Unidad 7

Gestión de seguridad

Bases de datos

Índice

Introducción

La información es el elemento más importante con el que una empresa puede trabajar, y la base de datos es la encargada de almacenarla. Como este elemento es uno de los más importantes y el éxito de la empresa pasa casi obligatoriamente por las bases de datos, es importante tener una gestión de la seguridad de los datos.

Las siglas CIDAN agrupan cinco normas que toda empresa debe de seguir con respecto a la información almacenada:

- **Confidencialidad.** Ningún usuario que no tenga permiso no debe de poder acceder a la información.
- **Integridad.** La información no debe de ser alterada.
- **Disponibilidad.** Siempre debemos de tener la información accesible en un corto periodo de tiempo.
- **Autenticación.** Los usuarios que estén autorizados al acceso a distintos tipos de información deben de autenticarse previamente.
- **No repudio.** No se pude negar la autoría de nada relacionado con la información.

En esta unidad vamos a ir viendo la disponibilidad de la información y como mediante el uso de distintas herramientas, garantizamos su integridad también.

Al finalizar esta unidad

- Sabremos por qué es necesario contar con una gestión de seguridad.
- Podremos diferenciar fallos físicos de lógicos.
- Conoceremos como luchar contra los distintos tipos de fallos.
- Seremos capaces de efectuar copias de seguridad
- Estaremos familiarizados con la problemática de la transferencia de datos ente sistemas gestores

7.1. Tipos de fallos

Se pueden clasificar los fallos en las bases de datos de varios tipos, pero la principal clasificación distingue entre fallos físicos y fallos lógicos.

7.1.1. Fallos físicos

Estos son los fallos derivados de problemas de hardware físico, ya sea del propio equipo que almacena la base de datos o de las instalaciones en las que se encuentre alojada. Los más comunes son:

- Averías en discos duros.
- Averías en servidores.
- Mal funcionamiento de la red.
- Problemas en suministros.
- Incendios, inundaciones, accidentes.
- Ataques físicos.
- Robos.

7.1.2. Fallos lógicos

Son las que tienen que ver con las incidencias que funcionan sobre el software:

- Errores de diseño de la base de datos.
- Falta de actualización de versiones del SGBD o del sistema operativo.
- Errores en las aplicaciones que acceden a la base de datos.
- Errores humanos de manipulación de la base de datos.
- Ataques lógicos.
- Virus.
- Mala gestión de la seguridad lógica.

Un falo lógico muy común en las bases de datos es cuando se almacenan contraseñas de aplicaciones en estas. Estas contraseñas deben de ir cifradas siempre para que cualquier usuario no pueda ver su contenido real. En algunas bases de datos, se ofrece un tipo de dato que las cifra en la misma base, pero si disponemos de esto, habrá que insertar el dato ya cifrado.

7.2. Recuperación de fallos

El principal rasgo de la seguridad es que nunca se puede garantizar una total seguridad. Aunque las precauciones que tomemos sean extremas, siempre habrá algún momento en el que estemos en peligro. Pero de entro de esta inseguridad, debemos de intentar protegernos lo mejor posible.

7.2.1. Fallos físicos

En la mayoría de los casos, un fallo físico se produce por la falta de prevención. Para poder hacer que los fallos se sucedan con grandes periodos de tiempo entre ellos, debemos de intentar incorporar estos elementos a nuestro sistema informático:

- **Sistemas redundantes de discos.** En cualquier servidor de bases de datos que esté medianamente bien montado debe de contar con un sistema RAID de discos redundantes. Esto se usa para que, si hay un error en un disco, los demás discos sigan funcionando y no ocasione perdida de información.
- **Elección acertada de servidores y contratos de mantenimiento.** Un servidor es por lo general el equipo más importante de toda una empresa, lo que implica que si se hace una inversión económica baja en estos y no se tiene una previsión en la necesidad de los recursos tendremos problemas bastantes serios en un futuro. La elección de los servidores es algo muy importante y complicado. Además, debemos siempre de intentar mantener un acuerdo firmado con los proveedores para el mantenimiento de estos porque es importante en caso de avería.
- **Gestión de información redundante.** Debe de existir un centro de contingencia de datos (CDC, contingency data center) que no debe de encontrarse muy lejos del CPD donde alojaremos los servidores de las bases de datos. En estos CDC debe estar el hardware más importante replicado, al igual que pasará con el software. Los datos de versiones de todos estos componentes físicos y lógicos deben de estar siempre actualizados para poder trabajar desde el CDC en caso de inoperatividad del CPD.
- **Gestión de backups.** Las copias de seguridad de las bases de datos deben de hacerse de manera frecuente e intentar almacenarlas de manera correcta. Estos deben estar siempre a disposición del administrador para poder asegurar la recuperación de los datos. Otra práctica que debe de seguirse con los backups es la de almacenarlos en soportes de almacenamiento secundario como pueden ser las cintas magnéticas. Estos deben de estar guardados en el CDC.

