Auditoría y Fortalecimiento de la Seguridad en Bases de Datos de Codearts Solutions

🔹 Fase 1: Análisis de vulnerabilidades en la base de datos

- Revisar los logs de consultas y accesos en MySQL/PostgreSQL para detectar anomalías (general_log, slow_query_log).
- Identificar usuarios con privilegios excesivos y accesos remotos no controlados.
- Analizar si existen vulnerabilidades de inyección SQL usando herramientas como SQLmap.
- Comprobar si las bases de datos están cifradas y si el tráfico entre cliente y servidor usa TLS.

Error común: Logs deshabilitados o incompletos que dificultan la detección.
Solución: Activar logs detallados y rotación para evitar pérdida de información.

🔹 Fase 2: Implementación de medidas de seguridad

- Configurar roles y permisos de usuario siguiendo el principio de mínimo privilegio.
- Habilitar cifrado de datos en reposo y en tránsito (SSL/TLS en MySQL y PostgreSQL).
- Restringir accesos remotos solo a IPs autorizadas mediante my.cnf o pg_hba.conf.
- Configurar firewall y listas de control de acceso (ACLs) para limitar conexiones sospechosas.
- Implementar copia de seguridad automatizada y cifrada para recuperación de datos.

Error común: Usuarios con permisos excesivos que aumentan el riesgo de explotación.
Solución: Auditar y ajustar permisos periódicamente, eliminando privilegios innecesarios.

🔹 Fase 3: Pruebas de seguridad y simulación de ataques

- Intentar realizar una inyección SQL controlada en formularios y API para verificar la resistencia del sistema.
- Simular un ataque de denegación de servicio enviando consultas pesadas a la base de datos.
- Monitorizar intentos de acceso no autorizado y comportamiento sospechoso de usuarios.

Error común: Falta de detección o respuesta a ataques de inyección SQL.
Solución: Implementar WAF o filtros de entrada y mejorar monitoreo y alertas.

🔹 Fase 4: Monitoreo y auditoría de accesos

- Activar logs avanzados de consultas y accesos con rotación de archivos de registro.
- Implementar alertas automáticas ante intentos de acceso fuera de horario laboral o desde ubicaciones desconocidas.
- Integrar la base de datos con un sistema de detección de intrusos (IDS) como OSSEC o Wazuh.

Error común: Alertas excesivas o ignoradas que reducen eficacia de la supervisión.
Solución: Afinar reglas de detección y capacitar al equipo para responder a eventos.