Estándar de competencias profesionales

Gestionar recursos y servicios en la nube

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP2735_3**
Estado	**BOE**
Publicación	**RD 546/2023**

Competencia profesional

Elementos de la competencia

EC1 Preparar los interfaces de acceso y uso, configurándolos para acceder a los servicios de la plataforma en la nube.

IC1.1 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.

IC1.2 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.

IC1.3 Las librerías de cliente para los lenguajes de computación a utilizar se descargan, usando los gestores de dependencias.

EC2 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.

IC2.1 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.

IC2.2 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.

IC2.3 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.

IC2.4 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.

EC3 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.

IC3.1 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.

IC3.2 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.

IC3.3 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.

IC3.4 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.

IC3.5 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".

IC3.6 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.

EC4 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.

IC4.1 Los recursos para facilitar la gestión, control y análisis de costes entre otros, se etiquetan asignando identificadores según nomenclatura especificada por la organización.

IC4.2 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.

IC4.3 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.

IC4.4 Las alertas de gastos se configuran, estableciendo canales de notificación a los responsables y/o acciones automáticas que reaccionen a dichos eventos.

IC4.5 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.

EC5 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.

IC5.1 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.

IC5.2 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.

IC5.3 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

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

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.

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).