- **Mirroring.** El mirroring es una técnica que consiste en la replicación de los datos en dos servidores distintos. Estos funcionan de manera similar a un RAID mirror, asegurando que la información esté intacta en caso de fallo de alguno de los servidores. También conlleva algunos retardos de tiempo, como en el RAID.
- **Plan de contingencia.** En todos los negocios que cuenten con sistemas informáticos hay que definir un plan que indique que pautas seguir en caso de problemas de fuerza mayor como puede ser un corte del suministro eléctrico inesperado. En este procedimiento debemos de tener en cuenta también las bases de datos alojadas en los servidores de la empresa.

7.2.2. Fallos lógicos

En informática, muchos fallos vienen dados de los problemas que puede haber a la hora de confeccionar el software y de establecer sus pautas. Esto tiene solución, pues se puede volver a implementar o retocar, pero el verdadero problema viene dado por los ataques que se pueden sufrir y que pueden traspasar nuestros perímetros de seguridad. Es recomendable abordar los siguientes aspectos de cara a los futuros problemas que puedan ocasionarse:

- **Acceso al servicio:** el acceso a ciertas informaciones y recursos de las bases de datos solo debe de hacerse de personal imprescindible.
- **Acceso al servidor:** debemos de acceder a los servidores usando usuario y contraseña.
- **Autenticación en el SGBD:** cuando entremos al sistema gestor de la base de datos, también debe de haber un usuario dado de alta para su acceso y este lógicamente debe ir asociado a una contraseña cifrada.
- **Gestión de perfiles y usuarios:** es imprescindible una adecuada configuración de los perfiles de usuario concretos para cada acción. Estos deben de estar muy limitados y solo poder realizar las funciones de nuevo imprescindibles, pues, aunque no sea con malicia, un desconocimiento de alguna tarea puede ocasionar futuros problemas graves.

7.3. Copias de seguridad

Las copias de seguridad o backups son herramientas que se usan en la informática para respaldar la información de modo que si ocurre un incidente que suponga la perdida de información esta esté replicada en algún sitio y se pueda recuperar.

Cuando se hace una restauración de una copia de seguridad esto implica que se recupera toda la información contenida en la copia.

7.3.1. Tipos de copias de seguridad

Hay veces en las que no es posible realizar copias de seguridad completas de toda la información almacenada, ya sea por falta de recursos o porque no es lo deseado y por eso tenemos tres tipos de copias de seguridad:

- **Completas o totales:** este tipo de copias almacenan en el backup toda la información que albergamos. Además, activan el atributo o flag de modificado para todos los archivos.
- **Incrementales:** en este tipo de copias solo se copia lo que ha sido cambiado o modificar y desactivan el flag de modificar de los archivos que se copian.
- **Diferenciales:** solo se copian los archivos modificados.

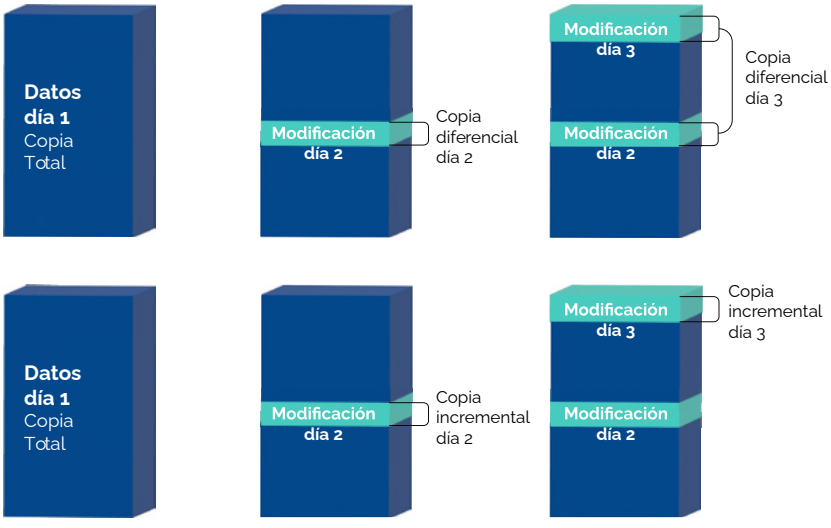

Imagen 1. Tipos de copia de seguridad.

