Curso: Salvaguarda y seguridad de los datos

Familia Profesional: Informática y comunicaciones
Modalidad: On-line (Teleformación)
Duración: 30 horas

Contenidos:

1. Salvaguarda y recuperación de datos

1.1Descripción de los diferentes fallos posibles (tanto físicos como lógicos) que se pueden plantear alrededor de una base de datos.

1.2Enumeración y descripción de los elementos de recuperación ante fallos lógicos que aportan los principales SGBD estudiados.

1.3Distinción de los diferentes tipos de soporte utilizados para la salvaguarda de datos y sus ventajas e inconvenientes en un entorno de backup.

1.4Concepto de RAID y niveles más comúnmente utilizados en las empresas:
- 1.4.1RAID5, RAID6.
- 1.4.2Clasificación de los niveles RAID por sus tiempos de reconstrucción.

1.5Servidores remotos de salvaguarda de datos.

1.6Diseño y justificación de un plan de salvaguarda y un protocolo de recuperación de datos para un supuesto de entorno empresarial.

1.7Tipos de salvaguardas de datos:
- 1.7.1Completa.
- 1.7.2Incremental.
- 1.7.3Diferencial.

1.8Definición del concepto de RTO (Recovery Time Objective) y RPO (Recovery Point Objective).

1.9Empleo 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

2.1Definición de SGBD distribuido. Principales ventajas y desventajas.

2.2Características esperadas en un SGBD distribuido.

2.3Clasificación de los SGBD distribuidos según los criterios de:
- 2.3.1Distribución de los datos.
- 2.3.2Tipo de los SGBD locales.

2.3.3Autonomía de los nodos.

2.4Enumeración y explicación de las reglas de DATE para SGBD distribuidos.

2.5Replicación de la información en bases de datos distribuidas.

2.6Procesamiento de consultas.

2.7Descomposición de consultas y localización de datos.

3. Seguridad de los datos

3.1Conceptos de seguridad de los datos: confidencialidad, integridad y disponibilidad.

3.2Normativa legal vigente sobre datos:

3.2.1Los datos de carácter personal y el derecho a la intimidad.
3.2.2Leyes de primera, segunda y tercera generación.
3.2.3Ley de protección de datos de carácter personal.
3.2.4La Agencia de Protección de Datos.
3.2.5Registro General de Protección de Datos.
3.2.6Argumentación 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.
3.2.6.1Tipos de amenazas a la seguridad:
3.2.6.1.1Accidentales: errores humanos, fallos software/hardware.
3.2.6.1.2Intencionadas: ataques directos e indirectos.
3.2.6.2Políticas de seguridad asociadas a BBDD:
3.2.6.2.1Perfiles de usuario.
3.2.6.2.2Privilegios de usuario.
3.2.6.2.3Vistas de usuario.
3.2.6.2.4Encriptación de datos.
3.2.6.3El lenguaje de control de datos DCL.
3.2.6.4Enumeración de los roles más habituales de los usuarios en SGBD.
3.2.6.5Implementación en al menos 2 SGDB.
3.2.6.6Seguimiento de la actividad de los usuarios:
3.2.7Enumeración de las distintas herramientas disponibles para seguir la actividad de los usuarios activos.
3.2.8Enumeración de las distintas herramientas y métodos para trazar las actividad de los usuarios desde un punto de vista forense.
3.2.9Empleo de una herramienta o método para averiguar la actividad de un usuario desde un momento determinado.
3.2.10Empleo de una herramienta o método para averiguar un usuario a partir de determinada actividad en la base de datos.
3.2.11Argumentación de las posibles implicaciones legales a la hora de monitorizar la actividad de los usuarios.

3.2.11.1Introducción básica a la criptografía:
3.2.11.1.1Técnicas de clave privada o simétrica.
3.2.11.1.2Técnicas de clave pública o asimétrica.
3.2.12La criptografía aplicada a: La autenticación, confidencialidad, integridad y no repudio.
3.2.13Mecanismos de criptografía disponibles en el SGBD para su uso en las bases de datos.
3.2.14Descripción de los mecanismos criptográficos que permiten verificar la integridad de los datos.
3.2.15Descripción de los mecanismos criptográficos que permiten garantizar la confidencialidad de los datos.
3.2.16Métodos de conexión a la base datos con base criptográfica.

3.3Desarrollo de uno o varios supuestos prácticos en los que se apliquen los elementos de seguridad vistos con anterioridad.

4. Transferencia de datos

4.1Descripción de las herramientas para importar y exportar datos:
4.1.1Importancia de la integridad de datos en la exportación e importación.

4.2Clasificación de las herramientas:
4.2.1Backups en caliente.
4.2.2Backups en frío.

4.3Muestra de un ejemplo de ejecución de una exportación e importación de datos.

4.4Migración de datos entre diferentes SGBD:

4.4.1Valoración 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.

4.5Empleo de alguno de los mecanismos de verificación del traspaso de datos.

4.6Interconexión con otras bases de datos.

4.7Configuración del acceso remoto a la base de datos:
4.7.1Enumeración de los Métodos disponibles.
4.7.2 Enumeración de las ventajas e inconvenientes.