Reto: Autenticación y Listas de Control de Acceso (ACL)

Empresa ficticia: **TecnoRed**

Objetivo

Aplicar conocimientos sobre autenticación y ACL para proteger recursos con herramientas digitales gratuitas.

Escenario

La empresa trabaja en la nube y debe proteger: **documentos compartidos**, **panel de administración** y **cuentas de correo**.
Misión: definir métodos de autenticación adecuados y diseñar reglas ACL para controlar quién puede acceder y qué puede hacer.

Mapa de controles (Rol → Autenticación → Reglas ACL → Riesgo)

Rol	Método de autenticación	Reglas ACL (permisos)	Riesgo si falla / no aplica
Directora	**SSO** (Google/Microsoft) + **MFA** (TOTP, códigos de respaldo) + FIDO2 Contraseña robusta + gestor de contraseñas.	**Acceso total** al panel Crear/leer/editar/eliminar Gestión de usuarios y permisos.	Compromiso completo del negocio si se omite MFA o se reutiliza contraseña.
Técnico de soporte	**SSO + MFA (TOTP)** Device trust (equipo corporativo) y IPs permitidas Sesiones: 8h.	Acceso **limitado a herramientas técnicas** (logs, monitoreo) Editar configuración **Sin** acceso a finanzas/RR.HH. **Sin** eliminar datos.	Elevación indebida de privilegios → cambios no autorizados o robo de credenciales.
Secretaria	Correo y Drive + **MFA** (SMS o TOTP) Gestor de contraseñas obligatorio.	Acceso a **carpetas de oficina/agenda** Leer y escribir **Sin** modificar ACL **Sin** panel ni herramientas técnicas.	Phishing → fuga de documentos y suplantación en calendarios.
Visitante	**Sin cuenta** Enlaces públicos con expiración + CAPTCHA.	Solo **lectura** de documentos públicos **Sin** descarga masiva ni indexación.	Configuración pública incorrecta → exposición de información.