



Seguridad y privacidad de la base de datos: Protección de su activo más valioso

Una guía completa para estudiantes y profesionales de informática

Agenda

Introducción

Contexto e importancia de la seguridad de las bases de datos en el mundo actual impulsado por los datos

Amenazas comunes

Comprendión de las vulnerabilidades y los ataques dirigidos a los sistemas de bases de datos

Medidas de protección

Soluciones técnicas y mejores prácticas para proteger los entornos de bases de datos

Marco legal

Reglamentos que rigen la privacidad de los datos y sus implicaciones

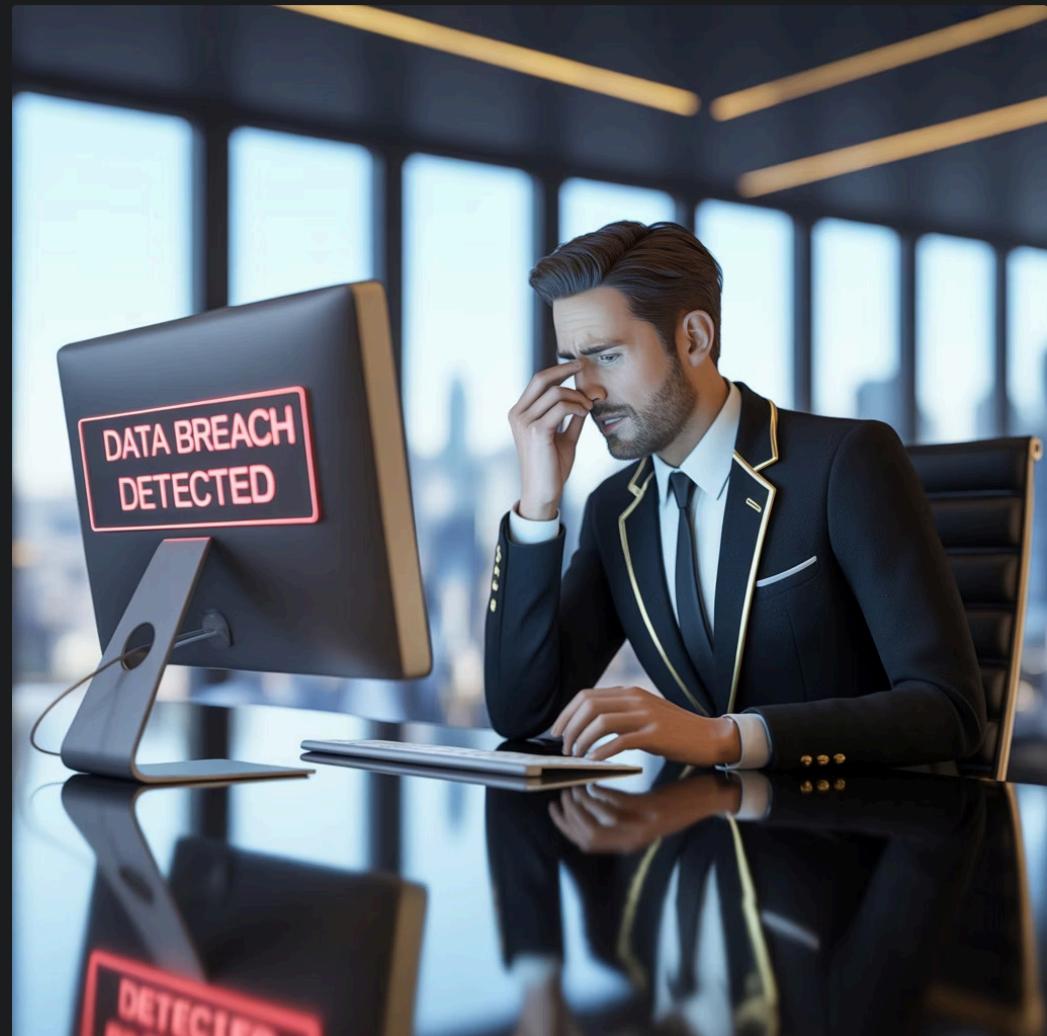
Al final de esta presentación, podrá identificar las amenazas comunes a las bases de datos, implementar herramientas de protección y navegar por el panorama legal de la privacidad de los datos.

