.
- Añadir recursos de monitorización y gestión de eventos a los ficheros de creación automatizada de infraestructura, incluyendo las configuraciones de dichos recursos y las etiquetas que identifiquen unívocamente los elementos descritos en la documentación del proyecto para el control del estado y rendimiento de los elementos de la arquitectura de los aplicativos.
- Configurar el despliegue de la función como servicio, garantizando la procedencia de unos orígenes definidos.
- Añadir etiquetas que identifiquen las funciones como servicio dentro de la plataforma, asegurando que sean unívocas, indicando elementos tales como el proyecto asociado y el rol dentro del mismo, entre otra información, de forma que sea posible agrupar los recursos.

C4: Aplicar procedimientos de preparación y de automatización del "backup" de infraestructuras de cómputo en plataforma de proveedor de nube para asegurar los datos y el estado de los recursos desplegados según las necesidades del proyecto.

CE4.1 Describir procedimientos de creación de planes de copias de seguridad, teniendo en cuenta opciones de retención, frecuencias de ejecución, regiones y zonas en las que pudieran estar desplegados los recursos.

CE4.2 Explicar el proceso de configuración de la disponibilidad de los datos, velocidad de recuperación y retención de las copias de seguridad, junto con las directrices de seguridad encriptado, meta información y duplicados a otros entornos, describiendo cómo establecer las opciones de "backup", teniendo en cuenta el contexto y sus necesidades, dentro de los estándares que la plataforma de la nube permite para poder usar los datos salvaguardados en distintas regiones o zonas o recuperación de "backup".

CE4.3 Reproducir el proceso de asociación de planes de seguridad establecidos y recursos definidos en una plataforma de una de las formas siguientes:
- Usando las etiquetas asociadas a los mismos.
- Asignando los recursos de forma directa.
- Agrupando por tipo de servicio del proveedor de nube.

CE4.4 Detallar los pasos para crear políticas de seguridad, explicando cómo definir estándares de copias de seguridad y planificaciones en una plataforma, según necesidades del contexto o estándares incluidos para la plataforma del proveedor de nube.

CE4.5 En un supuesto práctico de aplicación de procedimientos de preparación y de automatización del "backup" de infraestructuras de cómputo en plataforma de proveedor de nube para asegurar los datos y el estado de los recursos desplegados según las necesidades del proyecto:
- Elegir una región y zona de disponibilidad, tras autenticarse en una plataforma de nube, usando credenciales, interpretando las necesidades de arquitectura de la solución de la documentación técnica, tales como alta disponibilidad, localización de la plataforma o requisitos de red.
- Crear unos planes de copias de seguridad, teniendo en cuenta directrices respecto a retenciones, frecuencias de ejecución y las regiones y zonas en las que pudieran estar desplegados los recursos.
- Configurar la disponibilidad de los datos, velocidad de recuperación y retención de las copias de seguridad junto con las directrices de seguridad encriptado, meta información y duplicados a otros entornos, estableciendo las opciones de "backup", teniendo en cuenta las necesidades del contexto, dentro de los estándares que la plataforma de la nube permite para poder usar los datos salvaguardados en distintas regiones o zonas o recuperación de "backup".
- Asociar los planes de seguridad a los recursos definidos en la plataforma de una de las formas siguientes: usando las etiquetas asociadas a los mismos; asignando los recursos de forma directa; agrupando por tipo de servicio del proveedor de nube.
- Crear unas políticas de seguridad, definiendo estándares de copias de seguridad y planificaciones en la plataforma, siguiendo implementaciones incluidos para ella por un proveedor de nube.

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

C1 respecto a CE1.11 C2 respecto a CE2.5; C3 respecto a CE3.7 y C4 respecto a CE4.5.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Proponerse objetivos retadores que supongan un nivel de rendimiento y eficacia superior al alcanzado previamente.
Interpretar y ejecutar instrucciones de trabajo de forma precisa.
Demostrar flexibilidad para entender los cambios.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Cumplir las medidas que favorezcan el principio de igualdad de trato y de oportunidades entre hombres y mujeres.

Contenidos

1 Instancias de computación y grupos de cómputo

Elección y configuración de región y zona de disponibilidad. Necesidades de arquitectura: alta disponibilidad, localización de la plataforma o requisitos de red.
Tipos de instancia. Clasificación y características.
Creación de plantillas de ejecución de cómputo. Grupos de escalado. Instancias homogéneas.
Opciones de computación. Características de CPU, memoria y modo de virtualización. Reserva de recursos en la plataforma.
Recursos de computación. Administración. Tamaño, velocidad, memoria y características especiales de replicación.
Recursos de red. Selección de segmentos y direccionamiento de red correspondientes a una zona o región. Direccionamiento público.
Grupo de escalado. Comportamiento automatizado asociado. Creación y destrucción de recursos.
Recursos de monitorización. Clasificación y administración.
Configuración de seguridad en una instancia. Administración. Garantía de autenticidad.
Técnicas de etiquetado de instancias de computación.

2 Despliegue de contenedores para ejecutar aplicaciones

Administración de imágenes para despliegue de componentes de las aplicaciones sobre contenedores. Creación o localización en "hub" y descarga, configuración y almacenamiento en registro de imágenes.
Despliegue de un contenedor. Configuración mediante variables de entorno o ficheros de configuración. Asignación de recursos a cada componente.
Orquestación de nodos de cómputo. Grupos de cómputo. Autoescalado. Orquestación de balanceo y enrutado de los contenedores en la red.
Monitorización del estado y rendimiento de los contenedores. Opciones de monitorización del estado y rendimiento de los contenedores. Soluciones del proveedor de nube. Soluciones de monitorización particulares.

3 Despliegue de infraestructuras de funciones como servicio para ejecución de componentes de aplicaciones basados en funciones desplegadas sobre cómputo

Métodos de creación de funciones como servicio: codificación en alguno de los lenguajes de programación soportados; utilización de funciones existentes y publicadas en la plataforma; ejecución de un contenedor de cómputo; despliegue de aplicaciones ya preparadas por el proveedor de la nube; escritura de ficheros de código para definir las infraestructuras de cómputo.
Permisos para ejecutar la función como servicio. Roles.
Requisitos de almacenamiento persistente. Configuración de componentes de la arquitectura.

Recursos de monitorización y gestión de eventos. Ficheros de creación automatizada de infraestructura.
Despliegue de la función como servicio. Configuración. Garantía de procedencia de orígenes.
Etiquetado de identificación de funciones como servicio.

4 Preparación y automatización del "backup" de infraestructuras de cómputo

Planes de copias de seguridad. Opciones: (retención, frecuencias de ejecución, regiones y zonas de despliegue de recursos).
Configuración de la disponibilidad de los datos. Opciones: (velocidad de recuperación y retención de las copias de seguridad, directrices de seguridad encriptado, meta información y duplicados a otros entornos).
Asociación de planes de seguridad y recursos definidos en una plataforma. Procedimientos: (etiquetas asociadas, asignación directa de los recursos; agrupación por tipo de servicio del proveedor de nube).
Políticas de seguridad. Creación. Definición de estándares de copias de seguridad y planificaciones en una plataforma.

Parámetros de contexto de la formación

Espacios e instalaciones

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

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

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

MÓDULO FORMATIVO 4

Gestionar recursos de almacenamiento y de bases de datos en la nube

Nivel:	*3*
Código:	*MF2738_3*
Asociado a la UC:	*UC2738_3 - Gestionar recursos de almacenamiento y de bases de datos en la nube*
Duración (horas):	*150*
Estado:	*Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar criterios de selección del tipo de almacenamiento para los datos del sistema según requisitos funcionales y criterios de durabilidad, seguridad, fiabilidad, rendimiento y coste, para un almacenamiento eficiente en el entorno o proyecto.

CE1.1 Identificar los requisitos funcionales y no funcionales relativos al almacenamiento de objetos y ficheros, seleccionándolos en la documentación de un proyecto y describiendo las operaciones a realizar para implementarlos.

CE1.2 Describir los tipos posibles de almacenamiento que ofrecen los proveedores, identificando las características que afectan a la durabilidad, fiabilidad y rendimiento.

CE1.3 Identificar la disponibilidad geográfica de los servicios de almacenamiento proporcionados por cada proveedor, seleccionando la oferta disponible en la región o regiones de un hipotético despliegue.

CE1.4 Clasificar los precios de proveedores de nube, dependiendo del tipo almacenamiento para seleccionar el más económico.

CE1.5 Enumerar los tipos de servicio relacionados con el almacenamiento, tales como acceso, transferencia, operaciones de lectura y escritura, replicación, copia de respaldo y recuperación, describiendo su finalidad y características.

CE1.6 En un supuesto práctico de aplicación de criterios de selección del tipo de almacenamiento para los datos del sistema según requisitos funcionales y criterios de durabilidad, seguridad, fiabilidad, rendimiento y coste, para un almacenamiento eficiente en el entorno o proyecto:

- Comprobar que las operaciones de almacenamiento de objetos y de ficheros de un proveedor, cumplen unos determinados requisitos funcionales y no funcionales.
- Consultar los tipos de almacenamiento proporcionados por un proveedor, a partir de la documentación del mismo, para verificar cuál ofrece garantías según criterios de durabilidad, fiabilidad y rendimiento especificados.
- Descartar tipos de almacenamiento proporcionados por un proveedor no disponibles en la región o regiones donde el sistema vaya a desplegarse, consultando la documentación del proveedor sobre disponibilidad geográfica.
- Seleccionar el tipo de almacenamiento que resulte más económico, consultando las tablas de precios del proveedor de nube.
- Ajustar parámetros de almacenamiento que afecten a los costes de uso del servicio, incluyendo los de almacenamiento, acceso, transferencia, operaciones de lectura y escritura, replicación, copia de respaldo y recuperación, así como cualquier otro coste específico que el

proveedor haya asignado al almacenamiento escogido, a partir de la información proporcionada por el proveedor, y cumpliendo unos requisitos funcionales y no funcionales.

C2: Aplicar procedimientos de administración de los sistemas de almacenamiento de objetos en nube, configurando y monitorizando los mismos, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a unos requisitos.

CE2.1 Describir las posibilidades y técnicas de nomenclatura de contenedores (también conocidos como depósitos o "buckets") y de las etiquetas para metadatos, teniendo en cuenta las limitaciones técnicas del proveedor de nube, de modo que se facilite su administración.

CE2.2 Identificar clases de almacenamiento para contenedores, teniendo en cuenta los patrones de acceso a los datos, las limitaciones impuestas para cada clase en el proveedor de nube, y los costes asociados de almacenamiento y de recuperación de objetos, para poder definir las propias clases y, en su caso, los objetos.

CE2.3 Identificar regiones geográficas de almacenamiento de objetos que aseguren unos requisitos de latencia y coste eficientes, teniendo en cuenta las restricciones de residencia de los datos que se definan.

CE2.4 Explicar el proceso para definir parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, describiendo los pasos para configurarlos mediante herramientas gráficas, y/o de línea de comandos, y/o interfaces de programación (API), y/o infraestructura como código (IaC).

CE2.5 Enumerar parámetros de un sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, explicando los pasos para configurarlos y garantizar que la información almacenada en el sistema sea accesible por los perfiles y/o aplicaciones que se definan.

CE2.6 Identificar parámetros de acceso público para acceso HTTP o HTTPS usando un dominio personalizado, explicando cómo configurar en su caso un certificado SSL proporcionado por el proveedor de nube, para que los usuarios puedan acceder al contenido almacenado usando el dominio especificado.

CE2.7 Explicar el procedimiento para configurar políticas de ciclo de vida de los objetos, mediante las herramientas proporcionadas por el proveedor de nube o vía IaC, para que conforme pasa el tiempo los objetos cambien automáticamente de clase y, en su caso, se versionen o se borren, garantizando así las políticas de retención de datos que se definan.

CE2.8 Explicar el procedimiento para configurar políticas de replicación y copia de seguridad de los objetos, describiendo los pasos a seguir para asegurar que, en caso de pérdida de información, esta se puede recuperar en la forma y tiempos especificados en el proyecto.

CE2.9 En un supuesto práctico de aplicación de procedimientos de administración de los sistemas de almacenamiento de objetos en nube, configurando y monitorizando los mismos, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a unos requisitos:

- Definir nombres de contenedores (también conocidos como depósitos o "buckets") y de etiquetas para metadatos, teniendo en cuenta las limitaciones técnicas del proveedor de nube, para facilitar su administración.
- Definir una clase de almacenamiento -y en su caso, un objeto- para cada contenedor, teniendo en unos requisitos funcionales, unos patrones de acceso a los datos, unas limitaciones impuestas para cada clase en el proveedor de nube, y unos costes asociados de almacenamiento y de recuperación de objetos.

- Escoger una región geográfica de almacenamiento de objetos, seleccionándola de entre todas las soportadas por el proveedor de nube, para asegurar que los requisitos de latencia y coste son los más eficientes, teniendo en cuenta unas restricciones de residencia de los datos.
- Configurar unos parámetros de sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, mediante herramientas gráficas, y/o de línea de comandos, y/o interfaces de programación (API), y/o infraestructura como código (IaC) para garantizar el cumplimiento de unos requisitos.
- Configurar parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, para garantizar de forma demostrable que la información almacenada en el sistema solo es accesible por unos perfiles y/o aplicaciones definidos.
- Configurar unos parámetros de acceso público, en caso de que los requisitos especifiquen acceso HTTP o HTTPS usando un dominio personalizado, utilizando en su caso un certificado SSL proporcionado por el proveedor de nube, para que los usuarios puedan acceder al contenido almacenado usando el dominio especificado.
- Configurar unas políticas de ciclo de vida de los objetos, mediante las herramientas proporcionadas por el proveedor de nube o vía IaC, para que conforme pasa el tiempo los objetos cambien automáticamente de clase y, en su caso, se versionen o se borren, garantizando así unas políticas de retención de datos.
- Configurar una política de replicación y copia de seguridad de los objetos, verificándose para asegurar que, en caso de pérdida de información, esta se puede recuperar en la forma y tiempos que se especifiquen.

C3: Aplicar procedimientos de administración de sistemas de almacenamiento de ficheros en nube, tanto en dispositivos de bloque como en sistemas de almacenamiento en red, utilizando tanto herramientas gráficas como de línea de comandos, API ("Application Programming Interface"), y/o IaC para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a unos requisitos.

CE3.1 Identificar requisitos funcionales de almacenamiento, tales como patrones de acceso a los datos, durabilidad de los datos, limitaciones impuestas para cada clase en el proveedor de nube, y los costes asociados de almacenamiento y de recuperación de datos, consultando la documentación de un proveedor.

CE3.2 Identificar regiones geográficas de almacenamiento de ficheros que aseguren unos requisitos de latencia y coste eficientes, teniendo en cuenta las restricciones de residencia de los datos que se definan.

CE3.3 Enumerar parámetros del sistema relativos a cifrado, explicando cómo crear en su caso claves de cifrado específicas, y cómo configurarlos mediante las herramientas proporcionadas por el proveedor de nube vía IaC, para garantizar el cumplimiento de unos requisitos.

CE3.4 Enumerar parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, explicando el proceso para configurarlos y garantizar que la información almacenada en el sistema solo es accesible por unos perfiles y/o aplicaciones definidos.

CE3.5 Describir el procedimiento de montaje de un dispositivo de almacenamiento o de un sistema de ficheros, explicando los pasos a seguir para garantizar el acceso a los ficheros desde tantos puntos como se hayan definido en los requisitos y en modalidad de solo lectura o bien de lectura/escritura según se defina, explicando así mismo el proceso de desmontaje previo ordenado del dispositivo y en qué casos sería necesario.

CE3.6 Explicar el procedimiento para aplicar cambios durante el ciclo de vida del dispositivo o sistema de ficheros, tales como cambios de tamaño reservado, cambios en la clase de almacenamiento, modificaciones en la configuración, desmontaje del sistema de ficheros y/o borrado, describiendo los pasos a seguir, para adaptarse a los requisitos cambiantes de un proyecto.

CE3.7 Describir el procedimiento para configurar y verificar políticas o mecanismos de replicación y copia de seguridad de los dispositivos y/o ficheros, asegurando que, en caso de pérdida accidental de la información, ésta se puede recuperar en la forma y tiempos especificados en el proyecto.

CE3.8 En un supuesto práctico de aplicación de procedimientos de administración de sistemas de almacenamiento de ficheros en nube, tanto en dispositivos de bloque como en sistemas de almacenamiento en red, utilizando tanto herramientas gráficas como de línea de comandos, API, y/o IaC para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a unos requisitos:

- Escoger una clase de almacenamiento teniendo en cuenta unos requisitos funcionales, unos patrones de acceso a los datos, una durabilidad de los datos, unas limitaciones impuestas para cada clase en el proveedor de nube, y unos costes asociados de almacenamiento y de recuperación de datos.
- Escoger una región geográfica -y en su caso la replicación entre múltiples zonas o regiones- se escoge, para asegurar que los requisitos de latencia y coste son los más eficientes, teniendo en cuenta unas restricciones de residencia de los datos.
- Configurar unos parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, mediante herramientas proporcionadas por el proveedor de nube vía IaC, para garantizar el cumplimiento de unos requisitos.
- Configurar unos parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, usando las herramientas de un proveedor, para garantizar que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.
- Implementar el montaje de un dispositivo de almacenamiento o de un sistema de ficheros se implementa para garantizar el acceso a los ficheros desde tantos puntos como se hayan definido en los requisitos y en modalidad de solo lectura o bien de lectura/escritura según esté establecido, realizando un desmontaje previo ordenado del dispositivo si fuera necesario.
- Aplicar cambios durante el ciclo de vida del dispositivo o sistema de ficheros, tales como cambios de tamaño reservado, cambios en la clase de almacenamiento, modificaciones en la configuración, desmontaje del sistema de ficheros y/o borrado, entre otros, considerando la posibilidad de requisitos cambiantes.
- Configurar unas políticas o mecanismos de replicación y copia de seguridad de los dispositivos y/o ficheros, verificándolas para asegurar que, en caso de pérdida accidental de la información, ésta se puede recuperar en la forma y tiempo que se especifique.

