

**Objetivo:**

Garantizar que los derechos de acceso a sistemas, aplicaciones e información sean asignados, revisados y revocados conforme a las funciones y necesidades de los usuarios, evitando accesos no autorizados y minimizando riesgos a la seguridad.

**Declaración:**

La organización ha implementado un proceso formal para la gestión de los derechos de acceso, asegurando que estos sean otorgados según criterios claros, documentados y aprobados, y que se revisen periódicamente para mantener su adecuación.

**Alcance:**

Este control aplica a todos los usuarios, sistemas y recursos de información gestionados por la organización.

**Directrices:**

- Se definen criterios claros para la asignación de derechos de acceso basados en roles y responsabilidades.
- Los derechos de acceso son otorgados solo tras las debidas autorizaciones y verificaciones.
- Se realizan revisiones periódicas para validar la vigencia y pertinencia de los derechos asignados.
- Se implementan mecanismos para la revocación o modificación inmediata de derechos en caso de cambios en funciones o desvinculación.
- Se registra toda la gestión de derechos, incluyendo altas, modificaciones y bajas.
- Se capacita al personal en la importancia y procedimientos para la correcta gestión de derechos de acceso.

**Referencias relacionadas:**

- POL 005 — Política de control de acceso
- PRO 014 — Procedimiento para el Registro y Supervisión de Accesos
- FOR 003 — Registro de Autorización de Usuarios
- FOR 023 — Registro de Alta y Modificación de Usuario
- PSC 009 — Sensibilización y Capacitación

**Evidencias de implementación:**

- Registros documentados de asignación, modificación y revocación de derechos (FOR 003, FOR 023).

- Informes de revisiones periódicas de derechos de acceso.
- Documentación de políticas y procedimientos relacionados.
- Registros de capacitación y sensibilización.
- Reportes de incidentes y acciones correctivas vinculadas a la gestión de derechos.

## Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO