
	<b>PROCEDIMIENTO DE GESTIÓN DE ACCESOS</b>	Código: GS01-P24
		Versión: 1
		Página 1 de 19

## CONTENIDO

1	OBJETIVO .....	3
2	DESTINATARIOS .....	3
3	GLOSARIO .....	3
4	REFERENCIAS NORMATIVAS .....	5
5	GENERALIDADES .....	5
5.1	POLÍTICAS DEL PROCEDIMIENTO .....	6
5.2	ESTADOS DE UNA SOLICITUD .....	8
5.3	INTEGRACION CON OTRAS PRACTICAS DE GESTIÓN ITIL .....	9
6	REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO .....	9
7	DESCRIPCION DE ETAPAS Y ACTIVIDADES .....	12
7.1	ETAPA 1. CREAR CUENTA DE USUARIO .....	12
7.1.1	Solicitar la creación de cuenta de usuario .....	12
7.1.2	Validar y crear las solicitudes en la herramienta de gestión .....	13
7.1.3	Gestionar la solicitud .....	14
7.1.4	Ejecutar la lista de chequeo para la instrucción de ingreso a un nuevo usuario. 14	
7.2	ETAPA 2. CANCELAR CUENTAS DE USUARIOS .....	15
7.2.1	Solicitar la cancelación de cuentas de usuario .....	15
7.2.2	Crear las solicitudes en la herramienta de gestión .....	16
7.2.3	Notificar la cancelación de la cuenta de usuario.....	16
7.3	ETAPA 3. ACTUALIZAR PERMISOS EN CUENTAS DE USUARIOS.....	17
7.3.1	Notificar el traslado de un usuario .....	17
7.3.2	Validar los permisos actuales del usuario.....	17
7.3.3	Crear las solicitudes en la herramienta de gestión .....	17
7.3.4	Gestionar la solicitud y notificar al usuario.....	18


<b>Elaborado por:</b>  Nombre: Yeison Humberto Latorre Ruiz  Cargo: Coordinador Oficina de Tecnología	<b>Revisado y Aprobado por:</b>  Nombre: Francisco Andrés Rodríguez Eraso  Cargo: Jefe de Oficina de Tecnología e Informática	<b>Aprobación Metodológica por:</b>  Nombre: Ángel Augusto Velasco Mendoza  Cargo: Representante (E) de la Dirección para el Sistema de Gestión de Calidad  Fecha: 2021-02-16
---	---	---

Cualquier copia impresa, electrónica o de reproducción de este documento sin la marca de agua o el sello de control de documentos, se constituye en copia no controlada.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 2 de 19

7.4	ETAPA 4. REALIZAR SEGUIMIENTO Y CONTROL .....	18
7.4.1	Generar informe del estado de los accesos de los usuarios .....	18
7.4.2	Proponer y ejecutar mejoras al procedimiento.....	19
7.4.3	Producir y analizar mediciones del procedimiento.....	19
8	DOCUMENTOS RELACIONADOS.....	19
9	RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN .....	19

COPIA CONTROLADA

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 3 de 19

## 1 OBJETIVO

Definir los lineamientos para planificar y controlar el acceso de los usuarios a los sistemas de información de la Superintendencia de Industria y Comercio. A través de la descripción de las etapas de solicitud, revisión y atención de requerimientos de creación, cancelación de cuentas de usuarios que se realicen.

## 2 DESTINATARIOS

Este documento aplica a todos aquellos Servidores Públicos o Contratistas de la Superintendencia de Industria y Comercio, en adelante SIC, que participen directa o indirectamente en la gestión de las solicitudes de accesos que ingresan al Centro de Servicios Integrados de Tecnología - CSIT.

## 3 GLOSARIO

**ACCESO:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos tecnológicos de la SIC.

**ACTIVO DE INFORMACIÓN:** Es el elemento de información que se recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre en forma impresa, escrita, en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

**ANALISTA DEL CENTRO DE SERVICIOS INTEGRADOS DE TECNOLOGÍA:** es la persona encargada de registrar, canalizar, categorizar y solucionar las solicitudes de servicio de primer nivel, o en su defecto, escalar a los equipos de soporte para dar la solución final. Es llamado también Analista de primer nivel.

**AUTORIZADOR OTI:** responsable designado por la OTI para revisar, autorizar o denegar la ejecución de la solicitud, dando justificación de esta respuesta.

**CATEGORIZACIÓN:** es el listado de los servicios establecidos que se configuran en la herramienta de gestión, una vez ingresa un caso al Centro de Servicios Integrados de Tecnología (CSIT) o Mesa de Servicios, asigna una categoría dependiendo del tipo de solicitud y del grupo de trabajo responsable de su resolución.

**CENTRO DE SERVICIOS INTEGRADOS DE TECNOLOGÍA (CSIT):** Mesa de Servicios dispuesto por la OTI para atención a las solicitudes de tecnología.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 4 de 19

**CONFIDENCIALIDAD:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**COORDINADOR CSIT:** supervisor del Centro de Servicios Integrados de Tecnología.

