Salvaguarda y seguridad de los datos.

Área: INFORMÁTICA Y COMUNICACIONES
Modalidad: Teleformación
Duración: 70 h
Precio: 35.00€

Curso Bonificable
Contactar
Recomendar
Matricularme

CONTENIDOS

1. Salvaguarda y recuperación de datos

####

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

####

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

####

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

####

1.4. Concepto de RAID y niveles más comúnmente utilizados en las empresas:

####

1.4.1. RAID5, RAID6.

####

1.4.2. Clasificación de los niveles RAID por sus tiempos de reconstrucción.

####

1.5. Servidores remotos de salvaguarda de datos.

####

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

####

1.7. Tipos de salvaguardas de datos:

####

1.7.1. Completa.

####

1.7.2. Incremental.

####

1.7.3. Diferencial.

####

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

####

1.9. 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

####

2.1. Definición de SGBD distribuido. Principales ventajas y desventajas.

####

2.2. Características esperadas en un SGBD distribuido.

####

2.3. Clasificación de los SGBD distribuidos según los criterios de:

####

2.3.1. Distribución de los datos.

####

2.3.2. Tipo de los SGBD locales.

####

2.3.3. Autonomía de los nodos.

####

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

####

2.5. Replicación de la información en bases de datos distribuidas.

####

2.6. Procesamiento de consultas.

####

2.7. Descomposición de consultas y localización de datos.

####

3. Seguridad de los datos

####

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

####

3.2. Normativa legal vigente sobre datos:

####

3.2.1. Los datos de carácter personal y el derecho a la intimidad.

####

3.2.2. Leyes de primera, segunda y tercera generación.

####

3.2.3. Ley de protección de datos de carácter personal.

####

3.2.4. La Agencia de Protección de Datos.

####

3.2.5. Registro General de Protección de Datos.

####

3.2.6. 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.

####

3.2.6.1. Tipos de amenazas a la seguridad:

####

3.2.6.1.1. Accidentales: errores humanos, fallos software/hardware.

####

3.2.6.1.2. Intencionadas: ataques directos e indirectos.

####

3.2.6.2. Políticas de seguridad asociadas a BBDD:

####

3.2.6.2.1. Perfiles de usuario.

####

3.2.6.2.2. Privilegios de usuario.

####

3.2.6.2.3. Vistas de usuario.

####

3.2.6.2.4. Encriptación de datos.

####

3.2.6.3. El lenguaje de control de datos DCL.

####

3.2.6.4. Enumeración de los roles más habituales de los usuarios en SGBD.

####

3.2.6.5. Implementación en al menos 2 SGDB.

####

3.2.6.6. Seguimiento de la actividad de los usuarios:

####

3.2.7. Enumeración de las distintas herramientas disponibles para seguir la actividad de los usuarios activos.

####

3.2.8. Enumeración de las distintas herramientas y métodos para trazar las actividad de los usuarios desde un punto de vista forense.

####

3.2.9. Empleo de una herramienta o método para averiguar la actividad de un usuario desde un momento determinado.

####

3.2.10. Empleo de una herramienta o método para averiguar un usuario a partir de determinada actividad en la base de datos.

####

3.2.11. Argumentación de las posibles implicaciones legales a la hora de monitorizar la actividad de los usuarios.

####

3.2.11.1. Introducción básica a la criptografía:

####

3.2.11.1.1. Técnicas de clave privada o simétrica.

####

3.2.11.1.2. Técnicas de clave pública o asimétrica.

####

3.2.12. La criptografía aplicada a: La autenticación, confidencialidad, integridad y no repudio.

####

3.2.13. Mecanismos de criptografía disponibles en el SGBD para su uso en las bases de datos.

####

3.2.14. Descripción de los mecanismos criptográficos que permiten verificar la integridad de los datos.

####

3.2.15. Descripción de los mecanismos criptográficos que permiten garantizar la confidencialidad de los datos.

####

3.2.16. Métodos de conexión a la base datos con base criptográfica.

####

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

####

4. Transferencia de datos

####

4.1. Descripción de las herramientas para importar y exportar datos:

####

4.1.1. Importancia de la integridad de datos en la exportación e importación.

####

4.2. Clasificación de las herramientas:

####

4.2.1. Backups en caliente.

####

4.2.2. Backups en frío.

####

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

####

4.4. Migración de datos entre diferentes SGBD:

####

4.4.1. 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.

####

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

####

4.6. Interconexión con otras bases de datos.

####

4.7. Configuración del acceso remoto a la base de datos:

####

4.7.1. Enumeración de los Métodos disponibles.

####

4.7.2. Enumeración de las ventajas e inconvenientes.

METODOLOGIA

- **Total libertad de horarios** para realizar el curso desde cualquier ordenador con conexión a Internet, **sin importar el sitio desde el que lo haga**. Puede comenzar la sesión en el momento del día que le sea más conveniente y dedicar el tiempo de estudio que estime más oportuno.
- En todo momento contará con un el **asesoramiento de un tutor personalizado** que le guiará en su proceso de aprendizaje, ayudándole a conseguir los objetivos establecidos.
- **Hacer para aprender**, el alumno no debe ser pasivo respecto al material suministrado sino que debe participar, elaborando soluciones para los ejercicios propuestos e interactuando, de forma controlada, con el resto de usuarios.
- **El aprendizaje se realiza de una manera amena y distendida**. Para ello el tutor se comunica con su alumno y lo motiva a participar activamente en su proceso formativo. Le facilita resúmenes teóricos de los contenidos y, va controlando su progreso a través de diversos ejercicios como por ejemplo: test de autoevaluación, casos prácticos, búsqueda de información en Internet o participación en debates junto al resto de compañeros.
- **Los contenidos del curso se actualizan para que siempre respondan a las necesidades reales del mercado.** El departamento multimedia incorpora gráficos, imágenes, videos, sonidos y elementos interactivos que complementan el aprendizaje del alumno ayudándole a finalizar el curso con éxito.

REQUISITOS

Los requisitos técnicos mínimos son:

- Navegador Microsoft Internet Explorer 5.5 o superior, con plugin de Flash, cookies y JavaScript habilitados.
  No se garantiza su óptimo funcionamiento en otros navegadores como Firefox, Netscape, Mozilla, etc.
- Resolución de pantalla de 800x600 y 16 bits de color o superior.
- Procesador Pentium II a 300 Mhz o superior.
- 32 Mbytes de RAM o superior.