Contenido

Contenido:

1. OBJETIVO

Determinar las actividades a seguir para la custodia de las contraseñas de forma segura y centralizada, de los recursos tecnológicos y los sistemas de información del ICETEX, como pueden ser: servidores, aplicativos, software, Bases de Datos, entre otros, a través de una herramienta de custodia de contraseñas, a fin de controlar con seguridad las credenciales de administración de la infraestructura de TI y los sistemas de información.

2. DEFINICIONES

- **Director de Tecnología (Rol):** Director de Tecnología.
- **Coordinador GSI (Rol):** Coordinador del Grupo de Sistemas de Información.
- **Coordinador Infraestructura Tecnológica (Rol):** Coordinador del Grupo de Infraestructura.
- **Administrador privilegiado de la Plataforma de Custodia de Contraseña (Rol):** Profesional de la Dirección de Tecnología responsable de la administración de la herramienta de custodia de contraseñas.
- **Administrador de recursos tecnológicos (Rol):** Profesional de la Dirección de Tecnología encargado de la administración de recursos tecnológicos (servidores, aplicaciones, ambientes, infraestructura de TI, dispositivos) a cargo de la Dirección de Tecnología y que debe agregar los recursos y contraseñas en la herramienta de custodia de contraseñas.
- **Herramienta de custodia de contraseñas:** Software para almacenar y gestionar contraseñas, las cuales se guardan de manera cifrada, garantizando su confidencialidad y seguridad.
- **Recursos tecnológicos:** Corresponde a los activos tecnológicos, como: servidores, aplicaciones, ambientes, infraestructura de TI, dispositivos, entre otros.
- **Tipos de contraseñas:**
  Corresponde a las credenciales que se deben configurar en la herramienta de custodia de contraseñas de acuerdo con el rol del administrador de recursos tecnológicos:
  - De usuario administrador privilegiado de la herramienta.
  - De administrador(es) de recursos tecnológicos.

3. CONDICIONES GENERALES

- Todos los administradores de recursos tecnológicos y sistemas de información deben realizar la custodia de las contraseñas privilegiadas a su cargo, en la herramienta destinada para tal fin.
- EL jefe inmediato o quien el designe, debe realizar la solicitud de creación del usuario o sesión de la administración de contraseñas en la herramienta de gestión de contraseñas, siguiendo el procedimiento A7-1-05 Gestión de accesos y retiro de servicios, adjuntando el correo de aprobación.
- El administrador de la herramienta de gestión de contraseñas habilita los permisos a los administradores de recursos tecnológicos y sistemas de información, una única vez, para que puedan agregar los recursos a su cargo y mantener actualizadas las contraseñas
- El Coordinador y/o Director de tecnología, debe emitir la autorización al Administrador de la herramienta de custodia de contraseñas, para compartir las contraseñas de forma segura, al nuevo profesional encargado de la administración temporal. Aplica para casos especiales (por ejemplo, ausencia del Administrador de recursos tecnológicos).

4. ACTIVIDADES

4.1. Solicitar el acceso a la herramienta de gestión de contraseñas:

Descripción: EL jefe inmediato o quien el designe, debe solicitar al Administrador de la herramienta de gestión de contraseñas, que realice la activación del usuario de acuerdo a lo establecido en el procedimiento A7-1-05 Gestión de accesos y retiro de servicios.
Ejecutantes: Administrador privilegiado – Administrador de recursos tecnológicos.

4.2. Configurar Rol y reglas:

Descripción: Realizar la configuración del rol y reglas de seguridad para el administrador de recursos tecnológicos de acuerdo con sus responsabilidades, en la herramienta de custodia de contraseñas.
Ejecutantes: Administrador privilegiado.

4.3 Periodicidad de Cambio de claves:

Descripción: Debe configurarse en la herramienta de custodia de contraseñas la periodicidad de cambio de contraseñas para los administradores, para que se realicé como mínimo cada 90 días, teniendo en cuenta los lineamientos de la G71 - Guía de Contraseñas Seguras.
Ejecutantes: Administrador privilegiado.

5. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Asignar los roles a los administradores de Recursos.	Creación del del rol y reglas de seguridad para el usuario administrador de recursos en la herramienta de acuerdo con responsabilidades.	Reporte de usuarios / roles en la Herramienta de custodia de contraseñas.	Administrador privilegiado