1. **Habilitar auditoría y registrar eventos de base de datos.**

   La auditoría es fundamental para el monitoreo de accesos y cambios en los datos de la base de datos. Permite detectar comportamientos sospechosos y mantener un registro detallado de las actividades realizadas por los usuarios.

   Práctica:

   Activación de logs de auditoría: Tanto en MySQL como en SQLServer, puedes habilitar el registro de eventos de base de datos para auditar actividades como inserciones, actualizaciones, eliminaciones, y accesos a la base de datos.

   En MySQL:

   MySQL ofrece un plugin de auditoría llamado MySQL Enterprise Audit Plugin, disponible en las ediciones empresariales.

```
INSTALL PLUGIN audit_log SONAME 'audit_log.so';
SET GLOBAL general_log = 'ON';
SET GLOBAL log_output = 'TABLE';
```

   - Rendimiento: Los logs de auditoría pueden afectar el rendimiento, ya que cada acción de la base de datos será registrada. Para evitar sobrecargar el sistema, es recomendable establecer una política de retención de logs (por ejemplo, eliminar logs antiguos después de un cierto período).
   - Optimización: El uso de herramientas especializadas de auditoría (como las mencionadas) permite un registro más eficiente y detallado, con menos impacto en el rendimiento.

   Consideraciones adicionales:

   - Acceso a logs: Es importante controlar quién tiene acceso a los logs de auditoría, ya que contienen información sensible sobre las actividades de los usuarios.
   - Herramientas adicionales: Existen herramientas de auditoría adicionales que puedes integrar, como pgAudit en PostgreSQL o soluciones de terceros que ofrecen funcionalidades avanzadas de monitoreo y auditoría.