SOFTWARE A MEDIDA

Antes de Dibujar Pantallas, Decide Quién Puede Cambiar Qué

La aplicación funciona en la demostración porque quien la presenta puede hacerlo todo. El problema aparece cuando entra el equipo: alguien necesita preparar un pedido, pero también puede cambiar el precio, borrar el registro y exportar todos los clientes.

Describe Tareas, No Solo Cargos

Una lista de puestos no explica todos los permisos. Dos personas con el mismo cargo pueden trabajar con sucursales distintas. Empieza por tareas concretas: consultar, crear, corregir, aprobar, exportar o eliminar. Decide sobre qué datos puede actuar cada persona y cuándo necesita una segunda aprobación.

Lleva esas decisiones a ejemplos. Un encargado puede corregir una dirección antes del despacho, pero un cambio posterior quizá deba quedar como incidencia. La regla depende del proceso real y debe poder explicarse sin leer código.

Ocultar un Botón No Basta

El sistema debe comprobar los permisos donde procesa la operación, aunque la pantalla no muestre la acción. En las pruebas, intenta realizar una tarea con una cuenta que no tenga ese permiso y comprueba que se rechaza sin modificar datos. Repite la prueba con registros de otra sucursal o cliente cuando exista esa separación.

- Verifica qué puede hacer cada rol y qué debe quedar fuera de su alcance.
- Registra las modificaciones relevantes con su autor y fecha, sin guardar secretos en el historial.
- Define cómo se concede acceso temporal y quién lo retira.
- Incluye en la entrega una explicación de los permisos y una forma de revisarlos.

Un permiso que bloquea una tarea cotidiana acaba generando contraseñas compartidas o solicitudes para convertir a todos en administradores. Prueba las reglas con quienes harán el trabajo, y corrige el proceso antes de recurrir a esa salida.

Los permisos reducen lo que una cuenta puede hacer dentro del sistema. Necesitan pruebas y mantenimiento; no sustituyen la protección de dispositivos ni el control de las cuentas administradoras.

Una Comprobación Concreta

Escribe un permiso como una frase comprobable: una persona de ventas puede preparar una solicitud de devolución para su cliente, pero no aprobarla. En un entorno de prueba autorizado, comprueba la acción permitida, la aprobación prohibida y el acceso a la solicitud de otro cliente. Incluye exportaciones y acciones masivas en la misma revisión, porque una pantalla restringida puede tener otra ruta hacia los datos.

Documentación de apoyo: Lista de comprobación de autorización de OWASP.
https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

Para seguir leyendo: Cuando Alguien Se Va, ¿Qué Accesos Se Quedan?.
https://systems.kavaliero.com/blog/cuando-alguien-se-va-que-accesos-se-quedan

Si necesitas ayuda con este trabajo, consulta el alcance de Software a Medida.
https://systems.kavaliero.com/soluciones/software-a-medida