1. OBJETIVO

Establecer lineamientos, actividades y responsabilidades para gestionar de manera segura la recepción, custodia digital y el intercambio controlado de las credenciales de los usuarios por defecto con privilegios administrativos en las plataformas tecnológicas, sistemas operativos, bases de datos, servidores y redes de comunicación de la UAE DIAN, con el fin de garantizar la continuidad de la operación, la protección de los activos de información de la entidad y la preservación de la confidencialidad, integridad y disponibilidad de la información institucional en situaciones excepcionales o eventos extraordinarios.

2. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	*PR-IIT-0455	Gestión de accesos	Digital	Interno
Instructivo	IN-IIT-0273	Operaciones para la gestión de accesos	Digital	Interno
Manual	MN-IIT-0072	Manual de políticas y lineamientos de seguridad de la información	Digital	Interno
Formato	FT-TAH-1674	Control registro de asistencia reuniones	Digital	Interno
Formato	FT-IIT-2852	Información para custodia de credenciales	Digital	Interno
Formato	FT-IIT-2853	Entrega de contraseñas de cuentas de usuarios privilegiados	Digital	Interno

* Procedimiento al que pertenece este documento

3. DEFINICIONES Y SIGLAS

Todas las definiciones y siglas presentadas en el contenido de este documento están exhaustivamente detalladas y explicadas en el Anexo MN-IIT-0072 Definiciones y Siglas de Seguridad y Privacidad de la Información, el cual ha sido cuidadosamente elaborado para proporcionar una comprensión precisa y completa de los conceptos utilizados.

4. DESARROLLO DEL TEMA

Principios y lineamientos generales

La gestión de las cuentas privilegiadas y sus credenciales constituye un eje fundamental en las políticas de seguridad de la información de la UAE DIAN, teniendo como propósito esencial proteger la confidencialidad, integridad y disponibilidad de los datos institucionales y garantizar la continuidad operativa de los servicios críticos que apoyan los procesos misionales de la entidad.

La administración de estas credenciales debe enmarcarse en principios claros y precisos que aseguren el uso responsable y controlado de los accesos privilegiados, con especial énfasis en:

- **Gestión exclusiva de cuentas privilegiadas inhabilitadas o desactivadas**: Solo se custodiarán y administrarán credenciales que correspondan a cuentas privilegiadas que se encuentren inhabilitadas o desactivadas en las plataformas tecnológicas, sistemas operativos, bases de datos y redes de comunicación.
- **Uso excepcional y legítimo**: El uso de estas cuentas deberá realizarse **únicamente en casos excepcionales**, cuando exista una necesidad legítima que respalde técnicamente su utilización. Estos casos comprenden escenarios como actividades de gestión, mantenimiento, recuperación, migración de plataformas o atención de contingencias que requieran autenticarse con una cuenta privilegiada.
- **Documentación, justificación y trazabilidad**: Toda solicitud, entrega o uso de las credenciales privilegiadas debe ser documentada y justificada mediante la herramienta oficial de gestión de la mesa de servicio, asegurando la trazabilidad completa y la rendición de cuentas de cada acción realizada.
- **Generación segura de contraseñas**: Las contraseñas que se asocien a las cuentas privilegiadas deberán ser generadas utilizando herramientas institucionales seguras y ajustándose a los requisitos de complejidad definidos.
- **Custodia digital centralizada y segura**: Las credenciales privilegiadas deberán ser almacenadas exclusivamente en un repositorio digital seguro, cifrado y administrado por la Oficina de Seguridad de la Información - OSI, garantizando así la protección de la información y eliminando cualquier forma de custodia física o en papel que pueda implicar riesgos adicionales.
- **Seguimiento y revisión continua de controles:** La OSI realizará actividades de seguimiento y verificación periódica para evaluar el cumplimiento de estos principios y la efectividad de los controles establecidos en la gestión de las cuentas privilegiadas. Estas actividades se llevarán a cabo en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), como parte de los procesos de mejora continua y conforme a las políticas y lineamientos de la entidad.

4.1 Recepción y custodia digital de credenciales

A continuación, se detalla el paso a paso que debe seguirse para la recepción y custodia digital de las credenciales privilegiadas, garantizando que el proceso sea seguro, documentado y acorde a los lineamientos establecidos.

I. **Presentación de la solicitud**
El responsable técnico o jefe de área de la Dirección de Gestión de Innovación y Tecnología – DGIT presenta la solicitud formal de custodia de la credencial a través de la herramienta oficial de gestión de la mesa de servicio, anexando la justificación técnica y administrativa correspondiente, adjuntando el formato FT-IIT-2852 Información para custodia de credenciales.

II. **Validación de la solicitud**
La OSI revisa que la solicitud cumpla con los siguientes criterios:
- ✓ La cuenta corresponda a un usuario por defecto inhabilitado o desactivado.
- ✓ No exista almacenamiento de la contraseña en aplicaciones o servicios.
- ✓ El activo de información respalda procesos misionales y su indisponibilidad afecta el recaudo, los servicios aduaneros o cambiarios, y compromete la integridad y disponibilidad de la información, generando un alto impacto reputacional y legal.

Si la solicitud no cumple estos criterios, la OSI la devuelve con las observaciones necesarias para su ajuste o cierre.

III. **Generación y cambio de la contraseña**
Cuando la solicitud es validada, el funcionario de la Oficina de Seguridad de la Información procede, en reunión presencial con el responsable técnico, a:
- ✓ Generar una nueva contraseña utilizando herramientas institucionales seguras y cumpliendo con los requisitos de complejidad establecidos.
- ✓ Cambiar la contraseña y dejar la cuenta inhabilitada o desactivada.

IV. **Registro de la actividad**
Toda la actividad debe quedar registrada en la herramienta oficial de gestión (con su respectivo Formato FT-TAH-1674), incluyendo los participantes, la fecha y los resultados del proceso.

V. **Custodia digital de las credenciales**
La contraseña generada se almacena exclusivamente en el repositorio digital seguro y cifrado de la OSI, como único medio de custodia, garantizando acceso restringido y monitoreado para proteger la integridad y disponibilidad de la información.

Seguimiento y verificación
La OSI realiza actividades de **seguimiento y verificación periódica** en el marco del **SGSPI**, para revisar la efectividad de los controles y asegurar que la gestión de las credenciales se realice conforme a los más altos estándares de seguridad.

4.2 Intercambio seguro de contraseñas

Casos en los que se permite el intercambio seguro de credenciales privilegiadas:
El intercambio seguro de credenciales privilegiadas se permite únicamente en situaciones donde el acceso a estas cuentas es necesario para garantizar la continuidad de la operación o la seguridad de las plataformas tecnológicas. Estos casos comprenden:

- **Mantenimiento preventivo o correctivo**: Cuando las actividades de actualización o corrección de fallos de la plataforma solo pueden ser realizadas utilizando cuentas con privilegios elevados para evitar afectaciones en la operación.
- **Recuperación de acceso ante bloqueos u olvidos de cuentas administrativas estándar**: Cuando, por razones operativas o técnicas, el acceso administrativo estándar no está disponible y es necesario utilizar las cuentas privilegiadas para restablecer la funcionalidad del sistema.
- **Rotación obligatoria de contraseñas**: Cuando se cumple el periodo definido para la actualización periódica de las contraseñas privilegiadas, garantizando que estas se mantengan fuertes y seguras.
- **Fallos de acceso en cuentas estándar o activación del DRP**: Cuando existen fallas o problemas que impiden el acceso a cuentas estándar y se hace indispensable utilizar cuentas privilegiadas para garantizar la continuidad de los servicios críticos o activar planes de recuperación ante desastres (DRP).
- **Migraciones o restauraciones de plataformas tecnológicas**: Cuando es necesario realizar movimientos, actualizaciones o restauraciones de plataformas que requieran acceso privilegiado para ejecutar tareas críticas o reconfiguraciones esenciales.

Paso a paso del proceso

I. **Presentación de la solicitud**
El responsable técnico o jefe de área presenta la solicitud de intercambio de credenciales en la herramienta oficial de gestión, adjuntando el Formato FT-IIT-2853 Entrega de contraseñas de cuentas de usuarios privilegiados diligenciado y la justificación técnica y administrativa correspondiente.

II. **Validación de la solicitud**
La OSI revisa la solicitud para verificar que esté completa y que la justificación sea válida y necesaria. Si la solicitud cumple con estos criterios, se aprueba y se continúa con el proceso. Si no, se devuelve para ajuste o se cierra.

III. **Entrega cifrada de la contraseña**
Una vez aprobada la solicitud, la OSI extrae la contraseña del repositorio digital seguro, la cifra y la entrega al responsable mediante un medio seguro (correo electrónico cifrado), registrando el envío y los datos del receptor en la herramienta oficial de gestión.

IV. **Ejecución de las tareas y reporte de finalización**
El responsable técnico utiliza las credenciales entregadas exclusivamente durante el plazo autorizado para realizar las tareas justificadas, y posteriormente reporta la finalización de las actividades en la herramienta de gestión. Si se requiere prórroga, esta

debe ser justificada ante el director de la DGIT o delegado, quien aprueba la extensión y la deja documentada.

V. **Cambio final de contraseña e inactivación**
Una vez finalizado el uso, el Oficial de Seguridad de la Información y el administrador técnico realizan el cambio final de la contraseña y la inactivación de la cuenta en una reunión presencial. La nueva contraseña se actualiza en el repositorio digital seguro y se registra el cierre de la solicitud en la herramienta de gestión, asegurando la trazabilidad de todo el proceso.

VI. **Registro y control**
Toda actividad de intercambio debe quedar documentada y justificada en la herramienta de gestión, para asegurar la transparencia, la rendición de cuentas y el cumplimiento de las políticas de seguridad de la información.

5. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	24/06/2025		Versión Inicial Deroga el Anexo 3 Protocolo para manejo de Usuarios Privilegiados.	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	Coordinación de Procesos y Riesgos Operacionales - Subdirección de Procesos.
Revisó:	Andrés Ricardo Castelblanco Mendoza	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones
	Francisco Andrés Daza Cardona	Jefe	Oficina de Seguridad de la Información
Aprobó:	Andrés Ricardo Castelblanco Mendoza	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones
	Francisco Andrés Daza Cardona	Jefe	Oficina de Seguridad de la Información