C4: Aplicar técnicas de administración de los sistemas de bases de datos, utilizando tanto herramientas gráficas como de línea de comandos, API, y/o IaC, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a unos requisitos.

CE4.1 Describir procedimientos de selección de la región geográfica en un proveedor de servicios de bases de datos en la nube, explicando los pasos a seguir y criterios aplicables para asegurar que los requisitos de latencia y coste son eficientes, teniendo en cuenta las restricciones de residencia de los datos especificadas en el proyecto, y en su caso para la replicación entre múltiples zonas o regiones.

CE4.2 Enumerar parámetros del sistema relativos a cifrado, describiendo el proceso de creación de claves de cifrado específicas y su configuración mediante las herramientas proporcionadas por el proveedor de nube vía IaC, para garantizar unos requisitos.

CE4.3 Describir parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, explicando el proceso de configuración para garantizar que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.

CE4.4 Describir el procedimiento de adaptación de la BBDD a cambios tales como tamaño reservado, de capacidad de computación provisionada, de replicación de los datos, o modificaciones en la configuración, explicando los pasos a seguir para realizarlos mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD.

CE4.5 Detallar el procedimiento de aplicación y configuración de las políticas o mecanismos de replicación y copia de seguridad de la BBDD, mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD y describiendo los pasos a seguir para asegurar que, en caso de pérdida accidental de la información, ésta se puede recuperar en la forma y tiempo que se requiera.

CE4.6 Describir los procedimientos de monitorización activa de las operaciones de inserción y consulta, mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD, para detectar potenciales problemas que requieran cambiar la infraestructura, la configuración, o las aplicaciones que usan el sistema.

CE4.7 Explicar procedimientos de optimización no complejos, tanto a nivel de configuración como a nivel de rediseño del esquema o distribución de los datos, describiendo los pasos seguir para garantizar que el rendimiento y coste de las operaciones se mantiene dentro de unos requisitos.

CE4.8 En un supuesto práctico de aplicación de técnicas de administración de los sistemas de bases de datos, utilizando tanto herramientas gráficas como de línea de comandos, API, y/o IaC, para garantizar el almacenamiento, la seguridad, y los patrones de uso que mejor se ajusten a unos requisitos:

- Escoger una región geográfica y, en su caso, la replicación entre múltiples zonas o regiones, para asegurar que los requisitos de latencia y coste son los más eficientes, teniendo en cuenta las restricciones de residencia de los datos.
- Configurar parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, mediante las herramientas proporcionadas por el proveedor de nube vía IaC, para garantizar el cumplimiento de unos requisitos.
- Configurar parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, para garantizar que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.
- Aplicar cambios propios del ciclo de vida de la BBDD tales como modificación de tamaño reservado, de capacidad de computación provisionada, de replicación de los datos, o modificaciones en la configuración, entre otros, mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD.
- Configurar políticas o mecanismos de replicación y copia de seguridad de la BBDD, verificándolas para asegurar que, en caso de pérdida accidental de la información, ésta se puede recuperar en una forma y tiempos especificados.
- Monitorizar activamente el rendimiento de las operaciones de inserción y consulta, mediante las herramientas proporcionadas por el proveedor de nube o por la propia BBDD, para detectar potenciales problemas que requieran cambiar la infraestructura, la configuración, o las aplicaciones que usan el sistema.

- Efectuar optimizaciones no complejas, modificando a nivel de configuración o a nivel de rediseño del esquema o la distribución de los datos, para garantizar que el rendimiento y coste de las operaciones se mantiene dentro de los requisitos aceptables.

C5: --

CE5.1 --

C5: --

CE5.1 --

C5: Aplicar técnicas de gestión de los datos tanto desde el exterior, como entre sistemas de almacenamiento y bases de datos soportados por un proveedor de nube, utilizando tanto herramientas gráficas, como de línea de comandos, API y/o IaC, para facilitar el flujo de información en el sistema.

CE5.1 Enumerar opciones de transferencia y sincronización de datos, describiendo su funcionalidad, latencia y seguridad, explicando los pasos para configurarlas mediante herramientas proporcionadas por el proveedor de nube.

CE5.2 Describir procedimientos de configuración de conexiones mediante herramientas proporcionadas por el proveedor de nube, explicando los pasos a seguir para permitir el flujo de datos entre origen y destino de manera segura y eficiente.

CE5.3 Detallar procedimientos de provisionado de los dispositivos, en el caso de transferencia de datos offline, describiendo los mecanismos indicados por proveedores de nube para el envío del dispositivo físico entre proveedor y cliente, de cara a realizar la copia local de datos y el posterior envío al punto de destino, prestando especial atención a la seguridad y cifrado de los datos.

CE5.4 Describir procedimientos de configuración de parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría utilizando las herramientas proporcionadas por el proveedor de nube, explicando los pasos a seguir, para garantizar que la información transferida solo se envía entre los orígenes y destinos especificados y que nunca abandona la zona geográfica marcada en los requisitos del proyecto.

CE5.5 Explicar procedimientos de configuración de parámetros de sincronización de datos, tanto unidireccional como bidireccional, describiendo cómo aplicarlos para que ésta se realice de forma automática y desatendida cumpliendo unos requisitos de latencia.

CE5.6 Describir procedimientos de importación y/o exportación de datos de manera manual o supervisada, detallando los pasos a seguir para aquellos casos en los que los requisitos no impliquen replicación periódica.

CE5.7 Detallar procedimientos de monitorización de procesos de importación, exportación, y/o sincronización de datos, tanto automáticos como manuales, describiendo su uso para identificar problemas de conectividad o integridad de las transferencias y observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

CE5.8 En un supuesto práctico de aplicación de técnicas de gestión de los datos tanto desde el exterior, como entre sistemas de almacenamiento y bases de datos soportados por un proveedor de nube, utilizando tanto herramientas gráficas, como de línea de comandos, API y/o IaC, para facilitar el flujo de información en el sistema:

- Evaluar opciones de transferencia y sincronización de datos para seleccionar la mejor opción teniendo en cuenta los requisitos funcionales, de latencia y de seguridad establecidos en el proyecto, observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

- Consultar tablas detalladas de precios de un proveedor de nube sobre transferencia y sincronización de datos, asegurando que se están teniendo en cuenta todos los costes de uso del servicio, incluyendo los de transferencia entre diferentes zonas y/o regiones.
- Configurar conexiones, utilizando las herramientas proporcionadas por el proveedor de nube, para permitir el flujo de datos entre origen y destino de manera segura y eficiente.
- Efectuar un provisionado de los dispositivos, en el caso de transferencia de datos offline, mediante el mecanismo establecido por el proveedor de nube para que se envíe el dispositivo físico entre proveedor y cliente, de cara a realizar la copia local de datos y el posterior envío al punto de destino, prestando especial atención a la seguridad y cifrado de los datos.
- Configurar parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, utilizando las herramientas proporcionadas por el proveedor de nube para garantizar que la información transferida solo se envía entre los orígenes y destinos especificados y que nunca abandona la zona geográfica marcada en los requisitos del proyecto.
- Configurar parámetros de sincronización de datos, tanto unidireccional como bidireccional, para que ésta se realice de forma automática y desatendida, cumpliendo unos requisitos de latencia.
- Completar una importación y/o exportación de datos de manera manual o supervisada, para aquellos casos en los que los requisitos no impliquen replicación periódica.
- Monitorizar el proceso de importación, exportación, y/o sincronización de datos, tanto automático como manual, para identificar problemas de conectividad o integridad de las transferencias, observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

C5: --

CE5.1 --

C6: Aplicar técnicas de administración de la infraestructura de datos de nube híbrida, utilizando tanto herramientas gráficas, como de líneas de comandos, API, y/o IaC, para permitir la interoperabilidad de la nube con otros entornos, siguiendo los criterios de patrones de acceso, seguridad, durabilidad, fiabilidad y rendimiento.

CE6.1 Describir el proceso de implementación de una configuración sobre transferencia y sincronización de datos, explicando su aplicación paso a paso.

CE6.2 Explicar mecanismos avanzados entre sistemas que haya que tener en cuenta a la hora de escribir la configuración, tales como VPN o conexiones dedicadas, describiendo el proceso de verificación de la interconexión.