Por qué es importante la seguridad de las bases de datos

En el panorama digital actual, los datos se han convertido en uno de los activos más valiosos para las organizaciones de todos los tamaños. Las bases de datos almacenan información crítica que impulsa las operaciones comerciales, contiene detalles personales y alberga propiedad intelectual.

Las consecuencias de las filtraciones de bases de datos se extienden más allá de las pérdidas financieras inmediatas e incluyen:

- Daño a la reputación y pérdida de la confianza del cliente
- Sanciones legales y multas regulatorias
- Interrupción operativa e interrupciones del servicio
- Desventaja competitiva por la filtración de información patentada



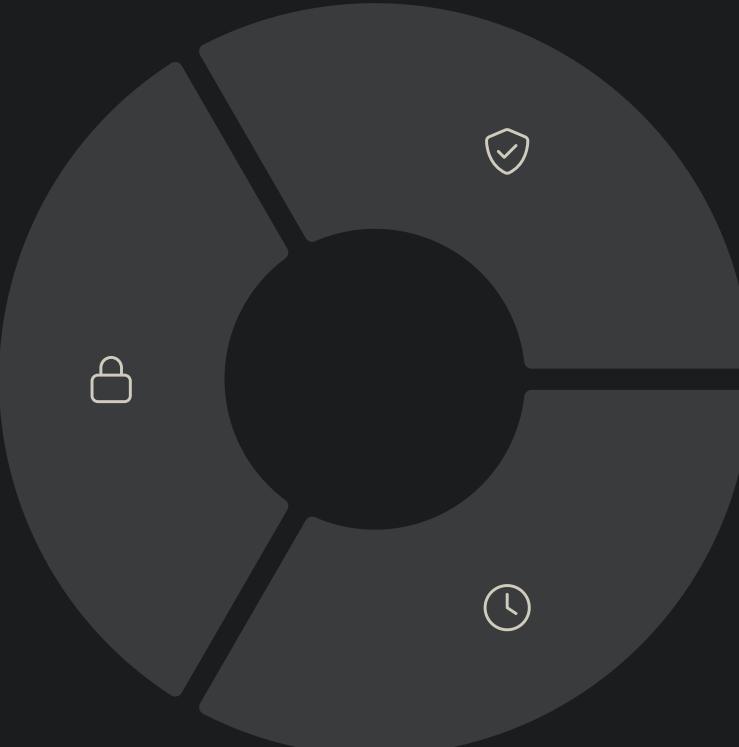
El costo promedio de una violación de datos alcanzó los \$4.45 millones en 2023, y la exposición de datos confidenciales se encuentra entre los tipos de incidentes de seguridad más comunes y costosos.

La tríada de seguridad para bases de datos

Confidencialidad

Garantizar que los datos sean accesibles solo para usuarios autorizados y evitar que la información confidencial se divulgue a terceros no autorizados.

- Controles de acceso
- Cifrado
- Enmascaramiento de datos



Integridad

Mantener la precisión y coherencia de los datos durante todo su ciclo de vida y evitar modificaciones no autorizadas.

- Sumas de comprobación
- Firmas digitales
- Restricciones y desencadenadores

Disponibilidad

Garantizar que los usuarios autorizados tengan acceso confiable y oportuno a los datos siempre que sea necesario.

