Tema 7
Seguridad en Bases de Datos

Grado en Ingeniería Informática

Bases de Datos

2020/21

Departamento de Tecnologías de la Información
Universidad de Huelva

Seguridad en Bases de Datos

Objetivos

- Conocer los principales **problemas** de seguridad en un SGBD
- Conocer los **mecanismos** básicos de seguridad en un SGBD

Contenidos

1. Introducción a la seguridad en bases de datos.
2. Mecanismos de seguridad.
3. Control de acceso.
4. El Administrador de la BD.
5. Mecanismos de acceso discrecional.
6. Sentencia Grant.
7. Sentencia Revoke.
8. Permisos sobre vistas.
9. Autorizaciones abandonadas.

10. Roles
11. Control de acceso obligatorio
12. Cifrado

Duración

- 2 clases

Bibliografía

- Capítulo 19 de [Silberschatz 06]
- Capítulo 19 de [Connolly 05]

1. Introducción

- Componentes lógicos de **datos**: tablas y vistas
- Componentes lógicos de **control**: procedimientos (y funciones) almacenados, disparadores, mecanismos de seguridad

- **Seguridad en BD:** Mecanismos que protegen a la BD frente a amenazas intencionadas o accidentales.
- Una BD es un **recurso corporativo esencial**. Pueden darse las siguientes situaciones:
  - Robo y fraude
  - Pérdida de confidencialidad
  - Pérdida de Privacidad
  - Pérdida de integridad
  - Pérdida de disponibilidad
- Actos intencionados o no intencionados

1. Introducción

- **Robo y fraude**
  - Abarca no solo la BD sino toda la organización
  - Reducir la probabilidad de que se produzcan estas acciones
  - Resultado: alteración de los datos, pérdida de confidencialidad y de privacidad

- **Pérdida de confidencialidad**
  - Necesidad de mantener en secreto ciertos datos
  - La pérdida de confidencialidad puede producir una pérdida de competitividad de la organización

- **Pérdida de privacidad**
  - Proteger los datos acerca de personas
  - La pérdida de privacidad puede hacer que alguien inicie acciones legales contra la organización por no custodiar correctamente sus datos

- **Pérdida de integridad**
  - Provoca la aparición de datos inválidos o corruptos
  - Afecta a la operación de la organización

1. Introducción

- **Pérdida de disponibilidad**
  - El sistema deja de estar accesible
  - Las aspiraciones de las organizaciones hoy en día es intentar hacer realidad los cinco nueves famosos de **disponibilidad**: **99,999%** ⇒

"inactividad de unos 5 minutos de al año"

Porcentaje de disponibilidad	Tiempo de inactividad aproximado por año
95%	18 días
99%	4 días
99,9%	9 horas
99,99%	1 hora
99,999%	5 minutos

Equivalencia entre disponibilidad y tiempo de inactividad

1. Introducción

- **Secreto**: No se debe permitir que ciertos usuarios accedan a datos a los que no están autorizados:
  - Ej: Un alumno no debe ver las notas de otro.
- **Integridad**: No se debe permitir que ciertos usuarios modifiquen datos a los que no están autorizados
  - Ej: Sólo los profesores deben modificar las notas de los alumnos.
- **Disponibilidad**: Sólo ciertos usuarios pueden ver y modificar ciertos datos.

- Las técnicas de seguridad en BD tratan de **minimizar las pérdidas** causadas por los eventos previos y sin restringir innecesariamente la actividad de los usuarios
- Incremento del número de delitos informáticos

