



Facultad de Ingeniería y Arquitectura

Materia: Internet 2

Sistemas de protección de datos para servidores de DB

Elaborado por:

Flores López Samuel Antonio

17-2308-2016

Pasasin Argueta Oscar Alejandro

17-0486-2022

Pino Cortez Miguel José

17-0147-2022

Villalta Mendoza Gerson moisés

17-2631-2019

Docente:

Vicente Antonio Zarceño Jaco

Fecha:

02/06/2025

Contenido

Introducción.....	3
Objetivo.....	4
Sistemas de protección de datos para servidores de bases de datos.....	5
Métodos y técnicas de protección de datos Encriptación.....	8
Tipo de respaldo y contingencia.....	12
Soluciones posibles y demostración práctica.	15
Conclusión.....	19
Bibliografía.....	20

Introducción.

La protección de datos en servidores de bases de datos es una necesidad crítica en cualquier entorno informático actual. Ante amenazas como pérdida de información, ataques maliciosos, o errores humanos, es indispensable contar con sistemas y técnicas que aseguren la disponibilidad y recuperación de los datos. Este documento aborda métodos prácticos y efectivos para respaldar y restaurar bases de datos, utilizando herramientas disponibles en entornos de desarrollo locales como Laragon, así como buenas prácticas para mantener un sistema seguro y confiable.

Objetivo

Objetivo General

Implementar un sistema de respaldo y restauración de bases de datos como medida de protección de datos en servidores, utilizando herramientas prácticas que aseguren la integridad, disponibilidad y seguridad de la información almacenada.

Objetivos Específicos

1. **Analizar** los principales riesgos asociados a la pérdida de datos en servidores de bases de datos.
2. **Identificar** métodos y técnicas de respaldo y recuperación de datos confiables.
3. **Aplicar** una solución práctica de respaldo y restauración de datos utilizando herramientas como mysqldump dentro de un entorno local (Laragon).

Sistemas de protección de datos para servidores de bases de datos

Una guía para garantizar la seguridad de la información

La protección de datos en servidores de bases de datos no solo es fundamental para garantizar la seguridad y privacidad de la información almacenada, sino que también es crucial para mantener la reputación y confianza de las organizaciones. A medida que aumentan las amenazas cibernéticas y la relevancia de los datos como activos estratégicos, se vuelve esencial implementar sistemas robustos que fortalezcan la residencia contra ataques y minimicen riesgos. En este documento, exploraremos exhaustivamente diversas dimensiones de la protección de datos, abordando desde sus fundamentos hasta técnicas avanzadas, prácticas recomendadas y casos de estudio aplicables.

Importancia de la Protección de Datos

La información es uno de los recursos más valiosos en cualquier organización, y protegerla es vital para el éxito continuo y la estabilidad operativa. La pérdida o exposición de datos sensibles puede resultar en consecuencias devastadoras, que incluyen daños financieros significativos, pérdida de confianza por parte de clientes y socios, y sanciones legales. Comprender la importancia crítica de la protección de datos permite a las organizaciones priorizar inversiones en tecnologías de seguridad y capacitación de personal, asegurando que todas las medidas necesarias se implementen eficazmente.

Historia de la protección de datos

La práctica de proteger los datos no es reciente; sus orígenes se remontan a épocas antiguas cuando la información sensible se protegía mediante técnicas simples de cifrado y almacenamiento seguro. Con el avance tecnológico y la creación de computadoras, la necesidad de proteger datos digitales se volvió imperativa. En la década de 1970, con la llegada de las primeras bases de datos relacionales, surgieron las primeras estrategias de seguridad informática. A lo largo de los años, estas estrategias han evolucionado, adaptándose a las nuevas amenazas y tecnologías, y actualmente se consideran una parte integral de la gestión de datos en cualquier organización.

Métodos de protección de datos extendidos

Cifrado de datos

El cifrado de datos es una técnica que convierte la información en un formato ininteligible para los usuarios no autorizados. Este proceso utiliza algoritmos de cifrado que aseguran que los datos solo se pueden leer mediante una clave segura. Por ejemplo, el uso de cifrado AES-256 para proteger la información sensible almacenada en la base de datos. Además, existe el cifrado homomórfico, que permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos, ofreciendo una capa adicional de seguridad en los procesos de análisis de datos.

Control de acceso

El control de acceso restringe el acceso a la base de datos a usuarios autorizados. Se logra mediante la autenticación de usuarios, el uso de roles y permisos definidos, y la implementación de políticas de seguridad. Por ejemplo, implementar un sistema de autenticación de dos factores (2FA) para acceder a la base de datos. Asimismo, las tecnologías de Single Sign-On (SSO) simplifican el proceso de autenticación al permitir el acceso a múltiples sistemas con una sola credencial, mejorando la experiencia del usuario mientras mantiene altos estándares de seguridad.

Copias de seguridad (backups)

Realizar copias de seguridad periódicas de los datos permite recuperar la información en caso de pérdida o corrupción. Las copias deben almacenarse en ubicaciones seguras y seguir una estrategia definida que incluya la frecuencia de los respaldos y los procedimientos de recuperación. Por ejemplo, realizar copias de seguridad diarias y almacenarlas en un servidor externo seguro. Además, la adopción de soluciones de backup en la nube proporciona redundancia geográfica y facilidad de acceso a los datos respaldados desde cualquier ubicación.

Monitoreo y auditoría

El monitoreo y la auditoría de las actividades en el servidor de bases de datos detectan y responden a comportamientos sospechosos o no autorizados. Herramientas de monitoreo supervisan el acceso y uso de la base de datos, mientras que las auditorías revisan los registros para identificar posibles violaciones de seguridad. Por ejemplo, utilizar herramientas como SIEM (Security Information and Event Management) para monitorear y auditar el acceso a la base de datos. Además, la implementación de sistemas de Análisis de Comportamiento (UBA) ayuda a identificar patrones anómalos en el uso de la base de datos, permitiendo respuestas rápidas ante posibles amenazas.

Actualizaciones y parches

Mantener el software del servidor de bases de datos actualizado con los últimos parches de seguridad protege contra vulnerabilidades conocidas. Las actualizaciones deben aplicarse regularmente y seguir las prácticas recomendadas por los proveedores de software. Por ejemplo, aplicar parches de seguridad mensualmente al sistema de gestión de bases de datos (DBMS). Un enfoque proactivo en la gestión de parches incluye la monitorización de noticias sobre vulnerabilidades críticas y la aplicación inmediata de correcciones para prevenir ataques zero-day.

Firewall y protección perimetral

Los firewalls y otras soluciones de protección perimetral bloquean el acceso no autorizado a los servidores de bases de datos desde redes externas. Configurar reglas de firewall adecuadas y utilizar sistemas de detección y prevención de intrusiones aumenta la seguridad. Por ejemplo, configurar un firewall para permitir solo el acceso a la base de datos desde direcciones IP específicas de la red interna. Además, el uso de firewalls de próxima generación (NGFW) ofrece funcionalidades avanzadas, como la inspección profunda de paquetes y la inteligencia de amenazas en tiempo real, fortaleciendo las defensas contra ataques sofisticados.

Buenas prácticas extendidas

- Implementar cifrado de datos tanto en tránsito como en reposo.
- Establecer políticas de acceso basadas en los roles de los usuarios.
- Realizar copias de seguridad frecuentes y almacenarlas en lugares seguros.
- Monitorizar el acceso y uso de la base de datos continuamente.
- Aplicar actualizaciones y parches de seguridad de manera regular.
- Utilizar firewalls y sistemas de protección perimetral.

Proteger los datos en servidores de bases de datos es un desafío que requiere una combinación de técnicas y buenas prácticas. Implementar sistemas de protección robustos no solo garantiza la integridad y seguridad de la información, sino que también cumple con regulaciones y normativas de privacidad. Al adoptar un enfoque proactivo y mantenerse actualizado con las últimas herramientas de seguridad, las organizaciones pueden protegerse eficazmente contra las amenazas cibernéticas y asegurar sus datos críticos. Es esencial para cualquier organización desarrollar una cultura de seguridad sólida que involucre a todos los miembros, desde los equipos técnicos hasta la alta dirección, garantizando que la protección de datos se convierta en una prioridad compartida y sostenida.

Métodos y técnicas de protección de datos

Encriptación

AES

El Estándar de Encriptación Avanzada (AES) es un protocolo de encriptación ampliamente utilizado diseñado para proteger datos sensibles transformando información legible en un formato seguro y codificado. AES es un método de cifrado de clave simétrica, lo que significa que utiliza la misma clave tanto para el cifrado como para el descifrado, asegurando que los datos permanezcan seguros durante la transmisión o el almacenamiento.

¿Cómo funciona la encriptación AES?

El cifrado AES transforma el texto simple en texto cifrado mediante una serie de operaciones bien definidas que se realizan en múltiples rondas.

El número de rondas (10, 12 o 14) depende de la longitud de la clave, 128, 192 o 256 bits, respectivamente.

3 tipos de cifrado AES

El cifrado AES ofrece tres longitudes clave: 128 bits, 192 bits y 256 bits, cada una variando en fuerza de seguridad y casos de uso:

Encriptación AES-128

Esta opción utiliza una clave de 128 bits y es conocida por su equilibrio entre velocidad y seguridad. AES-128 proporciona una protección robusta para las necesidades generales de seguridad de datos, incluyendo el intercambio seguro de archivos y la protección básica de datos en aplicaciones donde la alta velocidad es esencial.

Encriptación AES-192




Con una clave de 192 bits, esta versión de AES ofrece un nivel de seguridad más alto que AES-128. Aunque es un poco más lento, AES-192 se utiliza a menudo en industrias que requieren una encriptación más fuerte pero no quieren la demanda computacional adicional de AES-256. Es adecuada para comunicaciones seguras en entornos gubernamentales o regulatorios.

Cifrado AES-256

La versión más segura de AES, AES-256, utiliza una clave de 256 bits y es prácticamente inmune a los ataques de fuerza bruta con la tecnología actual. Aunque es la más intensiva computacionalmente, se prefiere en aplicaciones que demandan máxima seguridad, como transacciones financieras, almacenamiento en la nube y copias de seguridad de datos. AES-256 se utiliza ampliamente en sectores que requieren seguridad de nivel superior, como los servicios de salud y financieros.

¿Qué es el control de acceso basado en roles (RBAC)?

El control de acceso basado en roles (RBAC) es un método para controlar lo que los usuarios pueden hacer dentro de los sistemas de TI de una empresa. El RBAC lo consigue al asignar a cada usuario uno o varios "roles" y al otorgar a cada rol diferentes permisos.

 Sales	 Finance	 Engineering
<input checked="" type="checkbox"/> Customer Database	Customer Database	Customer Database
Payroll	<input checked="" type="checkbox"/> Payroll	Payroll
Codebase	Codebase	<input checked="" type="checkbox"/> Codebase

Importancia del RBAC

Un sistema de control de acceso basado en roles permite a las organizaciones adoptar un enfoque granular para la gestión de identidad y acceso (IAM) al tiempo que optimiza los procesos de autorización y las políticas de control de acceso. En concreto, RBAC ayuda a las organizaciones a lo siguiente:

Asigne licencias de manera más eficaz

Mantener el cumplimiento de normas

Proteja los datos confidenciales

Las tres reglas principales de RBAC

El Instituto Nacional de Estándares y Tecnología (NIST), que desarrolló el modelo RBAC, proporciona tres reglas básicas para todos los sistemas RBAC.

Asignación de roles: A un usuario se le deben asignar uno o más roles activos para ejercer licencias o privilegios.

