

Estándar de competencias profesionales

Desplegar Contratos Inteligentes ('Smart Contracts') sobre nodos de red DLT, Blockchain

Familia Profesional	Informática y Comunicaciones
Nivel	3
Código	ECP2633_3
Estado	BOE
Publicación	RD 884/2022

Competencia profesional

Elementos de la competencia

EC1 Instalar el nodo de la red, previa descarga desde los repositorios de la comunidad de desarrolladores, configurándolo según las especificaciones técnicas de la comunidad de desarrolladores y los procedimientos establecidos por el departamento de tecnologías de la información (IT) para desplegar del Contrato Inteligente ('Smart Contract').

IC1.1 El proceso de instalación se planifica, teniendo en cuenta a las características del sistema tal como volumen de datos esperados, tráfico de la red, seguridad de la información, entre otros, ajustándolo a los tiempos y tareas previstos en la planificación.

IC1.2 El nodo se instala localmente previa descarga desde los repositorios de la comunidad de desarrolladores, parametrizándola y de acuerdo a los estándares establecidos en la documentación técnica de despliegue, garantizando el buen funcionamiento del mismo.

IC1.3 La seguridad, resiliencia, rendimiento y calidad de la instalación se verifican mediante pruebas al efecto, utilizando los principios establecidos por la comunidad y el departamento IT.

IC1.4 La sincronización de la cadena de bloques se comprueba que es completa en el nodo, garantizando el intercambio de información con los nodos de la red DLT.

IC1.5 El acceso a la información de la cadena de bloques tal como bloques, transacciones y direcciones, se verifica a través de la interfaz de programación de aplicaciones del nodo.

- IC1.6** El software del nodo se actualiza con los mecanismos habilitados en el repositorio y siguiendo estándares definidos por la comunidad de desarrolladores y el departamento IT.
- IC1.7** La documentación de los procesos de instalación y actualización se elabora incluyendo las incidencias y soluciones adoptadas, siguiendo el formato establecido tal como tipo de documento, tamaño, tipografía, entre otros, según los estándares del departamento IT.
- EC2** Instalar el Contrato Inteligente ('Smart Contract'), desplegándolo según el procedimiento generado por la comunidad y por el departamento de tecnologías de la información (IT), y verificando su funcionalidad para integrar el producto desarrollado en la red DLT.
- IC2.1** La dirección desde la que se va a desplegar el Contrato Inteligente ('Smart Contract') se comprueba que cuenta con los suficientes recursos para su despliegue.
- IC2.2** El Contrato Inteligente ('Smart Contract') se instala, lanzando una transacción de despliegue, siguiendo los procedimientos establecidos tanto por la comunidad como por la organización, garantizando su buen funcionamiento.
- IC2.3** El despliegue del Contrato Inteligente ('Smart Contract') dentro de la cadena de bloques se verifica mediante la obtención de sus datos tales como dirección o bloque en el que se despliega, entre otros.
- IC2.4** El software se prueba verificando su funcionalidad tal como el acceso a los datos de la red descentralizada y la conexión en su caso con un 'backend' en función del tipo de red y del caso de uso, evaluando su usabilidad y siguiendo los parámetros de calidad establecidos por la comunidad y la organización.
- IC2.5** La nueva versión de un Contrato Inteligente ('Smart Contract') se actualiza en su caso, difundiendo la nueva dirección del contrato actualizado, garantizando la integridad, seguridad y disponibilidad de la información.
- IC2.6** Los trabajos realizados se documentan incluyendo las incidencias y soluciones adoptadas, y los procedimientos de restauración del servicio en caso de error, utilizando el formato que se establezca en los estándares que marque el departamento IT.
- EC3** Administrar los componentes software y hardware que forman el producto, configurándolos para garantizar su disponibilidad, rendimiento y seguridad acorde a los planes del departamento de tecnologías de la información (IT) y de la comunidad de desarrolladores para mantener el propio nodo.
- IC3.1** La capacidad de los componentes del sistema tales como la memoria, el disco, procesador, entre otros, se valora garantizando que se adecuan a las necesidades de rendimiento.

