**1. Objetivo**

Establecer los lineamientos para la creación, actualización, activación, desactivación y control de cuentas de usuario, correos institucionales, contraseñas y accesos al Dashboard del IMRD, garantizando la seguridad de la información y el acceso adecuado a los sistemas institucionales.

**2. Alcance**

Aplica a todos los funcionarios, contratistas y terceros que requieran acceso a:

- Correos institucionales
- Sistemas de información
- Dashboard del IMRD
- Plataformas tecnológicas institucionales

Incluye desde la solicitud de creación de cuentas hasta su eliminación o bloqueo.

**3. Roles y responsabilidades**

**Ingeniero de Sistemas Líder TIC:**

- Definir políticas de acceso y seguridad.
- Autorizar creación y eliminación de cuentas.
- Supervisar el cumplimiento del procedimiento.

**Técnico de Sistemas:**

- Crear, modificar y eliminar cuentas de usuario.
- Configurar correos institucionales.
- Asignar accesos al Dashboard IMRD.
- Gestionar restablecimiento de contraseñas.

**Jefes de Área / Supervisores:**

- Solicitar creación o modificación de accesos.
- Validar la necesidad de permisos.

**Usuarios:**

- Hacer uso adecuado de sus credenciales.
- Mantener la confidencialidad de sus contraseñas.

**4. Normatividad**

ISO/IEC 27001:2022 – Seguridad de la información

Política de Seguridad de la Información del IMRD

Lineamientos MinTIC sobre seguridad digital

**5. Términos y definiciones**

**Cuenta de usuario:** Identidad digital asignada a una persona para acceder a sistemas.

**Credenciales:** Usuario y contraseña asociados a una cuenta.

**Dashboard:** Plataforma de visualización y gestión de información institucional.

**Control de acceso:** Restricción de ingreso a sistemas según permisos definidos.

**6. Contenido**

| Ítem | Actividad | Descripción | Responsable | Documento o Registro |
|---|---|---|---|---|
| **1.** | Solicitud de Creación de Cuenta | El jefe de área solicita formalmente la creación de la cuenta de usuario al área TI mediante correo electrónico o formato establecido, incluyendo nombre completo, cargo, dependencia y tipo de acceso requerido. La solicitud debe contar con la aprobación del supervisor o responsable del área. | Jefe de Área | Correo electrónico de solicitud<br><br>**Formato de Solicitud Tecnologica** |
| **2.** | Creación de cuenta y correo institucional | El Ingeniero de sistemas crea la cuenta de usuario en los sistemas institucionales requeridos, genera el correo institucional conforme a la nomenclatura establecida, | Ingeniero Sistemas | **Inventario de Usuarios y Accesos** |

| | | | | |
|---|---|---|---|---|
| | | asigna los permisos de acceso de acuerdo con el perfil del cargo y registra la información en el inventario de usuarios para su control y seguimiento. | | Cuenta creada |
| **3.** | Creación o Asignación de Acceso al Dashboard IMRD | El Ingeniero de sistemas valida el perfil de acceso requerido de acuerdo con las funciones del usuario, configura los permisos en el Dashboard IMRD según el rol asignado (consulta, servicio. | Ingeniero Sistemas | Espacio habilitado<br><br>Evidencia de Activación de Usuario |
| **4.** | Cambio o restablecimiento de contraseña Zimbra | El Ingeniero de sistemas genera una contraseña temporal segura para el usuario, realiza la entrega de las credenciales a través de un medio seguro, garantiza la activación de la cuenta y solicita el cambio obligatorio de la contraseña en el primer inicio de sesión. | Ingeniero Sistemas | Evidencia de Cambio de Contraseña Inicial/ Contraseña restablecida |
| **5.** | Cambio o restablecimiento de contraseña Nextcloud | El usuario y el área TI gestionan las contraseñas garantizando el cumplimiento de las políticas de seguridad establecidas (mínimo 8 caracteres, combinación de letras, números y símbolos, cambio confidencialidad de las | Usuario / Ingeniero Sistemas | Contraseña actualizada |

| | | | | |
|---|---|---|---|---|
| | | credenciales). Para el restablecimiento, el usuario realiza la solicitud al área TI, se valida su identidad y se genera una nueva contraseña temporal segura, la cual debe ser cambiada en el primer inicio de sesión. | | |
| **6.** | Modificación de accesos | El jefe de área solicita al área TI la modificación de accesos de un usuario, indicando los permisos requeridos.<br><br>El Ingeniero Sistemas valida la necesidad del cambio de acuerdo con las funciones del cargo, actualiza los accesos en los sistemas institucionales y en el Dashboard IMRD, y verifica la correcta aplicación de los nuevos permisos. | Jefe de Área / Ingeniero Sistemas | Evidencia de Actualización de Permisos |
| **7.** | Desactivación o eliminación de cuentas | El Ingeniero Sistemas realiza la desactivación o eliminación de la cuenta del usuario cuando se presenta finalización de contrato, cambio de cargo o retiro del funcionario.<br><br>Se procede a bloquear el acceso de manera inmediata para evitar usos no autorizados.<br><br>posteriormente se elimina o archiva la cuenta de acuerdo con las políticas institucionales. | Ingeniero Sistemas | Cuenta deshabilitada/ Evidencia de Bloqueo de Acceso |

| | | | | |
|---|---|---|---|---|
| | | Finalmente, se registra la novedad para control y seguimiento. | | |
| **8.** | Control y Seguimiento de Accesos a Sistemas | Se realiza el control y seguimiento de los accesos a los sistemas de información institucionales mediante la verificación continua de usuarios activos, roles asignados y niveles de acceso, asegurando que correspondan a las funciones del cargo y cumplan con el principio de mínimo privilegio.<br><br>Durante este proceso se identifican accesos no autorizados, usuarios inactivos o permisos inadecuados, aplicando las acciones correctivas correspondientes, como modificación, bloqueo o eliminación de accesos.<br><br>Adicionalmente, de manera mensual se consolida la información registrada, mediante un informe en la que se detalla los resultados del seguimiento, se documentan los hallazgos, acciones realizadas y se generan conclusiones y recomendaciones, dejando evidencia del control efectuado. | Ingeniero Sistemas | **Formato – Informe mensual de control y seguimiento de accesos** |

## 7. Documentos relacionados

| Nombre del documento |
|---|
| Formato de Solicitud Tecnologica |
| Formato Inventario de Usuarios |
| Formato Informe mensual de control y seguimiento de accesos a sistemas |

## 8. Formalización de la versión actual

| | |
|---|---|
| **Elaboró** | Ingeniero de sistemas<br>09/04/2026 |
| **Actualizó** | Equipo de Calidad<br>09/04/2026 |
| **Aprobó** | Soraya Tatiana Cáceres Santos – Directora.<br>09/04/2026 |
| **Aprobó para el sistema de gestión** | Soraya Tatiana Cáceres Santos – Directora.<br>09/04/2026 |

| Fecha | Versión | Descripción |
|---|---|---|
| 09/04/2026 | 1 | Versión original |