**CORREO ELECTRÓNICO:** o en inglés e-mail (*electronic mail*), es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales. Su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

**DIRECTORIO ACTIVO:** herramienta que se utiliza para gestionar el acceso y los derechos.

**DISPONIBILIDAD:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

**ESPECIALISTA TI:** rol que se encarga de gestionar y solucionar servicios tecnológicos que tengan que ver con su competencia. Es llamado también Especialista de tercer nivel.


**INTEGRIDAD:** propiedad de salvaguardar la exactitud y estado completo de los activos.

**ITIL:** Conjunto de mejores prácticas destinadas a mejorar la gestión y provisión de servicios TI.

**MATRIZ DE CATEGORÍAS CSIT:** Listado de servicios tecnológicos ofrecidos por la OTI, bajo la cual se categorizan los servicios en la Herramienta de Gestión, es de uso exclusivo del CSIT.

**OTI:** Oficina de Tecnología e Informática de la Superintendencia de Industria y Comercio.

**SOLICITUD:** es una declaración formal de lo que se necesita, es también llamada Requerimiento.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 5 de 19

**SOLICITUD DE INFORMACIÓN:** hace referencia a todo tipo de solicitudes relacionadas con la entrega de información por parte del Centro de Servicios Integrados de Tecnología al solicitante, información relacionada con el estado de Solicitudes ya registradas, rutas en las cuales se encuentran formatos e instructivos, instrucciones acerca de cómo efectuar una solicitud de servicio que tiene un procedimiento definido y al momento no se cumple o el cómo diligenciar y autorizar los formatos preestablecidos para atender una solicitud.

**SOPORTE EN SITIO:** es la persona encargada de dar solución en sitio a las solicitudes que surjan de la infraestructura tecnológica de la SIC. Es llamado también Analista de segundo nivel.

**USUARIO:** Servidor Público o Contratista de la SIC que solicita un acceso para utilizar un servicio o un grupo de servicios proporcionados por la Oficina de Tecnología e Informática- OTI.


#### 4 REFERENCIAS NORMATIVAS

Jerarquía de la norma	Numero/Fecha	Título	Artículo	Aplicación Específica
Decreto Nacional	1008 del 14 de junio de 2018	Política de Gobierno Digital	Artículo 2.2.9.1.1.1 al 2.2.9.1.4.2	Aplicación total
NTC-ISO-IEC 27002	2013	Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información.	Aplicación total	Aplicación total

#### 5 GENERALIDADES

La Gestión de Accesos apoya la adecuada creación de cuentas de usuario y niveles de privilegio, lo cual es fundamental para preservar la confidencialidad, disponibilidad e integridad de activos de información, por ello se deben seguir un conjunto de pasos que garanticen la correcta asignación de permisos y faciliten la auditoría global de los usuarios. La identificación de los usuarios a través de sistemas de autenticación permitirá la identificación y aplicación de no repudio en las actividades diarias de los usuarios, además de controlar los niveles de acceso a recursos informáticos.

Existen tres clases tipos de cuentas de acceso:


	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 6 de 19

- Cuenta asignada a un Servidor Público, la cual será solicitada y aprobada solamente por el Grupo de Trabajo de Administración de Personal de la Superintendencia de Industria y Comercio.
- Cuenta asignada a un contratista la cual será solicitada y aprobada solamente por el Supervisor del contrato o Jefe, Director o Delgado o Coordinador del área alguna de las dependencias de la Superintendencia de Industria y Comercio.
- Cuenta de usuarios de los Administradores de Plataforma Tecnológica.


La Gestión de Accesos también se encargará del monitoreo de las cuentas activas, gestionando las solicitudes de actualización, reasignaciones, permisos y retiros, en este documento se detallará el proceso para cada una de estas solicitudes.

## 5.1 POLÍTICAS DEL PROCEDIMIENTO

- Todas las solicitudes de accesos (creación, modificación y cancelación), deben tramitarse por medio del Centro de Servicios Integrados de Tecnología. Para servidores públicos por medio del aplicativo dispuesto al Grupo de Administración de Personal y para contratistas a través de los Delegados, Directores, Jefes de Oficinas, Coordinadores de Grupo o quien ellos deleguen.
- En la creación de accesos de un colaborador nuevo a la Entidad, se debe asignar como mínimo el Conjunto Básico de Accesos, indicado en la actividad 7.1.2 de este documento.
- En caso que un contratista termine su contrato de forma anticipada se hará uso del GA01-F10 Formato Acta de Recibo Final y/o Informe Final de Ejecución como punto de control que asegura el retiro de los accesos al Contratista.
- El Gestor de Accesos deberá contar con el apoyo de la OTI en un informe semestral con los niveles de acceso o de privilegios asignados a los usuarios, a fin de analizar que sean apropiados de acuerdo con la misión de la SIC y se conserve la separación de funciones. De igual modo, la Gestión debe hacer revisión de los usuarios y accesos permitidos, mínimo una vez al mes, con el objetivo de garantizar que sea apropiado para los servicios ofrecidos y en caso dado, verificar e informar a la OTI las cuentas redundantes de usuarios.
- Los usuarios deben mantener la confidencialidad de sus contraseñas, evitando conservar registros de estas o compartirlas con demás personas.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 7 de 19