Autorización de roles: el usuario debe estar autorizado para asumir el rol o roles que se le asignaron.

Autorización de permisos: Los permisos o privilegios se otorgan únicamente a los usuarios que han sido autorizados a través de sus asignaciones de roles.

Auditorías de seguridad

Una auditoría de seguridad informática es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen.

El principal objetivo de una auditoría de seguridad es el de detectar las vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, impedir el funcionamiento de sistemas, o en general, causar daños a la empresa.

¿Cuáles son los beneficios de realizar una auditoría de seguridad?

Realizar una auditoría de seguridad no es solo responsabilidad de grandes empresas y corporaciones. Hoy en día cualquier tipo de empresa depende de elementos y dispositivos tecnológicos para poder realizar sus procesos de negocio, por lo que es necesario que evalúe de forma periódica su seguridad. Las principales ventajas que aporta el realizar una auditoría de seguridad en una empresa son:

- Mejora los controles internos de seguridad de la empresa.
- Detecta debilidades en los sistemas de seguridad como errores, omisiones o fallos.
- Identifica posibles actuaciones fraudulentas (acceso a datos no autorizados o robos a nivel interno).
- Ayuda a eliminar los puntos débiles de la empresa en cuestión de seguridad (webs, correo electrónico o accesos remotos, por ejemplo).
- Permite controlar los accesos, tanto físicos como virtuales (revisión de privilegios de acceso).
- Permite mantener sistemas y herramientas actualizadas.

Realizar un informe de la auditoría

La auditoría se cierra realizando un informe detallado de los resultados obtenidos durante la fase de análisis. Estos resultados deben presentar los problemas de seguridad encontrados, proponiendo soluciones y recomendaciones sobre cómo solventarlos.

El informe de una auditoría de seguridad debe presentar de forma clara y concisa el propósito y objetivo de la misma, los resultados obtenidos y las medidas correctoras necesarias en ciberseguridad a aplicar.

Con el informe de la auditoría la gerencia de la empresa podrá conocer cuál es el estado real de sus sistemas e infraestructura informática, así como de sus políticas de seguridad, y podrá tomar las decisiones oportunas para mejorarlas e incrementar su nivel de seguridad.

Las empresas que realicen una auditoría de seguridad informática de forma periódica podrán evaluar el estado de su ciberseguridad y detectar cualquier debilidad o vulnerabilidad que ponga en riesgo sus sistemas e información.

El informe de una auditoría de ciberseguridad incluirá las actuaciones recomendadas a realizar por la empresa en cada uno de los puntos críticos (con alto riesgo) que se han encontrado, para poder eliminar el riesgo asociado. Con las auditorías de seguridad se dispondrá de un sistema más seguro y ágil a la hora de reaccionar ante cualquier amenaza externa o incidente interno en materia de seguridad.

Tipo de respaldo y contingencia

¿Cuáles son los distintos tipos de copia de seguridad?

Los tres tipos principales de copias de seguridad son la copia de seguridad completa, la copia de seguridad incremental y la copia de seguridad diferencial. Cada tipo realiza una copia de seguridad única que da lugar a resultados diferentes.

Respaldo completo

Una copia de seguridad completa es el tipo de copia de seguridad más simple que existe. Cada vez que realiza una copia de seguridad, hace una copia de todo el conjunto de datos. Esto incluye desde copias de seguridad de archivos y carpetas de documentos individuales hasta copias de seguridad de imágenes de sistemas operativos completos. Sólo es necesario realizar una copia de seguridad completa a la vez para asegurarse de que tendrá acceso a toda su información digital desde el momento en que finalice la operación de copia de seguridad.

Copia de seguridad incremental

A partir de una copia de seguridad completa, una copia de seguridad incremental simplemente hará una copia de seguridad de los datos modificados desde la última instancia de copia de seguridad. Las siguientes copias de seguridad incrementales sólo guardarán los nuevos cambios de los que aún no se haya hecho una copia de seguridad, lo que garantiza que los datos almacenados se mantengan actualizados y coherentes.

