Estándar de competencias profesionales

Mantener el sistema de contenedores desplegado

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP2747_3**
Estado	**BOE**
Publicación	**RD 546/2023**

Competencia profesional

Elementos de la competencia

EC1 Integrar la conectividad a través de la red de datos entre el contenedor y los sistemas de monitorización y alarmas asociados, asegurando el flujo de información, cumpliendo las especificaciones y criterios de seguridad para permitir su interconexión.

IC1.1 La integración del contenedor con el sistema de monitorización se verifica, probando las comunicaciones y comprobando la integridad de los datos enviados y recibidos y que dichos datos son almacenados en el sistema remoto.

IC1.2 Los umbrales de los contadores y las cadenas de texto requeridas en los eventos se configuran, especificando valores recogidos en la documentación para generar diferentes tipos de indicadores.

IC1.3 Las reglas de agregado y correlación de contadores se configuran, aplicando la parametrización que figura en la documentación del proyecto, para crear nuevos indicadores.

IC1.4 Los eventos generados en el contenedor se integran en el sistema de gestión de alarmas comprobando su activación y/o recuperación, probando las comunicaciones y verificando que se almacenan en el sistema remoto para su gestión.

IC1.5 Los eventos recibidos en el sistema de gestión de alarmas se categorizan, agrupándolos usando parámetros tales como fecha de creación, origen, criticidad, entre otros, para la posterior notificación y tratamiento de la alarma.

IC1.6 Las comunicaciones entre el contenedor y los sistemas de monitorización y alarmas se auditan, verificando que sólo los protocolos y puertos requeridos para dicha comunicación están habilitados.

IC1.7 Las reglas de protección y seguridad entre el contenedor y el entorno de monitorización y alarmas se configuran, comprobando que no es posible otra comunicación distinta en dicho canal de comunicaciones.

EC2 Validar el sistema desplegado, comprobando su estado, indicadores y el rendimiento esperado, según especificaciones para monitorizar su funcionalidad y calidad de servicio.

IC2.1 Las métricas proporcionadas por la aplicación se documentan, explicando cada contador y su referencia asociada, verificando que se incluyen tanto indicadores de capacidad como de rendimiento y calidad.

IC2.2 Los indicadores se implementan, realizando las fórmulas y cálculos sobre los contadores proporcionados por el sistema, especificando los umbrales para cada tipo de indicador, documentando los valores máximos, mínimo y recomendado por el sistema.

IC2.3 Las posibles alarmas generadas por el sistema se documentan, indicando el origen, posible fallo e impacto en servicio derivado de cada alarma, adjuntando las guías para su manejo, indicando los pasos a seguir para el análisis y resolución de las mismas.

IC2.4 Las pruebas del aplicativo o componente se ejecutan, incluyendo pruebas funcionales, de aseguramiento de calidad del servicio, rendimiento y seguridad de la aplicación y de estrés, verificando que todos los parámetros están dentro de los umbrales marcados por las especificaciones.

IC2.5 Las pruebas ejecutadas se documentan, almacenando los resultados y evidencias de ejecución de cada caso, junto con los indicadores y archivos de registro.

IC2.6 Los indicadores y su evolución se monitorizan usando el sistema de monitorización, revisándolas periódicamente, comprobando que el rendimiento de la aplicación no se excede de los umbrales marcados y sus indicadores funcionan acorde con la carga de trabajo requerida a la aplicación.

EC3 Extraer datos e información, ejecutándolo manualmente o previa programación del proceso en su caso, para el control y toma de decisiones.

IC3.1 Los archivos de registro de la aplicación se observan periódicamente, chequeando que no existen errores internos derivados de algún posible fallo "software", salida inesperada de la aplicación o reinicio y reportando dichos fallos en caso de ocurrir.

IC3.2 Los accesos al sistema se monitorizan, detectando intentos con contraseña equivocada y alertando de conexiones por fuerza bruta, bloqueando los no permitidos para proteger la integridad de la aplicación.

IC3.3 Los datos generados por fallos o reinicios de la aplicación tales como volcados de memoria ("crashdumps"), registros de error ("log"), entre otros se revisan de forma periódica, monitorizando su aparición y reportando al diseñador del contenedor su frecuencia y contenido, para inspeccionar la aplicación y corregir el origen del fallo.