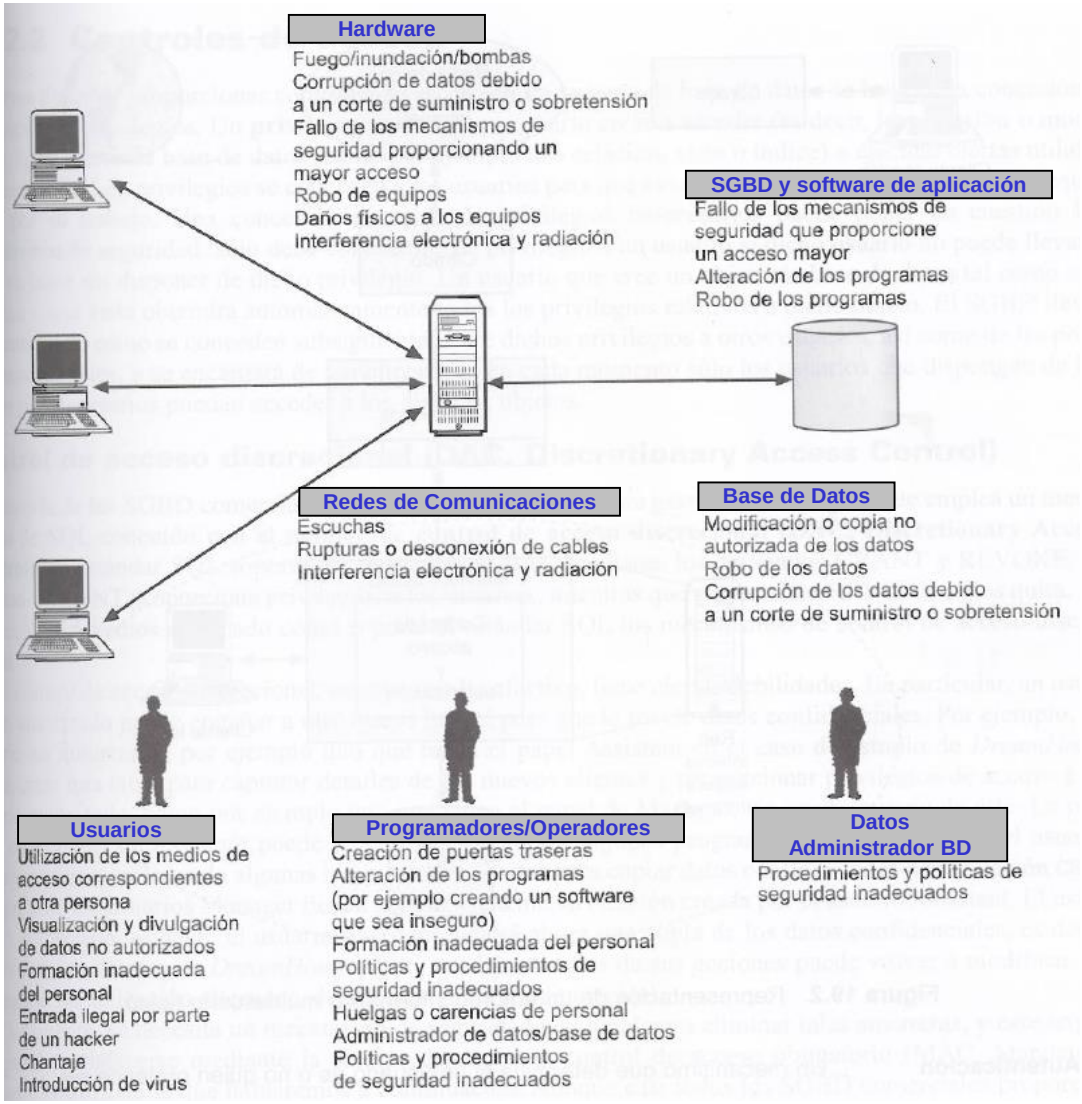
1.1. Ejemplos de amenazas

Amenza	Robo y Fraude	Pérdida de confidencialidad	Pérdida de privacidad	Pérdida de Integridad	Pérdida de disponibilidad
Utilizar los medios de acceso correspondientes a otra persona	✓	✓	✓		
Modificación o copia no autorizadas de los datos	✓			✓	
Alteración de un programa	✓			✓	✓
Políticas y procedimientos inadecuados que permiten que se produzca la consulta de datos tanto confidenciales como no confidenciales	✓	✓	✓		
Escuchas	✓	✓	✓		
Entrada ilegal por parte de un hacker	✓	✓	✓		
Chantaje	✓	✓	✓		
Creación de 'puertas traseras' en un sistema	✓	✓	✓		
Robo de datos, programas y equipos	✓	✓	✓		✓
Fallo de los mecanismos de seguridad, proporcionando un acceso superior al normal		✓	✓	✓	
Huelgas o carencias de personal				✓	✓
Formación inadecuada del personal		✓	✓	✓	✓

1.1. Ejemplos de amenazas

Amenza	Robo y Fraude	Pérdida de confidencialidad	Pérdida de privacidad	Pérdida de Integridad	Pérdida de disponibilidad
Visualización y divulgación de datos no autorizados	✓	✓	✓		
Interferencia electrónica de radiación				✓	✓
Corrupción de los datos debido a cortes de suministro o sobre-tensiones				✓	✓
Fuego (eléctrico, debido a un rayo o de otro tipo), inundacio-nes, bombas				✓	✓
Daños físicos a los equipos				✓	✓
Ruptura de desconexión de cables				✓	✓
Introducción de virus				✓	✓

1.2. Resumen de potenciales amenazas



2. Mecanismos de seguridad

- La política de seguridad especifica quién está autorizado a hacer qué
- Los mecanismos de seguridad permiten llevar a cabo una determinada **política de seguridad**
- En un SGBD hay dos tipos de mecanismos de seguridad:
  - Mecanismos de seguridad discrecional
  - Mecanismos de seguridad obligatorios
- **Autorización**: permiso o privilegio que permite a un usuario (o conjunto de usuarios) realizar una determinada operación sobre un cierto objeto de la BD
- Los permisos se conceden para que los usuarios puedan llevar a cabo su trabajo
- **Sólo debe concederse un privilegio si el usuario no puede llevar a cabo su trabajo sin disponer de ese privilegio**.

3. Control de acceso

- Evitar que personas no autorizadas tengan acceso al sistema, ya sea para:
  - Obtener información
  - Efectuar cambios mal intencionados en una porción de la BD.

- Creación de **cuentas de usuario** y **contraseñas** para que el SGBD controle el proceso de entrada al sistema.

- El **administrador** suele ser el responsable de crear cuentas de usuario individuales, identificadas mediante un nombre de usuario (único) y una contraseña
  - Seleccionada por el usuario
  - Conocida por el sistema
  - Asegurar que el usuario es quien dice ser

- Existen dos tipos de Control de Acceso:
  - Discrecional (Discretionary Access Control)
  - Obligatorio (Mandatory Access Control)

4. El Administrador de la BD

- Administrador de bases de datos (DBA) es la autoridad central que controla el sistema
- Es responsable de la seguridad global del sistema
- Tiene una cuenta privilegiada (cuenta del sistema) con capacidades que otros usuarios no tienen, como:
    - Creación de cuentas
    - Concesión de privilegios
    - Revocación de privilegios
    - Asignación de niveles de seguridad

5. Mecanismos de control acceso discrecional

- Basado en:
  - Permisos o privilegios sobre **tablas y vistas**
  - Mecanismos para asignar esos privilegios (y revocarlos)

- El **creador** de una tabla o vista obtiene automáticamente todos los permisos sobre ella
  - El SGBD controla quién tiene (y quien no) permisos sobre las tablas (seguimiento)
  - El SGBD asegura que se de acceso a los usuarios que tengan los permisos correspondientes.

- Utilización de los comando **GRANT y REVOKE**

- Tiene ciertas **debilidades** (alteración de programas de usuario)
  - Un usuario A puede crear una tabla con, por ejemplo, información sobre nuevos clientes y dar permiso de escritura a un usuario B (sin que él lo sepa) sobre esta tabla. A continuación, puede modificar algunos programas de usuario que maneja B para que escriban en la tabla la información sobre los nuevos clientes.
  - El usuario B no sabe que está modificando la tabla de nuevos clientes, cuya información podría estar siendo utilizada por A para fines inadecuados.