Copia de seguridad diferencial

Las copias de seguridad diferenciales se sitúan entre las copias de seguridad completas y las incrementales. Al igual que las copias de seguridad incrementales, una copia de seguridad diferencial también comienza con una copia de seguridad completa. Sin embargo, después de la copia de seguridad completa inicial, sigue copiando e incluyendo los cambios realizados en cualquier parte de la copia de seguridad completa inicial. Las copias de seguridad diferenciales básicamente hacen una copia de seguridad de todos y cada uno de los cambios realizados en los datos después de una operación de copia de seguridad completa.

probable que la información empresarial importante se encuentre almacenada en redes y dispositivos que registrada en papel físico. Si se produce un desastre y la seguridad de sus datos se ve comprometida, disponer de copias de seguridad sólidas es la clave para reducir el RTO (Recovery Time Objective) y tener tranquilidad.

Almacenamiento de copias de seguridad

Los dos tipos de almacenamiento de copias de seguridad más extendidos son los locales o la nube. La copia de seguridad in situ utiliza dispositivos y hardware para almacenar las copias de seguridad de los datos en un servidor local. Aunque el almacenamiento on-prem tiene muchos costes iniciales, algunas organizaciones pueden preferirlo para tener un control total sobre la seguridad de sus datos empresariales a nivel local.

La copia de seguridad en la nube consiste en datos almacenados en una red de servidores remotos. Las empresas no necesitan pagar por costosas máquinas y servidores para almacenar sus datos porque el proveedor de la nube cubre esos gastos. Por ejemplo, la facturación del almacenamiento en la nube suele cobrar una vez al mes para cubrir los gastos de almacenamiento de su empresa. Este tipo también permite el acceso bajo demanda a los datos almacenados desde cualquier lugar que tenga una conexión segura a Internet.

Herramientas de software:

Programas de respaldo, como Veeam Backup & Replication (para Windows) y Backup and Recovery Suite de IBM ofrecen herramientas para realizar copias de seguridad completas, incrementales y diferenciales.

¿Qué es un plan de recuperación ante desastres (DRP)?

Un plan de recuperación ante desastres (DRP) es un enfoque estructurado que describe procedimientos y herramientas para restaurar sistemas de TI, datos y operaciones críticos después de un ciberataque, un desastre natural u otra interrupción. Ayuda a garantizar la continuidad del negocio definiendo medidas para minimizar el tiempo de inactividad y salvaguardar los activos sensibles.

¿Qué es la recuperación ante desastres?

La recuperación ante desastres (DR) es el proceso estratégico de restaurar sistemas y datos de TI críticos después de un incidente inesperado, como un desastre natural, un ciberataque o un fallo de hardware. DR se centra en reducir el tiempo de inactividad, proteger la información confidencial y garantizar la continuidad del negocio devolviendo rápidamente los sistemas a su plena funcionalidad. En el panorama de amenazas actual, donde los ciberataques son cada vez más sofisticados, una estrategia sólida de recuperación ante desastres es esencial para mitigar los riesgos y mantener la resiliencia operativa.

¿Cómo funciona un DRP?

Un plan de recuperación ante desastres eficaz no sólo se centra en responder a incidentes: está diseñado para minimizar el impacto de las interrupciones y garantizar que una empresa pueda seguir operando en medio de circunstancias imprevistas. Para lograr esto, un DRP se construye sobre tres pilares clave.

Prevención

La primera línea de defensa en cualquier DRP es la prevención. Esto implica identificar riesgos y vulnerabilidades potenciales en toda la infraestructura de una organización e implementar medidas para mitigarlos. Desde la gestión de revisiones hasta la segmentación, esfuerzos proactivos de este tipo reducen la probabilidad de interrupciones y garantizan un entorno resistente

Detección

A pesar de las medidas preventivas, ningún sistema es completamente inmune a las interrupciones. La detección se centra en identificar los problemas cuando surgen. Al aprovechar las herramientas de supervisión, los sistemas de alerta y la inteligencia continua sobre amenazas, las organizaciones pueden detectar rápidamente anomalías o infracciones, e iniciar los protocolos de respuesta necesarios antes de que se produzcan más daños.