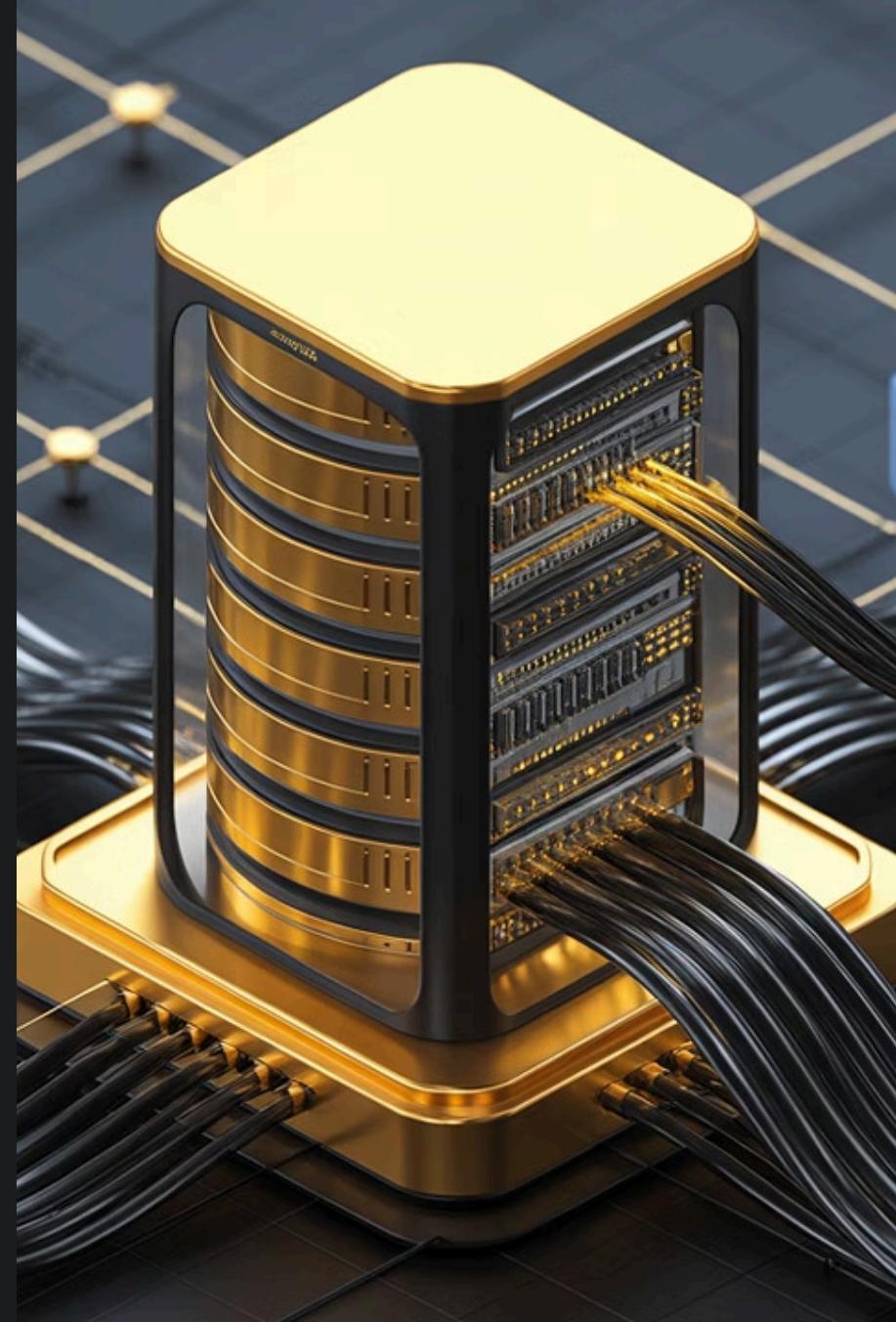
- Redundancia
- Copias de seguridad
- Recuperación ante desastres

Cualquier estrategia integral de seguridad de bases de datos debe abordar los tres componentes de esta tríada.

Amenazas comunes a las bases de datos

Los sistemas de bases de datos se enfrentan a una variedad de amenazas tanto de atacantes externos como de actores internos. Comprender estas amenazas es el primer paso para desarrollar contramedidas eficaces.

En las siguientes diapositivas, examinaremos las amenazas más importantes para la seguridad de las bases de datos y exploraremos sus implicaciones para las organizaciones que dependen de operaciones basadas en datos.