6. Sentencia Grant

- Sintaxis:
  - `GRANT lista_permisos ON objeto TO lista_usuario [WITH GRANT OPTION]`

- Tipos de permisos (o privilegios):
  - Conectar a la BD
  - Crear/modificar/borrar tablas y otros objetos
  - Ejecutar operaciones de selección, inserción, actualización y borrado

- Privilegios sobre tablas:

  - **SELECT** (nombreColumna): Se pueden leer todas las columnas (incluyendo aquellas que se añadan después con ALTER TABLE). Si se especifican atributos sólo se podrán leer los indicados.
  - **INSERT**: Se pueden insertar tuplas.
  - **UPDATE** (nombreColumna): Se pueden modificar tuplas. En caso de especificar atributos sólo se podrán actualizar los indicados
  - **DELETE:** Se pueden borrar tuplas.
  - **REFERENCES**(nombreColumna): Se pueden definir claves ajenas (en otras tablas) que hagan referencia al atributo especificado.

6. Sentencia Grant

- Si se especifica WITH GRANT OPTION, el permiso se puede propagar a otros usuarios

Ejemplos:

- Conexión y creación de objetos al usuario Juan
  - `grant connect, resource to juan;`
- Inserción, borrado y actualización del campo sueldo de la tabla empleados a Ana
  - `grant insert, delete, update (sueldo) on empleatos to ana;`
- Selección de los campos ident y nombre de empleados a Ana con posibilidad de propagación
  - `grant select (ident,nombre) on empleados to ana with grant option;`
- Visualización del campo sueldo a Ana y Pedro
  - `grant select (sueldo) on empleados to ana, pedro;`
- Actualización del sueldo para Juan
  - `grant update (sueldo) on empleados to juan;`

7. Sentencia Revoke

- Mediante este comando se pueden **cancelar** (revocar) permisos que el usuario tenía anteriormente.

- Sintaxis:
  - `REVOKE [GRANT OPTION FOR] permisos ON objeto FROM usuarios {RESTRICT | CASCADE}`

- **GRANT OPTION FOR**: cancela la opción GRANT OPTION.
- **Cascade**: los permisos se cancelan de los usuarios que lo han obtenido sólo de éste.
- **Restrict**: El SGBD no revocará la autorización si el usuario ya ha concedido algún permiso utilizando la autorización que se le intenta revocar *(opción por defecto)*

Ejemplos:

- `Revoke select on empleados from ana cascade;`
- `Revoke select on empleados from ana restrict;`

8. Permisos sobre vistas

- Las vistas son **relaciones virtuales** que se establecen sobre una tabla.

- Junto con GRANT y REVOKE, las vistas son un mecanismo muy poderoso de control de acceso.

Ejemplo:

- Si el propietario A de una relación R desea que otro usuario B pueda leer únicamente ciertos campos de R, A puede crear una vista de R que incluya sólo esos atributos, y después otorgar a B el permiso Select sobre la vista.

8. Permisos sobre vistas

Sintaxis:

```
create view nombre_vista [(columna [,columna…])]
  as sentencia_select
  [with check option];
```

Sobre las vistas:

- No se pueden crear índices
- Para cambiar su definición hay que volverlas a crear
- La sentencia select de la vista no puede tener:
  - INTO
  - UNION
  - ORDER BY

La clausula WITH CHECK OPTION:

- asegura que las operaciones LMD (insert, delete, update) que se lleven a cabo usando la vista, pasen un control de integridad que corresponda a los criterios de definición de la propia vista
- por ejemplo, en una vista definida sobre la tabla matricula que selecciona las tuplas del curso 2012/13, no se podría insertar una tupla correspondiente a otro curso

