SUPERINTENDENCIA DE SOCIEDADES

PROCEDIMIENTO DE GESTION USUARIOS DE LA PLATAFORMA TECNOLÓGICA

1. INFORMACIÓN GENERAL.

1.1 OBJETIVO	Gestionar el proceso de creación, activación/desactivación, modificación, eliminación y divulgación de las cuentas de usuario de red y de los sistemas de información de la Entidad (internos y externos para el acceso a los activos de información.
1.2. RESPONSABLE	Coordinador Grupo de Sistemas y Arquitectura de Tecnología
1.3. ALCANCE	Es aplicable a los sistemas de información, aplicaciones y servicios informáticos que permitan la gestión de cuentas de usuarios y roles.
1.4. DEFINICIONES	**Nombre de usuario:** Es el identificador del usuario para ingresar a un a un sistema de información, terminal, o computador personal. **Clave de acceso o contraseña:** Combinación de letras, símbolos y/o números que deben digitarse para obtener acceso a un sistema de información, terminal, o computador personal. Estas llaves si son utilizadas en forma personal, secreta, e intransferible, garantizan una adecuada utilización, resguardo y confiabilidad de la información. **Credenciales de Acceso:** Es la que se asocia a un único usuario el cual requiere para acceder un nombre de usuario y contraseña. **Servicios de la plataforma tecnológica** Todos aquellos servicios controlados por componentes de Tecnologías de la Información y comunicaciones y administrados desde el centro de cómputo de la Entidad. **Rol:** Son las funciones que cada usuario tiene que cumplir dentro del sistema. **Perfil:** es una colección de permisos que definen el acceso a un conjunto de transacciones en el sistema **Usuario:** Es una persona que utiliza un sistema o un servicio informático. Para la superintendencia de sociedades se asigna el carácter de usuario a funcionarios, contratistas, pasantes, judicantes o cualquier otra persona que deba ejercer funciones en la Entidad y requiera el uso de servicios de la plataforma tecnológica. **Usuarios o cuentas Privilegiadas:** Son credenciales que han sido entregadas a usuarios a los que se le han asignados accesos con funciones que permiten realizar múltiples acciones administrativas que requieren conocimiento técnico especializado.

1.5. RESPONSABILIDADES:	**Directores o coordinadores, jefe de Área, Supervisores del Contrato:** Encargados de autorizar el personal a su servicio para la creación, activación/desactivación, modificación de cuentas de usuarios. **Dirección de Talento Humano:** Encargada de reportar novedades de personal de planta, judicantes, pasantes etc. **Propietario de la información:** responsables funcionales de las diferentes aplicaciones, quienes conocen la operación de los accesos y permisos de cada aplicación y son los encargados de monitorear que los accesos se otorguen garantizando el mínimo privilegio y la segregación de roles y permisos. **Usuario Técnico Interno – Rol de Administrador Funcional:** Rol responsable de realizar la creación, modificación, eliminación e inactivación de los usuarios en un sistema de información institucional (por ejemplo, Moodle, Kactus, Postal etc.) o externo (por ejemplo, Siif Nación, Secop, Sigep, etc.) **Dirección de Tecnologías de la Información y las Comunicaciones:** Es la encargada a través del administrador de Directorio Activo, de la creación, activación/desactivación de cuentas de usuarios de red y correo, una vez son notificados por parte de los jefes de área o directores o supervisor del contrato.

2 GENERALIDADES – NORMAS GENERALES

Las políticas generales sobre control de acceso se encuentran documentadas en el GC-PO-001 Documento de Políticas del SGI y los lineamientos generales en el documento GC-MO-001 Documento de Modelos del SGI Numeral Política de control de acceso, estos lineamientos normalizan las actividades referentes al acceso a los sistemas de información (Aplicaciones), Red, Internet, correo electrónico, Bases de datos y el presente procedimiento servirá de guía para cumplir con estas políticas.

- Cada funcionario o persona debidamente autorizada que ingrese a la Superintendencia de Sociedades tiene derecho y acceso a unos recursos logísticos y de infraestructura tecnológica; se le asignarán unas credenciales de acceso a través de un nombre de usuario y su correspondiente contraseña los cuales le permitirán acceder a la red de datos y podrá tener acceso a la información y a los servicios informáticos generales, de acuerdo con el perfil y rol asignado.

- Solo funcionarios autorizados en Tecnología y de las áreas propietarias de la información, pueden realizar actualización de usuarios y contraseñas basados en requerimientos formales por los medios de comunicación autorizados en Supersociedades.

- La cuenta de usuario y los tokens son de uso único e intransferible y de responsabilidad de la persona a la que está asignada.
- Los requerimientos de actualización (creación, retiro, modificación, activación e inactivación) de las credenciales de acceso nombres de usuario y contraseñas sobre componentes tecnológicos, son responsabilidad de los propietarios de la infraestructura en el caso de tecnología y de los propietarios de información en el caso de los sistemas de información.
- Los propietarios de la información deberán designar a un funcionario a quien se le otorgará el rol de Administrador funcional, quien tendrá la responsabilidad de otorgar los accesos, perfiles y permisos sobre el sistema de información de su responsabilidad y gestionará todas las novedades, cumpliendo con las políticas y normas aquí establecidas.
- Todo usuario que se cree debe estar asociado a un funcionario o contratista quien será responsable del acceso. No se deben crear usuarios genéricos. Si es necesario crear un usuario que no tenga asociado un nombre de funcionario o contratista (cuentas de servicio o aplicación), este debe ser revisada y justificada por el solicitante.
- Cada vez que un usuario sea trasladado a otra área o cambie de perfil, se debe realizar el ajuste de los accesos de acuerdo con el nuevo perfil asignado.
- Una cuenta de usuario debe tener asociada como mínimo la siguiente información: nombre del usuario, contraseña, cédula, jefe inmediato, área a la que pertenece, buzón de correo, para permitirle acceder a recursos locales o de red, a través del Directorio Activo o aplicación
- Se debe evitar el uso de claves compartidas genéricas o para grupos, la identificación y autenticación en los sistemas de cómputo debe ser única y personalizada.
- Todos los servicios que se expongan en la Web, que requieran autenticación deben contar con certificado digital.
- Los propietarios de la información deberán realizar revisión periódica de los accesos otorgados, con el fin de garantizar que los usuarios cuenten con los permisos necesarios para el desarrollo de su función.
- Los propietarios de la información deben garantizar la correcta segregación de permisos y accesos a las aplicaciones y sistemas de los cuales son responsables.
- La administración técnica de la plataforma tecnológica de la Superintendencia está a cargo única y exclusivamente de la Dirección de Tecnología de la Información y las Comunicaciones, a través de su equipo de Ingenieros.

2.1. APROVISIONAMIENTO DE LOS ACCESOS A LOS USUARIOS

2.1.1. Solicitud de Acceso:

De acuerdo con el documento GTH-I-001 INSTRUCTIVO PARA INGRESOS, REUBICACIÓNES Y RETIROS DE FUNCIONARIOS, el Grupo de Administración del Talento Humano, cinco (5) días hábiles antes del ingreso, reubicación o retiro, reportará por el medio autorizado, la novedad de personal al Coordinador del Grupo de sistemas y Arquitectura de Tecnología y/ a quien este delegue para la configuración del equipo de cómputo. De igual manera a otras áreas para la actualización de usuarios en los sistemas correspondientes a su perfil. Y en casos específicos a la mesa de ayuda al correo soporte@supersociedades.gov.co.

- Los medios autorizados para reportar las novedades del personal, o asignaciones de usuarios administradores, son: el correo electrónico y/o el trámite 46001 de Postal.
- Es responsabilidad del jefe directo del funcionario, pasante, judicante o contratista solicitar Autorización de Servicios Informáticos para Usuarios, por medio del trámite 46001. Se debe indicar los servicios y sistemas a los cuales se está autorizando el funcionario. En caso de que la forma no contenga los servicios o sistemas requeridos, se deben anotar en el campo de observación.
- Es responsabilidad de los administradores funcionales de la dependencia propietaria del sistema de información o servicio de la plataforma tecnológica, realizar la actualización de las cuentas de usuario de acuerdo con el rol que se indique para el funcionario, según número de tramite 46001.
- Es responsabilidad del funcionario asignado al caso, en el área de Sistemas realizar toda la gestión de usuarios con los administradores funcionales y técnicos correspondientes, dependiendo de los servicios autorizados por el jefe inmediato, en el formato correspondiente, previa aprobación del Coordinador Grupo de Sistemas y Arquitectura de Tecnología o a quién él delegue. Así mismo, almacenar en un sitio específico los requerimientos realizados de gestión de acceso, como soporte a las revisiones y configuraciones que se realicen.
- Es responsabilidad de la Mesa de Ayuda gestionar cualquier incidente que se presente con la actualización de cuentas de usuario mediante la revisión y/o coordinación con los encargados de las plataformas tecnológicas.
- Los Administradores técnicos de los Sistemas de Información y los responsables de los servicios de la plataforma tecnológica y seguridad, realizarán semestralmente una revisión integral de los usuarios. Como soporte se debe realizar un acta de revisión y actualización.
- En caso de encontrarse diferencias se deben realizar las actualizaciones de usuarios correspondientes en cada uno de los sistemas de información y plataformas tecnológicas.
- Cuando sea aplicable, dependiendo de los Sistemas de Información, se asignarán permisos de acceso por grupos de usuarios y no a individuos.
- Cuando sea aplicable los sistemas de información o servicios de la plataforma tecnológica, realizaran su autenticación a través del Directorio Activo como estándar corporativo.
- Por ningún motivo se permitirá la suplantación de usuarios, el uso indebido de los recursos tecnológicos o el acceso no autorizado a los sistemas de información o de los servicios de la plataforma tecnológica.

La siguiente tabla muestra los perfiles técnicos y funcionales que utilizan los sistemas de información que actualmente gestionan usuarios:

2.1.2. Perfiles de acceso:

Se establecen los siguientes tipos de perfiles o roles de accesos con los cuales debe contar un sistema de información:

TIPO DE PERFIL DE ACCESO	DESCRIPCIÓN
Rol Superadministrador (SA)	Corresponde al acceso que cuenta con todos los privilegios a todos y cada uno de los servicios, sistemas operativos, herramientas, bases de datos y componentes tecnológicos

TIPO DE PERFIL DE ACCESO	DESCRIPCIÓN
	que requieran credenciales de acceso para su administración. Las cuentas de usuario de superadministrador son entregadas normalmente por las entidades que venden las plataformas tecnológicas y son cuentas que solo se deben usar por una primera vez cuando se configure la plataforma y se generen usuarios administradores. Tiene privilegios de configurar la plataforma, configurar la seguridad, configurar recursos, creación de usuarios y grupos de usuarios. Esta cuenta se cataloga como Privilegiada
Rol Servicio (RS)	Corresponde al acceso a sistemas de información y o aplicaciones que cuentan con funciones sobre procesos automáticos de ejecución, conexión o de interrelación con otros procesos. Deben estar bajo responsabilidad de algún funcionario.
Rol Institucional (RI)	Corresponde al acceso creado para desarrollar actividades propias de un proceso de negocio como por ejemplo un buzón de correo para dar respuesta interna o externa a requerimientos de información. Deben estar bajo responsabilidad de algún funcionario.
Rol Administrador Funcional (RAF)	Corresponde al acceso de los sistemas de información o aplicaciones que cuentan con un funcionario encargado del módulo de administración de usuarios y de quien dependen las actividades de: - Registro y actualización, modificación y eliminación o inactivación de usuarios, contraseñas y permisos. son asignados garantizando el mínimo privilegio a usuarios nombrados no genéricos.
Rol Administrador técnico (RT)	Corresponde al acceso con privilegios sobre un componente exclusivo de la infraestructura y puede configurar el componente, configurar la seguridad y configurar recursos, son asignados garantizando el mínimo privilegio a usuarios nombrados no genéricos.
Rol Usuario (RU)	Corresponde al acceso que utilizan el sistema de información o la aplicación para ejecutar las funcionalidades propias del mismo. son asignados garantizando el mínimo privilegio a usuarios nombrados no genéricos.

2.1.3. Tipos de usuarios:

La Superintendencia de Sociedades tendrá una clasificación general de usuarios que permita identificar el nivel y el alcance de cada funcionario con respecto al sistema de administración de usuarios. Los tipos de control de acceso establecidos son:

TIPO DE USUARIO	DESCRIPCIÓN	ALCANCE
Usuario Interno	Funcionarios o colaboradores de la Superintendencia de sociedades con privilegios suficientes para hacer uso de los recursos de los sistemas de información a los cuales tiene derechos de acceso.	Estos usuarios tendrán acceso monitoreado a los sistemas de información de Supersociedades. - Sistemas aplicativos - Sistemas Administrativos - Sistemas Gerenciales. - Sistemas de información externos con los que Supersociedades tiene convenio contractual Podrán actualizar o consultar información de acuerdo con los privilegios que se les otorga.
Usuario Externo	Corresponde a los usuarios clientes de Supersociedades o terceros con relación contractual con privilegios de acceso, que harán uso de los recursos de los sistemas de información a los cuales tiene derechos de acceso.	Estos usuarios tendrán acceso monitoreado a los sistemas de información de Supersociedades: - Sistemas Aplicativos - Sistemas Administrativos - Sistemas Gerenciales - Sistemas de información externos con los que Supersociedades tenga convenio contractual. Podrán actualizar o consultar información de acuerdo con los privilegios que se les otorga.
Usuario Técnico Interno	Corresponde a los usuarios a quienes se les asigna la labor de administración de acceso de los sistemas de información, a los sistemas	Estos usuarios podrán: -Crear usuarios - Ajustar configuraciones - Actualizar usuarios. - Asignar permisos y roles.

TIPO DE USUARIO	DESCRIPCIÓN	ALCANCE
	operativos y redes. (SA, ROOT, ADMIN, TFS)	- Asignar claves iniciales de acceso. - Instalación de herramientas, complementos, software y/o aplicaciones. Técnicos externos no deben tener este tipo de cuentas.
Usuario Técnico Externo	Funcionarios externos a la Superintendencia de Sociedades a los cuales se les entrega la administración de plataformas o componentes puntuales para garantizar la funcionalidad de esta, restringida únicamente a la labor de administración encomendada por la Supersociedades. Funcionarios de entidades externas a Supersociedades, poseedoras de sistemas de información a los cuales ingresan sus funcionarios.	Estos usuarios podrán: - Crear usuarios dentro de la plataforma asignada - Actualizar usuarios. - Asignar permisos y roles. - Asignar contraseñas iniciales de acceso - Ejecutar procesos de administración, monitoreo y respaldo -Diagnosticar fallas y proponer alternativas de solución -Realizar reporte de la gestión realizada mensualmente.
Usuario Técnico de Servicio	Son usuarios especiales que se utilizan para la ejecución de servicios específicos, subir servicios, conectividad entre aplicativos, ejecutar tareas sobre bases de datos y ejecución de procesos. No pueden ser usuarios internos, externos, técnicos internos, técnicos externos, Son cuentas de servicio.	Estos usuarios siempre tendrán un responsable en las áreas técnicas.

2.1.4. Aplicación de Novedades:

Las novedades que hacen parte del proceso de aprovisionamiento de la gestión de la identidad del usuario a través del directorio activo y en los diferentes sistemas y/o aplicativos son:

- Ingreso de Personal
    - Novedad talento humano (para funcionarios y estudiantes en práctica)
    - Novedad supervisor de contrato (contratistas directos y soportes externos)
- Asignación y finalización temporal de funciones en un Grupo diferente
- Designación y/o asignación Temporal de Funciones
- Encargo de Funciones (Sin fecha límite)
- Retiro de Personal
    - Novedad talento humano (para funcionarios y estudiantes en práctica)
    - Novedad supervisor de contrato (contratistas directos y soportes externos)
- Reubicación (sin fecha límite)

Para la aplicación de estas novedades se realizan las actividades y se aplican condiciones especiales, que se reflejan en la siguiente tabla:

Novedad	Acciones Realizadas	Soporte
Ingreso de Personal	• Creación de la cuenta de D.A teniendo en cuenta el estándar de creación de usuarios • Solicitud de creación de cuenta de correo • Adición de la cuenta del funcionario a la lista de distribución de correo del Grupo. • Ajustar la descripción del cargo del funcionario • Asignación del jefe directo del funcionario • Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	• No se recibe ningún memorando • La asignación de permisos en D.A se realiza una vez se recibe formato 46001
Asignación temporal de funciones en un Grupo diferente	• Adición de la cuenta del funcionario a la lista de distribución de correo del nuevo Grupo. • Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	• Se recibe memorando con fechas y grupo • No se recibe formato 46001 por si debe realizar nuevas funciones
Finalización de Asignación temporal de funciones en un el Grupo diferente	• Retiro de la cuenta del funcionario a la lista de distribución de correo del nuevo Grupo.	• Ocasionalmente se recibe memorando de terminación • No se recibe formato 46001 por si debe retirar nuevas funciones