Acceso no autorizado

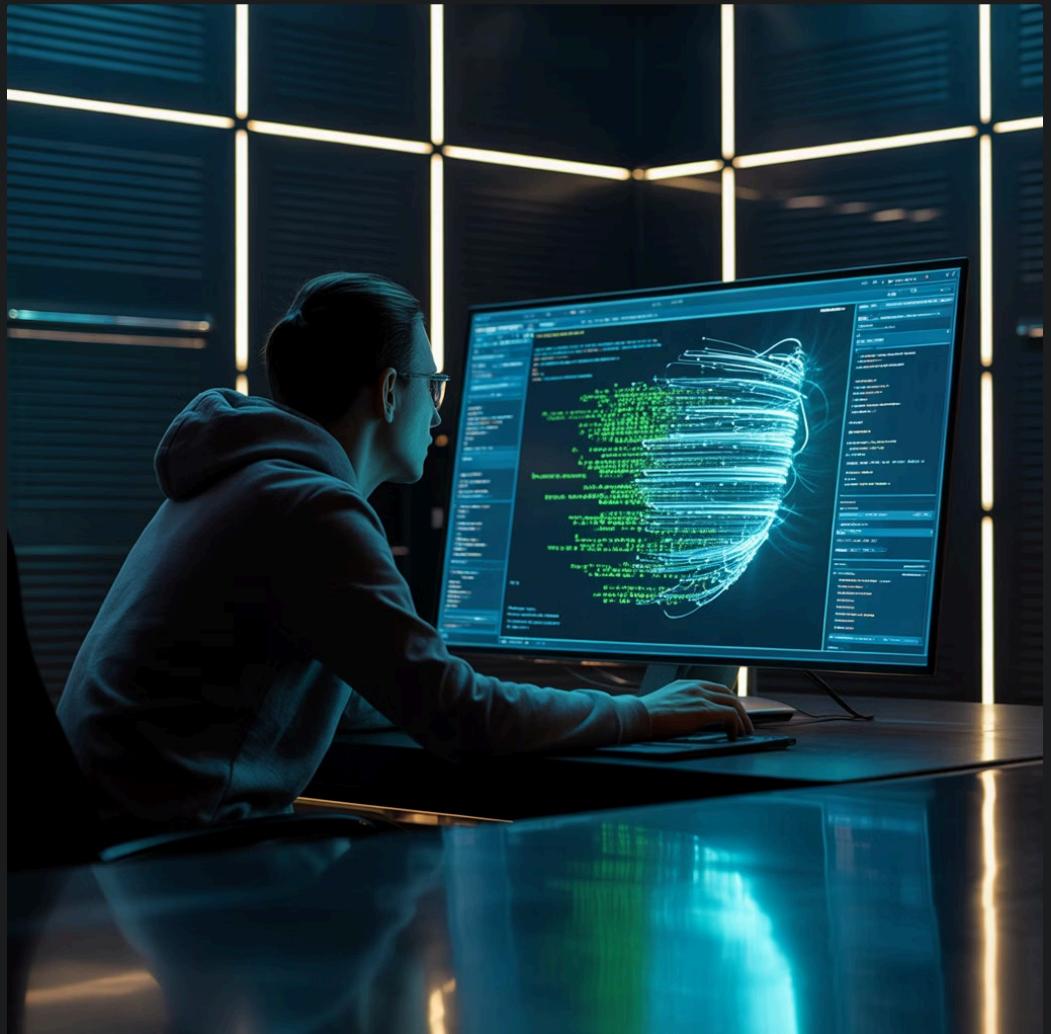
Qué es:

El acceso no autorizado ocurre cuando personas acceden a sistemas de bases de datos sin los permisos adecuados, lo que podría exponer información confidencial.

Vectores de ataque comunes:

- Credenciales débiles o robadas
- Secuestro de sesión
- Escalada de privilegios
- Contraseñas de base de datos predeterminadas/sin cambios

⊗ **Ejemplo del mundo real:** En 2019, una importante institución financiera experimentó una violación en la que un empleado accedió a registros de clientes sin autorización, exponiendo información personal y financiera de más de 100 millones de clientes.



Ataques de inyección SQL

1

¿Qué es la inyección SQL?

Una técnica de inyección de código donde se insertan sentencias SQL maliciosas en los campos de entrada para que el motor de la base de datos las ejecute.

2

Cómo funciona

Los atacantes manipulan los campos de entrada del usuario para injectar comandos SQL que modifican las consultas, omitiendo la autenticación o extrayendo datos.

3

Ejemplo de ataque

Nombre de usuario: admin' --

Contraseña: [cualquier cosa]

El operador de comentario (--) hace que la base de datos ignore la verificación de la contraseña.

4

Prevención

Utilice consultas parametrizadas, validación de entrada, procedimientos almacenados y marcos ORM. Implemente el principio del mínimo privilegio para las cuentas de la base de datos.



