

Estándar de competencias profesionales

Configurar y gestionar bases de datos relacionales

Familia Profesional **Informática y Comunicaciones**
Nivel **3**
Código **ECP0225_3**
Estado **BOE**
Publicación **RD 150/2022**

Competencia profesional

Elementos de la competencia

EC1 Elaborar el diseño físico de las bases de datos cumpliendo los requerimientos de explotación de la base de datos para que los datos se ajusten a las restricciones descritas en el diseño lógico previo.

IC1.1 El diseño lógico se valora, adaptándolo, si procede, a las características del entorno (número de usuarios, volumen de datos, volatilidad, tráfico de datos estimados, entre otros) y a las normas de calidad de la organización.

IC1.2 Las tablas, vistas, índices y otros objetos propios de un gestor de base de datos se crean, codificando sentencias DDL o usando herramientas administrativas del Sistema Gestor de Bases de Datos (SGBD).

IC1.3 El espacio y las restricciones físicas de la base de datos se asignan, determinándose de acuerdo con las características lógicas definidas y a los requerimientos de explotación.

IC1.4 Las bases de datos distribuidas y la información se mantienen disponibles y en la versión apropiada en cada nodo, respetando los requerimientos de los datos.

IC1.5 Los mecanismos necesarios para la sincronización de las bases de datos distribuidas se establecen, manteniendo la sincronización entre ellas.

IC1.6 El esquema de distribución de los nodos de bases de datos distribuidas y los fragmentos en el caso de estar particionada se realizan, teniendo en cuenta la organización lógica de la base de datos, la ubicación de las aplicaciones, sus características de acceso.

IC1.7 Los mecanismos de balanceo de lecturas y escrituras y tolerancia a fallos en bases de datos distribuidas se implementan, instalando y configurando el 'middleware' y los dispositivos físicos que los habilitan.

IC1.8 El diccionario de datos se actualiza en aquellas tareas de mantenimiento de la base de datos que lo requieran, preservando su integridad.

EC2 Implantar la política de control de acceso en los gestores de bases de datos garantizando su seguridad siguiendo las normas de la organización para cumplir la normativa de protección de datos.

IC2.1 Los perfiles de seguridad se definen, ajustándose de acuerdo con la política de seguridad de la organización, mediante guiones de sentencias DCL y/o herramientas administrativas.

IC2.2 El registro de actividad se configura, parametrizándolo para llevar a cabo el seguimiento de las actividades realizadas por los usuarios y para detectar deficiencias en los sistemas de control de acceso.

IC2.3 Las medidas de implantación de la política de seguridad se documentan, ajustándose a los estándares de la organización.

EC3 Programar copias de seguridad, planificándolas puntual o periódicamente, permitiendo la recuperación de los datos en caso necesario, para mantener la integridad de la base de datos, cumpliendo las normas de seguridad de la organización.

IC3.1 La política de copias de seguridad y recuperación ante un desastre se define, aplicándola, siguiendo las normas de seguridad de la organización y los requerimientos de cada base de datos.

IC3.2 La información de los SGBD existentes en el centro de respaldo se mantiene actualizada, permitiendo que pueda ser recuperada en casos de desastre.

IC3.3 El almacenamiento de las copias se supervisa, comprobando que se cumplen los estándares de la organización (armarios ignífugos, ubicación física de la copia diferente a la fuente, entre otros).

IC3.4 Las copias de seguridad se recuperan a petición del responsable de los datos, siguiendo las normas de la organización.

EC4 Habilitar el acceso a las bases de datos, respetando la confidencialidad, integridad y disponibilidad de la información para cumplir con la normativa de protección de datos.

IC4.1 La carga inicial de datos se ejecuta en la base de datos, comprobando que el resultado corresponde a la información original para garantizar su coherencia.

- IC4.2** Las conexiones para el acceso desde clientes se habilitan, dependiendo de las redes disponibles y siguiendo los protocolos de seguridad y procedimientos establecidos por la organización.
- IC4.3** Los mecanismos de recuperación de transacciones se habilitan, garantizando la integridad de la información al realizar operaciones sobre los datos.
- IC4.4** Los mecanismos disponibles en el SGBD se habilitan, configurándolos para garantizar la confidencialidad e integridad de la información que se obtiene y que se almacena en la base de datos (criptografía, suma de comprobación 'checksum', algoritmos de firma, entre otros).
- IC4.5** La estrategia de ejecución y la optimización de consultas se establecen, minimizando los tiempos de respuesta y las transferencias de datos a través de la red.
- IC4.6** Las restricciones de uso de la base de datos se especifican para garantizar el rendimiento óptimo, documentándolas según establezca la organización.
- IC4.7** Los datos se importan o exportan, usando las herramientas disponibles y procedimientos establecidos por la entidad responsable para la transferencia de información entre unas bases de datos o sistemas y otras.
- IC4.8** La información en las bases de datos distribuidas se replica, estableciendo los mecanismos de soporte de tolerancia a fallos y balanceo de escrituras y lecturas entre otros, según la documentación técnica.

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. Conjunto ('cluster') y centros de respaldo. Herramientas de diseño de bases de datos. Herramientas de administración de SGBD. Soportes de copias de seguridad. Herramientas ofimáticas. Sistemas gestores de bases de datos. Diccionarios de datos (o catálogo, o tablas de sistema). Lenguajes de manipulación de datos. Lenguajes de control y definición de datos. Herramientas de gestión de archivos de 'log'. Lenguajes estructurados. Herramientas de control de cambios. Planificadores de tareas. Monitores de rendimiento. Herramientas de depuración. Optimizadores de consultas.

Información utilizada o generada

Normas externas de trabajo (normativa de protección de datos, normativa sobre prevención de riesgos laborales). Normas internas de trabajo (Organigrama de la organización, normas de seguridad -plan de seguridad- y calidad de la organización, Diseños lógico y físico de la Base de Datos, Libro de registro de las copias de seguridad, Medidas de implantación de la política de seguridad, protocolos y procedimientos de operación). Documentación técnica (Manuales de administración y operación de los SGBD, manuales de instalación del sistema operativo, manual de operación del sistema operativo, diccionario de datos, documentación técnica sobre redes de comunicaciones de datos, manuales de herramientas administrativas, manuales de ayuda en línea, asistencia técnica en línea).