Objetivo:
Garantizar que los mecanismos de autenticación utilizados para acceder a sistemas y servicios sean seguros, confiables y protejan contra accesos no autorizados.

Declaración:
La organización ha implementado políticas, procedimientos y controles técnicos que aseguran la autenticación segura de usuarios y dispositivos, utilizando métodos apropiados según el nivel de riesgo y criticidad de los sistemas.

Alcance:
Este control aplica a todos los sistemas, aplicaciones y servicios que requieran autenticación para acceder a la información o recursos de la organización.

Directrices:

- **Se definen requisitos mínimos para contraseñas, incluyendo longitud, complejidad y caducidad.**
- **Se promueve el uso de autenticación multifactor (MFA) para accesos sensibles o críticos.**
- **Se implementan controles para proteger las credenciales durante su almacenamiento y transmisión.**
- **Se establecen procedimientos para la recuperación segura de credenciales y restablecimiento de contraseñas.**
- **Se monitorea y registra el uso de mecanismos de autenticación para detectar actividades sospechosas.**
- **Se capacita al personal en buenas prácticas de autenticación y seguridad de credenciales.**

Referencias relacionadas:

- **POL 004 — Política de contraseñas**
- **POL 005 — Política de control de acceso**
- **PRO 014 — Procedimiento para el Registro y Supervisión de Accesos**
- **FOR 003 — Registro de Autorización de Usuarios**
- **PSC 009 — Sensibilización y Capacitación**

Evidencias de implementación:

- **Documentación de políticas y procedimientos de autenticación segura.**
- **Registros de configuración y monitoreo de mecanismos de autenticación.**
- **Informes de auditoría sobre seguridad de autenticación.**
- **Registros de capacitación y sensibilización.**
- **Reportes de incidentes relacionados con accesos no autorizados y acciones correctivas.**

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO