## DATOS IDENTIFICATIVOS DE LA UNIDAD FORMATIVA

| | | | |
|---|---|---|---|
| UNIDAD FORMATIVA | SALVAGUARDA Y SEGURIDAD DE LOS DATOS. | DURACIÓN<br>Específica | 70 |
| Código | UF1473 | | |
| Familia profesional | INFORMÁTICA Y COMUNICACIONES | | |
| Área Profesional | Sistemas y telemática | | |
| Certificado de profesionalidad | ADMINISTRACIÓN DE BASES DE DATOS | Nivel | 3 |
| Módulo formativo | Gestión de bases de datos. | Duración | 200 |
| Resto de unidades formativas que completan el módulo | Bases de datos relacionales y modelado de datos | Duración | 70 |
| | Lenguajes de definición y modificación de datos SQL. | | 60 |

## Apartado A: **REFERENTE DE COMPETENCIA**

Esta unidad formativa se corresponde con la RP2, RP3 y RP4 respecto a las copias de seguridad y cifrado.

## Apartado B: **ESPECIFICACIÓN DE LAS CAPACIDADES Y CONTENIDOS**

### Capacidades y criterios de evaluación

C1: Mantener la seguridad de los accesos a las bases de datos garantizando la confidencialidad.

CE1.1 Explicar los métodos para la definición de perfiles de acceso

CE1.2 Explicar los conceptos disponibles en el SGBD para la aplicación de las políticas de seguridad (roles, login, usuarios, grupos, permisos, privilegios, ...)

CE1.3 Describir la legislación de protección de datos vigente y los mecanismos del SGBD que permiten garantizar el cumplimiento de la misma.

CE1.4 Describir los principios sobre la protección de datos

CE1.5 Describir los derechos de las personas

CE1.6 Identificar las herramientas para llevar a cabo el seguimiento de la actividad de los usuarios

CE1.7 Enumerar los posibles mecanismos de criptografiado disponibles en el SGBD: De los datos en la base de datos y de las comunicaciones

CE1.8 Describir los dos grandes grupos de técnicas criptográficas: de clave pública y de clave privada (asimétrica o simétrica).

CE1.9 Enumerar los problemas que se pueden resolver utilizando técnicas criptográficas: Autenticación, confidencialidad, integridad, no repudio.

CE1.10 En un supuesto práctico con un esquema de base de datos definido y una especificación de su uso, determinar las obligaciones en relación con la normativa vigente:

- Reconocer el tipo de contenido según la normativa vigente (Titularidad pública o privada, tipo de información...).
- Determinar si la información es ajustada a los fines.
- Determinar cuáles son las obligaciones a cumplir según la información disponible.

CE1.11 En un supuesto práctico, sobre una BBDD en funcionamiento, y partiendo del plan de seguridad y normas de la organización:

- Establecer los perfiles de acceso a la base de datos necesarios de acuerdo con unas características de uso dadas en el diseño lógico, con las normas de seguridad de la organización y respetando la legalidad vigente.
- Crear y mantener los perfiles de seguridad definidos mediante sentencias DCL y /o herramientas administrativas.
- Crear los usuarios de la base de datos adaptándolos a los perfiles de seguridad establecidos.
- Configurar el registro de actividad para llevar a cabo el seguimiento de las actividades realizadas por los usuarios y detectar deficiencias en los sistemas de control de acceso.
- Documentar las medidas de implantación de la política de seguridad a nivel de usuario.

C2: Garantizar la salvaguarda y recuperación de la información almacenada en las bases de datos de acuerdo a las necesidades de cada una de ellas.

CE2.1 Describir los principales fallos posibles en una base de datos: fallo de algún soporte físico, fallos lógicos: fallo interno de la base de datos, procesos abortados, transacciones canceladas...).

CE2.2 Describir los principales medios que aporta el SGBD para la recuperación de los fallos lógicos y cual es su utilidad en el contexto

de un fallo lógico: Salvaguardas y tipos disponibles, archivos de registro de transacciones, espacios de rollback...
CE2.3 Detallar las principales características y formas de acceso a los medios secundarios de almacenamiento.
CE2.4 Enumerar y describir las diferentes técnicas de realización de copias de seguridad (incrementales, acumulativas y completas).
CE2.5 Identificar la normativa legal vigente aplicable a la planificación de sistemas de copia de seguridad, en función de los diferentes tipos de contenidos almacenados.
CE2.6 Explicar el funcionamiento de los mecanismos de conexión con servidores remotos de salvaguarda para realización de copias de seguridad.
CE2.7 En un supuesto práctico, sobre una BBDD en funcionamiento, y partiendo del plan de seguridad y normas de la organización:

- Definir la política de copias de seguridad y recuperación ante un desastre de acuerdo a las normas de seguridad de la organización, a los requerimientos de cada base de datos y a la normativa legal vigente.
- Planificar la realización de las copias de seguridad, calculando sus costes, en función de los estándares de la organización (características, temporalización, almacenamiento, ventanas de tiempo para ejecución por lotes, etc.).
- Calcular los recursos necesarios para ejecutar la planificación establecida sobre una base de datos dada
- Disponer los procedimientos adecuados para implementar la planificación de las copias mediante guiones de comandos y/o herramientas administrativas.
- En caso de existir un centro de respaldo de la BBDD, realizar las operaciones necesarias para mantener la información que contiene actualizada: Enlazado con el servidor remoto, exportación e importación de datos, etc.
- Recuperar en condiciones de integridad las copias de seguridad.
- Documentar la implementación realizada del plan de copias de seguridad, dispositivos implicados y procedimientos ante de recuperación ante desastres.

C3: Exportar e importar datos de la Base de Datos garantizando su integridad
CE3.1 Explicar los mecanismos de importación y exportación de datos posibles (Exportación directa de los recursos físicos –Espacios de tabla transportables, Archivos, etc.– que componen la base de datos a otro SGBD similar, exportación e importación directa mediante el enlazado de bases de datos, exportación e importación de datos a través de una estructura intermedia).
CE3.2 Describir las herramientas de importación y exportación disponibles en el SGBD concreto especificando las ventajas e inconvenientes de cada una de ellas, cuándo es apropiado su uso teniendo en cuenta las consideraciones de rendimiento de cada una de ellas, la posibilidad de automatización, la flexibilidad en cuanto a formatos de datos reconocidos y potencia en la transformación de datos.
CE3.3 Describir las herramientas de verificación de integridad de la estructura de una base de datos disponibles en el SGBD.
CE3.4 Describir las consecuencias posibles en la realización de importaciones y exportaciones de datos sin registro de log teniendo en cuenta la oposición existente entre las consideraciones de rendimiento y a recuperación ante un fallo.
CE3.5 Describir los mecanismos de configuración de juegos de caracteres y otros relativos a la internacionalización del sistema, para evitar problemas en la carga de campos de tipo carácter, numéricos con y sin punto decimal y de tipo fecha.
CE3.6 En un supuesto práctico, sobre una BBDD configurada y un conjunto de ficheros planos y otras bases de datos con unas estructuras conocidas:

- Determinar el procedimiento de carga inicial de datos en la BBDD para cada conjunto de datos. Establecer las herramientas a utilizar y los mecanismos de creación inicial de los índices.
- Realizar la carga inicial de datos garantizando la integridad de los datos.
- Si fuese necesario importar datos a la BBDD (desde otra BBDD u otra fuente de información), seleccionar el método más adecuado para realizarlo de acuerdo a las necesidades y normas de la organización.
- Si fuese necesario exportar datos desde la BBDD (hacia otra BBDD u otro destino de información), seleccionar el método más adecuado y las transformaciones de datos necesarias para realizarlo de acuerdo a las necesidades y normas de la organización.
- Realizar la transferencia de datos (importación / exportación) según el método seleccionado y garantizando la integridad de la información.
- Realizar operaciones básicas de alta, baja modificación y consulta manual sobre una base de datos en funcionamiento.

## Contenidos

**1. Salvaguarda y recuperación de datos**

- Descripción de los diferentes fallos posibles (tanto físicos como lógicos) que se pueden plantear alrededor de una base de datos.
- Enumeración y descripción de los elementos de recuperación ante fallos lógicos que aportan los principales SGBD estudiados.
- Distinción de los diferentes tipos de soporte utilizados para la salvaguarda de datos y sus ventajas e inconvenientes en un entorno de backup.
- Concepto de RAID y niveles más comúnmente utilizados en las empresas:
  - RAID5, RAID6.
  - Clasificación de los niveles RAID por sus tiempos de reconstrucción.

- Servidores remotos de salvaguarda de datos.
- Diseño y justificación de un plan de salvaguarda y un protocolo de recuperación de datos para un supuesto de entorno empresarial.
- Tipos de salvaguardas de datos:
    - Completa.
    - Incremental.
    - Diferencial.
- Definición del concepto de RTO (Recovery Time Objective) y RPO (Recovery Point Objective).
- Empleo de los mecanismos de verificación de la integridad de las copias de seguridad.