8. Permisos sobre vistas

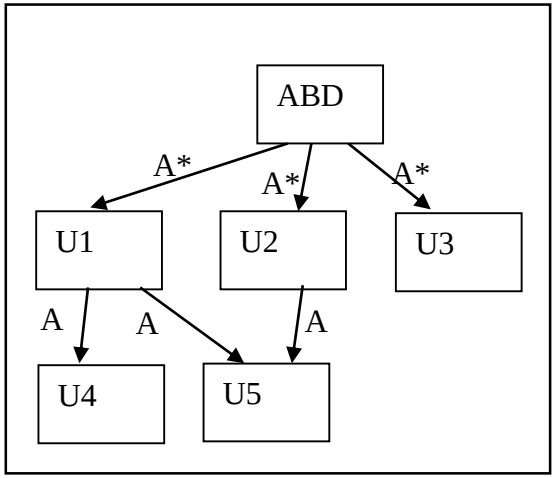
Actualización de vistas

- **Las vistas no se pueden actualizar si:**
  - asocian más de dos tablas mediante un JOIN
  - existen funciones de agregación
  - aparece la cláusula GROUP BY
  - aparece la palabra reservada DISTINCT o UNIQUE
  - las columnas derivadas tampoco se pueden actualizar

- Hay que tener en cuenta que, al modificar una vista, es necesario que **se sigan cumpliendo** las restricciones definidas sobre la tabla de definición de la vista

9. Autorizaciones abandonadas

- Supongamos que el ABD concede una determinada autorización A a los usuarios U1, U2 y U3 y que además, el ABD autoriza a que éstos puedan a su vez transmitirla a otros usuarios (llamaremos A* a la autorización A más el derecho a transmitir A).
- U1 transmite su privilegio a U5 y U4.
- U2 también hace uso al derecho a transmitir autorizaciones, de tal manera que transmite su privilegio a U5.
- Supongamos, por último, que ni U1, U2, U3,U4 ni U5 son propietarios del objeto involucrado en la autorización A, ni que son ABD.
- Podemos representar la secuencia de concesión de autorizaciones mediante el siguiente grafo, que denominaremos ***grafo de autorizaciones***



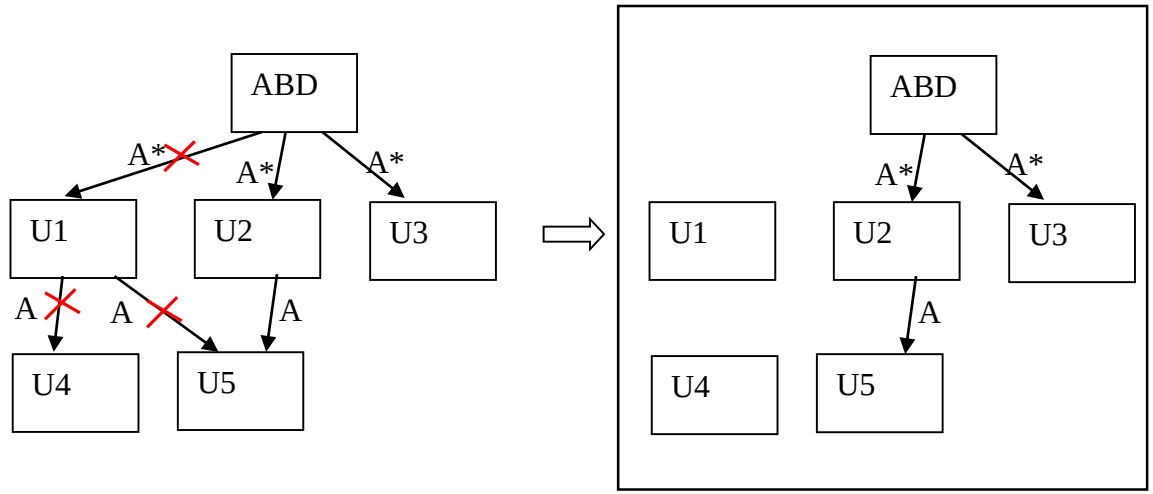
9. Autorizaciones abandonadas

- Supongamos ahora que el ABD retira a U1 su autorización, **dado que U4 la ha recibido de U1 se debe retirar también su autorización**.

