TECNOLOGÍAS

EL DOBLE FACTOR DE AUTENTICACIÓN (2FA)

es una medida de seguridad adicional a la contraseña que protege cuentas y sistemas digitales, reduciendo el riesgo de accesos no autorizados.

BENEFICIOS:

- **Mayor seguridad** en cuentas institucionales.
- Control de accesos y **detección de intentos sospechosos.**
- **Prevención** de pérdida de información valiosa.

TIPOS:

- **Mensaje de texto o correo:**
  Código temporal enviado al usuario.
- **Aplicaciones de autenticación:**
  Generan códigos temporales (ej. Google Authenticator.)
- **Llaves de seguridad o tokens físicos:**
  Dispositivos con códigos actualizados periódicamente

BUENAS PRÁCTICAS:

- **No compartir** códigos de autenticación.
- Configurar **métodos de recuperación.**
- **Cambiar la contraseña** si se recibe un código no solicitado.
- Usar 2FA solo en **dispositivos propios.**

Para activar 2FA en cuentas institucionales, se recomienda contactar al delegado del CTO. Implementar esta medida fortalece la seguridad de la información y protege contra accesos no autorizados y filtraciones de datos.

LA SEGURIDAD DIGITAL
ES RESPONSABILIDAD DE TODOS

ALCALDÍA DE
SANTIAGO DE CALI