La diferencial real entre una copia de seguridad incremental y una diferencial es que en la segunda nunca se desactiva el flag de modificado.

Es conveniente que las copias de seguridad no se espacien mucho en el tiempo, porque si por ejemplo realizamos una copia el lunes y los datos los perdemos jueves, los de martes y miércoles no se podrán recuperar.

7.3.2. Restauración de los backups

Para restaurar una copia de seguridad solo tenemos que seguir los siguientes tres pasos:

- **Paso 1.** Se restaura la última copia de seguridad total.
- **Paso 2.** Si tenemos copias de seguridad incrementales se restauran de la más antigua a la más moderna siempre que sean posteriores a la copia de seguridad total.
- **Paso 3.** Si tenemos copias de seguridad diferenciales y no haya ninguna total o incremental posterior, se restaura la más moderna de estas.

7.3.3. Consejos a la hora de realizar copias de seguridad

A la hora de realizar copias de seguridad debemos de tener en cuenta los siguientes aspectos de manera fundamental:

- **Orden y claridad**: el nombre que le pongamos a la copia debe de ofrecernos una buena descripción de que contiene y de cuando es la copia.
- **Comprobación de las copias:** debemos de comprobar habitualmente si las copias de seguridad se realizan y si se encuentran en buen estado.
- **Localización:** debemos de intentar que las copias se almacenen en un lugar distinto al de la realización, porque en caso de fallo físico perderíamos ambas informaciones.
- **Automatización**: es conveniente que esta tarea se automatice para ahorrar costes.
- **Calendario:** todos los backups deben de estar planificados además de su tipo.
- **Simulacros:** es conveniente que se realicen simulacros de perdida de datos para poder comprobar que la restauración funcionaria.
- **Protección:** los backups deben de tener una protección igual a la del sistema cuando no superior para evitar ataques y filtraciones.

7.4. Transferencia de datos entre SGBD

Cuando pasamos de un sistema gestor de bases de datos a otro, la tarea de traspaso no es nada fácil. Todos usan los mismos estándares, pero cada desarrollador ha establecido distintos criterios de cara a la gestión de ciertos tipos de datos.

A continuación, explicamos los cambios de datos ente las grandes compañías desarrolladoras de SGBD:

	Oracle	MySQL	Microsoft SQL Server	PostgreSQL
Cadenas de caracteres	CHAR, VARCHAR2, CLOB, NCLOB, NVARCAHR2, NCHAR	CHAR, BINARY, VARCHAR, VARBINARY, TEXT, TINYTEXT, MEDIUMTEXT, LONGTEXT	CHAR, VARCHAR, TEXT, NCHAR, NVARCHAR, NTEXT	CHAR, VARCHAR, TEXT
Números exactos	NUMBER	TINYINT, SMALLINT, MEDIUMINT, INT, BIGINT, DECIMAL	TINYINT, SMALLINT, INT, BIGINT, NUMERIC, DECIMAL, SMALLMONEY, MONEY	SMALLINT, INTEGER, BIGINT, DECIMAL, NUMERIC
Números aproximados	BINARY_FLOAT, BINARY_DOUBLE	FLOAT, DOUBLE	FLOAT, REAL	REAL, DOUBLE, PRECISION
Fechas, horas e intervalos	DATE, TIMESTAMP, INTERVAL	DATETIME, DATE, TIMESTAMP, YEAR	DATE, DATETIMEOFFSET, DATETIME2, SMALLDATETIME, DATETIME, TIME, TIMESTAMP	DATE, TIME, TIMESTAMP, INTERVAL
Valores lógicos	No se aplica	BIT, BOOLEAN = sinónimo de TINYINT	BIT	BOOLEAN
Objetos binarios	BLOB, RAW, LONG RAW, BFILE	TINYBLOB, BLOB, MEDIUMBLOB, LONGBLOB	BINARY, VARBINARY, IOMAGE, FILESTREAM	BYTEA
Otros	SPATIAL, IMAGE, AUDIO, VIDEO, DICOM, XMLType	ENUM, SET, tipos de datos GIS	CURSOR, HIERARCHYID, UNIQUEIDENTIFIER, SQL_VARIANT, CML, TABLE	ENUM, POINT, LINE, LSEG, BOX, PATH, PLYGON, CIRCLE, CIDR, INET, MACADDR, BIT, UUID, XML, JSON, arrays,composites, rangos, tipos definidos por el usuario

Cuadro 1. Tipos de datos de los SGBD más usados.

www.universae.com