CE6.3 Detallar el procedimiento de conexión desde el exterior, usando SSH o VPN o bien los mecanismos básicos de red privada proporcionados por los proveedores de nube, para permitir el flujo de datos entre origen y destino de manera segura y eficiente.

CE6.4 Describir el procedimiento de configuración de la visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, asignando los parámetros relativos de un sistema, para garantizar que la información transferida solo se envía entre los orígenes y destinos especificados y que nunca abandona una zona geográfica concreta.

CE6.5 Explicar el procedimiento de configuración de la sincronización de datos, tanto unidireccional como bidireccional, indicando los parámetros a asignar para que ésta se realice de forma automática y desatendida, cumpliendo unos requisitos de latencia.

CE6.6 Describir el procedimiento de importación y/o exportación de datos, explicando cómo completarlo de manera manual o supervisada, en contraposición a la replicación periódica, conectándose a la infraestructura de nube y lanzando la operación.

CE6.7 Detallar el procedimiento de monitorización de procesos de importación, exportación, y/o sincronización de datos, tanto automáticos como manuales, explicando cómo identificar problemas de conectividad o integridad en las transferencias y observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

CE6.8 En un supuesto práctico de aplicación de técnicas de administración de la infraestructura de nube híbrida, utilizando tanto herramientas gráficas, como de líneas de comandos, API, y/o IaC, para permitir la interoperabilidad de la nube con otros entornos, siguiendo los criterios de patrones de acceso, seguridad, durabilidad, fiabilidad y rendimiento:

- Verificar una implementación de una configuración definida, consultando y cotejándola con una documentación con instrucciones sobre transferencia y sincronización de datos.
- Comprobar que existen mecanismos avanzados entre los sistemas implicados, tales como VPN o conexiones dedicadas, verificando si hay que tenerlos en cuenta a la hora de escribir la configuración.
- Configurar conexiones usando SSH o VPN, en caso de conexión con el exterior, o los mecanismos de red privada proporcionados por los proveedores de nube, para permitir el flujo de datos entre origen y destino de manera segura y eficiente.
- Configurar la visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, asignando los parámetros del sistema relativos, para garantizar que la información transferida solo se envía entre los orígenes y destinos especificados y que nunca abandona una zona geográfica concreta.
- Configurar la sincronización de datos, tanto unidireccional como bidireccional, asignando parámetros para que ésta se realice de forma automática y desatendida, cumpliendo unos requisitos de latencia.
- Completar la importación y/o exportación de datos de manera manual o supervisada, para aquellos casos en los que los requisitos no impliquen replicación periódica, conectándose a la infraestructura de nube y lanzando la operación.
- Monitorizar los procesos de importación, exportación, y/o sincronización de datos, tanto automáticos como manuales, para identificar problemas de conectividad o integridad en las transferencias, observando que no hay pérdida de conexión y que los metadatos del destino se corresponden a los del origen.

C7: Aplicar técnicas de administración de sistemas de transformación y análisis de datos (OLAP), utilizando tanto herramientas gráficas como de línea de comandos y/o API, para garantizar el almacenamiento, la seguridad, y los patrones de uso.

CE7.1 Explicar criterios de selección de una región geográfica y en su caso, para la replicación entre múltiples zonas o regiones, asegurando unos requisitos de latencia y coste eficientes, teniendo en cuenta unas restricciones de residencia de los datos.

CE7.2 Explicar procedimientos de configuración de parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, usando las herramientas proporcionadas por el proveedor de nube vía IaC.

CE7.3 Detallar procedimientos de configuración de parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, garantizando de forma demostrable que la información almacenada en el sistema solo es accesible por los perfiles y/o aplicaciones definidos en el proyecto.

CE7.4 Describir procedimientos de configuración de la retención y/o particionado y/o compactación de datos, asignando parámetros del sistema OLAP relativos, para mantener el equilibrio entre la información disponible para análisis y el coste de almacenamiento.

CE7.5 Explicar procedimientos de monitorización de trabajos de carga y transformación de datos (ETL) verificando que no existen errores en los archivos log del sistema y que el tiempo de ejecución no se degrada y describiendo cómo detectar posibles problemas.

CE7.6 Detallar procedimientos de configuración de políticas o mecanismos de replicación y copia de seguridad de los datos en el sistema OLAP, verificando que, en caso de pérdida accidental de la información, ésta se puede recuperar en una forma y tiempo concretos.

CE7.7 Describir el procedimiento de monitorización activa del rendimiento de las operaciones y del espacio de almacenamiento ocupado, mediante las herramientas proporcionadas por un proveedor de nube, para detectar potenciales problemas.

CE7.8 En un supuesto práctico de Aplicación de técnicas de administración de sistemas de transformación y análisis de datos (OLAP), utilizando tanto herramientas gráficas como de línea de comandos y/o API, para garantizar el almacenamiento, la seguridad, y los patrones de uso:

- Escoger una región geográfica y en su caso, la replicación entre múltiples zonas o regiones, asegurando unos requisitos de latencia y coste eficientes, teniendo en cuenta unas restricciones de residencia de los datos.
- Configurar unos parámetros del sistema relativos a cifrado, incluyendo en su caso la creación de claves de cifrado específicas, mediante las herramientas proporcionadas por el proveedor de nube vía IaC.
- Configurar unos parámetros del sistema relativos a visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría, garantizando de forma demostrable que la información almacenada en el sistema solo es accesible por unos perfiles y/o aplicaciones concretas.
- Configurar una retención y/o particionado y/o compactación de datos, asignando los parámetros del sistema OLAP relativos, para mantener el equilibrio entre la información disponible para análisis y el coste de almacenamiento.
- Monitorizar trabajos de carga y transformación de datos (ETL) para detectar posibles problemas que requieran la intervención del equipo de ingeniería de datos, validando que no existen errores en los archivos log del sistema y que el tiempo de ejecución no se degrada.
- Las políticas o mecanismos de replicación y copia de seguridad de los datos en el sistema OLAP se configuran, verificando que, en caso de pérdida accidental de la información, ésta se puede recuperar en una forma y tiempo concretos.
- Monitorizar activamente el rendimiento de las operaciones y el espacio de almacenamiento ocupado, mediante las herramientas proporcionadas por el proveedor de nube, para detectar potenciales problemas.

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

C1 respecto a CE1.6; C2 respecto a CE2.9; C3 respecto a CE3.8; C4 respecto a CE4.8; C5 respecto a CE5.8; C6 respecto a CE6.8 y C7 respecto a CE7.8.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Proponerse objetivos retadores que supongan un nivel de rendimiento y eficacia superior al alcanzado previamente.
Interpretar y ejecutar instrucciones de trabajo de forma precisa.
Demostrar flexibilidad para entender los cambios.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Cumplir las medidas que favorezcan el principio de igualdad de trato y de oportunidades entre hombres y mujeres.

Contenidos

Cifrado. Parámetros relativos. Proceso de creación y configuración de claves de cifrado específicas. Herramientas de proveedores de nube y/o IaC.
Visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría. Configuración y parámetros. Acceso por los perfiles y/o aplicaciones concretas.
Mantenimiento de la BBDD. Cambios de tamaño reservado, de capacidad de computación provisionada, de replicación de los datos. Modificaciones en la configuración.
Replicación y copia de seguridad de la BBDD. Herramientas proporcionadas del proveedor de nube y/o de la BBDD. Recuperación de datos en forma y tiempo concretos.
Monitorización activa de las operaciones de inserción y consulta. Herramientas del proveedor de nube y/o de la propia BBDD. Detección y resolución de potenciales problemas.

5 Gestión de los datos desde el exterior y entre sistemas de almacenamiento y bases de datos soportados por un proveedor de nube

Transferencia y sincronización de datos. Funcionalidad, latencia y seguridad.
Configuración de conexiones. Seguridad y eficiencia.
Provisionado de los dispositivos. Transferencia de datos offline. Envío del dispositivo físico entre proveedor y cliente. Seguridad y cifrado de los datos.
Visibilidad, acceso, seguridad, monitorización, observabilidad y auditoría. Configuración y parámetros. Seguridad en el acceso y zona geográfica.
Sincronización de datos unidireccional y bidireccional. Configuración y parámetros. Sincronización automática y desatendida. Garantía de requisitos de latencia.
Importación y/o exportación de datos periódicos y no periódicos. Procedimiento manual o supervisado. Monitorización del proceso. Detección y solución de problemas.

Parámetros de contexto de la formación

Espacios e instalaciones

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

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

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

MÓDULO FORMATIVO 5

Despliegue de servicios administrados en la nube

Nivel: *3*
Código: *MF2739_3*
Asociado a la UC: *UC2739_3 - Desplegar servicios administrados en la nube*
Duración (horas): *90*
Estado: *Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de despliegue de recursos en la nube de manera automática a través de plantillas de ficheros para estandarizar el aprovisionamiento mediante infraestructura como código (IaC).

CE1.1 Clasificar recursos a desplegar en la nube de manera conjunta, tales como tipo de servicios, arquitectura, configuración y proveedor donde realizar el despliegue, entre otros, determinando el estado final que se desea alcanzar, considerando el proveedor de nube en el que se realizará el despliegue.

CE1.2 Enumerar servicios de motor de despliegue de infraestructura como código y conectores en un proveedor de nube, detallando sus características para su posterior selección y configuración que permita la ejecución automática del despliegue de los recursos a aprovisionar, previa verificación de que se tienen los permisos requeridos para su aprovisionamiento.

CE1.3 Interpretar la sintaxis de los ficheros y las plantillas de automatización del despliegue en una plataforma de nube, explicando sus características.

CE1.4 Describir el proceso de creación de plantillas y ficheros, explicando cómo asignar valores a parámetros, referencias, variables de configuración y estado final de los recursos en la nube a desplegar.

CE1.5 Explicar el procedimiento de validación de unas plantillas y la sintaxis de los ficheros, describiendo cómo crear el plan de despliegue con el motor de despliegue de infraestructura como código.

CE1.6 En un supuesto práctico de aplicar técnicas de despliegue de recursos en la nube de manera automática a través de plantillas de ficheros para estandarizar el aprovisionamiento mediante infraestructura como código (IaC):

- Determinar unos recursos a desplegar en la nube de manera conjunta, tales como tipo de servicios, arquitectura, configuración y proveedor donde realizar el despliegue, entre otros, analizando el estado final que se desea alcanzar, considerando el proveedor de nube en el que se realizará el despliegue.
- Seleccionar un servicio de motor de despliegue de infraestructura como código y conectores, configurándolos para permitir la ejecución automática del despliegue de los recursos a aprovisionar en el proveedor de nube y verificando que se tienen los permisos requeridos para su aprovisionamiento.
- Crear unas plantillas y ficheros, asignando valores a parámetros, referencias, variables de configuración y estado final de los recursos en la nube a desplegar.
- Validar las plantillas y sintaxis de los ficheros se validan, creando el plan de despliegue con el motor de despliegue de infraestructura como código.

- Comparar el estado de la infraestructura actual y el estado deseado final, validando los pasos y tareas que se requieren llevar a cabo tales como creación y configuración de los recursos u otros para dejar la infraestructura en el estado solicitado.
- Ejecutar un plan de despliegue, creando y configurando los recursos en la nube de acuerdo a las plantillas y ficheros generados.
- Revisar los resultados de aprovisionamiento de los recursos en la nube, validando que el estado final de los recursos a desplegar en el proveedor de nube es el establecido de acuerdo a la información de las plantillas y ficheros.
- Documentar las plantillas y ficheros creados, incluyendo procedimientos de actualización, compartiéndolos en un repositorio de código para su reutilización.

C2: Aplicar procedimientos de despliegue de servicios de mensajería asíncrona para optimizar la transmisión y el procesamiento de los flujos de datos que se intercambian entre múltiples fuentes (publicadores) y distribuirlos a múltiples receptores (subscriptores), monitorizando los resultados.

CE2.1 Describir el proceso de habilitación de un servicio de mensajería asíncrona, detallando cómo activarlo en la consola y cómo se verifican los permisos para su aprovisionamiento.

CE2.2 Enumerar las funcionalidades de un servicio de mensajería asíncrona, explicando cómo configurar el tema -recurso al que los publicadores envían mensajes-, subscripciones para la entrega de mensajes, tipo de entrega y parámetros de reintento y eliminación de los mensajes.

CE2.3 En un supuesto práctico de aplicación de procedimientos de despliegue de servicios de mensajería asíncrona para optimizar la transmisión y el procesamiento de los flujos de datos que se intercambian entre múltiples fuentes (publicadores) y distribuirlos a múltiples receptores (subscriptores), monitorizando los resultados:
- Aprovisionar un servicio de mensajería asíncrona, habilitándolo en la consola, verificando que se tienen los permisos necesarios para su aprovisionamiento.
- Configurar un servicio de mensajería asíncrona, incluyendo el tema -recurso al que los publicadores envían mensajes-, subscripciones para la entrega de mensajes, tipo de entrega y parámetros de reintento y eliminación de los mensajes.
- Monitorizar el proceso de almacenamiento y entrega de un servicio de mensajería asíncrona, verificando que los mensajes son entregados a los suscriptores del tema.

C3: Aplicar procedimientos de despliegue de servicios de ejecución de trabajos por lotes para la ejecución de manera repetitiva de trabajos sin supervisión directa del usuario, monitorizando los resultados.

CE3.1 Describir el proceso de habilitación de un servicio de automatización de ejecución de trabajos por lotes, detallando cómo activarlo en la consola.

CE3.2 Enumerar las funcionalidades de un servicio de automatización de ejecución de trabajos por lotes, explicando cómo configurarlo con información de nombre, programación de la frecuencia de ejecución del trabajo, reintentos ante fallos, y objetivos del trabajo a ejecutar, servicio de nube a llamar o extremo HTTP, detallando el proceso de activación de la planificación de la ejecución y de verificación de que se tienen los permisos requeridos por el servicio.

CE3.3 En un supuesto práctico de aplicación de procedimientos de despliegue de servicios de ejecución de trabajos por lotes para la ejecución de manera repetitiva de trabajos sin supervisión directa del usuario, monitorizando los resultados:
- Aprovisionar un servicio de automatización de ejecución de trabajos por lotes, habilitándolo en la consola en caso necesario.

- Configurar el trabajo por lotes a automatizar, incluyendo información de nombre, programación de la frecuencia de ejecución del trabajo, reintentos ante fallos, y objetivos del trabajo a ejecutar, servicio de nube a llamar o extremo HTTP, activando la planificación de la ejecución y verificando que se tienen los permisos requeridos por el servicio.
- Monitorizar la ejecución de un trabajo automatizado, validando que el trabajo se ha ejecutado según una planificación supuesta y en los tiempos de ejecución requeridos en ella.

C4: Aplicar técnicas de aprovisionamiento de servicios de integración y despliegue continuo (CI/CD) para automatizar la compilación y despliegue de código en los entornos de ejecución, monitorizando los resultados.

CE4.1 Definir la utilidad de los servicios de integración y despliegue continuo (CI/CD) para automatizar la compilación y despliegue de código en los entornos de ejecución, explicando sus características.

CE4.2 Explicar el procedimiento para aprovisionar un servicio de CI/CD, detallando cómo incluir un repositorio de código para la compartición de versiones de código entre desarrolladores, servicio de compilación y despliegue según el lenguaje y tecnología a utilizar y para el almacenamiento de los activos de código, compiladores o imágenes de contenedores generados.

CE4.3 Describir el proceso para establecer unos entornos de ejecución, indicando cómo configurarlos de acuerdo a las estrategias y recursos de despliegue de la organización, identificando su propósito y procedimiento de actualización de las versiones a desplegar.

CE4.4 Determinar cómo se configuran unos permisos de acceso a los servicios y plantillas de trabajos de compilación, repositorios de código, activos e imágenes y entornos de ejecución, asignando las autorizaciones para permitir su acceso.

CE4.5 Interpretar parámetros de automatización de las tareas de compilación y despliegue y eventos de activación, determinando los eventos que inician tanto la ejecución, como la publicación de una nueva versión en el repositorio de código, describiendo como definir, en su caso, una planificación de ejecución en periodos de tiempo.

CE4.6 En un supuesto práctico de aplicación de técnicas de aprovisionamiento de servicios de integración y despliegue continuo (CI/CD) para automatizar la compilación y despliegue de código en los entornos de ejecución, monitorizando los resultados:
- Aprovisionar un servicio de CI/CD, incluyendo repositorio de código para la compartición de versiones de código entre los desarrolladores, servicio de compilación y despliegue según el lenguaje y tecnología a utilizar y para el almacenamiento de los activos de código, compiladores o imágenes de contenedores generados.
- Establecer unos entornos de ejecución, configurándolos de acuerdo a unas estrategias y recursos de despliegue, identificando su propósito y procedimiento de actualización de las versiones.
- Configurar unos permisos de acceso a los servicios y plantillas de trabajos de compilación, repositorios de código, activos e imágenes y entornos de ejecución, asignando las autorizaciones para permitir su acceso.
- Configurar unos parámetros de automatización de las tareas de compilación y despliegue y eventos de activación, bien especificando los eventos que inician la ejecución como la publicación de una nueva versión en el repositorio de código o bien definiendo una planificación de ejecución en periodos de tiempo.
- Monitorizar la ejecución y los "logs", revisando los trabajos que no hayan finalizado con éxito para determinar los motivos.

C5: Aplicar procedimientos de despliegue de soluciones de terceros, seleccionándolas desde el "marketplace" para automatizar el despliegue de paquetes de "software".

