Desafío de Autenticación y Autorización Diego Cabré 26489744-0

1. ¿Cómo se autentica y autoriza el acceso físico a áreas restringidas?

Se realiza mediante sistemas de control de acceso como tarjetas RFID, lectores biométricos o códigos PIN. El sistema valida la identidad del usuario y verifica si cuenta con permisos para ingresar al área.

2. Escenario: un empleado pierde su tarjeta de acceso. ¿Cuáles son los pasos para gestionar esta situación?

1. Notificar de inmediato al departamento de seguridad.
2. Desactivar la tarjeta perdida en el sistema.
3. Emitir una nueva tarjeta con los permisos correspondientes.
4. Registrar el incidente y tomar medidas para prevenir recurrencias.

3. Ejemplo de una política de contraseñas y cómo se implementa.

Política: Las contraseñas deben tener al menos 12 caracteres, incluir mayúsculas, minúsculas, números y símbolos.
Implementación: Configuración de directivas de grupo (GPO) o ajustes en el sistema para exigir estos criterios y forzar el cambio cada 90 días.

4. Proceso de autenticación de dos factores (2FA) y métodos adicionales.

En el 2FA, el usuario ingresa su contraseña (primer factor) y luego un código enviado por SMS, correo electrónico o una app de autenticación (segundo factor). Métodos adicionales incluyen biometría y llaves de seguridad físicas como YubiKey.

5. Procedimientos para asignar privilegios administrativos a un nuevo usuario.

1. Validar la solicitud y aprobación por un supervisor.
2. Crear la cuenta del usuario en el sistema.
3. Asignar privilegios mediante grupos o roles.
4. Registrar la acción y realizar una revisión periódica de permisos.

6. Manejo de identificación y notificación en caso de brecha de seguridad.

1. Detectar y confirmar la brecha.
2. Identificar los usuarios afectados.
3. Notificar a los usuarios explicando el incidente y medidas de mitigación.
4. Reportar a las autoridades si aplica.

7. Asegurar la robustez de las contraseñas utilizadas para la autenticación.

Se aplican requisitos mínimos de complejidad, políticas de expiración, prohibición de contraseñas previas y verificación contra listas de contraseñas comprometidas.

8. Escenario de prueba: autenticación fallida por falta de segundo factor.

Si el usuario no proporciona el segundo factor, el acceso se deniega y se registra el intento fallido. Se notifica al usuario para que intente nuevamente o solicite asistencia al soporte técnico.

9. Protocolos específicos para la autenticación y autorización.

En entornos corporativos se utilizan protocolos como LDAP, Kerberos y OAuth 2.0 para autenticación; y mecanismos como ACLs (Listas de Control de Acceso) y RBAC (Control de Acceso Basado en Roles) para autorización.

10. Garantizar la integridad y confidencialidad de los datos durante la autenticación.

Se utilizan canales cifrados como HTTPS/TLS, almacenamiento seguro de contraseñas mediante hashing con sal (bcrypt, Argon2) y validación de datos para evitar ataques de intermediario o inyección.