Breve descripción del flujo de permisos y aprobaciones

1) Base de permisos (RBAC)

El sistema usa control de acceso por permisos (RBAC):

- Cada usuario tiene un rol (`STANDARD` o `SUPERVISOR`).
- Cada rol tiene permisos asignados en BD (`permissions` + `role_permissions`).
- En cada endpoint protegido se validan:
    1. autenticación (token JWT válido),
    2. autorización (permiso requerido).

Ejemplos de permisos clave:

- `TASK_VIEW_ALL`
- `TASK_CREATE`
- `TASK_EDIT_UNIT`
- `TASK_COMPLETE_UNIT`
- `TASK_DELETE_UNIT`
- `TASK_APPROVE_CHANGES`

---

2) Flujo de aprobación

1. Un usuario `STANDARD` crea una solicitud en `task_change_requests` con estado `PENDING`.
2. Un `SUPERVISOR` de la misma unidad consulta pendientes.
3. El supervisor decide `APPROVED` o `REJECTED`.
4. Si aprueba, se aplica el cambio sobre `tasks`.
5. Si rechaza, la solicitud queda `REJECTED` con comentario de revisión.
6. En ambos casos se conserva trazabilidad (solicitud y eventos).

---

3) Regla por tipo de usuario

STANDARD

- Puede solicitar editar/completar/eliminar tareas de su unidad.
- No puede aprobar ni rechazar solicitudes.

SUPERVISOR

- Puede revisar y decidir solicitudes pendientes de su unidad.
- Tiene permiso de aprobación (`TASK_APPROVE_CHANGES`).
- En operaciones propias, el flujo puede autoaprobarse según la lógica del servicio.

---

4) Controles de integridad importantes

- Solo se procesan solicitudes en estado `PENDING`.
- El supervisor que decide debe pertenecer a la misma unidad de la solicitud.
- La decisión válida es únicamente `APPROVED` o `REJECTED`.
- Se registra auditoría de cambios para trazabilidad.

---

5) Resultado funcional

Este flujo garantiza:

- separación entre quien solicita y quien aprueba,
- control por unidad organizacional,
- permisos explícitos por rol,
- historial completo de decisiones y cambios.