CE5.1 Enumerar catálogos de soluciones del "marketplace", interpretando las especificaciones de despliegue, costes estimados o manuales de fabricantes, licenciamiento y los requisitos recogidos en la documentación técnica de las soluciones.

CE5.2 Interpretar parámetros de configuración de un catálogo, tales como nombre, zona y red dónde se realizará el despliegue, claves de autenticación, parámetros de capacidad de cómputo y almacenamiento según las necesidades de uso, explicando cómo asignar permisos para el aprovisionamiento de los servicios a utilizar.

CE5.3 Describir el procedimiento para el despliegue automático de la solución desde el catálogo, monitorizando los pasos de despliegue.

CE5.4 Explicar el proceso de verificación de la instalación y configuración de la solución desplegada, mediante la ejecución de una serie de pruebas como la revisión de "logs" de despliegue, acceso a recursos y test de funcionamiento de la solución.

CE5.5 En un supuesto práctico de aplicar procedimientos de despliegue de soluciones de terceros, seleccionándolas desde el "marketplace" para automatizar el despliegue de paquetes de "software":

- Revisar un catálogo de soluciones del "marketplace", interpretando las especificaciones de despliegue, costes estimados o manuales de fabricantes, licenciamiento y los requisitos recogidos en la documentación técnica de las soluciones.
- Seleccionar una solución a desplegar del catálogo, configurando los parámetros tales como nombre, zona y red dónde se realizará el despliegue, claves de autenticación, parámetros de capacidad de cómputo y almacenamiento según las necesidades de uso, y asignando permisos para el aprovisionamiento de los servicios a utilizar.
- Solicitar desde el catálogo el despliegue automático de la solución, monitorizando los pasos de despliegue.
- Verificar la instalación y configuración de la solución desplegada, mediante la ejecución de una serie de pruebas como la revisión de "logs" de despliegue, acceso a recursos y test de funcionamiento de la solución.
- Documentar los procedimientos de operación y mantenimiento de la solución, incluyendo tareas de monitorización, revisión de "logs", actualización de nuevas versiones, y borrado.
- Comprobar los datos finales de configuración de la solución, ubicación, las URL de acceso, operación y seguridad, verificando que quedan documentados en la plataforma.

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

C1 respecto a CE1.6; C2 respecto a CE2.3; C3 respecto a CE3.3; C4 respecto a CE4.6 y C5 respecto a CE5.5.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Proponerse objetivos retadores que supongan un nivel de rendimiento y eficacia superior al alcanzado previamente.
Interpretar y ejecutar instrucciones de trabajo de forma precisa.
Demostrar flexibilidad para entender los cambios.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.

Cumplir las medidas que favorezcan el principio de igualdad de trato y de oportunidades entre hombres y mujeres.

Contenidos

1 Despliegue automático de recursos en la nube mediante infraestructura como código (IaC)

Clasificación de recursos a desplegar en la nube de manera conjunta: tipo de servicios, arquitectura, configuración y proveedor donde realizar el despliegue.
Servicios de motor de despliegue de infraestructura como código (IaC). Conectores en proveedores de nube. Permisos requeridos para su aprovisionamiento.
Ficheros y las plantillas de automatización del despliegue en una plataforma de nube. Sintaxis.
Creación de plantillas y ficheros. Parámetros, referencias y variables de configuración. Validación. Plan de despliegue.

2 Despliegue de servicios de mensajería asíncrona de nube y ejecución de trabajos por lotes

Servicios de mensajería asíncrona de nube. Habilitación y activación en la consola. Permisos para su aprovisionamiento.
Funcionalidades de los servicios de mensajería asíncrona en la nube. Configuración, suscripciones y monitorización.
Servicios de automatización de ejecución de trabajos por lotes. Habilitación y activación en la consola.
Funcionalidades de los servicios de automatización de ejecución de trabajos por lotes. Configuración, activación de la planificación de la ejecución y verificación de permisos.

3 Despliegue de servicios de ejecución de trabajos por lotes

Servicios de automatización de ejecución de trabajos por lotes. Habilitación y activación en la consola.
Funcionalidades de los servicios de automatización de ejecución de trabajos por lotes. Configuración, activación de la planificación de la ejecución y verificación de premisos.

3 Aprovisionamiento de servicios de integración y despliegue continuo (CI/CD) en la nube

Servicios de integración y despliegue continuo (CI/CD). Automatización de la compilación y despliegue de código en entornos de ejecución.
Aprovisionamiento del servicio de CI/CD. Repositorios de código.
Establecimiento de entornos de ejecución.
Permisos de acceso a los servicios y plantillas de trabajos de compilación, repositorios de código, activos e imágenes y entornos de ejecución.
Parámetros de automatización de las tareas de compilación y despliegue y eventos de activación. Planificación de ejecución en periodos de tiempo.

4 Despliegue de soluciones de terceros, seleccionándolas desde el "marketplace" para automatizar el despliegue de paquetes de "software".

Catálogos de soluciones del "marketplace". Especificaciones de despliegue y costes estimados. Licenciamiento y requisitos.
Configuración del catálogo. Parámetros: nombre, zona y red dónde se realizará el despliegue, claves de autenticación, parámetros de capacidad de cómputo y almacenamiento. Permisos.

Despliegue automático de la solución desde el catálogo. Monitorización del despliegue.
Verificación de la instalación y configuración de la solución desplegada. Pruebas y revisión de "logs".

Parámetros de contexto de la formación

Espacios e instalaciones

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

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

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

MÓDULO FORMATIVO 6

Automatización de despliegues en la nube

Nivel: *3*
Código: *MF2740_3*
Asociado a la UC: *UC2740_3 - Automatizar despliegues en la nube*
Duración (horas): *120*
Estado: *Tramitación BOE*

Capacidades y criterios de evaluación

C1: Aplicar procedimientos de gestión de repositorios de código fuente del software y de servicios asociados a las aplicaciones de sistemas, organizando los orígenes del código fuente, ajustando los parámetros de autenticación y validando las modificaciones y las dependencias del código fuente, para facilitar su mantenimiento, recuperación y permitir la trazabilidad del sistema.

CE1.1 Clasificar los orígenes del código fuente, explicando los procedimientos para organizarlos y permitir su uso consistente.

CE1.2 Describir parámetros del sistema que afectan a la autenticación y autorización, explicando cómo se ajustan a las necesidades de acceso, integración con herramientas y seguridad.

CE1.3 Explicar el proceso de validación de modificaciones sobre el código fuente, aplicando guías de desarrollo, flujos de trabajo y políticas tales como aprobación, asignación o revisión, entre otras.

CE1.4 Describir técnicas de medición de parámetros de calidad sobre el código fuente asociado a los sistemas explicando los pasos a seguir para aplicar unos estándares de calidad y ejecutar acciones correctivas.

CE1.5 Explicar los procesos de copia de seguridad y recuperación del código fuente, describiendo los pasos para su configuración, gestión y uso de repositorios de gran tamaño.

CE1.6 Detallar los procesos de validación de dependencias externas de paquetes, librerías o integraciones, explicando los mecanismos de configuración para garantizar la seguridad, soportabilidad, rendimiento, y publicación.

CE1.7 En un supuesto práctico de aplicación de procedimientos de gestión de repositorios de código fuente del software y de servicios asociados a las aplicaciones de sistemas, organizando los orígenes del código fuente, ajustando los parámetros de autenticación y validando las modificaciones y las dependencias del código fuente, para facilitar su mantenimiento, recuperación y permitir la trazabilidad del sistema:

- Organizar unos orígenes de código fuente con una estructura que permita su uso de forma consistente.
- Ajustar parámetros del sistema que afecten a la autenticación y autorización según unas necesidades de acceso e integración con herramientas y seguridad.
- Validar unas modificaciones sobre el código fuente, siguiendo unas guías de desarrollo y flujos de trabajo y políticas tales como aprobación, asignación o revisión, entre otras.
- Medir unos parámetros de calidad definidos sobre el código fuente asociado a los sistemas, aplicando unos estándares de calidad y ejecutando acciones correctivas.

- Ejecutar un proceso de copia de seguridad y recuperación del código fuente, programando su activación de forma periódica, siguiendo el resultado un proceso de validación donde se consideren las actuaciones necesarias para su optimización y la gestión de repositorios de gran tamaño.
- Validar dependencias externas de paquetes, librerías o integraciones, siguiendo unas líneas prácticas en los ámbitos de seguridad, soportabilidad, rendimiento, y publicación.

C2: Aplicar procedimientos de modificación de código fuente de despliegue y plantillas responsables de la creación de los servicios en la nube, en condiciones de operación, calidad y seguridad para simplificar la operación y el despliegue.

CE2.1 Describir herramientas y plataformas de nube tales como como plantillas declarativas del servicio o hardware, línea de comandos (CLI), API ("Application Programming Interface"), automatismos mediante lenguajes de programación, entre otras, explicando el proceso de creación de servicios aplicables.

