

Estándar de competencias profesionales

Preparar el entorno de despliegue en contenedores

Familia Profesional	Informática y Comunicaciones
Nivel	3
Código	ECP2743_3
Estado	BOE
Publicación	RD 546/2023

Competencia profesional

Elementos de la competencia

EC1 Crear el acceso a los repositorios de código de infraestructura y/o servicios, o en su caso, solicitar la creación del mismo, verificando la conexión, comprobando las herramientas de gestión y validación, para su uso en el desarrollo y despliegue, siguiendo procedimientos, estándares y políticas de seguridad definidas por la entidad responsable del desarrollo, para facilitar a los usuarios y/o grupos de gestión el uso de los repositorios de código de infraestructura y/o servicios en las fases de desarrollo y despliegue.

IC1.1 El acceso a los recursos y herramientas para desplegar y/o gestionar los entornos de producción definidos en la arquitectura del proyecto se solicita al departamento o persona responsable del mismo, usando los canales de comunicación acordados entre desarrolladores y responsables de sistemas, o bien se verifica o bien se crea en su caso, para tener control de acceso y mantener el registro de acceso.

IC1.2 Los accesos al código fuente se configuran para ser gestionados a través de las herramientas proporcionadas por la entidad responsable del desarrollo, parametrizando la seguridad y las políticas de acceso, a través de los usuarios y/o grupos asignados.

IC1.3 Las herramientas de validación de calidad y seguridad del código, y dependencias de librerías externas o integraciones se verifican, previa instalación en su caso, comprobando su funcionalidad para ser usadas por los usuarios y/o grupos de gestión.

EC2 Validar la calidad y seguridad de las modificaciones previas al despliegue, usando las herramientas de gestión y validación y siguiendo procedimientos, estándares y políticas de seguridad definidas por la entidad responsable del desarrollo.

IC2.1 Las modificaciones del código fuente se validan, ejecutando pruebas de calidad mediante herramientas específicas, documentándolas con las guías de desarrollo y los flujos de trabajo y/o políticas definidas por la entidad responsable del desarrollo.

IC2.2 Las comprobaciones de parámetros de seguridad del código definidos en los estándares de la entidad responsable del desarrollo, se ejecutan mediante herramientas específicas, de forma periódica según el método definido por la propia entidad, para garantizar su buena praxis.

IC2.3 Las dependencias del código de librerías externas o integraciones se validan, mediante herramientas de comprobación, para verificar la seguridad y funcionalidad e integración con el resto de componentes del aplicativo antes del despliegue.

EC3 Crear o, en su caso, configurar entornos de revisión y/o producción, mediante ficheros de parámetros y creando flujos de trabajo, siguiendo procedimientos, estándares y políticas de seguridad definidas por la entidad responsable del desarrollo para validar el despliegue.

IC3.1 Los ficheros de definición de infraestructura como código y SDH ("Software Define Hardware") se crean, usando el lenguaje propio de la plataforma de despliegue proporcionada por la entidad responsable del desarrollo, previa identificación de los entornos de despliegue del código, artefactos e imágenes de contenedores.

IC3.2 Los flujos de trabajo para el despliegue del entorno "hardware" se crean, usando las credenciales proporcionadas, aplicando las configuraciones definidas, para crear el entorno de desarrollo o producción.

IC3.3 Las definiciones técnicas de uso de control y de seguridad se configuran para cada entorno, especificando:

- Roles de acceso del usuario.
- Roles de acceso del código.
- Acceso al almacenamiento.
- Acceso a las API ("Application Programming Interface"), entre otros recursos, siguiendo las indicaciones de la entidad responsable del desarrollo para su posterior gestión.

IC3.4 La infraestructura definida en los ficheros al efecto se crea dentro de la plataforma proporcionada por la entidad responsable del desarrollo, usando las credenciales facilitadas, para su posterior integración en los flujos de trabajo.

IC3.5 La infraestructura creada se verifica después del despliegue, comprobando que se obtiene acceso a todos los recursos de infraestructura.

EC4 Instalar en su caso el "software" de automatización y gestión de paquetes y dependencias, y de administración de la configuración del "software", creando flujos de mantenimiento y despliegue sobre las plataformas seleccionadas por la entidad responsable del desarrollo, configurando los parámetros de uso para preparar la automatización del despliegue.

IC4.1 Las herramientas de automatización y gestión de paquetes y dependencias se instalan en la infraestructura seleccionada, actualizándolas según las directrices de versión y documentación del fabricante.

IC4.2 Los flujos para mantenimiento se crean, usando las herramientas para la automatización de la administración de la configuración del "software" y servicios de los sistemas desarrollados.

IC4.3 Los flujos para mantenimiento se verifican, probando que las acciones automatizadas generan los resultados esperados según la documentación del proyecto.

EC5 Definir las variables de trabajo, configurándolas dentro de cada entorno para ser usadas por los contenedores que tienen el código y que se crean de forma dinámica y para ejecutar la aplicación.

IC5.1 Las reglas de seguridad, niveles de servicio y consumo definidas en el proyecto, se aplican como configuraciones dentro de las herramientas de despliegue, para parametrizar la ejecución de los contenedores.

IC5.2 Las métricas para elaborar informes de rendimiento y planificación ("capacity plan"), anticipar el crecimiento y facilitar la gestión de los recursos que requieren las herramientas se recogen, incluyéndolas en las herramientas de monitorización.

IC5.3 La documentación sobre el uso de los despliegues de código e imágenes de contenedores se redacta, para facilitar la reutilización de los componentes ya preparados, almacenándola en los repositorios de código para servir como guía o modelo para posteriores desarrollos y despliegues.

IC5.4 Las acciones automáticas basadas en eventos disparados por errores tales como:

- Fallos de trabajo en los flujos.
- Disponibilidad de componentes de integración.
- Fallos de acceso.
- Estado de finalización.

IC5.4 Entre otros, se incorporan en las herramientas desplegadas, para ajustar el rendimiento y mantener los recursos utilizados en niveles óptimos.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Conexión a la red. Equipamiento informático: equipos, componentes, periféricos, cableado, entre otros. Sistemas operativos. Navegadores. Lenguajes de "scripting". Lenguajes estructurados para automatizaciones. Lenguajes declarativos. Utilidades y aplicaciones incorporadas a los sistemas operativos. Herramientas de comunicación y colaboración en equipo. Sistemas gestores de repositorios de código fuente. Servicios de transferencia de ficheros y conexión remota. Herramientas de gestión y control de cambios, incidencias y configuración. Repositorio de artefactos/imágenes. Servidor de despliegues. Servidores de infraestructura. Sistema de monitorización. Sistema de orquestación de contenedores.

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; diseño y especificaciones de los servicios a desplegar y operar; plan de seguridad, operación y calidad; acuerdos de nivel de servicio -SLA-; documentación de configuración de sistemas y servicios; plan de pruebas e informe de fallos; especificaciones de la arquitectura de referencia de servicio corporativo; documentación asociada a los scripts desarrollados; documentación de las pruebas de funcionamiento de los servicios y aplicaciones desarrolladas). Documentación técnica (documentación técnica asociada a servicios informáticos; manuales de funcionamiento de las herramientas de gestión del ciclo de vida del "software", bases de datos de vulnerabilidades).