**ACTIVIDAD 3**

**SEGURIDAD**

**INTEGRANTES**

Cesar Augusto Ospina Ruiz

Nini Yohana Grandas Téllez

**GESTION DE BASE DE DATOS**

**DOCENTE**

Hugo Alexander Balbin Espinal

**FUNDACION UNIVERSITARIA CATOLICA DEL NORTE**

**MEDELLÍN – ANTIOQUIA**

**FEBRERO 23 DEL 2025**

**TABLA DE CONTENIDO**

[INTRODUCCIÓN 3](#_Toc193556181)

[CLAVE PARA INGRESO A LA BASE DE DATOS 4](#_Toc193556182)

[CREACIÓN DE PERFILES DE ACCESO A LA BASE DE DATOS. 6](#_Toc193556183)

[Explicar cómo se hace la copia de seguridad (Backup) en la base de datos y hacer una copia de está. 9](#_Toc193556184)

[¿Qué más otras opciones de seguridad implementaría en la Base de Datos? 9](#_Toc193556185)

[CONCLUSIÓN 11](#_Toc193556186)

# INTRODUCCIÓN

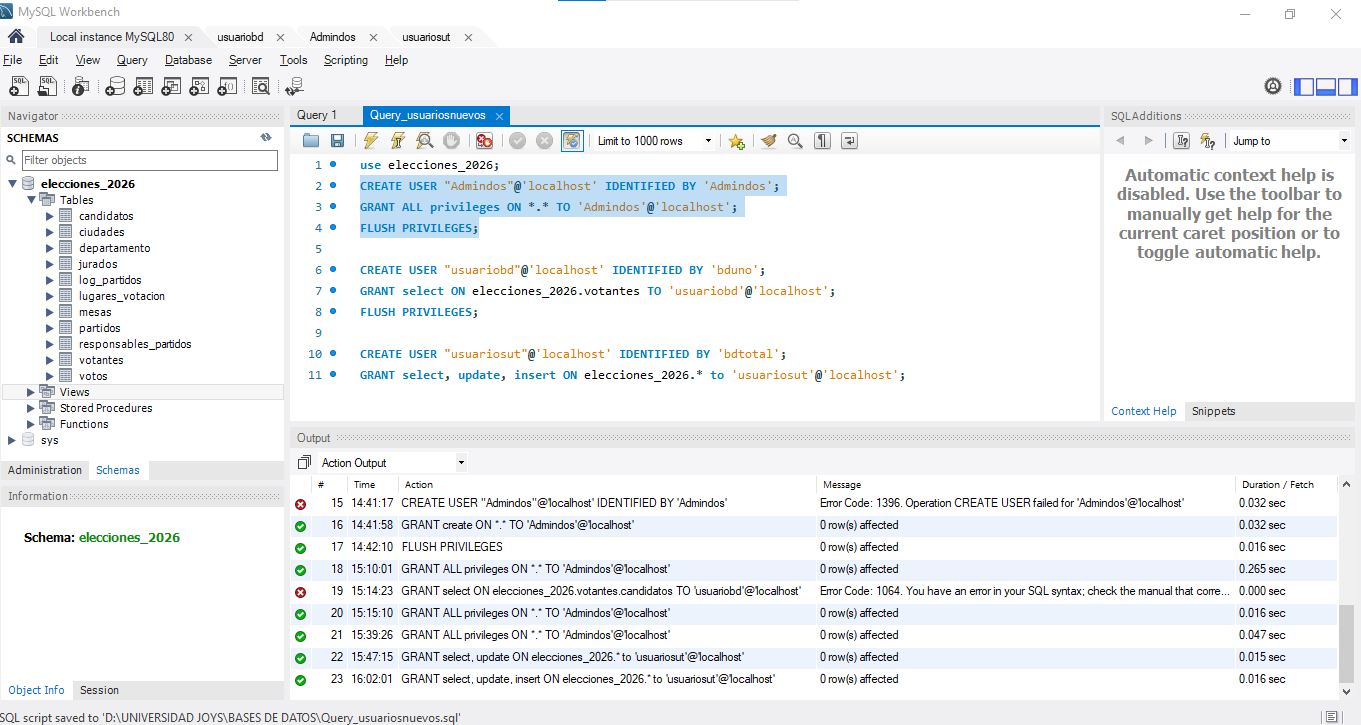
En la era digital, la seguridad de las bases de datos se ha convertido en un pilar esencial para proteger la integridad, confidencialidad y disponibilidad de la información, un activo invaluable en el mundo actual. Dado que estas almacenan datos sensibles y críticos, es fundamental implementar medidas que las resguarden contra accesos no autorizados, pérdidas y ataques cibernéticos. Este documento explora estrategias clave para fortalecer la protección de una base de datos MySQL, incluyendo la configuración de contraseñas robustas, la creación de perfiles de acceso personalizados, la realización de copias de seguridad y la adopción de opciones de seguridad adicionales. Además, se aborda la publicación segura de la base de datos en un entorno web, garantizando un acceso controlado para usuarios administrativos y clientes finales. Con estas medidas, se busca no solo proteger los datos, sino también consolidar la confianza en los sistemas digitales.