CE2.2 Explicar los procedimientos para definir parámetros de automatismo del ciclo de vida de los servicios en la nube, considerando:
- Características propias del despliegue de las versiones de los datos de las aplicaciones, tales como creación de bases de datos, movimiento o transformación de la información y metadatos, entre otras.
- Características propias del despliegue de las versiones del software, tales como la gestión de la configuración de las aplicaciones, entre otras.

CE2.3 Explicar los procedimientos para definir parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube, considerando:
- Características propias del despliegue de las versiones del código fuente de las aplicaciones, tales como contenedores, máquinas virtuales, scripts, código binario, entre otros.
- Elementos que permitan su reutilización en otros despliegues, tales como nombre del servicio, región geográfica, recursos asignados, permisos, confirmando que son únicos en los casos necesarios.

CE2.4 Detallar procedimientos de verificación del código fuente de despliegue, plantillas declarativas del servicio o cualquier proceso responsable del despliegue, explicando mecanismos para comprobar que sea idempotente, su ejecución robusta y que proporciona predictibilidad bajo distintas circunstancias.

CE2.5 En un supuesto práctico de aplicación de procedimientos de modificación de código fuente de despliegue y plantillas responsables de la creación de los servicios en la nube, en condiciones de operación, calidad y seguridad para simplificar la operación y el despliegue:
- Crear unos servicios de forma automatizada, modificándolos, si fuera necesario, empleando las capacidades de las herramientas y plataformas de nube seleccionadas como plantillas declarativas del servicio o hardware, línea de comandos (CLI), API, automatismos mediante lenguajes de programación, entre otras.
- Definir parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube, considerando características propias del despliegue de las versiones de los datos de las aplicaciones, tales como creación de bases de datos, movimiento o transformación de la información y metadatos, entre otras.
- Definir parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube, considerando características propias del despliegue de las versiones del software, tales como la gestión de la configuración de las aplicaciones, entre otras.
- Definir parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube, considerando características propias del despliegue de las versiones del código fuente de

las aplicaciones, tales como contenedores, máquinas virtuales, scripts, código binario, entre otros.
- Definir parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube, considerando elementos que permitan su reutilización en distintos despliegues, tales como nombre del servicio, región geográfica, recursos asignados, permisos, confirmando que son únicos en los casos necesarios.
- Verificar el código fuente de despliegue, plantillas declarativas del servicio o cualquier proceso responsable del despliegue, comprobando que sea idempotente, su ejecución robusta y proporcionando predictibilidad bajo distintas circunstancias.

C3: Aplicar técnicas de configuración de servicios de comunicación y colaboración en función de las necesidades de uso, para automatizar las interacciones con los repositorios de código fuente y las herramientas de gestión de proyectos.

CE3.1 Clasificar plataformas de comunicación y herramientas de gestión de proyectos, describiendo el procedimiento para su configuración con los repositorios de código fuente que permitan la recepción automática de cambios de estado y contenido.

CE3.2 Explicar criterios de seguridad y disponibilidad para determinar plataformas de comunicación empleadas en la organización se determinan, de modo que se pueda enviar notificaciones.

CE3.3 Identificar tipos de notificaciones por métricas, alertas o reglas definidas en los repositorios de código fuente, estados de tareas, peticiones de cambios al sistema, entre otras, explicando los mecanismos para su configuración.

CE3.4 Explicar los procesos de configuración de plataformas de comunicación, documentación y herramientas de gestión de proyectos, detallando los pasos para conectar con los repositorios de código fuente, de tal modo que permitan la asignación de elementos de ambos sistemas de forma bidireccional, tales como la modificación de código fuente a tarea, resolución de errores ("bugs") a modificación de código fuente, entre otras.

CE3.5 En un supuesto práctico de aplicación de técnicas de configuración de servicios de comunicación y colaboración en función de las necesidades de uso, para automatizar las interacciones con los repositorios de código fuente y las herramientas de gestión de proyectos:
- Emplear unas plataformas de comunicación y herramientas de gestión de proyectos, siguiendo la configuración con los repositorios de código fuente que permitan la recepción automática de cambios de estado y contenido.
- Determinar unas plataformas de comunicación, según criterios de seguridad y disponibilidad, para notificar a los responsables de los sistemas afectados por métricas, alertas o reglas definidas en los repositorios de código fuente, estados de tareas, peticiones de cambios al sistema, entre otras.
- Configurar las plataformas de comunicación, documentación y herramientas de gestión de proyectos empleadas, conectándolas con los repositorios de código fuente, de tal modo que permitan la asignación de elementos de ambos sistemas de forma bidireccional, tales como la modificación de código fuente a tarea, resolución de errores ("bugs") a modificación de código fuente, entre otras.

C4: Aplicar procedimientos de gestión de procesos de integración y despliegue continuo (IC/DC) para configurar e implantar las versiones de las aplicaciones desarrolladas, en condiciones de operación, calidad y seguridad.

CE4.1 Describir estrategias de prueba de diagnóstico con herramientas integradas, explicando los pasos a seguir para proporcionar información sobre resultados y acciones relativas a fallos.

CE4.2 Explicar técnicas de resolución de fallos de ejecución, calidad, seguridad y rendimiento de las aplicaciones del sistema, mediante automatización y empleando estrategias de prueba.

CE4.3 Explicar procedimientos de instalación y configuración de herramientas de gestión de paquetes y dependencias, parametrizando la actualización, garantizando el versionado y priorización según indique el fabricante de la herramienta y describiendo la documentación del proceso.

CE4.4 Detallar los parámetros del sistema que afectan a la integración con dependencias externas en el proceso de compilación del código fuente, explicando el proceso para ajustarlos a políticas de calidad, seguridad y rendimiento tales como cobertura de código, pruebas de software, análisis de seguridad, dependencias de librerías, entre otras.

CE4.5 Explicar el proceso de mantenimiento de herramientas para la administración de la configuración del software y servicios de los sistemas, detallando los pasos para aplicar la configuración deseada de forma automática.

CE4.6 Describir el procedimiento de configuración de servicios responsables de la ejecución de procesos y/o compilación del software y servicios necesarios para las aplicaciones de la organización, explicando los pasos para garantizar su disposición de uso para evitar problemas en su ejecución y mantenerlos monitorizados para uso óptimo en seguridad, rendimiento y capacidad, como por ejemplo análisis de errores, accesos, duración, rendimiento, capacidad en compilación, entre otros.

CE4.7 Explicar el proceso de ajuste de parámetros de los servicios responsables de la ejecución de procesos y despliegue del software y servicios en lo que respecta a la orquestación de flujos de aprobación, seguridad, auditoría, automatización, priorización de despliegues o correcciones críticas y configuraciones del software asociado, detallando los pasos a seguir y criterios a aplicar.

CE4.8 Explicar el proceso de ajuste de parámetros de los servicios responsables de la ejecución de procesos y despliegue del software y servicios, de modo que se sigan unas características no-funcionales definidas para el tiempo de pérdida de servicio de las aplicaciones, tales como "Blue/green", "canary", "ring", balanceo de carga ("traffic-splitting deployment"), despliegue incremental, entre otras.

CE4.9 En un supuesto práctico de aplicación de procedimientos de gestión de procesos de integración y despliegue continuo (IC/DC) para configurar e implantar las versiones de las aplicaciones desarrolladas, en condiciones de operación, calidad y seguridad:

- Resolver fallos de ejecución, calidad, seguridad y rendimiento de las aplicaciones del sistema se mediante automatización, empleando unas estrategias de pruebas e incluyendo las pruebas de diagnóstico con las herramientas integradas, proporcionando información sobre resultados y acciones a los fallos diagnosticados.
- Instalar unas herramientas de gestión de paquetes y dependencias, configurándolas y actualizándolas, siguiendo unas directrices de versionado, priorización y la documentación del fabricante de la herramienta.
- Ajustar parámetros del sistema que afectan a la integración con dependencias externas en el proceso de compilación del código fuente, garantizando la calidad, seguridad y rendimiento tales como cobertura de código, pruebas de software, análisis de seguridad, dependencias de librerías, entre otras.
- Mantener las herramientas para la administración de la configuración del software y servicios de los sistemas desarrollados, siguiendo la configuración para cada una de las aplicaciones de forma automática.
- Configurar unos servicios responsables de la ejecución de procesos y/o compilación del software y servicios, garantizando su disposición de uso para evitar problemas en su ejecución, manteniéndolos monitorizados para uso óptimo en seguridad, rendimiento y capacidad, como

por ejemplo análisis de errores, accesos, duración, rendimiento, capacidad en compilación, entre otros.
- Ajustar parámetros de los servicios responsables de la ejecución de procesos y despliegue del software y servicios, según necesidades en lo que respecta a la orquestación de flujos de aprobación, seguridad, auditoría, automatización, priorización de despliegues o correcciones críticas y configuraciones del software asociado.
- Configurar parámetros de servicios responsables de la ejecución de procesos y despliegue del software y servicios, siguiendo unas características no-funcionales definidas para el tiempo de pérdida de servicio de las aplicaciones establecidas en una estrategia de despliegue, tales como "Blue/green", "canary", "ring", balanceo de carga ("traffic-splitting deployment"), despliegue incremental, entre otras.