**2. Bases de datos distribuidas desde un punto de vista orientado a la distribución de los datos y la ejecución de las consultas**

- Definición de SGBD distribuido. Principales ventajas y desventajas.
- Características esperadas en un SGBD distribuido.
- Clasificación de los SGBD distribuidos según los criterios de:
    - Distribución de los datos.
    - Tipo de los SGBD locales.
    - Autonomía de los nodos.
- Enumeración y explicación de las reglas de DATE para SGBD distribuidos.
- Replicación de la información en bases de datos distribuidas.
- Procesamiento de consultas.
- Descomposición de consultas y localización de datos.

**3. Seguridad de los datos**

- Conceptos de seguridad de los datos: confidencialidad, integridad y disponibilidad.
- Normativa legal vigente sobre datos:
    - Los datos de carácter personal y el derecho a la intimidad.
    - Leyes de primera, segunda y tercera generación.
    - Ley de protección de datos de carácter personal.
    - La Agencia de Protección de Datos.
    - Registro General de Protección de Datos.
    - Argumentación desde un punto de vista legal las posibles implicaciones legales que tiene que tener en cuenta un administrador de bases de datos en su trabajo diario.
        - Tipos de amenazas a la seguridad:
            - Accidentales: errores humanos, fallos software/hardware.
            - Intencionadas: ataques directos e indirectos.
        - Políticas de seguridad asociadas a BBDD:
            - Perfiles de usuario.
            - Privilegios de usuario.
            - Vistas de usuario.
            - Encriptación de datos.
        - El lenguaje de control de datos DCL.
        - Enumeración de los roles mas habituales de los usuarios en SGBD.
        - Implementación en al menos 2 SGDB.
        - Seguimiento de la actividad de los usuarios:
    - Enumeración de las distintas herramientas disponibles para seguir la actividad de los usuarios activos.
    - Enumeración de las distintas herramientas y métodos para trazar las actividad de los usuarios desde un punto de vista forense.
    - Empleo de una herramienta o método para averiguar la actividad de un usuario desde un momento determinado.
    - Empleo de una herramienta o método para averiguar un usuario a partir de determinada actividad en la base de datos.
    - Argumentación de las posibles implicaciones legales a la hora de monitorizar la actividad de los usuarios.
        - Introducción básica a la criptografía:
            - Técnicas de clave privada o simétrica.
            - Técnicas de clave pública o asimétrica.
        - La criptografía aplicada a: La autenticación, confidencialidad, integridad y no repudio.
        - Mecanismos de criptografía disponibles en el SGBD para su uso en las bases de datos.
        - Descripción de los mecanismos criptográficos que permiten verificar la integridad de los datos.
        - Descripción de los mecanismos criptográficos que permiten garantizar la confidencialidad de los datos.
        - Métodos de conexión a la base datos con base criptográfica.
    - Desarrollo de uno o varios supuestos prácticos en los que se apliquen los elementos de seguridad vistos con anterioridad.

**4. Transferencia de datos**

- Descripción de las herramientas para importar y exportar datos:
  - Importancia de la integridad de datos en la exportación e importación.
- Clasificación de las herramientas:
  - Backups en caliente.
  - Backups en frío.
- Muestra de un ejemplo de ejecución de una exportación e importación de datos.
- Migración de datos entre diferentes SGBD:
- Valoración de los posibles inconvenientes que podemos encontrar a la hora de traspasar datos entre distintos SGBD y proponer soluciones con formatos de datos intermedios u otros métodos.
- Empleo de alguno de los mecanismos de verificación del traspaso de datos.
- Interconexión con otras bases de datos.
- Configuración del acceso remoto a la base de datos:
  - Enumeración de los Métodos disponibles.
  - Enumeración de las ventajas e inconvenientes.

## Apartado C: **REQUISITOS Y CONDICIONES**

Deberá cumplir alguno de los requisitos siguientes:

- Estar en posesión del título de Bachiller.
- Estar en posesión de algún certificado de profesionalidad de nivel 3.
- Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado superior o haber superado las correspondientes pruebas de acceso a ciclos de grado superior.
- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener, de acuerdo con la normativa que se establezca, los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.

En relación con las exigencias de los formadores o de las formadoras, instalaciones y equipamientos se atenderá las exigencias solicitadas para el propio certificado de profesionalidad.