IC3.4 El rendimiento del equipo se comprueba, evaluando y comparando indicadores tales como uso de CPU, ocupación de memoria, acceso a disco y otros, para comprobar que se cumplen las especificaciones del proyecto.

EC4 Ejecutar procesos de "backup", programándolos y ejecutándolos para garantizar la integridad y disponibilidad de la aplicación.

IC4.1 Los "backup" de la aplicación se programan, configurándolos para que sean ejecutados periódicamente, verificando su ejecución para que se asegure la recuperación del sistema en caso de fallo.

IC4.2 Los ficheros de "backup" producidos por la aplicación se exportan a un medio externo, comprobando que son almacenados de acuerdo a las políticas de almacenamiento, rotación y limpieza establecidas en las especificaciones del proyecto.

IC4.3 El mantenimiento preventivo de los "backup" se realiza de forma periódica, asegurando que la última copia de seguridad puede ser restaurada, instanciando dicha copia en una plataforma de pruebas y verificando el despliegue del contenedor.

EC5 Instalar actualizaciones de nuevas versiones de "software", comprobando la existencia de parches de mantenimiento y de corrección de posibles vulnerabilidades para garantizar la seguridad y funcionalidad.

IC5.1 El "software" de base de la aplicación se mantiene, revisando en el repositorio la aparición de nuevas versiones que solucionen problemas encontrados durante las pruebas o reportados durante la vida de la aplicación e instalándolas en su caso.

IC5.2 Las vulnerabilidades sobre los componentes usados internamente por el contenedor o la aplicación se examinan, a partir de escaneados de código, binarios y librerías o buscando información en foros del programador del componente, estudiando su posible afectación y consecuencias e implementando posibles soluciones recomendadas si existieran.

IC5.3 La actualización de los paquetes de "software" se realiza de forma periódica, descargando de un repositorio propio o externo, instalando los cambios y verificando que no se produce

pérdida de los datos previamente almacenados para asegurar la integridad de la aplicación y la disponibilidad de la información.

IC5.4 Los problemas que aparezcan durante el proceso de actualización "software" se resuelven en su caso, en entornos previos, realizando un análisis del problema, identificando su naturaleza, en los márgenes de tiempo y el nivel de calidad requerido y reportando al diseñador de la aplicación.

IC5.5 El funcionamiento de la aplicación una vez actualizada o corregida y la integridad de los datos se chequea, ejecutando las pruebas acordadas en entornos previos y producción, según las especificaciones del proyecto, para verificar su funcionamiento.

IC5.6 La actualización de las versiones "software" se documenta, actualizando el repositorio de incidencias, incluyendo información tal como el nombre y versión de la aplicación actualizada, información acerca de las incidencias generadas e incompatibilidades detectadas, incremento o decremento de rendimiento, garantizando la trazabilidad de los procesos, de cara a facilitar su seguimiento.

EC6 Ejecutar tareas de terminación del contenedor, eliminando programas y datos relacionados en condiciones de seguridad, para reutilizar el almacenamiento.

IC6.1 La aplicación "software" desplegada en contenedor se termina cuando no va a ser usada, verificando que todos los recursos usados por el contenedor en la infraestructura han quedado liberados, tales como CPU, memoria y espacio de almacenamiento en disco, entre otros.

IC6.2 Las copias de seguridad ("backup") y los archivos de registro almacenados en servidores externos se eliminan, sobreescribiendo el espacio de disco usado previamente o utilizando alguna técnica similar, asegurando que no es posible su restauración mediante técnicas de recuperación de datos.

IC6.3 Los datos en posibles bases de datos internas de la aplicación que contengan información confidencial o sensible, se borran destruyendo su contenido acorde con los procedimientos que garantizan la protección de datos personales.

IC6.4 La conectividad e integración del contenedor con el entorno de monitorización y alarmas se desconfigura, eliminando la conectividad a través de la red de datos y todas las referencias introducidas en los sistemas de monitorización y alarmas relativas a la aplicación "software" del contenedor.

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 copia de seguridad. Herramientas de gestión y control de cambios, incidencias y configuración. Repositorio de artefactos/imágenes. Servidor de despliegues. Servidores de infraestructura. Sistema de monitorización.

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 asociado a servicios informáticos; manuales de funcionamiento de las herramientas de gestión del ciclo de vida del "software", bases de datos de vulnerabilidades).