- La gestión del acceso físico a la Entidad (Tarjetas de acceso, ingreso de personal nuevo o visitante) se realiza de acuerdo con el GA03-P01 Procedimiento Servicios Administrativos.
- El acceso al datacenter principal de la SIC, se realizará de acuerdo con los procedimientos del proveedor. Para el acceso al datacenter ubicado en las instalaciones de la SIC, los Especialistas del Proveedor de TI tienen autorización y deben realizar el registro de ingreso y salida en el formato GS01-F05 Control de Acceso al Centro de Cómputo. Para el ingreso de personal diferente al Proveedor de TI, deberá ser autorizado por Coordinador del Grupo de Trabajo de Servicios Tecnológicos o el Jefe de la Oficina de Tecnología e Informática.
- Los Coordinadores del Grupo de Trabajo de Sistemas de Información y del Grupo de Trabajo de Gestión de Información y Proyectos Informáticos, o quien ellos deleguen, deberán enviar por correo electrónico al Centro de Servicios Integrados de Tecnología las solicitudes de accesos a las bases de datos mediante el formato GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de la SIC.
- Los accesos de los administradores de plataforma deberán ser gestionados de conformidad con el procedimiento del proveedor de TI contratado, quien debe garantizar el uso de buenas prácticas (Contraseñas robustas e intransferibles, repositorios seguros de contraseñas, acceso de acuerdo con perfil), dicho procedimiento deberá ser socializado al Coordinador del Grupo de Trabajo de Servicios Tecnológicos quien debe realizar las observaciones pertinentes, cuando identifique un posible riesgo de seguridad.
- El Proveedor de Servicios de Tecnología debe mantener actualizado los datos del personal especializado a su cargo y sus funciones, herramientas, cuentas y plataformas que administra cada uno. Deberá también informar los cambios de personal, con el fin de realizar supervisión de los requisitos del contrato.
- Cuando exista cambio de personal especializado del Proveedor de Servicios de Tecnología, se debe realizar un Acta de Entrega en el cual se deje constancia del estado de la infraestructura y de este modo, tener la información suficiente para el cambio de las contraseñas de las plataformas que se encontraban a su cargo.
- La información debe estar disponible sólo para usuarios autorizados.
- Cada usuario de un sistema de información puede disponer de una identificación única (ID). Sólo se permiten identificadores de grupo cuando se justifican por razones operativas. No se deben crear cuentas de usuario genéricas si estas van destinadas a un Servidor Público o Contratista.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 8 de 19


- El otorgamiento de un determinado nivel de acceso a un usuario o aplicativo en un sistema de información debe ser autorizado previamente por el/los dueños de los procesos, o quien él delegue, a los cuales pertenecen los datos gestionados por los sistemas de información a los que se solicita acceso, siempre partiendo del concepto de que se debe autorizar el mínimo nivel de privilegios necesarios para la realización de las funciones del usuario o el funcionamiento del aplicativo.
- No se permiten la creación de cuentas redundantes de usuarios para un mismo servicio y se debe conservar la separación de funciones.
- En caso de que la solicitud de creación de cuenta de usuario vulnera las Políticas de Control de Acceso, se debe informar el caso al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue, para revisar el motivo por el cual no se puede dar trámite a la solicitud.
- Todas las solicitudes de creación de usuarios de correo electrónico de contratistas deben ser autorizadas por el Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue.
- Cuando Entidades externas requieran acceso a información o sistema de información de la SIC, se debe contar con un acuerdo de confidencialidad que establezca las condiciones para la protección de la información. En consecuencia, la OTI debe tramitar el respectivo acceso con el CSIT, solo si ya cuenta con este documento firmado.
- Cuando se realice prórroga o renovación de un contrato la modificación de la vigencia de la cuenta debe ser solicitada por el Jefe inmediato o Supervisor del Contrato, indicando nombres completos del contratista, número de documento de identidad, número de contrato, nueva fecha finalización del contrato al correo [mesadeservicios@sic.gov.co](mailto:mesadeservicios@sic.gov.co).

Nota: Los roles y responsabilidades se encuentran detallados en el “Anexo 1. Roles y Responsabilidades de Gestión de Accesos”

## 5.2 ESTADOS DE UNA SOLICITUD

- Registrado: estado de la solicitud al momento de ser creado y genera un ID de identificación de la solicitud.
- En Autorización: la solicitud está en espera de autorización por parte del Autorizador de la OTI.
- Denegado: la solicitud se ha rechazado en la fase de autorización, por parte del Autorizador de la OTI.



