



Audit DB es la solución de auditoría de bases de datos para el Cumplimiento y Seguridad. Monitorea la efectividad de las políticas de seguridad y el acceso y uso inapropiado de datos críticos de la organización.

Audit DB combina la evaluación de seguridad y el monitoreo de la actividad de la base de datos de forma automatizada y continua en una solución que responde las preguntas: ¿Qué es lo que puede pasar con mis datos? y ¿Qué fue lo que sucedió con mis datos? Contempla dos áreas críticas de auditoría:

#### Evaluación de la Seguridad:

- Evaluación continua de la base de datos para obtener una visión exhaustiva de los riesgos en los datos. De acuerdo a una evaluación inicial, se establece una línea base que se monitorea para encontrar desviaciones subsecuentes. La información de las evaluaciones se consolida en un repositorio a partir del cual se generan reportes detallados para el análisis de hallazgos.

#### Monitoreo de la Actividad:

- Auditoría continua de la actividad de la base de datos para tener un entendimiento completo de “Quién hizo qué cosa con los datos y cuándo”. Utiliza agentes no invasivos para auditar actividades DML, DDL y SELECT. La actividad se recolecta del log de transacciones de la base de datos y/o de la captura del tráfico TCP/IP de la red y se importa a un repositorio central para análisis y generación de reportes.



#### COMPONENTES DE AUDIT DB

**Consola de Administración (Management Console)** – consola multi-usuario que asigna roles distintos en el proceso de auditoría. El administrador despliega los agentes de recolección y define la frecuencia y configuración de cada agente para recolectar y transferir la información al repositorio.

**Agentes Recolectores (Data Collectors)** – agentes sin “triggers” responsables de recolectar la información de modificaciones y visualización de los datos y de la actividad de cambios de estructura y de login.

**Alertas (Alerting)** – proporciona notificaciones casi en tiempo real de cambios DDL (incluyendo permisos y esquema) y de la actividad de login.

**Netwatch** – consiste en procesos que capturan paquetes de la red, monitoreando el tráfico hacia el servidor auditado. Método alternativo al Log Collector.

**Repositorio (Repository)** – una base de datos SQL, que recibe y consolida la información recogida por el agente recolector.

**Reportes (Reporting)** – aplicación de servidor distribuida que provee capacidades de administración, programación y visualización de reportes. El Servidor de Reportes tiene un conjunto de reportes de auditoría ya listos.

#### Con Audit DB se enfrentan las Debilidades de Control en el Acceso a los Datos

- Audit DB satisface las mejores prácticas de auditoría incluyendo la segregación de funciones, con roles y privilegios de usuarios que separan las funciones de administración de las de auditoría
- Se automatiza el proceso de monitoreo y auditoría con una pista de auditoría confiable, evitando la revisión inadecuada de logs de auditoría
- Captura toda la actividad sobre los datos, incluyendo aquella con acceso directo a información sensible, logrando el monitoreo de usuarios privilegiados
- Reporta autorizaciones cuestionables en base a las desviaciones de la política, permitiendo identificar fallas en la eliminación y actualización de cuentas de usuarios

#### Use Audit DB para

- Revisar el impacto antes/después de la manipulación de datos
- Validar cambios estructurales en bases de datos críticas
- Asegurar la privacidad de los datos por medio de una auditoría selectiva
- Recibir alertas en tiempo real de eventos en bases de datos críticas
- Garantizar una configuración y autorizaciones seguras
- Revisar y administrar los datos de auditoría en un repositorio central y seguro

#### PLATAFORMAS SOPORTADAS

DB2 para AIX  
 Microsoft SQL Server  
 ORACLE  
 Sybase

# Log Explorer

Análisis de Transacción, Auditoría y Recuperación de Datos para SQL Server

Log Explorer es la solución líder en análisis de transacciones y recuperación de datos que mejora la disponibilidad e integridad de sus datos. Al proveer un acceso sin precedentes hacia el log de transacciones de la base de datos, Log Explorer brinda la habilidad de entender y resolver problemas de la base de datos. Identifique fácilmente el origen de los cambios en los datos, recupere de forma selectiva datos que hayan sido modificados, borrados o truncados, y exporte información para análisis de seguimiento de la auditoría y generación de reportes.

Recuperar una base de datos desde los respaldos es penoso y las transacciones posteriores al punto de error se pierden. Log Explorer ofrece una recuperación selectiva de los datos para campos, registros o tablas enteras.

Por medio de la reparación y recuperación de datos en línea, Log Explorer ayuda a maximizar la disponibilidad de la base de datos y evitar los complicados métodos tradicionales de recuperación de datos.

## Utilice Log Explorer para Microsoft SQL Server para:

- Identificar, restaurar la fuente de cualquier cambio en datos, esquemas o permisos
- Recibir notificaciones inmediatas vía correo electrónico cuando ocurren eventos clave en la base de datos
- Encontrar y resolver rápidamente problemas de errores de usuarios y de aplicación, utilizando poderosos filtros para analizar el Log de Transacciones
- Reversar una o múltiples transacciones
- Recuperar tablas eliminadas o truncadas
- Reparar datos a distintos niveles de detalle seleccionando transacciones individuales o un conjunto de ellas
- Exportar información de las transacciones para su análisis

**El Grupo Eniac proporciona la tecnología, el soporte técnico y funcional, la implementación, entrenamiento y el acompañamiento que le garantizan el éxito en la gestión de base de datos.**



**Eniac, C.A.**  
Caracas, Venezuela  
Telf. +58 (212) 7095600  
[www.eniac.com](http://www.eniac.com)  
[info@eniac.com](mailto:info@eniac.com)

**The Eniac Corp.**  
San Juan, Puerto Rico  
Telf. +1 (787) 7934044  
[www.eniac-corp.com](http://www.eniac-corp.com)  
[info@eniac-corp.com](mailto:info@eniac-corp.com)

**XopanTech, S.A. de C.V.**  
México, D.F.  
Telf. +52 (55) 55111522  
[www.xopan.com](http://www.xopan.com)  
[info@xopan.com](mailto:info@xopan.com)

## Los productos Lumigent contribuyen de manera fundamental a:

- Verificar y controlar la Integridad de la información y de los Controles de los Sistemas y Aplicaciones
- Prevenir/detectar el Fraude
- Prevenir/detectar cambios a las estructuras de las bases de datos
- Supervisar la autorización y asignación de permisos para el acceso a las Bases de Datos
- Reparar Bases de Datos dañadas y recuperar tablas truncadas o borradas por fallas en aplicaciones, en el DBMS, en los equipos o por errores en la administración
- Satisfacer las regulaciones internacionales sobre privacidad y seguridad
- Notificar automáticamente a los supervisores sobre cambios en las estructuras de la base de datos

## Desempeño

Los productos de Lumigent, no afectan el desempeño de los sistemas críticos, no interrumpen la operación y son muy fáciles de instalar y usar. Los usuarios principales son Auditores de Sistemas, Administradores de Bases de Datos, Operadores de TI, Desarrolladores de Aplicaciones, Oficiales de Seguridad y Supervisores de Calidad.