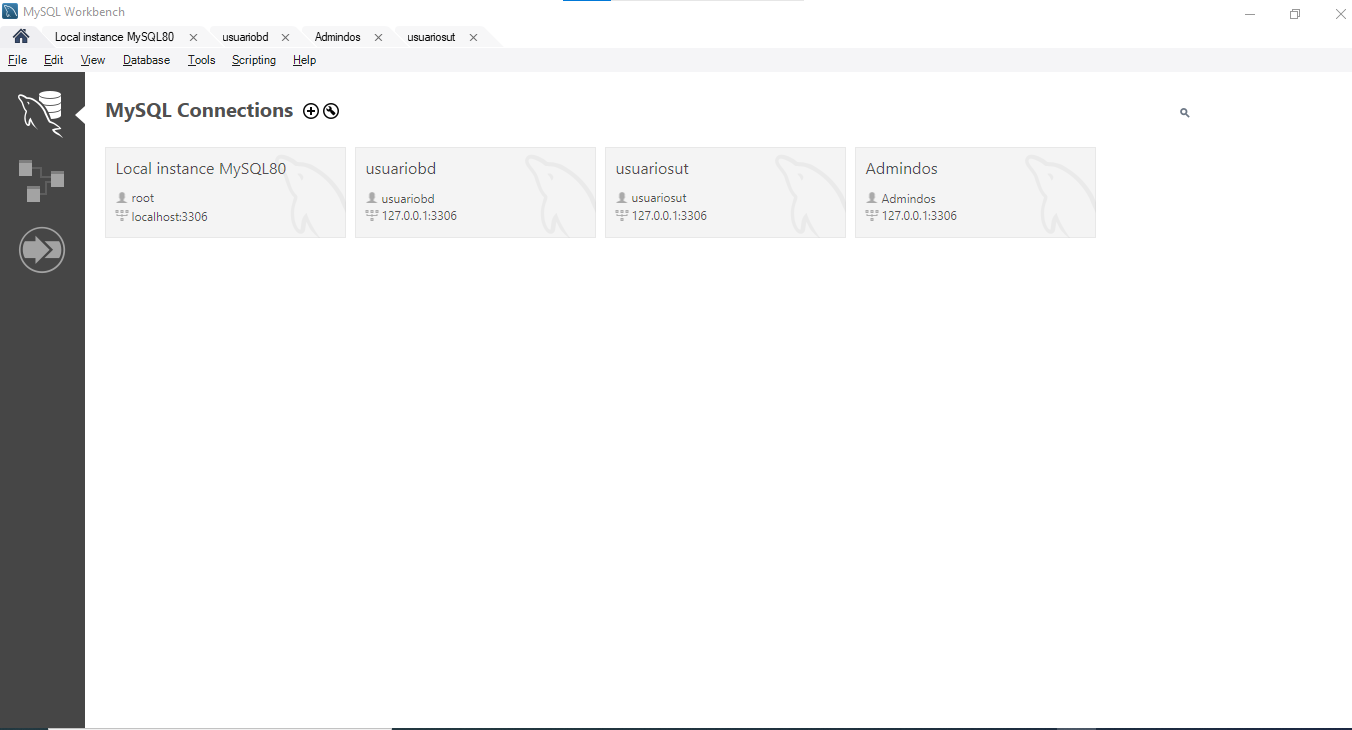
# CLAVE PARA INGRESO A LA BASE DE DATOS

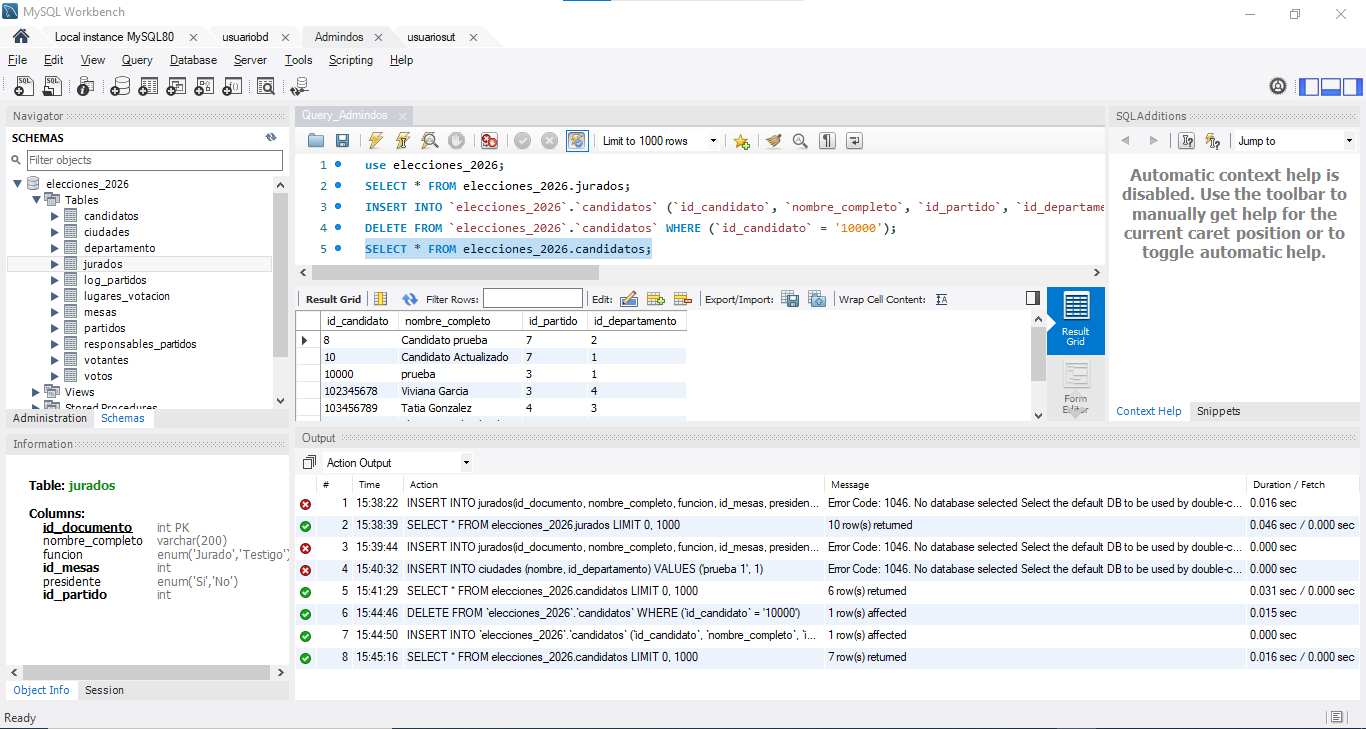
CREATE USER "Admindos"@'localhost' IDENTIFIED BY 'Admindos';

GRANT ALL privileges ON \*.\* TO 'Admindos'@'localhost';

FLUSH PRIVILEGES;





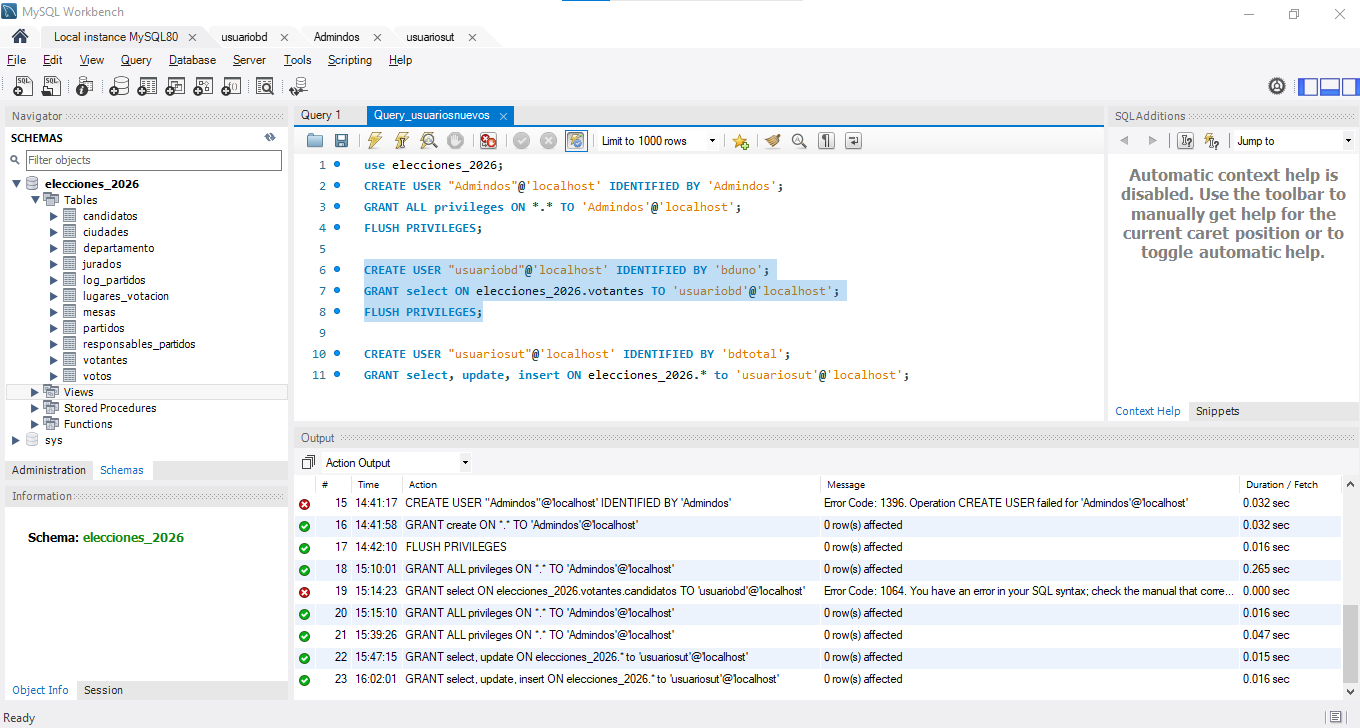


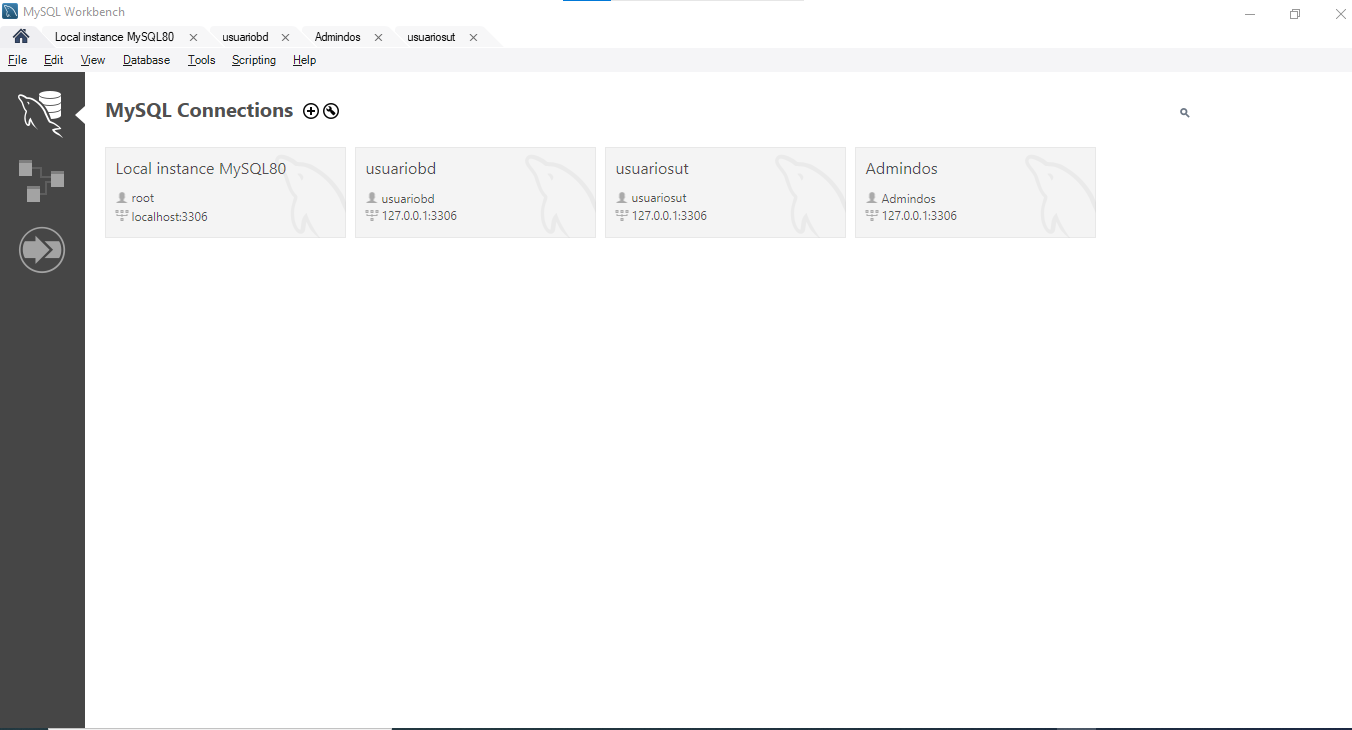
# CREACIÓN DE PERFILES DE ACCESO A