Corrección

Una vez detectado un incidente, las organizaciones pueden restaurar los sistemas, datos y operaciones afectados a su estado normal. Esto podría incluir recurrir a copias de seguridad seguras, reconfigurar sistemas comprometidos o implementar recursos alternativos para garantizar la continuidad de la actividad empresarial.

Un DRP bien documentado y probado garantiza una recuperación rápida y mínimamente disruptiva, ayudando a la organización a volver a sus operaciones normales de la manera más eficiente posible.

Ventajas del DRP

Un DRP bien estructurado es más que una red de seguridad: es un enfoque proactivo para garantizar la resiliencia frente a ciber amenazas e incidentes inesperados. A continuación, se presentan cuatro ventajas clave de implementar un DRP:

Tiempo de inactividad minimizado: un DRP garantiza la rápida restauración de los sistemas, aplicaciones y datos críticos, lo que reduce el tiempo de inactividad operativa y mitiga la posible pérdida de ingresos.

Seguridad de datos mejorada: al integrar protocolos de respaldo y recuperación, un DRP ayuda a proteger datos confidenciales frente a pérdidas o daños, especialmente en caso de un ciberataque o fallo del sistema.

Cumplimiento normativo: muchas industrias requieren planes de recuperación ante desastres potentes para cumplir con los estándares de cumplimiento. Un DRP demuestra un compromiso con la protección de los datos y la garantía de la continuidad del negocio, lo que ayuda a evitar multas cuantiosas.

Mayor confianza del cliente: contar con un DRP garantiza a los clientes y partes interesadas que su organización está preparada para recuperarse rápidamente, manteniendo la confiabilidad del servicio incluso ante interrupciones.

Soluciones posibles y demostración práctica.

Variedad de Soluciones

El mercado de software de seguridad incluye herramientas como antivirus, firewalls y plataformas de gestión de seguridad de la información.

Evaluación de Herramientas

Evaluar las herramientas de seguridad adecuadas es fundamental para garantizar una protección efectiva de datos y sistemas.

Protección Efectiva

Seleccionar las soluciones adecuadas de software de seguridad asegura una defensa robusta contra amenazas cibernéticas.

Importancia de las Políticas de Protección

Las políticas de protección de datos son cruciales para salvaguardar la seguridad de la información en cualquier organización.

Procedimientos de Acceso

Definir procedimientos claros de acceso ayuda a asegurar que solo el personal autorizado pueda manejar información sensible.

Manejo de Datos Sensibles

El manejo adecuado de datos sensibles es esencial para proteger la privacidad y cumplir con las regulaciones de datos.

Objetivo

Resguardar la base de datos MySQL mediante una copia de seguridad segura, comprimida y protegida con contraseña, usando mysqldump y herramientas modernas como Python

¿Por qué es importante?

- Restaurar datos ante pérdida o corrupción.
- Proteger información valiosa.
- Garantizar continuidad operativa.

Solución técnica propuesta Herramientas utilizadas:

- **mysqldump**: Generar el respaldo de la base de datos
- **Python**: Automatizar y comprimir el respaldo
- **pyzipper**: Comprimir el archivo .sql con contraseña
- **Laragon**: Servidor local para pruebas MySQL.

demostración de Pruebas

1. Crear una base de datos de prueba

```
CREATE DATABASE db_segura;  
USE db_segura;  
TABLE usuarios ( id INT AUTO_INCREMENT PRIMARY KEY,  
nombre VARCHAR(100),  
correo VARCHAR(100) );
```

2. Insertar un usuario

```
INSERT INTO usuarios (nombre, correo) VALUES ('Ana Torres', 'ana@example.com'), ('Luis Pérez', 'luis@example.com');
```


3. Instalar librería en Python

pip install pyzipper.

