PERMISOS

Cuando Alguien Se Va, ¿Qué Accesos Se Quedan?

La despedida fue cordial. Se devolvió el portátil y se cerró el correo. Dos semanas después, una carpeta sigue compartida con una cuenta personal y una herramienta de facturación continúa usando una clave creada por quien se fue. No hace falta un conflicto para que queden accesos olvidados.

Separa a la Persona de lo que Mantiene Funcionando

Antes de la salida, identifica las cuentas de trabajo, los equipos y las tareas automáticas que dependen de esa persona. Una integración puede fallar si desactivas su cuenta sin transferirla. Esa dependencia debe corregirse, no convertirse en una razón para dejarle permisos indefinidamente.

- Transfiere archivos, calendarios y responsabilidades a las personas autorizadas, según el procedimiento de la empresa.
- Retira roles y revisa sesiones, dispositivos, aplicaciones conectadas y claves de integración en cada servicio.
- Cambia las credenciales compartidas que la persona conocía y reduce su uso cuando puedas sustituirlas por accesos individuales.
- Comprueba enlaces públicos o invitaciones a cuentas externas que permitan acceder sin la cuenta corporativa.

Comprueba desde una Cuenta que Ya No Tiene Permiso

Una lista marcada como completada no demuestra que la baja haya llegado a todas las herramientas. Con una cuenta de prueba autorizada, verifica que los permisos retirados se rechazan donde corresponde. No pidas a la persona que entregue sus credenciales privadas ni entres a su correo personal.

Registra quién hizo la retirada y cuándo se comprobó. Si algo debe conservarse, documenta su motivo, responsable y plazo conforme a las políticas aplicables. Recursos humanos, operaciones y quien administra los sistemas necesitan coordinar la misma salida.

La revisión también revela una mejora para las próximas incorporaciones: asignar accesos por función desde el primer día facilita saber qué quitar cuando cambia esa función.

> *Retirar permisos reduce el acceso futuro, pero no borra copias que ya se hayan descargado. La conservación de datos y comunicaciones requiere criterios propios, además de la baja técnica.*

Una Comprobación Concreta

Piensa en un informe programado por alguien que deja la empresa. Eliminar su cuenta puede retirar el acceso y detener también una tarea legítima. Identifica al responsable, las credenciales utilizadas y el destino del informe; transfiérelo mediante el procedimiento del proveedor y verifica ambos resultados: el informe sigue funcionando y la persona ya no conserva los permisos retirados.

Documentación de apoyo: Guía de OWASP para revisar permisos.
https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

Para seguir leyendo: Antes de Dibujar Pantallas, Decide Quién Puede Cambiar Qué.
https://systems.kavaliero.com/blog/el-software-a-medida-empieza-por-los-permisos

Si necesitas ayuda con este trabajo, consulta el alcance de Auditoría y Pentesting Corporativo.
https://systems.kavaliero.com/soluciones/auditoria-pentesting