1. OBJETIVO

Establecer los lineamientos para la generación, almacenamiento, uso y actualización de la credencial USERDES, para mantener la protección de los activos de información de la entidad y la preservación de la confidencialidad, integridad y disponibilidad.

2. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	*PR-IIT-0455	Gestión de accesos	Digital	Interno
Procedimiento	PR-IIT-0457	Gestión de Cambios.	Digital	Interno
Formato	FT-IIT-2853	Entrega de contraseñas	Digital	Interno

* Procedimiento al que pertenece este documento

3. DEFINICIONES Y SIGLAS

Esquema de control dual: Proceso que consiste en utilizar dos o más entidades distintas (por lo general, personas) de manera coordinada para proteger funciones o información confidencial.
Fuente: UAE DIAN – Oficina de Seguridad de la Información.

Generador de clave segura: Herramienta para generar claves de forma aleatoria y segura.
Fuente: UAE DIAN – Oficina de Seguridad de la Información.

Gestor de Secretos: Herramienta de seguridad de la información para proteger las claves criptográficas y otros secretos usados por las aplicaciones y los servicios en la nube con Microsoft Azure Key Vault.
Fuente: UAE DIAN – Oficina de Seguridad de la Información.

OSI: Oficina de Seguridad de la Información

SYGA SXXI: Sistema de Información y Gestión Aduanera.

USERDES: usuario de conexión a la base de datos del sistema SYGA SXXI.

4. DESARROLLO DEL TEMA

Este protocolo busca asegurar que el acceso a la credencial **USERDES** se limite estrictamente a los casos necesarios, minimice los riesgos de exposición y permita una trazabilidad completa de cada acción realizada.

4.1 Roles y responsabilidades de la Custodia

Rol	Responsabilidad
Oficina de Seguridad de la Información (OSI)	Emitir lineamientos para la custodia segura de credenciales. Monitorear el cumplimiento del de las actividades del presente protocolo para custodia de la credencial **USERDES**. Validar las solicitudes de acceso y actuar como custodio de la clave del gestor de secretos.
Dirección de Gestión de Innovación y Tecnología	Actuar como custodio de la clave de acceso al gestor de secretos. Liderar la gestión técnica de la credencial **USERDES**, asegurando su almacenamiento seguro, la implementación del esquema de control dual y la disposición de la infraestructura tecnológica necesaria para el cumplimiento del protocolo.
Administradores de Bases de Datos (DBA) y Administradores de servidores de aplicación SYGA	Disponer la infraestructura necesaria en los servidores de bases de datos y de aplicación del sistema **SYGA** para que el o los custodios realicen el cambio periódico de la clave de **USERDES**, sin acceder ni tener conocimiento directo de la misma.

4.2 Custodia y Almacenamiento de la Credencial USERDES

4.2.1 Generación y almacenamiento seguro:

La contraseña de USERDES debe generarse con al menos 32 caracteres utilizando un generador de claves seguro autorizado por la DIGIT y cumplir con los siguientes criterios:

- Incluir caracteres numéricos.
- Incluir caracteres alfabéticos en minúscula y mayúscula.
- Incluir uno o más de los siguientes caracteres especiales: !"#$%&'()*+,-./:;<=>?@[]^_{|}~.

- No contener caracteres similares consecutivos.

La contraseña será dividida en dos partes, cada una de ellas será generada, conocida y custodiada por siguientes actores:

- Primer custodio: Director(a) de Gestión de Innovación y Tecnología.
- Segundo custodio: Jefe de la OSI.

Solo mediante la combinación de ambas partes podrá accederse a la credencial completa, asegurando así el esquema de control dual.

La contraseña será almacenada en una base de datos cifrada dentro de un gestor de secretos seguro, garantizando su protección contra accesos no autorizados. El gestor de secretos debe cumplir con principios de autenticación, no repudio y trazabilidad, permitiendo registrar y auditar cada acceso realizado.

Prohibido: Almacenar la clave de **USERDES** en archivos digitales no cifrados, correos electrónicos o documentos accesibles en la red.

4.2.2 Solicitudes de uso:

Cualquier acceso al gestor de secretos debe registrarse en la mesa de servicio con:

- Fecha y hora de solicitud.
- Motivo.
- Responsable del acceso.
- Solicitud autorizada por el Director de Gestión de Aduanas, el Director Gestión de Innovación y Tecnología y la Oficina de Seguridad de la Información

4.3 Restricciones en el uso de la credencial

4.3.1 Prohibición de conocimiento directo:

- Ningún administrador debe conocer la contraseña permanentemente.
- Solo se accederá mediante la solicitud aprobada y bajo supervisión del Director de Gestión de Innovación y Tecnología y por el Jefe de la OSI.

4.3.2 Uso limitado y justificado:

- **USERDES** solo se utilizará para gestión de sesiones de la base de datos de SYGA.
- Cualquier uso fuera de lo definido se considerará un acceso no autorizado y se derivará en las investigaciones pertinentes.

4.3.3 Cambio periódico de la contraseña:

- La clave de **USERDES** deberá ser actualizada cada vez que sea utilizada; Sin embargo, si no se ha utilizado, deberá actualizarse al menos una vez cada dos meses para mantener las condiciones de seguridad requeridas. Así mismo, deberá actualizarse cuando cambie al menos uno de los custodios de la credencial.
- Dado que el cambio de contraseña genera indisponibilidad, cada actualización deberá gestionarse previamente a través de una solicitud de ventana de cambio, la cual deberá ser revisada y aprobada por el Comité de Cambios, de acuerdo con el procedimiento PR-IIT-0457 Gestión de Cambios.

4.4 Auditoría y Control Manual de Accesos

4.4.1 Registro obligatorio en la mesa de servicio:

- Toda solicitud de acceso será registrada en la herramienta de gestión de la mesa de servicio y debe incluir el formato FT-IIT-2853 firmado por los responsables.

4.4.2 Revisión periódica de accesos:

- La OSI realizará comprobaciones trimestrales para verificar el cumplimiento de la actualización de credenciales, y que la clave de acceso al gestor de secretos se mantenga bajo control dual.
- Se verificará el cumplimiento de las restricciones de uso.

4.4.3 Alertas ante anomalías:

- La OSI verificarán los registros de acceso en **SYGA** para detectar actividad inusual.

5. CONTROL DE CAMBIOS

Este protocolo deberá revisarse al menos una vez al año, o cuando ocurran cambios relevantes en la infraestructura tecnológica, las normativas internas o surjan amenazas emergentes, en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de la DIAN.

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	24/06/2025		Versión Inicial	Esta versión corresponde a Información Pública

Elaboró:	Alvaro Antonio Sarria Romero, Felipe Alberto Portocarrero Ramirez. **Elaboración técnica**	Gestor IV Gestor III	Oficina de Seguridad de la Información
	Tito Alejandro Menjura Murcia, César Augusto Garzón Baquero **Elaboración metodológica**	Gestor II Gestor I	Subdirección de Procesos.
Revisó:	Tony Samir Peña Guzman	Director	Dirección de Gestión de Innovación y Tecnología
Aprobó:	Francisco Andres Daza Cardona	Jefe	Oficina de Seguridad de la Información