LA BASE DE DATOS.

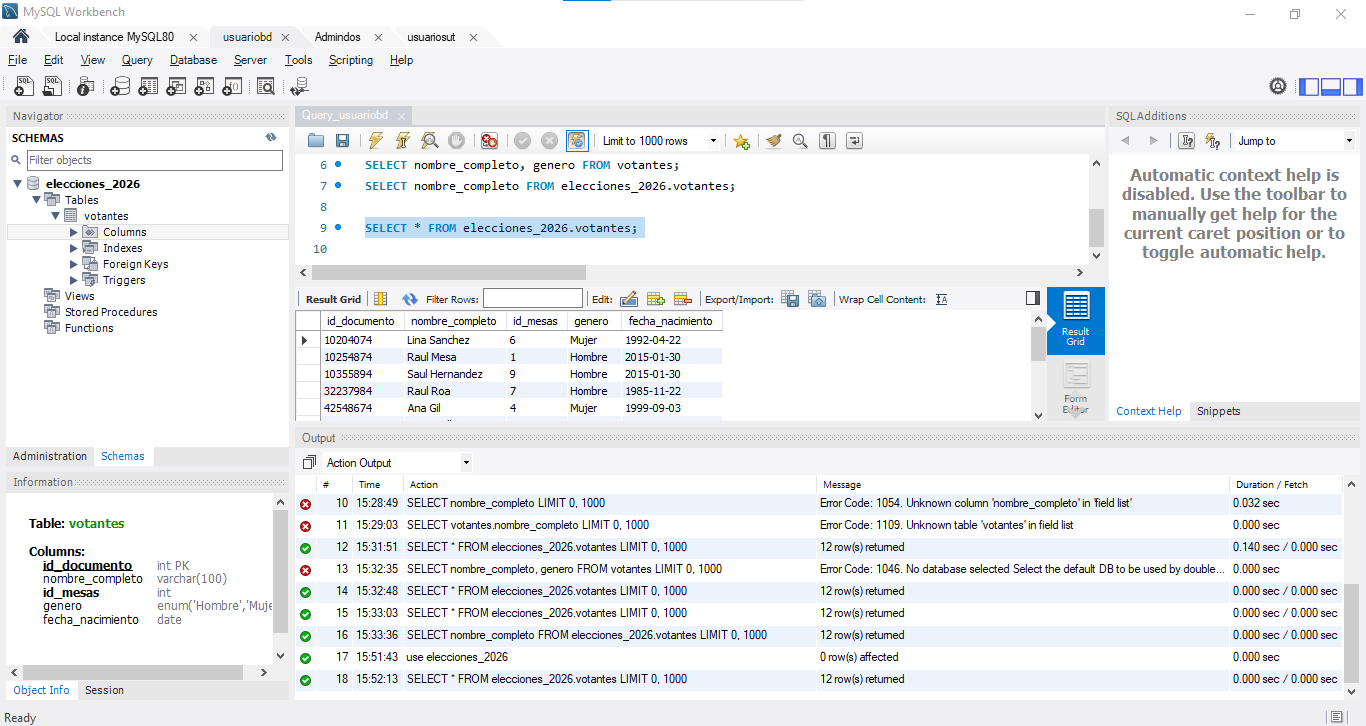
CREATE USER "usuariobd"@'localhost' IDENTIFIED BY 'bduno';

GRANT select ON elecciones\_2026.votantes TO 'usuariobd'@'localhost';

FLUSH PRIVILEGES;

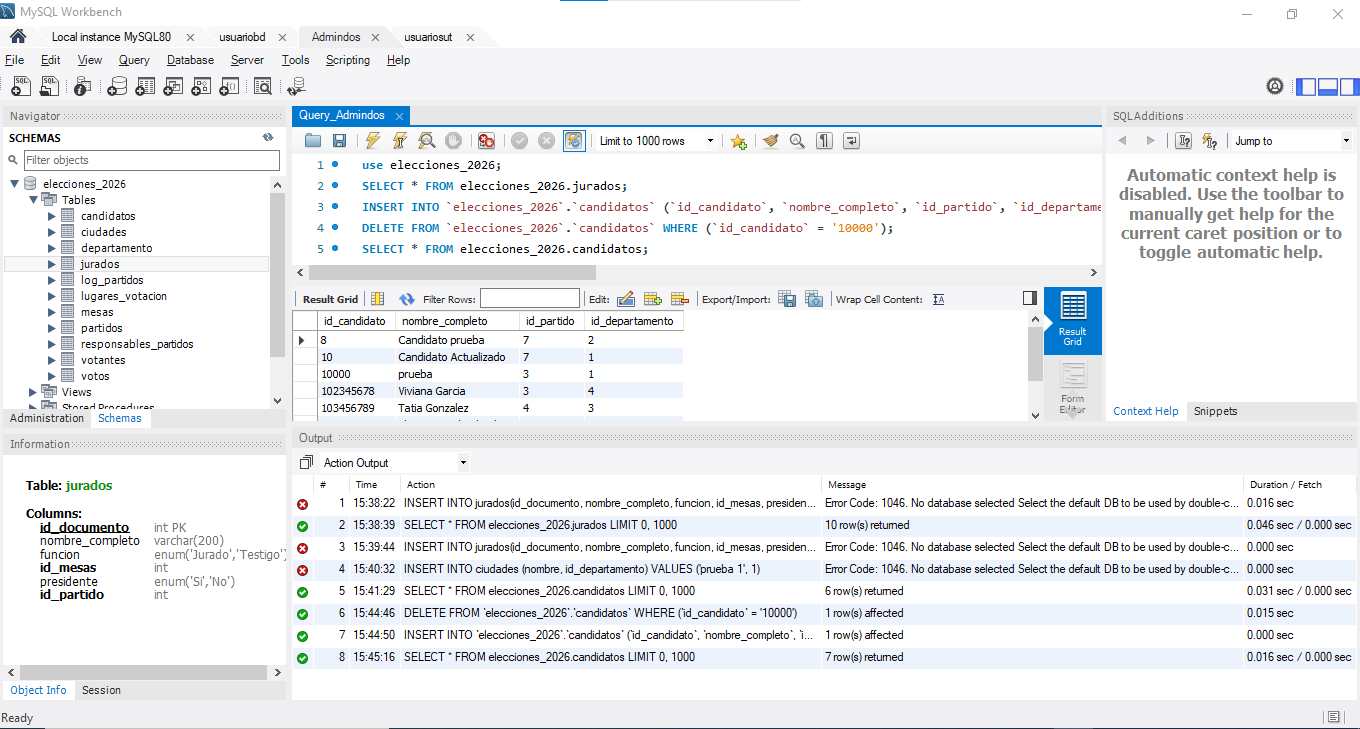






CREATE USER "usuariosut"@'localhost' IDENTIFIED BY 'bdtotal';

GRANT select, update, insert ON elecciones\_2026.\* to 'usuariosut'@'localhost';



# Explicar cómo se hace la copia de seguridad (Backup) en la base de datos y hacer una copia de está.

La actividad queda registrada en el video y se envía copia con el documento.

# ¿QUÉ MÁS OTRAS OPCIONES DE SEGURIDAD IMPLEMENTARÍA EN LA BASE DE DATOS?

Para mejorar la seguridad de una base de datos, además de las medidas básicas como contraseñas fuertes y cifrado, podríamos implementar:

* **Autenticación multifactor (MFA):** Exigir más de un método de verificación (como una contraseña y un código enviado al teléfono) para acceder a la base de datos, reduciendo el riesgo de accesos no autorizados.
* **Cifrado de datos en reposo y en tránsito:** Usar algoritmos como AES-256 para proteger los datos almacenados y protocolos como TLS para asegurar las comunicaciones entre la base de datos y las aplicaciones.
* **Auditorías y monitoreo continuo:** Registrar todas las actividades (inicios de sesión, consultas, cambios) y configurar alertas para detectar comportamientos sospechosos, como intentos de acceso fallidos repetidos.
* **Enmascaramiento de Datos** Oculta información sensible en entornos de prueba o desarrollo, mostrando solo datos ficticios o enmascarados. Esto evita que datos reales se expongan accidentalmente.
* **Parches y actualizaciones regulares:** Mantener el software de la base de datos actualizado para corregir vulnerabilidades conocidas.