Pérdida y corrupción de datos

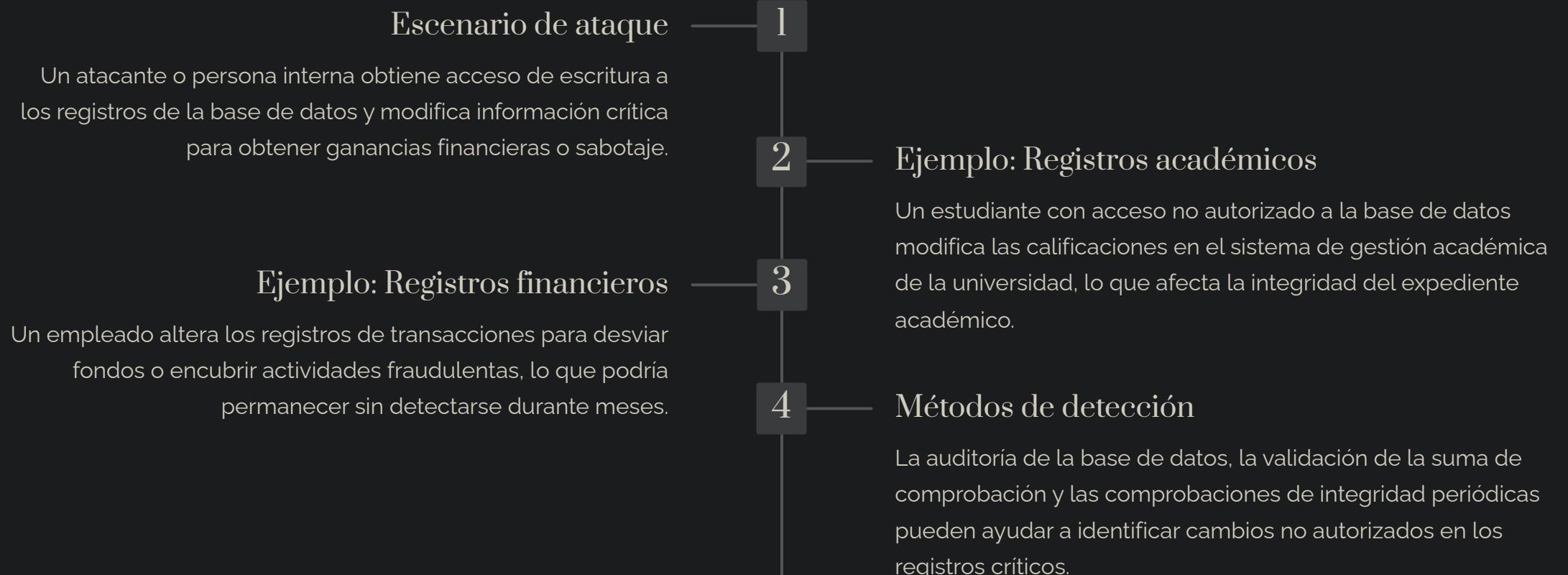
Causas:

- Fallos de hardware (fallos de disco, fallos de servidor)
- Errores de software o incompatibilidades
- Error humano (eliminaciones o modificaciones accidentales)
- Ataques maliciosos (ransomware, wipers)
- Desastres naturales que afectan a los centros de datos

Consecuencias:

- Interrupciones del servicio que afectan a las operaciones
- Pérdidas financieras por el tiempo de inactividad del negocio
- Daño a la reputación y pérdida de la confianza del cliente
- Problemas de cumplimiento legal y normativo
- Pérdida permanente de información irremplazable

Modificaciones no autorizadas



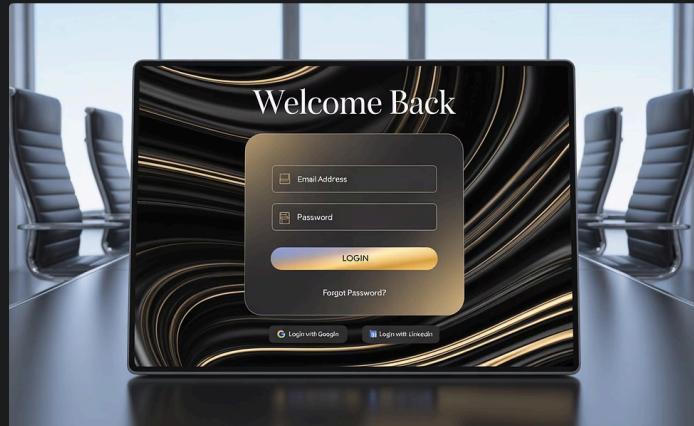
La integridad de los registros de la base de datos es particularmente crítica para los sistemas que sirven como fuentes autorizadas de información, como las bases de datos financieras, de atención médica o académicas.

Medidas de protección: Descripción general

La seguridad eficaz de la base de datos requiere un enfoque de múltiples capas que combine controles técnicos, políticas administrativas y concientización sobre la seguridad. Las siguientes diapositivas explorarán las medidas de protección clave que forman la base de una estrategia sólida de seguridad de la base de datos.



Mecanismos de autenticación



Basado en contraseñas

- Políticas de contraseñas seguras
- Rotación regular de contraseñas
- Bloqueo de cuenta después de intentos fallidos

Los sistemas de bases de datos modernos deben implementar múltiples factores de autenticación para verificar la identidad del usuario antes de otorgar acceso a datos confidenciales.



Autenticación de dos factores (2FA)

- Algo que sabes (contraseña)
- Algo que tienes (dispositivo)
- Aumenta significativamente la seguridad



Autenticación biométrica

- Reconocimiento de huellas dactilares
- Reconocimiento facial
- Escaneo de iris

Autorización y control de acceso

Principio del privilegio mínimo

A los usuarios se les deben otorgar solo los permisos mínimos necesarios para realizar las funciones de su trabajo. Esto limita el daño potencial de las cuentas comprometidas.

Control de acceso basado en roles (RBAC)

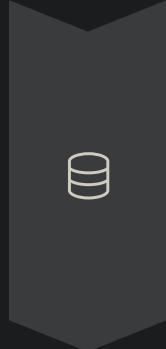
Los permisos se asignan a roles en lugar de usuarios individuales, lo que simplifica la administración y garantiza políticas de seguridad coherentes.

Seguridad a nivel de fila y columna

Controles de acceso detallados que restringen qué filas o columnas de datos puede ver o modificar un usuario en función de sus atributos o rol.

- | | |
|---|--|
| 1 | Administrador de la base de datos
Acceso completo a todos los objetos de la base de datos y funciones administrativas |
| 2 | Usuario de la aplicación
Acceso de lectura/escritura a tablas específicas a través de procedimientos almacenados predefinidos |
| 3 | Usuario de informes
Acceso de solo lectura a datos no confidenciales, a menudo a través de vistas que enmascaran campos confidenciales |
| 4 | Auditor
Acceso de solo lectura a registros y pistas de auditoría sin capacidad de modificar los datos |

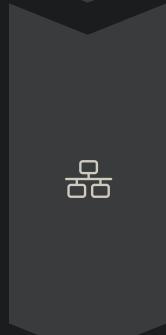
Cifrado de datos



Datos en reposo

Cifrado de archivos de bases de datos almacenados en el disco mediante TDE (Cifrado de datos transparente) o tecnologías similares.

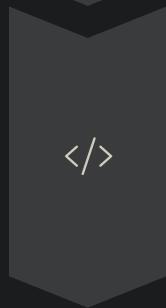
Protege contra el acceso no autorizado a los medios de almacenamiento físico o a los archivos de copia de seguridad.



Datos en tránsito

Cifrado de datos a medida que viajan entre la base de datos y las aplicaciones mediante protocolos como TLS/SSL.

Evita las escuchas ilegales y los ataques de intermediarios en las comunicaciones de red.



Datos en uso

Tecnologías emergentes para proteger los datos mientras se procesan en la memoria.

Incluye técnicas como el cifrado homomórfico y los enclaves seguros.

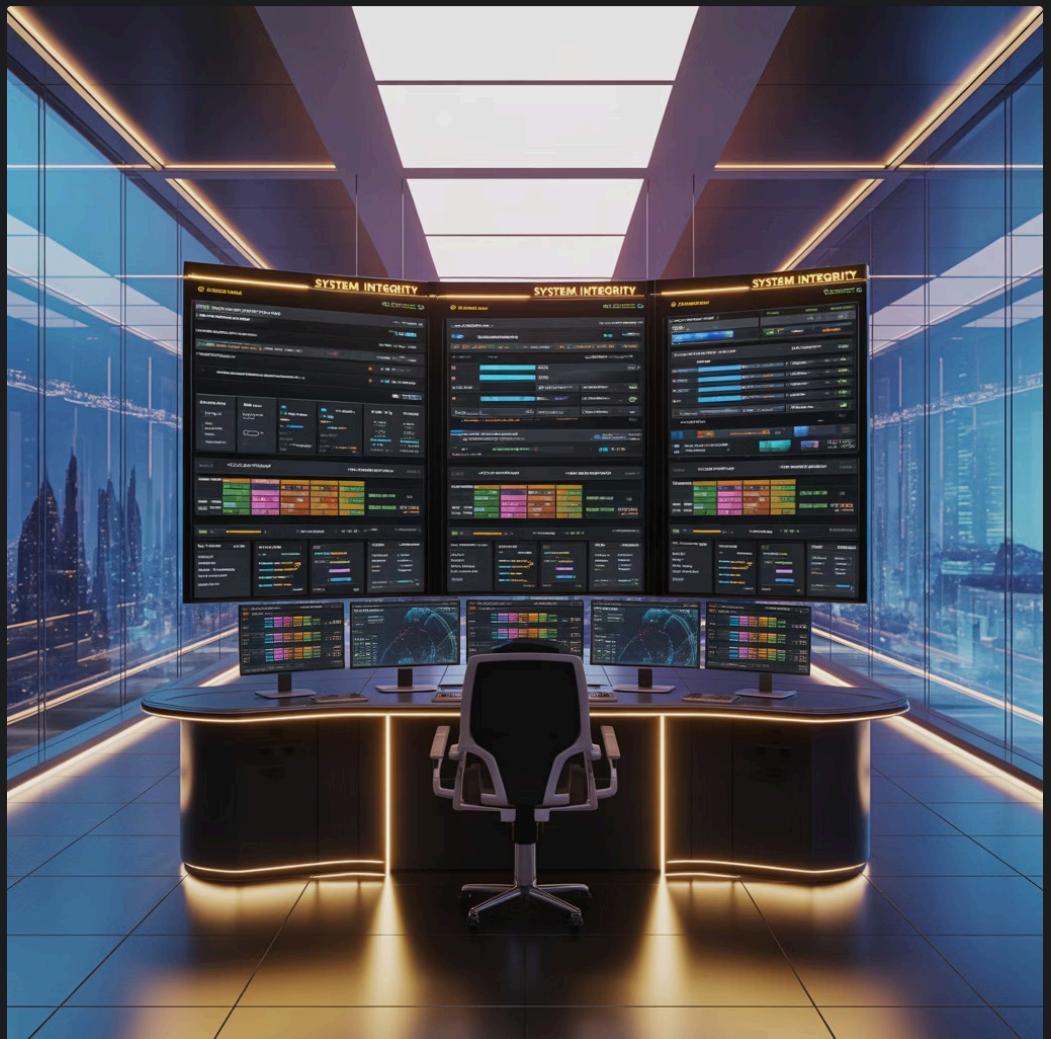


Auditoría y Monitoreo

Monitoreo de Actividad de la Base de Datos

El monitoreo en tiempo real de todas las acciones de la base de datos ayuda a detectar actividades sospechosas y proporciona un registro de auditoría para el análisis forense.

- Seguimiento de los inicios de sesión de los usuarios y los intentos de autenticación
- Monitoreo de los cambios de esquema y las acciones administrativas
- Registro de patrones de acceso a datos y ejecución de consultas
- Alertas sobre violaciones de políticas y comportamientos inusuales



ⓘ Mejores Prácticas: Implemente el análisis automatizado de los registros de auditoría de la base de datos utilizando herramientas de gestión de eventos e información de seguridad (SIEM) para identificar rápidamente posibles incidentes de seguridad.

Estrategias de respaldo y recuperación

Tipos de respaldo

- **Respaldo completo:** Copia completa de toda la base de datos
- **Respaldo diferencial:** Cambios desde el último respaldo completo
- **Respaldo incremental:** Cambios desde el último respaldo de cualquier tipo
- **Respaldo de registro de transacciones:** Registro de todas las transacciones

La regla 3-2-1

Mantenga al menos tres copias de datos en dos tipos de almacenamiento diferentes con una copia almacenada fuera del sitio o en la nube.