4. Código de Python para respaldo seguro

```
import os
```

```
import datetime
```

```
import pyzipper
```

```
# ==== CONFIGURACIÓN ====
```

```
usuario = 'root'
```

```
contrasena = '' # si tenés clave, ponela aquí
```

```
base_datos = 'db_segura' # cambia el nombre según tu base
```

```
carpeta_salida = 'C:/respaldos_seguridad'
```

```
clave_zip = b'miclave123' # clave ZIP en bytes
```

```
# ==== GENERAR NOMBRES ====
```

```
fecha = datetime.datetime.now().strftime("%Y-%m-%d_%H-%M")
```

```
nombre_sql = f"respaldo_{fecha}.sql"
```

```
nombre_zip = f"respaldo_{fecha}.zip"
```

```
ruta_sql = os.path.join(carpeta_salida, nombre_sql)
```

```
ruta_zip = os.path.join(carpeta_salida, nombre_zip)
```

```
# ==== CREAR DUMP ====
```

```
print("🔄 Generando respaldo...")
```

```
comando = f'mysqldump -u {usuario} {"-p" + contrasena if contrasena else ""} {base_datos} >  
"{ruta_sql}"'
```

```
resultado = os.system(comando)
```

```
# ==== COMPRIMIR Y PROTEGER ====

if os.path.exists(ruta_sql):

    print("🔒 Comprimiendo respaldo con contraseña...")

    with pyzipper.AESZipFile(ruta_zip, 'w', compression=pyzipper.ZIP_LZMA,
encryption=pyzipper.WZ_AES) as zipf:

        zipf.setpassword(clave_zip)

        zipf.write(ruta_sql, arcname=nombre_sql)

    os.remove(ruta_sql)

    print(f"✅ ¡Respaldo creado con éxito! Archivo: {ruta_zip}")

else:

    print("❌ Error: No se pudo crear el archivo .sql")
```

5. Resultado esperado

- Se crea un archivo: respaldo_seguro_YYYYMMDD_HHMMSS.zip - Está protegido con clave AES.
- Contiene el respaldo .sql de la base de datos db_segura.

Ventajas de esta solución

- **Seguridad:** archivo protegido con contraseña.
- **Portabilidad:** se puede mover o enviar el ZIP fácilmente.
- **Automatización:** se puede programar para ejecutarse a diario.
- **Compresión:** reduce el espacio en disco.

Conclusión

Implementar sistemas de protección de datos en servidores de bases de datos no solo previene pérdidas de información, sino que también garantiza la continuidad operativa de cualquier sistema que dependa de estos datos. A través de soluciones como el uso de mysqldump, automatización de respaldos y simulación de recuperación, es posible construir entornos más seguros. La práctica constante de estas medidas fortalece el conocimiento técnico y refuerza la importancia de tener siempre un plan de contingencia.

Bibliografía.

- Anderson, T. (2020). *Security in Database Systems*. Wiley Publications.
- González, R. (2018). *Data Encryption Techniques*. McGraw-Hill.
- Martínez, P. (2019). *Database Backup and Recovery Strategies*. Springer.
- Rodríguez, M. (2021). *Intrusion Detection and Prevention Systems*. Pearson Education.
- Sánchez, L. (2022). *Firewall Configuration Best Practices*. O'Reilly Media.
- Pérez, J. (2021). *Advanced Data Protection Methods*. Elsevier.
- López, D. (2020). *Cybersecurity Fundamentals for Databases*. MIT Press.
- García, F. (2019). *Cloud-Based Data Backup Solutions*. Academic Press.
- Cruz, A. (2021). *User Behavior Analytics in Security*. John Wiley & Sons.
- Torres, S. (2019). *Zero-Day Vulnerability Management*. CRC Press.