# SEGURIDAD
# EN BASE DE DATOS

## Objetivo

- Conocer los términos y conceptos para gestionar la seguridad de una base de datos en una organización identificando los riesgos y estableciendo los controles necesarios para mitigarlos

## Objetivo

- En las bases de datos se plantean problemas de seguridad como la compartición de datos, acceso a estos, protección contra fallos, contra accesos no permitidos, etc.
- El DBMS facilita mecanismos para prevenir los fallos (subsistema de control), para detectarlos (subsistema de detección) y para corregirlos (subsistema de recuperación).
- Aspectos fundamentales de la seguridad:
  - Confidencialidad. No desvelar datos a usuarios no autorizados. Comprende también la privacidad (protección de datos personales).
  - Accesibilidad o disponibilidad. La información debe estar disponible y también el acceso a los servicios.
  - Integridad. Permite asegurar que los datos no han sido falseados o modificados de forma indebida.

## Seguridad y Auditoria

- Las bases de datos son el activo más importante para las organizaciones.
- Los datos confidenciales en manos ajenas puede ser muy riesgoso.
- Por ello se deben controlar aspectos cruciales en la seguridad de la misma.
- Con la auditoría de bases de datos se busca monitorear y garantizar que la información está segura, además de brindar ayuda a la organización para detectar posibles puntos débiles y así tomar precauciones para resguardar aún más los datos.

## Ejercicio 1: Identificación de Activos

Identifique 3 Activos de Información:

- ✓ _____
- ✓ _____
- ✓ _____

## Ejercicio 2: Identificación de Amenazas

Identifique 3 Amenazas:

- ✓ _____
- ✓ _____
- ✓ _____

## Ejercicio 3: Identificación de Vulnerabilidades

Identifique 3 Vulnerabilidades:

- ✓ _____
- ✓ _____
- ✓ _____

## ¿Qué es un Activo de información?

**Es todo aquello que tiene valor para la organización y por lo tanto requiere protección:**

**Documentos en papel**: contratos, guías
**Software:** aplicativos y software de sistemas
**Dispositivos físicos**: computadoras, medios removibles
**Personas**: clientes, personal, etc.
**Imagen y reputación de la Institución**: marca
**Servicios**: comunicaciones, internet, energía.

## Tipos de Activos que requieren protegerse




***Activo de Información es todo lo que es o contiene información. Si la información no está dentro, no es un activo de información. No confundir con activos fijos.***

LA CONTRALORÍA GENERAL DE LA REPÚBLICA

## Seguridad vía SQL

**Privilegios:**

- **Nivel de cuenta. Privilegios de usuario. CREATE SCHEMA, CREATE TABLE, CREATE VIEW, ALTER, DROP, MODIFY, SELECT**
- **Nivel de relación. Se aplican a las relaciones individuales: SELECT, MODIFY, REFERENCES.**
- **Los privilegios se dan o quitan con GRANT y REVOKE.**
- **Además se pueden crear y eliminar roles de usuario con CREATE ROLE… y DROP ROLE…**

## Encriptación

- **La encriptación es básicamente transformar datos en alguna forma que no sea legible sin el conocimiento de la clave o algoritmo adecuado. El propósito de esta es mantener oculta la información que consideramos privada a cualquier persona o sistema que no tenga permitido verla.**

## Encriptación

- **La encriptación es el proceso de volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave.**
- **Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.**

# Proceso de Encriptación

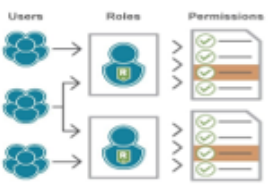
- **Texto a codificar:** **ENCRYPTION**
- **Caracteres del Texto:** **E N C R Y P T I O N**
- **Códigos ASCII:** **69 78 67 82 89 80 84 73 79 78**
- **Texto codificado:** **“œ?©Ÿ?¨**

# Usuario

- ✓ **Un usuario es un nombre definido en la base de datos que puede conectarse a ella y acceder a determinada información según los permisos que tenga asignados por el administrador**
- ✓ **El objetivo de la creación de usuarios es establecer una cuenta segura y útil, que tenga los privilegios adecuados y los valores por defecto apropiados**

## Rol

- **Un rol es el conjunto de permisos. Los roles permiten agrupar los derechos y gestionar más fácilmente los diferentes usuarios.**
- **Siempre es preferible asignar los derechos a los roles y posteriormente asignar los roles a los usuarios que tenga asignados por el administrador**




## Rol en MS SQL Server

- **Cada rol agrupa un conjunto de permisos**
- **Facilitan la administración de la seguridad**
- **Se definen a nivel de servidor, independiente, de las bases de datos**
- **Un inicio de sesión puede pertenecer a cero o más roles de servidor**
- **Un inicio de sesión que pertenezca a un rol de servidor adquiere los permisos de ese rol**

Microsoft SQL Server

# Privilegios

- **Los privilegios son atributos que permiten a un usuario realizar determinadas operaciones dentro de una BD o acceder a objetos de otros usuarios**
- **Existen dos tipos de privilegios:**
  - **Privilegios sobre los objetos**
  - **Privilegios del sistema**