C5: Aplicar procedimientos de configuración de mecanismos de automatización para el despliegue de código fuente de software y servicios, garantizando la monitorización, registro de las aplicaciones, recuperación, crecimiento y aplicando criterios de optimización de costes.

CE5.1 Explicar servicios responsables de la gestión de la configuración y/u orquestación de la infraestructura, describiéndolos.

CE5.2 Describir estándares y políticas de monitorización, recuperación, crecimiento y operación entre otras para automatizar servicios responsables de la gestión de la configuración y/u orquestación de la infraestructura.

CE5.3 Explicar procedimientos para ejecutar mecanismos de despliegue desarrollados, siguiendo validaciones del código fuente y los servicios desplegados automática o manualmente y cumpliendo unas políticas de registro de aplicaciones, gobierno, seguridad, pruebas y monitorización.

CE5.4 Detallar procedimientos de configuración de mecanismos de despliegue, incorporando acciones automáticas en base a eventos o registros producidos por las aplicaciones y los servicios, permitiendo recuperar estados previos a situaciones de fallo o pérdida de servicio.

CE5.5 Explicar procedimientos para configurar mecanismos de despliegue, de modo que incorporen acciones automáticas en base a eventos o registros producidos por las aplicaciones, usuarios y los servicios, permitiendo reducir el coste y manteniendo las políticas de la organización del servicio tales como su disponibilidad, escalabilidad, rendimiento y recuperación entre otras.

CE5.6 En un supuesto práctico de aplicación de procedimientos de configuración de mecanismos de automatización para el despliegue de código fuente de software y servicios, garantizando la monitorización, registro de las aplicaciones, recuperación, crecimiento y aplicando criterios de optimización de costes:
- Automatizar unos servicios responsables de la gestión de la configuración y/u orquestación de la infraestructura siguiendo unos estándares y políticas de monitorización, recuperación, crecimiento y operación entre otras.
- Ejecutar mecanismos de despliegue desarrollados, siguiendo validaciones del código fuente y los servicios desplegados automática o manualmente y cumpliendo con unas políticas de registro de aplicaciones, gobierno, seguridad, pruebas y monitorización definidas.
- Configurar mecanismos de despliegue, incorporando acciones automáticas en base a eventos o registros producidos por las aplicaciones y los servicios, permitiendo recuperar estados previos a situaciones de fallo o pérdida de servicio.
- Configurar mecanismos de despliegue se configuran, incorporando acciones automáticas en base a eventos o registros producidos por las aplicaciones, usuarios y los servicios, permitiendo

reducir el coste y manteniendo unas políticas de servicio tales como su disponibilidad, escalabilidad, rendimiento y recuperación entre otras.

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

C1 respecto a CE1.7; C2 respecto a CE2.5; C3 respecto a CE3.5; C4 respecto a CE4.9 y C5 respecto a CE5.6.

Otras Capacidades:

Finalizar el trabajo atendiendo a criterios de idoneidad, rapidez, economía y eficacia.
Proponerse objetivos retadores que supongan un nivel de rendimiento y eficacia superior al alcanzado previamente.
Interpretar y ejecutar instrucciones de trabajo de forma precisa.
Demostrar flexibilidad para entender los cambios.
Mostrar una actitud de respeto hacia los compañeros, procedimientos y normas de la empresa.
Cumplir las medidas que favorezcan el principio de igualdad de trato y de oportunidades entre hombres y mujeres.

Contenidos

1 Gestión de repositorios de código fuente del software y de servicios

Orígenes del código fuente. Procedimientos de organización y uso consistente.
Autenticación y autorización: parámetros. Procedimientos de ajuste a las necesidades de acceso. Integración con herramientas y seguridad.
Proceso de validación de modificaciones sobre el código fuente. Guías de desarrollo, flujos de trabajo. Políticas: aprobación, asignación o revisión, entre otras.
Técnicas de medición de parámetros de calidad sobre el código fuente asociado. Estándares de calidad. Procedimiento de aplicación de acciones correctivas.
Procesos de copia de seguridad y recuperación del código fuente. Configuración, gestión y uso de repositorios de gran tamaño.
Procesos de validación de dependencias externas de paquetes, librerías o integraciones. Mecanismos de configuración para garantizar la seguridad, soportabilidad, rendimiento, y publicación.

2 Modificación de código fuente de despliegue y plantillas responsables de la creación de los servicios en la nube

Herramientas y plataformas de nube. Plantillas declarativas del servicio o hardware, línea de comandos (CLI), API, automatismos mediante lenguajes de programación, entre otras. Proceso de creación de servicios aplicables.
Procedimientos para definir parámetros de automatismo del ciclo de vida de los servicios en la nube. Características del despliegue de las versiones de los datos. Características del despliegue de las versiones del software. Gestión de la configuración.
Procedimientos para definir parámetros de los artefactos para el automatismo del ciclo de vida de los servicios en la nube. Características propias del despliegue de las versiones del código fuente de las aplicaciones: contenedores, máquinas virtuales, scripts, código binario, entre otros. Reutilización en otros despliegues.

3 Servicios de comunicación y colaboración

Plataformas de comunicación y herramientas de gestión de proyectos. Clasificación. criterios de seguridad y disponibilidad. Procedimientos de configuración con los repositorios de código fuente.
Tipos de notificaciones por métricas, alertas o reglas definidas en los repositorios de código fuente, estados de tareas, peticiones de cambios al sistema, entre otras. Mecanismos para su configuración.
Procesos de configuración de plataformas de comunicación, documentación y herramientas de gestión de proyectos. Conexión con los repositorios de código fuente.

4 Gestión de procesos de integración y despliegue continuo (IC/DC)

Estrategias de prueba de diagnóstico con herramientas integradas. Acciones relativas a fallos.
Técnicas de resolución de fallos de ejecución, calidad, seguridad y rendimiento de las aplicaciones del sistema. Automatización y estrategias de prueba.
Procedimientos de instalación y configuración de herramientas de gestión de paquetes y dependencias. Actualización y versionado.
Integración con dependencias externas en el proceso de compilación del código fuente. Parámetros. Garantía de calidad, seguridad y rendimiento.
Mantenimiento de herramientas para la administración de la configuración del software y servicios de los sistemas. Aplicación automática de la configuración.
Procedimiento de configuración de servicios. Servicios responsables de la ejecución de procesos y/o compilación del software. Servicios necesarios para las aplicaciones de la organización. Garantía de disposición de uso. Monitorización.
Proceso de ajuste de parámetros de los servicios responsables de la ejecución de procesos y despliegue del software en lo que respecta a la orquestación de flujos de aprobación, seguridad, auditoría, automatización, priorización de despliegues o correcciones críticas. Configuraciones del software asociado.
Proceso de ajuste de parámetros de los servicios responsables de la ejecución de procesos y despliegue del software y servicios. Características no-funcionales para el tiempo de pérdida de servicio de las aplicaciones: "Blue/green", "canary", "ring", balanceo de carga ("traffic-splitting deployment"), despliegue incremental, entre otras.

5 Mecanismos de automatización para el despliegue de código fuente de software y servicios

Servicios responsables de la gestión de la configuración y/u orquestación de la infraestructura. Estándares y políticas de monitorización, recuperación, crecimiento y operación para su automatización.
Procedimientos para ejecutar mecanismos de despliegue. Validaciones del código fuente y los servicios desplegados automática o manual. Políticas de registro de aplicaciones, gobierno, seguridad, pruebas y monitorización.
Mecanismos de despliegue. Acciones automáticas en base a eventos o registros producidos por las aplicaciones y los servicios. Recuperación de estados previos a situaciones de fallo o pérdida de servicio. Acciones automáticas en base a eventos o registros producidos por las aplicaciones, usuarios y los servicios. Reducción de coste. Mantenimiento de políticas de la organización del servicio: disponibilidad, escalabilidad, rendimiento y recuperación entre otras.

Parámetros de contexto de la formación

Espacios e instalaciones

Los talleres e instalaciones darán respuesta a las necesidades formativas de acuerdo con el contexto profesional establecido en la unidad de competencia asociada, teniendo en cuenta la normativa

aplicable del sector productivo, prevención de riesgos laborales, accesibilidad universal, igualdad de género y protección medioambiental. Se considerará con carácter orientativo como espacios de uso:

- Instalación de 2 m² por alumno o alumna.

Perfil profesional del formador o formadora:

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