- Sin embargo, U5 recibió la autorización tanto de U1 como de U2.

- Como el ABD no ha retirado la autorización de U2, U5 conservará su privilegio (**aunque pierde el heredado de U1**).

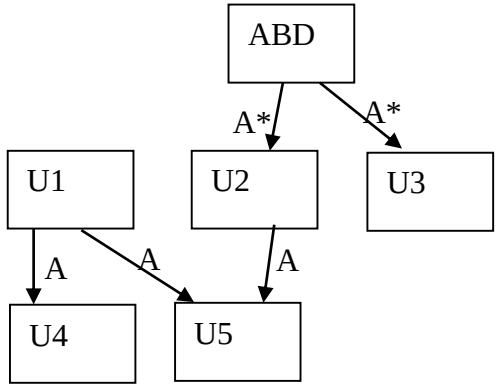
- Como consecuencia, tenemos un nuevo grafo de autorizaciones.



9. Autorizaciones abandonadas

- SQL estándar prohíbe explícitamente que puedan quedar **autorizaciones abandonadas**

- Si la retirada de la autorización del ABD a U1, sólo implicase la retirada de la autorización a U1, el grafo de autorizaciones quedaría de la siguiente manera:

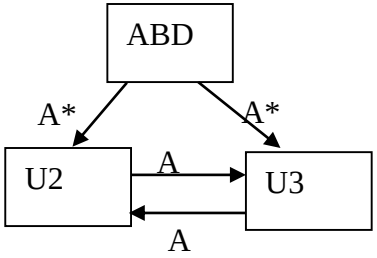


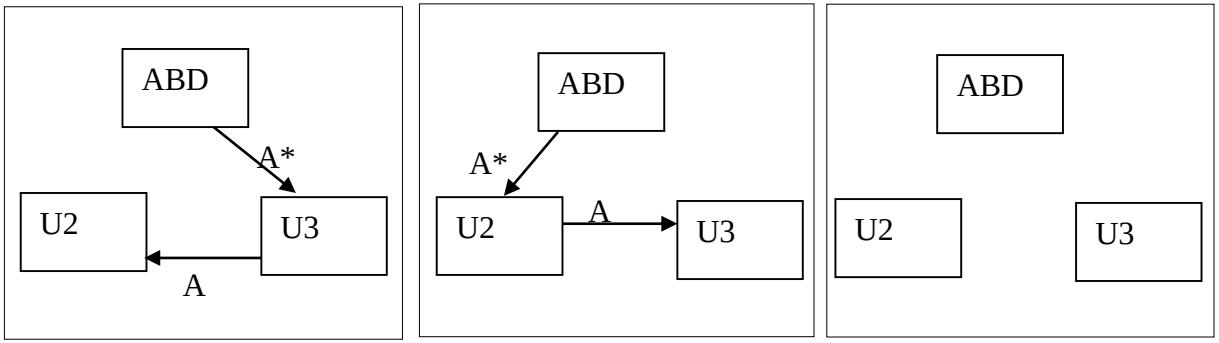
- ¿Cómo es posible que U4 (o U5) pueda haber recibido una autorización A de parte de U1, cuando éste no está, aparentemente, en posesión de dicha autorización?

    - U1 fuese el propietario del objeto involucrado en la autorización,
    - o que U1 fuese realmente ABD

9. Autorizaciones abandonadas

- Un par de usuarios (U2 y U3) podrían intentar eludir las reglas de retirada de autorizaciones concediéndose autorización mutuamente





10. Roles

- Un **rol** se puede considerar como un grupo de una serie de privilegios sobre objetos de la BD, con un nombre determinado.

- Los roles se pueden conceder a los **usuarios** o bien a otros **roles**.

Ejemplo: Un banco con muchos cajeros. Cada cajero debe tener las mismas autorizaciones para las mismas relaciones.

  – Es muy engorroso que, cada vez que se contrate a un nuevo cajero, se le concedan todas esas autorizaciones individualmente.

  – Una alternativa es crear un identificador de cajero y permitir a cada cajero conectarse a la BD utilizando ese identificador. El problema es que no sería posible identificar exactamente al cajero que ha realizado una determinada transacción, con lo que tendríamos problemas de seguridad.

  – Para solucionarlo, se pueden especificar las autorizaciones que deben tener los cajeros (rol) e identificar cuales de los usuarios de la base de datos son cajeros. Cuando se contrate a un nuevo cajero, se le debe asignar un identificador de usuario e identificarle como cajero

10. Roles

- El uso de los roles tiene la ventaja de requerir a los usuarios que se conecten con su propio identificador de usuario

Sintaxis:

- `Create role nombre_rol;`
- `Grant nombre_rol to lista_usuario;`

11. Control de acceso obligatorio

- Intenta solucionar los problemas del control de acceso discrecional

- Características del control de acceso obligatorio:

  - Se basa en la creación de una política de seguridad que no puede ser modificada por usuarios individuales.
  - Muchos SGBD implementan el control de acceso discrecional, pocos el control de acceso obligatorio.
  - A cada objeto de la BD se le asigna un **nivel de seguridad**.
  - A cada sujeto (usuario o programa) se le asigna un **nivel de seguridad**.

    Ejemplo: Se pueden definir los siguientes niveles de seguridad:
    - TS (Top Secret)
    - S (Secreto)
    - C (Confidencial)
    - U (No clasificado).
      - » Donde: TS>S>C>U

  - Se imponen una serie de reglas de lectura y escritura de objetos de la BD por parte de los usuarios

11. Control de acceso obligatorio

- Modelo **Bell-LaPadula**.

  – A cada sujeto *s* (usuario, cuenta, programa) y a cada objeto *o* (relación, tupla, columna, vista, operación) se le asigna un nivel de seguridad TS, S, C o U.

  NS: indica el nivel (o clasificación) de seguridad de un objeto o sujeto

  Ejemplo: NS(*s*) o NS(*o*)

  – Propiedad de seguridad simple: Ningún sujeto puede leer un objeto cuya clasificación de seguridad sea más alta que la suya

  – Propiedad * (o propiedad estrella): Un Sujeto tiene prohibido escribir un objeto que tenga una clasificación de seguridad más baja que la suya.

11. Control de acceso obligatorio

Modelo de Seguridad Multinivel: Asigna a cada sujeto (usuario o cuenta, o programa) y a cada objeto (tabla, fila, columna, vista…) un nivel de seguridad (TS, S, C, U)

Empleado original

Nombre		Salario		Rendimiento		NSt
Silva	U	4000	C	Regular	S	S
Bravo	C	5000	S	Bueno	C	S

Aspecto de Empleado después de filtrar los usuarios de clasificación C

Nombre		Salario		Rendimiento		NSt
Silva	U	4000	C		C	C
Bravo	C		C	Bueno	C	C

Aspecto de Empleado después de filtrar los usuarios de clasificación U

Nombre		Salario		Rendimiento		NSt
Silva	U		U		U	U

12. Cifrado

- ✓ Codificación de los datos mediante un algoritmo especial que hace que éstos no sean legibles por ningún programa que no disponga de la clave de descifrado
- ✓ Se pueden codificar datos especialmente confidenciales, como precaución frente amenazas externas o frente a intentos de acceder a ellos.
- ✓ Al cifrar/descrifrar existe cierta degradación en el rendimiento.
- ✓ El cifrado también protege a los datos transmitidos a través de las líneas de comunicaciones.
- ✓ Hay dos tipos de técnicas:
  - Irreversibles
    - los datos sólo pueden continuar usándose para obtener información estadística válida
  - Reversibles
    - Clave de cifrado para cifrar los datos (texto en claro)
    - Algoritmo de cifrado, que, junto con la clave de cifrado, transforma el texto en claro en texto cifrado.
    - Clave de descifrado para descifrar el texto cifrado
    - Algoritmo de descifrado, que, junto con la clave de descifrado, transforma el texto cifrado en texto en claro.