- IC3.2** El rendimiento se comprueba midiendo tiempos de respuesta y capacidad de transferencia de la red proporcionados por el departamento IT y cotejándolo con los valores recomendados por la comunidad de desarrolladores.
 - IC3.3** Las herramientas de monitorización se instalan en su caso, comprobando la carga de la red, del hardware y el software, entre otros para garantizar el buen funcionamiento del producto siguiendo las recomendaciones de la organización.
 - IC3.4** La información de la cadena de bloques se visualiza utilizando un explorador de bloques o una herramienta similar.
 - IC3.5** Las claves criptográficas se crean invocando el comando específico de la Blockchain siguiendo los estándares de seguridad de la organización y la comunidad, para almacenarlas posteriormente.
 - IC3.6** Los cortafuegos se configuran, parametrizando las reglas de acceso a la red en que se encuentra el nodo de acuerdo a las 'buenas prácticas' generadas por la organización.
 - IC3.7** Las operaciones de administración y configuración se documentan incluyendo las incidencias y soluciones adoptadas y utilizando los estándares de tipo de documento, tamaño y formato que definen los protocolos del departamento IT.
- EC4** Gestionar los componentes de red, monitorizando el nodo y parametrizando los servicios, para asegurar la buena comunicación entre el nodo local y la red DLT según las necesidades establecidas por la comunidad de desarrolladores.
- IC4.1** Los servicios de red se configuran, asignando valores a los parámetros propios de cada uno, siguiendo las directrices del departamento de comunicaciones garantizando el funcionamiento de la misma y la conexión con los servicios de 'backend'.
 - IC4.2** Los parámetros de conexión entre el nodo local y la red DLT se definen de modo que se eviten pérdidas de servicio en el resto de los componentes de la red corporativa utilizando los procedimientos del departamento de comunicaciones.
 - IC4.3** El nodo se monitoriza, incluyéndolo en los sistemas de monitorización de red de la compañía para garantizar la recolección de información en caso de pérdida de servicio.
 - IC4.4** Las incidencias detectadas se documentan, para enviarlas a los responsables del departamento de comunicaciones, indicando la causa del problema, las acciones realizadas y su resolución.
- EC5** Desplegar los mecanismos de seguridad de acceso al nodo recomendados en el plan de seguridad y por la comunidad de desarrolladores para garantizar la confidencialidad, integridad y disponibilidad y el control de acceso.

- IC5.1** Las políticas de acceso al sistema donde se aloja el nodo se definen, estableciendo usuarios, roles y permisos y aplicándolos según los parámetros establecidos por el departamento responsable de la seguridad.
- IC5.2** La configuración de seguridad del nodo se implementa, configurando claves, puertos y/o el acceso remoto, entre otros, siguiendo las directrices establecidas por la comunidad de desarrolladores.
- IC5.3** La clave privada generada en la instalación del nodo se mantiene segura, almacenando copias de respaldo siguiendo las directrices del departamento responsable de la seguridad.
- IC5.4** El nodo se incluye en los sistemas de monitorización del departamento responsable de la seguridad, garantizando la recolección de información y alerta temprana en caso de incidencia.
- IC5.5** Los procesos de seguridad implementados se documentan incluyendo las incidencias y soluciones adoptadas, siguiendo los estándares de formato, tamaño y tipo de letra que indican los procedimientos del departamento responsable de la seguridad para su almacenamiento y posterior utilización.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Equipos informáticos y periféricos. Sistemas operativos y parámetros de configuración. Sistemas de almacenamiento. Clúster y centros de respaldo. Herramientas de seguridad y antivirus. Herramientas de gestión de archivos de registro (log). Herramientas de depuración. Herramientas de control de cambios. Planificadores de tareas. Monitores de rendimiento. Acceso a Internet. Herramientas software de instalación. Cortafuegos. Soporte software criptográfico para generación y almacenamiento de claves.

Información utilizada o generada

Normas externas de trabajo (normativa aplicable en materia de seguridad, protección de datos, propiedad intelectual e industrial; normativa aplicable de planificación de la acción preventiva). Normas internas de trabajo (plan de seguridad; plan de calidad; documentación de trabajos de despliegue, mantenimiento,

administración e incidencias; plan de prevención de riesgos laborales -ergonomía-). Documentación Técnica (manuales de administración y operación de los nodos de la red; manuales de despliegue de los Contratos Inteligentes -'Smart Contracts'-; manuales de configuración de cortafuegos; manuales de herramientas administrativas; manuales de ayuda en línea; manuales de seguridad en el ámbito de 'Smart Contracts').