Persistencia de DoltSharp

1. **Almacenamiento de Información:**

* El sistema debe almacenar de manera persistente toda la información relevante para la gestión de tareas, proyectos, usuarios y estados.
* Debe utilizarse una base de datos relacional para garantizar la integridad de los datos y permitir relaciones eficientes entre tareas, usuarios y proyectos.

1. **Redundancia de Datos:**

* Se implementarán mecanismos de redundancia de datos para evitar la pérdida de información crítica en caso de fallos del sistema. Esto puede incluir la replicación de bases de datos para asegurar que siempre haya una copia disponible.
* Utilizar clusters de bases de datos que proporcionen alta disponibilidad y recuperación automática en caso de fallos.

1. **Respaldo de Información:**

* El sistema deberá realizar respaldos automáticos periódicos de toda la base de datos para proteger la información contra pérdidas accidentales.
* Los respaldos deben programarse diariamente y almacenarse en un entorno seguro, preferiblemente en servidores externos o en la nube.

1. **Tiempo de Respuesta en Consultas:**

* El sistema debe garantizar un tiempo de respuesta óptimo para las consultas, especialmente en la recuperación de tareas y proyectos. Las consultas de datos deben procesarse en menos de 2 segundos bajo carga normal.
* Se utilizarán índices en la base de datos para mejorar la eficiencia en las consultas más frecuentes.

1. **Escalabilidad:**

* La estructura de la base de datos debe ser escalable para manejar un crecimiento en el número de usuarios y la cantidad de datos generados sin sacrificar el rendimiento.
* El sistema debe permitir la expansión hacia soluciones de almacenamiento en la nube o bases de datos distribuidas conforme aumente la demanda.

1. **Seguridad del Almacenamiento:**

* Todos los datos almacenados deben estar cifrados para proteger la confidencialidad, especialmente la información sensible de los usuarios como contraseñas, emails y otros datos personales.
* El sistema debe cumplir con las normativas de protección de datos, como GDPR, para asegurar el manejo adecuado de la información de los usuarios.

1. **Acceso y Control de Versiones:**

* Implementar un control de versiones en los registros más importantes para poder rastrear cambios y revertir a versiones anteriores en caso de error.
* Solo usuarios con permisos adecuados deben poder acceder a información sensible o modificar tareas críticas, garantizando un sistema de roles y permisos bien estructurado.

1. **Mantenimiento de Archivos Históricos:**

* El sistema debe mantener un registro histórico de las tareas y proyectos completados, con opciones para archivarlos, pero manteniéndolos accesibles bajo demanda.
* Las tareas archivadas no deben interferir con el rendimiento de las consultas sobre las tareas activas.