* **Segmentación de red:** Usa firewalls para restringir el acceso a la base de datos desde redes no autorizadas. Implementa una **red privada virtual (VPN)** para accesos remotos seguros. Limita las conexiones a la base de datos solo a direcciones IP confiables.
* **Detección de intrusos y prevención (IDS/IPS):** Implementar sistemas que identifiquen y bloqueen intentos de explotación o ataques en tiempo real.
* **Políticas de retención y eliminación:** Definir cuánto tiempo se guardan los datos y eliminarlos de forma segura cuando ya no sean necesarios, minimizando riesgos de exposición.
* **Se puede implementar soluciones como:**
  + **Database Activity Monitoring (DAM)**: Para monitorear y analizar actividades en la base de datos.
  + **Data Loss Prevention (DLP)**: Para prevenir fugas de datos sensibles.
  + **Intrusion Detection Systems (IDS)**: Para detectar intentos de intrusión.

# CONCLUSIÓN

La seguridad en las bases de datos es un componente esencial para gestionar y proteger la información en la era digital. La implementación de una estrategia integral que combine contraseñas seguras, perfiles de acceso personalizados, copias de seguridad periódicas, cifrado de datos y auditorías de acceso garantiza la integridad, confidencialidad y disponibilidad de los datos frente a amenazas internas y externas. Publicar la base de datos en un entorno web, con medidas como validación de entradas y controles de acceso a nivel de aplicación, permite una gestión eficiente y segura, tanto para administradores como para usuarios finales. Este proceso, lejos de ser estático, exige una evaluación y actualización constantes para adaptarse a nuevas vulnerabilidades y tecnologías, consolidando así un sistema estable, confiable y protegido.