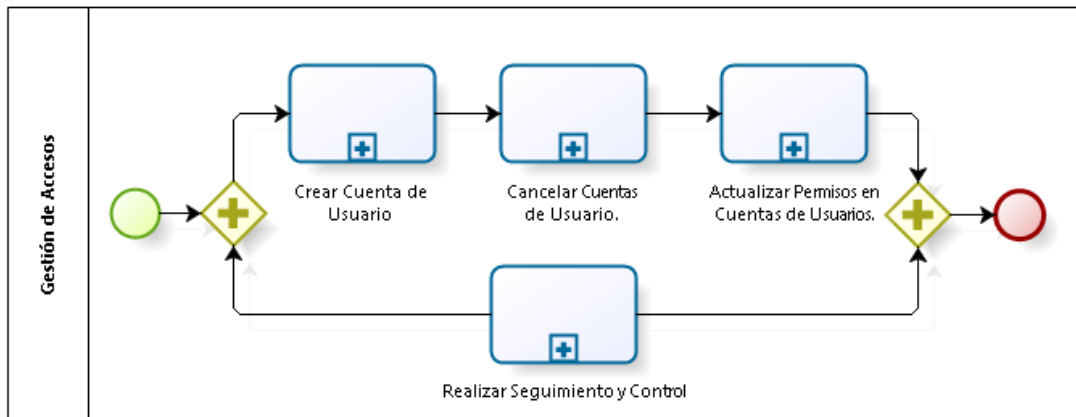
	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 9 de 19

- Aprobado: la solicitud se ha aprobado en la fase de autorización y está pendiente por ejecutar.
- En proceso: el responsable comienza la atención de la solicitud.
- Suspendido: por una causa justificada no se puede avanzar en la solución, lo anterior bajo los criterios del documento Manejo de Suspendidos.
- Solucionado: se ha dado solución a la solicitud. Se envía encuesta de satisfacción al usuario quien tiene 3 días hábiles para responderla.
- Cerrado: la solicitud pasa a este estado después de que ha finalizado el aseguramiento de calidad, lo anterior al ser calificada positivamente la encuesta o si en 3 días hábiles no es contestada, el sistema la cierra automáticamente. En caso de ser calificada negativamente la encuesta de satisfacción, la solicitud se reabre y pasa a estado En Proceso para su atención y solución.
- Anulado: estado al cual se pasan las solicitudes que son registradas por error o las solicitudes que se encuentran duplicadas.

### 5.3 INTEGRACION CON OTRAS PRACTICAS DE GESTIÓN ITIL

- Mesa de Servicios: punto único de contacto con los usuarios para los servicios de TI contratados.
- Gestión de Catálogo de Servicios: relación entre los servicios y los tipos de solicitudes de accesos.
- Gestión de Niveles de Servicios: tiempos de atención y solución de las solicitudes.
- Gestión de Incidentes: solicitudes que provienen de Incidentes, al reportar problemas con accesos previamente otorgados.
- Gestión de Solicitudes: La solicitud de un nuevo acceso o actualización de este, es un requerimiento estándar por lo que se debe gestionar según las actividades descritas en el Procedimiento GS01-P12 Gestión de Solicitudes.

## 6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO



No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	<b>CREAR CUENTA DE USUARIO.</b>	<p>Correo con necesidad de creación de una cuenta de usuario nueva.</p> <p>GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de la SIC</p> <p>Solicitud en estado En Proceso y en Autorización</p>	<p>En esta etapa se reciben y gestionan las solicitudes de creación de cuentas de usuario. Comprende las siguientes actividades:</p> <ul style="list-style-type: none"> <li>- Solicitar la creación de cuenta de usuario</li> <li>- Validar y crear las solicitudes en la herramienta de gestión.</li> <li>- Gestionar la solicitud.</li> <li>- Ejecutar la lista de chequeo para la instrucción de ingreso a un nuevo usuario.</li> </ul>	<p>Delegados, Directores, Jefes de Oficinas, Coordinadores de Grupo o quien ellos deleguen.</p> <p>Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue.</p> <p>Analista de Accesos.</p> <p>Profesional de Accesos.</p> <p>Grupo Autorizador de OTI.</p>	<p>Solicitud en estado Solucionado.</p> <p>Correo que informa la creación de la cuenta de usuario.</p> <p>GS01-F04. Lista de chequeo para instrucción de ingreso a un nuevo usuario.</p>
2	<b>CANCELAR CUENTAS DE USUARIO.</b>	<p>Correo Finalización del contrato.</p> <p>Terminación anticipada o cesión de contrato.</p> <p>Retiro de un servidor público de la entidad.</p> <p>GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de la SIC</p> <p>Solicitud en estado En Proceso y en Autorización.</p>	<p>En esta etapa se procede a cancelar las cuentas de usuario cuando se cumplen las condiciones pertinentes para ello. Comprende las siguientes actividades:</p> <ul style="list-style-type: none"> <li>- Solicitar la cancelación de cuentas de usuarios.</li> <li>- Crear las solicitudes en la herramienta de gestión.</li> <li>- Notificar la cancelación de la cuenta de usuario.</li> </ul>	<p>Analista de Accesos</p> <p>Profesional de Accesos.</p> <p>Delegados, Directores, Jefes de Oficinas, Coordinadores de Grupo o quien ellos deleguen.</p>	<p>Cuenta de usuario cancelada.</p> <p>Correo electrónico que notifica la cancelación de la cuenta de usuario.</p> <p>Solicitud en estado Solucionado.</p>

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
3	<b>ACTUALIZAR PERMISOS EN CUENTAS DE USUARIOS.</b>	<p>Correo Traslado de un servidor público entre dependencias.</p> <p>GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de la SIC</p> <p>Solicitud en estado En Proceso y en Autorización.</p>	<p>En esta etapa se reciben las solicitudes de actualización de cuentas de usuario de servidores públicos. Comprende las siguientes actividades:</p> <ul style="list-style-type: none"> <li>- Notificar el traslado de un usuario.</li> <li>- Validar los permisos actuales del usuario.</li> <li>- Crear las solicitudes en la herramienta de gestión.</li> <li>- Gestionar la solicitud y notificar al usuario.</li> </ul>	<p>Coordinador Grupo de Administración de Personal.</p> <p>Delegados, Directores, Jefes de Oficinas, Coordinadores de Grupo o quien ellos deleguen.</p> <p>Analista de Accesos.</p> <p>Profesional de Accesos.</p> <p>Grupo Autorizador de OTI.</p>	<p>Correo electrónico con la solicitud de validación de permisos.</p> <p>Cuenta de usuario con los privilegios ajustados.</p> <p>Solicitud en estado Solucionado.</p> <p>GS01-F04. Lista de chequeo para instrucción de ingreso a un nuevo usuario.</p>
4	<b>REALIZAR SEGUIMIENTO Y CONTROL</b>	<p>Solicitudes presentadas en el periodo de evaluación.</p> <p>Definición del Procedimiento y actualización.</p> <p>Dudas/observaciones de la operación.</p> <p>Oportunidades de mejora</p>	<p>En esta etapa se describen las actividades que realiza el Gestor de Solicitudes de manera transversal a las actividades del procedimiento y presenta las siguientes actividades:</p> <ul style="list-style-type: none"> <li>- Generar informe del estado de los accesos de los usuarios.</li> <li>- Proponer y ejecutar mejoras al procedimiento.</li> <li>- Producir y analizar mediciones del procedimiento.</li> </ul>	<p>Gestor de Solicitudes</p>	<p>Acciones de Mejora implementadas.</p> <p>Posible actualización Matriz de Categorías CSI.</p> <p>Capacitaciones.</p> <p>Correos.</p>

## 7 DESCRIPCIÓN DE ETAPAS Y ACTIVIDADES

### 7.1 ETAPA 1. CREAR CUENTA DE USUARIO

#### 7.1.1 Solicitar la creación de cuenta de usuario

##### **Para contratistas y proveedores:**

Para solicitar la creación de cuentas de usuario en los sistemas de información de la SIC, los Delegados, Directores, Jefes de Oficinas, Coordinadores de Grupo o quien ellos deleguen, deben remitir la siguiente información al CSIT enviando correo electrónico a [mesadeservicios@sic.gov.co](mailto:mesadeservicios@sic.gov.co).

a) Información solicitada en el siguiente cuadro:

No. Cédula	Fotocopia Cédula	Nombres y apellidos	Contratista - No. Contrato	Ubicación piso	Dependencia en la que laborará	Fecha inicio contrato	Fecha fin contrato	Perfil asociado Para Usuario de Dominio y Sistemas de Trámites
	Adjuntar al correo		Digitar SI o NO y el número del contrato vigente					


Nota: La columna "Perfil asociado" hace referencia a los permisos de consulta en el Sistema Trámites y usuario de Red que debe tener el usuario nuevo. Para ello se debe colocar como referencia la cuenta de un usuario del área para que quede con los mismos permisos.

- b) Listar los sistemas de información y el perfil que el usuario requiere para desempeñar sus funciones, por ejemplo, usuario de red, correo y trámites.
- c) Para Contratistas, adjuntar al correo fotocopia del contrato.

##### **Para servidores públicos:**

A través de la actualización del aplicativo dispuesto al Grupo de Administración de Personal para reportar el ingreso, retiro y traslado de servidores públicos, se informará al CSIT, mediante correo electrónico a la [mesadeservicios@sic.gov.co](mailto:mesadeservicios@sic.gov.co) comunicando que un nuevo servidor público ingresó a la entidad y la dependencia a la cual pertenecerá.

Para crear cuentas de usuarios en las bases de datos, se debe remitir el GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 13 de 19

la SIC, aprobado por el Coordinador del Grupo de Trabajo de Servicios Tecnológicos.

Para crear cuentas de correo de grupos especiales o de eventos, la solicitud debe ser remitida por el Delegado, Coordinador o Jefe de oficina de la SIC, indicando el nombre sugerido y los datos de quien será el responsable de la misma.

### 7.1.2 Validar y crear las solicitudes en la herramienta de gestión

El Centro de Servicios Integrados de Tecnología procede a validar el cumplimiento de las políticas de operación.

En toda creación de usuario se debe tener en cuenta el siguiente Conjunto Mínimo de Accesos:

Conjunto Mínimo de Accesos	Contratista	Servidor Público
Usuario de Dominio	X	X
Correo	X*	X
Sistema de Trámites	X	X
<b>VPN<sup>1</sup></b>	<b>X</b>	<b>X</b>
SIGEPSIC		X
Registro Horario		X
Sistema de Pagos	X	
Aranda	X	X

\*En caso que sea requerido.

Los permisos diferentes, se tramitarán como accesos específicos y deben indicar los Sistemas de Información y los módulos a los cuales se requiere el acceso.

Para los diferentes accesos y/o servicios solicitados, es necesario crear los siguientes casos y asignarlos de acuerdo con la Matriz de Categorías CSIT:

- Usuario de dominio
- Correo electrónico
- Creación en la base de datos del aplicativo Sistema de Trámites.
- Servicios adicionales: VPN<sup>1</sup>.
- Soporte en sitio para la configuración de perfil y los que haya lugar.

<sup>1</sup> Este servicio será incluido en el Conjunto Mínimo de Accesos únicamente en el escenario que, por fuerza mayor, los Funcionarios y Contratistas de la SIC deban realizar trabajo en casa ante un escenario de pandemia, desastre, política de teletrabajo o regulaciones tomadas por las autoridades competentes.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 14 de 19

- Permisos en Sistemas de información (la cantidad de casos de acuerdo con los accesos que se soliciten).

Nota: Las solicitudes de servicios adicionales sólo podrán ser gestionadas bajo la aprobación del Grupo Autorizador OTI y de acuerdo con la Matriz de Categorías CSIT.

Para Contratistas, el Analista de Accesos debe validar si existe un usuario previamente creado en el Directorio Activo, a fin de enviar correos a los Supervisores de Contratos (nuevo y antiguo) para validación de permisos requeridos, en caso que el Contratista se vincule a una dependencia diferente a la que anteriormente laboró.

Esta actividad es realizada por el Analista de Accesos.

### **7.1.3 Gestionar la solicitud**

Si la solicitud cumple con las políticas de control de acceso, el Profesional de Accesos ejecutará las acciones pertinentes para crear los perfiles en los sistemas de información o permitir los accesos a los servicios solicitados, documentará y solucionará el caso.

Si el caso es atendido por el Soporte en Sitio, se procede antes de la solución del caso con la actividad 7.1.4.

Se debe tener en cuenta que solo se asignará los privilegios y permisos que el usuario necesita, restringiendo los accesos a la información que no le competen. La asignación y entrega de contraseña debe ser realizada de acuerdo con la política de contraseñas referida en el documento GS02-I06 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI.

Una vez validados los accesos se procederá con la documentación y solución al caso, la herramienta de gestión automáticamente enviará notificación al solicitante, vía email, con el resultado de la solicitud.

Esta actividad es realizada por el Analista de Accesos, Especialista del Proveedor de TI o Profesional de la Oficina de Tecnología e Informática.

### **7.1.4 Ejecutar la lista de chequeo para la instrucción de ingreso a un nuevo usuario.**

Para todos los servidores públicos, contratistas que ingresen por primera vez a la entidad, el Analista de Soporte en Sitio validará junto al usuario que la configuración

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 15 de 19

de perfil en el equipo es la adecuada y realizará pruebas de ingreso a los diferentes servicios solicitados, de acuerdo con el formato GS01-F04 Lista de chequeo para instrucción de ingreso a un nuevo usuario y se procederá con la documentación y solución al caso adjuntando el formato firmado. La herramienta de forma automática envía al solicitante la solución dada mediante correo electrónico.

En caso que falte el acceso a algunos de los servicios o aplicativos, el Analista de Soporte en Sitio realizará la respectiva nota en el caso que corresponda y comunicará al Gestor de Accesos para agilizar el trámite, suspendiendo su caso de configuración de acuerdo con la política 5.1.5. del Procedimiento GS01-P12 Gestión de Solicitudes.

## **7.2 ETAPA 2. CANCELAR CUENTAS DE USUARIOS**

### **7.2.1 Solicitar la cancelación de cuentas de usuario**

#### **Para contratistas y proveedores**

La deshabilitación de cuentas de usuario de contratistas y proveedores puede presentarse por cualquiera de los siguientes casos:

a) Cuando finaliza la fecha del contrato:

La información del campo “fecha fin contrato” reportado en la solicitud de creación la cuenta de usuario será utilizada para programar la deshabilitación automática de las cuentas de usuario. Si el sistema de información no permite la configuración de bloqueo automática, el administrador del sistema de información por parte de la OTI, debe bloquear manualmente la cuenta de usuario en la fecha prevista.

Como punto de control se tiene el GA01-F10. Formato Acta de Recibo Final y/o Informe Final de Ejecución, revisado por el CSIT y firmado por el Jefe de la OTI.

b) Cuando se presenta una terminación anticipada o cesión de contrato:

Los Delegados, Directores, Jefes de Oficinas o Coordinadores de Grupo deben solicitar al CSIT mediante correo electrónico a [mesadeservicios@sic.gov.co](mailto:mesadeservicios@sic.gov.co) la cancelación de la cuenta de usuario.

#### **Para servidores públicos**

A través de la actualización del aplicativo dispuesto al Grupo de Administración de Personal para reportar el ingreso, retiro y traslado de servidores públicos, se

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 16 de 19

informará al CSIT mediante correo electrónico a [mesadeservicios@sic.gov.co](mailto:mesadeservicios@sic.gov.co) comunicando que un servidor público se retiró de la entidad.

Como punto de control se tiene el GT02-F19. Entrega de Documentos y Bienes a Cargo del Servidor Público, revisado por el CSIT y firmado por el Jefe de la OTI.

Para cancelar cuentas de usuarios en las bases de datos, se debe remitir el GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de la SIC, aprobado por el Coordinador del Grupo de Trabajo de Servicios Tecnológicos.

Para eliminar cuentas de correo de grupos especiales o de eventos, la solicitud debe ser enviada por el Delegado, Coordinador o Jefe de oficina de la SIC o el responsable de la misma al CSIT.

### **7.2.2 Crear las solicitudes en la herramienta de gestión**

El CSIT genera el caso y en conjunto con los administradores de los sistemas de información en la OTI, debe realizar la cancelación de cuentas de usuario, la revocación de la contraseña y la destitución de privilegios (incluidas las solicitudes de revocación de cuentas de usuario de teletrabajo - VPN).

Para la eliminación de los diferentes accesos y/o servicios solicitados, es necesario crear los siguientes casos y asignarlos de acuerdo con la Matriz de Categorías CSIT:


- Usuario de dominio
- Correo electrónico
- Los permisos en Sistemas de información quedarán deshabilitados dado que están alineados con Directorio Activo, sólo deben crearse para los casos en los que no se tenga la anterior condición.
- Servicios adicionales: VPN.

Esta actividad es realizada por el Analista de Accesos.

### **7.2.3 Notificar la cancelación de la cuenta de usuario**

El Profesional de Accesos ejecutará las acciones pertinentes para eliminar los perfiles en los sistemas de información o eliminar los accesos a los servicios solicitados, documentará y solucionará el caso. La herramienta de forma automática envía al solicitante la solución dada mediante correo electrónico.



	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 17 de 19

Esta actividad es realizada por el Especialista del Proveedor de TI o Profesional de la Oficina de Tecnología e Informática.

### **7.3 ETAPA 3. ACTUALIZAR PERMISOS EN CUENTAS DE USUARIOS**

#### **7.3.1 Notificar el traslado de un usuario**

Los traslados aplican para servidores públicos y se reportan a través de la actualización del aplicativo del Grupo de Administración de Personal dispuesto para reportar el ingreso, retiro y traslado de un servidor público, se informará al CSIT mediante correo electrónico a [mesadeservicios@sic.gov.co](mailto:mesadeservicios@sic.gov.co) comunicando que un servidor público pertenecerá a una nueva dependencia.

Para actualizar cuentas de usuarios en las bases de datos, se debe remitir el GS01-F18 formato de creación, modificación y/o eliminación de usuarios en bases de datos de la SIC, aprobado por el Coordinador del Grupo de Trabajo de Servicios Tecnológicos.

#### **7.3.2 Validar los permisos actuales del usuario**

El Analista de Accesos debe informar por correo electrónico al Jefe inmediato antiguo (Información tomada del Directorio de Servidores Públicos de la SIC), el traslado del usuario y solicitar la validación de si se deben mantener o revocar permisos a algún aplicativo. Una vez se tenga respuesta, crear los casos respectivos de acuerdo con la Matriz de Categorías CSIT.

En caso de reportarse vacaciones o licencias, se creará caso para el Analista de Accesos y Especialista del Proveedor de TI para correo, de acuerdo con la Matriz de Categorías CSIT y a fin de documentar dicho estado en el Directorio Activo y bloquear correo electrónico.

#### **7.3.3 Crear las solicitudes en la herramienta de gestión**

Para actualizar los diferentes accesos y/o servicios solicitados, es necesario crear los siguientes casos y asignarlos de acuerdo con la Matriz de Categorías CSIT:

- Permisos en Sistemas de información (la cantidad de casos de acuerdo con los accesos que se soliciten).
- Servicios adicionales: VPN.
- Soporte en sitio para la configuración de perfil y los que haya lugar.

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 18 de 19

Nota: La modificación de servicios adicionales sólo podrá ser gestionadas bajo la aprobación del Grupo Autorizador OTI y de acuerdo con la Matriz de Categorías CSIT.

Esta actividad es realizada por el Analista de Accesos.

### **7.3.4 Gestionar la solicitud y notificar al usuario**

El Profesional de Accesos ejecutará las acciones pertinentes para modificar los privilegios de las cuentas de usuario en los sistemas de información de la SIC, de acuerdo con la solicitud de los Delegados, Directores, Jefes de Oficinas o Coordinadores de Grupo, previa validación del cumplimiento la política de control de acceso del documento GS02-I06 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI, documentará y solucionará el caso.

En caso de ser necesario, el Profesional de Accesos puede escalar la solicitud al Analista de Soporte en Sitio con el fin de realizar validación y pruebas con el Usuario. Si dichas pruebas no son satisfactorias, se devuelve el caso al Profesional de Accesos con el fin de revisar nuevamente y encontrar la solución.

En caso que falte el acceso a algunos de los servicios o aplicativos, el Analista de Soporte en Sitio realizará la respectiva nota en el caso que corresponda y comunicará al Gestor para agilizar el trámite, suspendiendo su caso de configuración de acuerdo con la política 5.1.5. del Procedimiento GS01-P12 Gestión de Solicitudes.


Una vez validados los accesos se deberá diligenciar junto al usuario el formato GS01-F04. Lista de chequeo para instrucción de ingreso a un nuevo usuario y se procederá con la documentación y solución al caso adjuntando el formato firmado. La herramienta de forma automática envía al solicitante la solución dada mediante correo electrónico.

Esta actividad es realizada por el Analista de Accesos, Especialista del Proveedor de TI, Profesional de la Oficina de Tecnología e Informática o Analista de Soporte en Sitio.

## **7.4 ETAPA 4. REALIZAR SEGUIMIENTO Y CONTROL**

### **7.4.1 Generar informe del estado de los accesos de los usuarios**

Teniendo en cuenta la base de datos actualizada donde figuran todos los usuarios a los que se les ha generado accesos y con el apoyo de los Profesionales de los diferentes Sistemas de Información de la SIC, el Gestor de Accesos validará el

	PROCEDIMIENTO DE GESTIÓN DE ACCESOS	Código: GS01-P24
		Versión: 1
		Página 19 de 19

estado de los accesos de los usuarios a fin de restringir los no autorizados o no utilizados.

Esta actividad es realizada por el Gestor de Accesos.

#### **7.4.2 Proponer y ejecutar mejoras al procedimiento.**

Esta actividad se realiza para promover la adecuada ejecución del procedimiento y difundir sus actualizaciones o cambios, aclarar las dudas u observaciones que se generen en los responsables de gestionar las solicitudes de accesos.

Todo el conjunto de actividades debe enfocarse en la mejora continua y es realizada por el Gestor de Accesos.

#### **7.4.3 Producir y analizar mediciones del procedimiento.**

Obtener las mediciones de la gestión para identificar su comportamiento y tendencias, con base en dichas mediciones y sus resultados, se identificarán mejoras conforme lo dispuesto en el Instructivo CI01-I04 Planes de Mejoramiento.

Todo el conjunto de actividades debe enfocarse en la mejora continua y es realizada por el Gestor de Accesos.

### **8 DOCUMENTOS RELACIONADOS**

- GS01-P12 Procedimiento Gestión de Solicitudes.
- GS02-I06 Políticas del Sistema de Gestión de Seguridad de la Información SGI
- GA01-F10. Formato acta de recibo final y/o informe final de ejecución.
- GT02-F19. Entrega de documentos y bienes a cargo del servidor público.
- GS01-F04. Lista de chequeo para instrucción de ingreso a un nuevo usuario.
- GS01-F05. Formato de control de acceso al centro de cómputo.

### **9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN**

El documento se actualiza complementando información en el punto 5 Generalidades, agregando Políticas de Operación, Roles y Responsabilidades, Estados de una Solicitud, Integración con otras prácticas de gestión ITIL. Se relaciona la cuarta etapa llamada Realizar Seguimiento y Control. Cambia el nombre de Procedimiento de Creación, Cancelación y Actualización de Cuentas de Usuarios a Procedimiento de Gestión de Accesos.

---

Fin documento