Planificación de la recuperación

- Defina el objetivo de punto de recuperación (RPO): pérdida de datos aceptable
- Defina el objetivo de tiempo de recuperación (RTO): tiempo de inactividad aceptable
- Pruebe periódicamente los procedimientos de recuperación
- Documente y automatice los procesos de recuperación





Marco Legal: Regulaciones de Privacidad de Datos

La seguridad de la base de datos no es solo una necesidad técnica, sino también un requisito legal. Varias leyes y regulaciones en todo el mundo exigen la protección de la información personal y confidencial.

Comprender los marcos legales aplicables es esencial para implementar medidas de seguridad de bases de datos que cumplan con las normas y evitar sanciones.

Regulaciones clave de privacidad de datos

Argentina: Ley 25.326

- Requisito de consentimiento informado
- Derecho a acceder, rectificar y eliminar datos personales
- Registro de bases de datos en la Dirección Nacional de Protección de Datos Personales
- Requisito de medidas de seguridad de datos

UE: RGPD

- Requisitos estrictos de consentimiento
- Derecho al olvido
- Portabilidad de datos
- Privacidad por diseño
- Sanciones significativas (hasta el 4% de los ingresos globales)

Otras regulaciones regionales

- Brasil: LGPD
- California: CCPA/CPRA
- Canadá: PIPEDA
- China: PIPL

El principio común en todas las regulaciones: las personas son dueñas de sus datos personales y tienen derechos con respecto a su recopilación, uso y protección.

Aplicaciones académicas de la privacidad de los datos

Protección de datos de los estudiantes

- Los registros académicos deben protegerse contra el acceso no autorizado
- La información personal de los estudiantes requiere el consentimiento explícito para ser compartida
- Las plataformas educativas deben implementar medidas de seguridad adecuadas

⚠ Importante: Las instituciones educativas deben equilibrar el acceso abierto al conocimiento con la protección de la información confidencial de los estudiantes.

Plataformas académicas comunes

- Sistemas de gestión del aprendizaje (Moodle)
- Sistemas de información estudiantil (SIU-Guaraní)
- Bases de datos y repositorios de investigación



Las instituciones educativas enfrentan desafíos únicos al equilibrar la libertad académica, la eficiencia administrativa y los requisitos de protección de la privacidad.

Caso de estudio: Análisis de violación de base de datos

El incidente

En 2019, una importante plataforma de redes sociales descubrió un acceso no autorizado a su base de datos de usuarios, exponiendo información personal de más de 500 millones de usuarios en todo el mundo.

Medidas preventivas

La implementación de una segmentación adecuada de la base de datos, una autenticación más sólida, una supervisión exhaustiva y la minimización de datos podrían haber evitado o limitado la infracción.

1

2

3

4

Lo que falló

Los controles de acceso inadecuados, el cifrado insuficiente de los datos confidenciales y la detección tardía de la intrusión permitieron a los atacantes extraer datos durante meses.

Consecuencias legales

La empresa enfrentó investigaciones regulatorias en varios países, demandas colectivas y multas que superaron los \$500 millones por violaciones de las leyes de protección de datos.

El análisis de las infracciones del mundo real proporciona información valiosa sobre las vulnerabilidades comunes y las contramedidas eficaces para la seguridad de la base de datos.

Conclusiones clave

1 La seguridad es multifacética

La seguridad de la base de datos requiere una combinación de controles técnicos, políticas administrativas y concientización sobre la seguridad.

2 Defensa en profundidad

Implemente varias capas de protección para garantizar que el fallo de un solo control de seguridad no comprometa todo el sistema.

3 Cumplimiento legal

La seguridad de la base de datos no es solo una necesidad técnica, sino también un requisito legal con sanciones importantes por incumplimiento.

4 Responsabilidad ética

Más allá de los requisitos técnicos y legales, proteger los datos confidenciales es una obligación ética para con las personas cuya información se confía a sus sistemas.



"La seguridad no es un producto, sino un proceso". — Bruce Schneier