Novedad	Acciones Realizadas	Soporte
	• Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	
Designación Temporal de Funciones de Coordinación o Asignación de Funciones de Coordinación	• Adición de la cuenta del funcionario a la lista de distribución Coordinadores. • Se informa a personal gestión realizada • Retiro de la cuenta del funcionario de la lista de distribución Coordinadores, una vez se cumpla plazo • Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	• No se recibe ningún memorando • No se modifica Manager Original de la Coordinación
Encargo de Funciones (Sin fecha limite)	• Adición de la cuenta del funcionario a la lista de distribución de correo del nuevo Grupo. • Modificación de la descripción del cargo del funcionario • Asignación de personal a cargo • Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	• No se recibe ningún memorando
Novedad Retiro de Personal	• Retiro de la cuenta del funcionario de los grupos de D.A • Adición de la cuenta al grupo Usuarios Inactivos • Desactivación de la cuenta de D.A. • Solicitud de desactivación de la cuenta de correo electrónico • Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	• No se recibe ningún memorando • Se dan tres días después de la fecha de retiro para realizar backup de la información del funcionario

Novedad	Acciones Realizadas	Soporte
Reubicación (sin fecha límite)	• Retiro de la cuenta del funcionario de los grupos de D.A • Adición de la cuenta del funcionario a la lista de distribución de correo del nuevo Grupo. • Modificación de la descripción del cargo del funcionario • Asignación del nuevo manager del funcionario • Se informa a Recursos Humanos y a Mesa de Ayuda gestión realizada	• Se recibe memorando con fechas, grupo y cargo a desempeñar • Se requiere trámite del formato 46001, para asignación de permisos de acuerdo a nuevas funciones. • Los usuarios conservan los permisos básicos en D.A (Usuarios de dominio)

2.1.5. Estándar de creación de usuarios:

Con el fin de generar un estándar para la creación de usuarios de red y de aplicaciones internas que se utilizan, el nombre de usuario debe generarse de la siguiente forma y debe ser el mismo en todas las aplicaciones en donde sea creado:

1. Primer nombre seguido del signo (.), más el primer apellido; si ya existe este usuario
2. Primer nombre más la primera letra del segundo nombre seguido del signo (.), más el primer apellido; si ya existe este usuario.
3. Primer nombre seguido del signo (.), más el primer apellido más la primera letra del segundo apellido; si ya existe este usuario.
4. Primer nombre más la primera letra del segundo nombre seguido del signo (.), más el primer apellido más la primera letra del segundo apellido.
5. Primera letra del primer nombre, más el segundo nombre seguido del signo (.), más el primer apellido; si ya existe este usuario.
6. Primera letra del primer nombre seguido del segundo nombre más el signo (.), más el primer apellido, más la primera letra del segundo apellido; si ya existe este usuario.
7. Primera letra del primer nombre seguido de segundo nombre más el signo (.), más la primera letra del primer apellido más el segundo apellido.

Ejemplos: Jose Pedro Pinchao Martinez

1.Jose.pinchao@supersociedades.gov.co
2.Josep.pinchao@supersociedades.gov.co
3.Jose.pinchaom@supersociedades.gov.co
4.Josep.pinchaom@supersociedades.gov.co
5. Jpedro.Pinchao@supersociedes.gov.co
6.JPedro.pinchaoM@supersociedades.gov.co
7.JPedro.Pmartinez@supersociedades.gov.co

Nota: mientras el proceso de identidad se mantenga Onpremise, estas nomenclaturas están limitadas a 24 caracteres en su parte inicial, si se llega a migrar a la nube de M365 no se tendrá esta restricción.

Nota: Para las aplicaciones externas el administrador de los accesos deberá dar cumplimiento a lo establecido en la entidad externa para su creación, en caso de no contar con un estándar deberá aplicar lo aquí establecido.

2.1.6. Ausencias o Licencias:

- Cuando la ausencia sea mayor a cinco días, el profesional de Talento Humano o el supervisor del contrato, realiza la solicitud a través de correo electrónico a la mesa de ayuda, indicando el nombre del usuario, el tiempo de duración de la ausencia y el motivo
- En caso de vacaciones o ausencias de los funcionarios es responsabilidad del jefe inmediato solicitar a la mesa de ayuda el acondicionamiento de las herramientas para que el funcionario encargado utilice sus propias credenciales de acceso (usuario y contraseña) utilizando el procedimiento de soporte técnico, mantenimiento preventivo y correctivo GINF-PR-002.

  Por ejemplo: Servicio Telefónico, Correo Electrónico, Internet, Impresión, Carpetas compartidas que utilice tanto de lectura como de actualización, detallando expresamente el nombre y ubicación, Sistema de Información y su respectivo rol, tanto de consulta como de actualización, entre otros

2.1.7. Eliminación de usuarios de las aplicaciones no conectadas al directorio activo:

Para el retiro de un usuario de las diferentes aplicaciones existentes en la Superintendencia de Sociedades, es necesario que se cumplan los siguientes pasos:

a. En los cinco (5) días hábiles antes del retiro de un funcionario, el Grupo de Administración de personal debe enviar por algún medio autorizado, el documento GTH-I-001 INSTRUCTIVO PARA INGRESOS, REUBICACIÓNES Y RETIROS DE FUNCIONARIOS, con la novedad de personal, a los diferentes administradores de los sistemas de información con los cuales el funcionario que se retira tiene relación en sus actividades laborales.
b. Los diferentes administradores funcionales de los sistemas de información deben realizar la inactivación (no borrado) del usuario en cada uno de los sistemas a su cargo.
c. Para aquellos aplicativos donde la mesa de ayuda tenga la función de administrador funcional de los usuarios, deben realizar la inactivación (no borrado) del funcionario en cada uno de los sistemas.

NOTA: En caso de presentarse un incidente de seguridad donde esté involucrado un usuario, se procederá al reporte y apertura del incidente de seguridad para realizar el diagnóstico, seguimiento y escalamiento ante los Entes competentes para determinar la acción a seguir, de carácter sancionatoria o legal si es del caso.

2.1.8. Entrega de Credenciales de acceso:

Una vez creado el acceso a la Red y el correo electrónico, se debe hacer entrega de las credenciales de acceso a la cuenta de correo personal reportada en el momento de la solicitud, en este correo se debe diligenciar e incluir en el correo el formato **GINT-F-026 ACEPTACIÓN DE CONDICIONES COMO USUARIO** debidamente diligenciado con el fin de darles a conocer las responsabilidades que tienen frente al acceso otorgado, incluyendo el nombre, la cédula y las credenciales de accesos otorgados, convirtiéndolo en .PDF y cifrándolo con contraseña. El correo electrónico debe ir con acuse de recibo y lectura.

Una vez dado de alta el nuevo usuario, se genera una contraseña genérica, la cual es informada por la mesa de ayuda al usuario, quien debe realizar cambio inmediato de dicha contraseña.

Los usuarios que reciben cuentas de usuario deben comunicar conformidad de recibo.

2.2. GESTIÓN DE CONTRASEÑAS

La contraseña es un código único, personal e intransferible, que no debe ser divulgado o compartido con terceras personas, el no observar esta buena práctica constituye una violación a las políticas de seguridad de la información de la entidad.

Un usuario registrado y autorizado en la Entidad, se debe autenticar siempre con su contraseña personal para acceder a los Sistemas de Información y a los servicios de la plataforma tecnológica.

Toda cuenta de usuario de la plataforma tecnológica debe identificar una persona en la vida real, funcionario, contratista o tercero, no se deben permitir el uso de cuentas genéricas o anónimas (ej: pasante).

En caso de requerirse el acceso a las cuenta de un funcionario que se encuentre fuera de las instalaciones de la Entidad, únicamente el jefe inmediato o superior realizará la solicitud escrita a la Coordinación del Grupo de Sistemas y Arquitectura de Tecnología o a la Dirección de Tecnología y esta autorizará al funcionario encargado de la gestión de usuarios para asignar una contraseña temporal con una duración específica, y luego la cuenta será desactivada; el solicitante será responsable de lo que suceda con los activos de información y la seguridad por la duración del evento.

Una vez el funcionario retorne a las oficinas deberá ser informado del cambio de contraseña y solicitará la activación de su cuenta actualizando su contraseña. Manteniendo la confidencialidad de la misma.

El usuario es el responsable de garantizar la seguridad de la información a su cargo, la cual está disponible en medios electrónicos y a través de documentos físicos, utilizando para ello en todo

momento las mejores prácticas de manejo documental, contraseñas seguras y dándole a esta el uso adecuado.

Las contraseñas de Rol usuario tendrán un periodo de vigencia de sesenta (60) días, cumplido este periodo, para poder tener acceso a los servicios informáticos, el sistema de autenticación solicitará el cambio obligatorio de la contraseña.

Las contraseñas de los roles Rol Administrador técnico (RT) y Rol Administrador funcional (RAF) tiene cambio obligatorio cada 30 días o cuando se sospeche que puedan estar comprometidas.

Es importante precisar que el código de usuario y la contraseña, es el mecanismo de autenticación ante la Entidad para el uso de los recursos tecnológicos y de información, esta identificación, permite manejar los perfiles y permisos de los usuarios, hacer el seguimiento y trazabilidad en caso de problemas de acceso y seguridad.

Únicamente las cuentas de acceso privilegiado deberán ser entregadas semestralmente y en la custodia debe ser almacenada en un lugar seguro, con los datos del remitente, la fecha y el sistema, para ser utilizados en caso de una contingencia o de ausencia del líder del proceso.

Además del nombre del usuario y la contraseña, se aplicará en Supersociedades, un doble factor de autenticación, para mejorar la seguridad de acceso.

Las contraseñas nunca se deberán almacenarse en sistemas de computador, en un formato no protegido, ni deben guardarse en los navegadores de internet.

El sistema de autenticación no permite crear contraseñas que ya fueron usadas.

Para las cuentas de acceso privilegiado Rol Superadministrador (SA), Rol Servicio (RS), Rol Institucional (RI), las contraseñas tendrán una vigencia de 30 días, y al crearlas, deben tener mínimo doce (12) caracteres de longitud cumpliendo las recomendaciones contenidas en esta guía, para estas cuentas, los intentos fallidos de autenticación serán hasta cuatro (4) y si sobrepasa este límite, la cuenta quedará bloqueada por 24 horas y para desbloquearla, se requiere generación de solicitud mediante formato 46001.

En caso de revelación o compromiso de las credenciales que pudiera generar un evento o incidente de seguridad se deberá notificar siguiendo lo establecido en la GINT-G-006 GestionIncidentes

2.2.1. Parámetros para construir contraseñas Seguras o Fuertes:

Una contraseña segura, es un código especial para proteger sus recursos informáticos, debe contener letras mayúsculas y minúsculas, con números y caracteres especiales sin espacios, y tiene como finalidad disminuir la posibilidad de acceso no autorizado y que sea utilizada por un tercero, para suplantarnos ante la organización ocasionando fraude o falsificación.

Para esto se deben observar ciertas recomendaciones al momento de su creación, como por ejemplo no utilizar datos personales, tales como nombres, números de identificación, fechas que puedan ser utilizados por terceros para adivinar nuestra contraseña.

Existen algunas guías para crear contraseñas fuertes, ellas son importantes para evitar el uso de su identidad por parte de personal no autorizado (suplantación):

- Elija contraseñas con mínimo nueve (9) caracteres de longitud.
- Utilice números dentro de su contraseña no utilice un nombre, una cadena de números, sus credenciales (nombre de usuario o username) ni ninguna palabra común que aparezca en un diccionario.
- Utilizar mayúsculas y minúsculas intercaladas.
- Algunos caracteres especiales pueden ser utilizados. Sin embargo, tenga en cuenta que algunas aplicaciones no pueden aceptar caracteres especiales. Si este problema se encuentra, cambiar su contraseña a una combinación de letras y números debería resolver el problema. Ejemplos de caracteres especiales generalmente permitidos se muestran a continuación: $ - . , ! %
- Uno de los métodos de generación de contraseñas más fáciles de recordar y más difíciles de violar es el de contraseña pseudo-aleatoria. En este caso, la contraseña se genera a partir de una frase fácil de recordar que es importante para el usuario. Esta frase puede ser una frase de un libro que le gusta en especial, las palabras de una canción que siempre recuerde con facilidad, una frase que usted nunca olvidará.

La clave para el éxito de la contraseña es crear una frase que le sea fácil de recordar, pero nadie lo atribuiría a Ud, por ejemplo, los siguientes métodos para construirlas:

Método: Elija las dos primeras letras de cada palabra, hasta un total de caracteres como resultado y cambie algunos caracteres por números. En el ejemplo, se cambiaron las ‘O’ por ceros (‘0’)	Frase Personal: "Era una noche oscura y tormentosa ...". Contraseña: E1noyt1
Método: Elija primera letra de cada palabra, seguido por la edad de su sobrino.	Frase Personal: Fecha de Nacimiento de mi Hermano: 25 de Abril del Setenta y Tres Contraseña: fnh25a73
Método: Elija la primera letra de la mayoría de las palabras, y sustituya algunos números por letras.	Frase Personal: "Oh Gloria Inmarcesible, Oh Júbilo Inmortal…" Contraseña: 0glin0j

2.2.2. Evitar una Contraseña Débil:

Al crear contraseñas, evitar el texto siguiente:

- Contraseñas fáciles de adivinar, como contraseñas en blanco o palabras como “contraseña”, “amor”, “super”, etc.
- Su nombre, nombre del cónyuge o de su hijo, · El nombre de su mascota
- Nombres de amigos cercanos o compañeros de trabajo
- Nombres de sus personajes favoritos de fantasía
- El nombre de su jefe
- El nombre, en general, de alguien
- Cadenas de números o letras, al igual que 1234, abcde
- El nombre de su equipo
- Su número de teléfono o su número de placa
- Cualquier parte de sus documentos de identificación
- Una fecha de nacimiento
- Otra información suya que sea fácil de obtener (por ejemplo, dirección, ciudad, oficina)
- Una palabra en un diccionario de cualquier idioma
- Nombres de lugares o nombres propios
- Las contraseñas con una sola letra repetida como ’aaaa’
- Patrones simples de letras en el teclado, como asdf
- Todo lo anterior escrito hacia atrás
- Cualquiera de las anteriores seguida o precedida de un solo dígito (número)

2.2.3. Caracteres Especiales No Permitidos

En este momento, los siguientes caracteres están excluidos de la lista de caracteres especiales por ser incompatibles con algunos sistemas:

- Espacio, "Comilla Doble", · 'Comilla simple', · `Backtick`, · & Ampersand: &
- Paréntesis (izquierdo o derecho ( ), · | Barra |, · < Inferior a <, · > Superior a

2.2.4. Como Cambiar Su Contraseña

- Presionar simultáneamente las teclas CTRL+ALT+SUPR, aparece la pantalla de Seguridad de Windows.
- Seleccione la opción de Cambiar Contraseña.
- Escriba la contraseña anterior.
- Escriba la contraseña nueva dos veces, la segunda vez es para reconfirmar la contraseña.
- Aparece un aviso informando que la contraseña ha sido cambiada con éxito.
- Si necesita ayuda en esta tarea, contacte a la mesa de ayuda y/o al Oficial de Seguridad de la Entidad y ellos le apoyarán.

2.2.5. Doble Factor De Autenticación

Para mejorar la seguridad de acceso a la red de Supersociedades y proteger las cuentas de usuarios, la plataforma OFICCE 365 nos ofrece contar con otro factor de autenticación, además de la contraseña normal.

El doble factor de autenticación se trata de una medida de seguridad extra que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS

Para obtener el doble factor hay que relacionar la cuenta de correo y el número del teléfono celular, al cual llegará un mensaje SMS con el código del factor de autenticación.

El funcionario responsable de aplicar el doble factor de autenticación requiere el medio por el cual enviarlo para parametrizarlo en el sistema. En SuperSociedades, se usará el número del teléfono celular del funcionario al que se le asignará.

El funcionario al que se le asigna doble factor de autenticación, cada vez que solicite un acceso a un servicio de office 365 (correo electrónico, TEAMS, etc..) le aparecerá una pantalla solicitándolo y seleccionando el medio a enviarlo. El código hay que leerlo del mensaje SMS en el celular y digitarlo en el campo que aparece en la pantalla.

Este código es al igual que la contraseña, es personal e intransferible.

El uso de doble factor de autenticación se trata de una medida de seguridad obligatoria y solo se podrá exceptuar por casos de fuerza mayor y por un tiempo limitado, si un usuario no está de acuerdo con esta medida deberá justificar ante su superior inmediato la situación quien autorizara el uso de la cuenta sin MFA y diligenciará en formato GINT-F-022 Consentimiento informado para el doble factor de autenticación y asumirá la responsabilidad de los eventos o incidentes que se puedan presentar en caso de que una contraseña de usuario sea comprometida.

2.2.6. Intentos de autenticación

Como mecanismo de protección, cinco (5) intentos fallidos de autenticación hacen que el sistema bloquee la cuenta por 15 minutos.

2.2.7. Bloqueo De Pantalla

Como mecanismo de seguridad, el sistema bloquea la pantalla cuando detecta que la estación de trabajo está desatendida por más de cinco (5) minutos, para activarla, el sistema solicita nuevamente digitar usuario y contraseña.

2.3. GESTION DE CREDENCIALES DE ACCESO PRIVILEGIADAS

Corresponden a este grupo los accesos otorgados a los diferentes usuarios técnicos especializados a quienes se les asignan los roles: Rol Superadministrador (SA), Rol Servicio (RS), Rol Institucional (RI), cuyas credenciales son calificadas como **cuentas de acceso privilegiado**.

Las cuentas de acceso privilegiado en los sistemas de Información o servicios de la plataforma tecnológica deben ser gestionadas únicamente por el Coordinador del Grupo de sistemas y Arquitectura de Tecnología, mediante correo electrónico al administrador correspondiente.

Los propietarios de los sistemas de información deben garantizar la administración de cuentas de acceso privilegiado las cuales cuentan con perfiles especiales de consulta para auditoria de los sistemas de información y por tiempo limitado, cuando sea posible.

Los usuarios que tengan cuentas de acceso privilegiado no deben acceder los datos de los sistemas contenidos en los recursos que administran. su perfil es solo de administración del recurso.

Los usuarios que tengan cuentas de acceso privilegiado deben hacer entrega semestral y/o en caso de retiro de la Entidad de las credenciales de acceso al director de Tecnología de la información y las comunicaciones de manera segura indicando el sistema o servicio al que se accede para que sea conservada bajo la custodia y resguardarla en caso de contingencia o falta del funcionario.

El cambio de las contraseñas de los accesos privilegiados se realizará máximo cada tres meses o cuando se realice actividad que pueda comprometer la misma; este cambio estará a cargo de los administradores de cada servicio y una vez se realice el cambio de claves, deberán ser entregadas al director de Tecnologías de la información y las comunicaciones para custodia.

2.3.1. Entrega de Cuentas de acceso Privilegiado

El director de Tecnologías de la información y las comunicaciones debe hacer la solicitud de entrega de las credenciales 2 veces al año (1 por semestre), pero es responsabilidad de los administradores actualizarla cada vez que se realicen cambios sobre la información.

Para tal fin, el Director de la DTIC, podrá solicitar la entrega de las credenciales de manera física o digital en cuyos casos siempre los administradores de plataformas usuarios con cuentas privilegiadas de (servidores, sistemas de información, bases de datos, infraestructura, entre otros) deben diligenciar todos los campos del formato GINT-F-023 Seguridad para Respaldo de Contraseñas, si la entrega es física deberán entregar en sobre sellado el formato y escribir en el sobre el nombre del ingeniero que hace la entrega, en cuyo caso se deberá definir un lugar seguro para su custodia o delegar a quien considere pertinente para su tenencia.

Si la entrega se realiza de manera digital, se debe cifrar el archivo GINT-F-023 Seguridad para Respaldo de Contraseñas con contraseña y entregarlo al director de tecnologías de la información y las comunicaciones vía correo electrónico, el envío de las contraseñas para

apertura del archivo cifrado debe ser enviado por un medio diferente, el cual definirá el director y/o a quien este delegue para la recepción del mismo.

2.3.2. Recepción y validación de Cuentas de acceso privilegiadas

Las credenciales entregadas ya sea física o digitalmente deben conservarse en un lugar seguro quedando bajo responsabilidad y custodia de dicha información la persona a quien el Director Delegue

El funcionario que reciba las credenciales de apertura de los archivos cifrados, debe validar la información que está recibiendo para constatar la veracidad de los usuarios y las contraseñas que recibe tomando una muestra de los mismos, en caso de que la entrega se realice por retiro del funcionario debe validar cada una de ellas.

Para los archivos digitales entregados por los administradores se conservarán en un lugar diferente al archivo que contiene las contraseñas de apertura.

En caso de revelación o compromiso de las credenciales que pudiera generar un evento o incidente de seguridad se deberá notificar siguiendo lo establecido en la GINT-G-006 GestionIncidentes

2.4. GESTION DE TOKENS

Los administradores funcionales de las aplicaciones que requieran el uso de firmas digitales deberán realizar el trámite correspondiente ante la entidad certificadora y llevar un control de los accesos otorgados, con el fin de realizar de manera oportuna la inactivación de estos cuando ya no se requieran.

El administrador funcional debe velar por que el acceso a la aplicación del tercero sea únicamente para las personas autorizadas y cumpliendo con el principio de mínimo privilegio.

En caso de pérdida o hurto del token deberá notificarlo de acuerdo con el procedimiento establecido por la entidad emisora y al interior de la Superintendencia, siguiendo lo establecido en la GINT-G-006 GestionIncidentes

3 DESCRIPCION DE LA ACTIVIDAD

Símbolo	Nombre del símbolo	Función
	Inicio/Fin	Se utiliza para indicar en donde comienza o finaliza el procedimiento.

	Actividad	Se utiliza para representar la ejecución de una actividad al interior del proceso.
	Decisión	Se utiliza para indicar que se debe evaluar una condición y plantear la selección de una alternativa.
	Conector de actividades	Se utiliza para conectar dos actividades o puntos del flujograma (solo se emplea si las actividades o puntos están en la misma página del flujograma)
	Conector de página	Se utiliza para conectar dos actividades o puntos del flujograma (solo se emplea si las actividades o puntos están páginas diferentes del flujograma)
	Proceso predefinido	Se utiliza para indicar que hay un proceso predefinido para la ejecución de una actividad.

Flujograma	Descripción	Responsable	Documentos o formatos	Puntos de control
	Inicio			
	Reporte de novedad de personal El grupo de Administración de personal realiza comunicación por el medio autorizado, indicando: el tipo de novedad (Ingreso, retiro, reubicación), Nro documento de identidad, Nombres y Apellidos, tipo de planta, cargo, dependencia, grupo, fecha de ingreso, fecha de finalización (en caso de funcionario, judicante, pasante y contratista)	Grupo de Administración de personal	GTH-I-001 Instructivo para ingresos, reubicaciones y retiros de funcionarios Correo electrónico y/o tramite 46001 de Postal.	
	Configuración de cuentas de usuario. - Actualización (Creación, Retiro, Modificación) de cuentas de usuario en: - Activación y desactivación de cuentas en Directorio Activo. - Activación y desactivación correo institucional - Servicios tecnológicos a que tenga derecho e indicados en el requerimiento del Grupo de Talento Humano. - Adición y retiro de listas de distribución - Asignación Manager del funcionario - Ajustar descripción del cargo - Asignación de personal a cargo, si es el caso. - Informar gestión a Recursos Humanos y jefes inmediatos. - Solicitar a Mesa de Ayuda la preparación y entrega del recurso tecnológico al funcionario.	Funcionarios Autorizados del Grupo de sistemas y arquitectura tecnológica.	Correo Electrónico y datos de radicación o documento de tramite 46001. GINT-F-026 Aceptación de condiciones como usuario	
1	**Trámite de asignación y configuración de equipo de cómputo.** Prepara e instala equipo en puesto de trabajo asignado al funcionario, instala los	Mesa de ayuda	Correo Electrónico	

Flujograma	Descripción	Responsable	Documentos o formatos	Puntos de control
1	sistemas operativos y de información requeridos en el tramite 46001. Realiza pruebas con el usuario y en caso de falta de acceso a componentes tecnológicos gestiona su actualización ante el área correspondiente.			
1 → 2	**Solicitud de servicios.** Las solicitudes de servicio deben realizarse a la mesa de ayuda por la herramienta autorizada en los siguientes casos: • Cuando ocurra una novedad de Ingreso, retiro o reubicación de un funcionario del área, el jefe inmediato debe reportarla al Grupo de Administración de personal para su trámite. • Para retiros y reubicaciones el jefe inmediato debe solicitar el retiro de los perfiles y accesos que el funcionario tenia y solicitar la asignación de los nuevos perfiles y servicios requeridos. Generar tramite 46001 y anexarlo a la solicitud. • Para los retiros, se debe asegurar que las cuentas de usuario sean bloqueadas primero en los aplicativos a los cuales el funcionario tiene autorización y por último en el Directorio Activo.	Jefe Inmediato	Correo con datos de radicación o documento de tramite 46001. Directorio Activo Correo Electrónico	

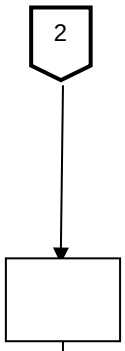
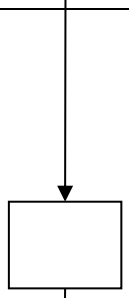
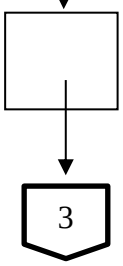
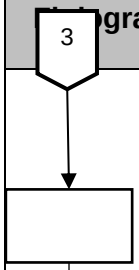
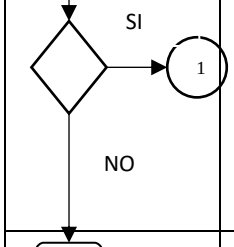
Flujograma	Descripción	Responsable	Documentos o formatos	Puntos de control
	**INACTIVACIÓN DE USUARIOS DE LAS APLICACIONES NO CONECTADAS AL DIRECTORIO ACTIVO** El Grupo de Administración de personal realiza solicitud a administradores de los sistemas, para la inactivación de funcionarios que se retiran. Administradores de Sistemas inactivan a funcionarios que se retiran. Revisión semestral de funcionarios que se retiran .vs. sistemas de información, mediante listado de retiros entregado por el Grupo de Administración de personal a administradores de sistemas.	Grupo de Administración de personal Administradores de sistemas de información y plataformas.	GTH-I-001 Instructivo para ingresos, reubicaciones y retiros de funcionarios Correo electrónico y/o tramite 46001 de Postal. Actas de revisión.	**X**
	**ENTREGA SEMESTRAL CREDENCIALES DE ACCESO CUENTAS PRIVILEGIADAS** Semestralmente los usuarios que poseen cuentas de acceso privilegiado deberán hacer entrega al Director de tecnologías de la información y las comunicaciones las cuentas para custodia	Administradores de sistemas de información y plataformas.	Correo electrónico GINT-F-023 Seguridad para Respaldo de Contraseñas	**X**
	**Revisión de estado de usuarios.** El Grupo de Administración de personal semestralmente, debe emitir un listado de funcionarios activos y retirados por dependencia y entregarlo al funcionario autorizado de la gestión de usuarios del Grupo de sistemas y arquitectura tecnológica, para realizar revisión. El funcionario del Grupo de Sistemas y Arquitectura Tecnológica, debe realizar	Funcionarios Autorizados del Grupo de sistemas y arquitectura tecnológica. Mesa de Ayuda Administradores de sistemas de	Listado de novedades de personal y funcionarios activos Actas de revisión	**X**

Diagrama	Descripción	Responsable	Documentos o formatos	Puntos de control
	junto con la mesa de ayuda, una revisión integral de usuarios, comparando la lista enviada por Personal VS los registros incluidos en cada sistema de información o plataforma tecnológica. Dependiendo de la cantidad de usuarios actualizados, puede realizar la revisión totalmente o a una muestra.	información y plataformas.		
	**¿Se requieren actualizaciones?** En caso de requerirse actualizaciones es necesario gestionar correcciones en todos los sistemas y plataformas tecnológicas.	Administradores de sistemas de información y plataformas	Sistemas actualizados	
	**Fin**			

4 CONTROL DE CAMBIOS.

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	30-09-2018	14-10-2018	Creación del documento	Director Informática
002	15-10-2018	11-11-2019	Se adicionan actividades del funcionario asignado a la creación de las cuentas de usuario y los soportes exigidos para su creación. Se incluye lo correspondiente a la administración de usuarios de la herramienta TFS.	Coordinador Grupo de Sistemas y Arquitectura de Tecnología
003	12-11-2019	22-12-2021	Se incluyen instrucciones para los administradores de los sistemas que no tienen autenticación con el directorio activo para la desactivación de usuarios de las diferentes aplicaciones. Se modifica la frecuencia de revisión de anual a semestral.	Coordinador Grupo de Sistemas y Arquitectura de Tecnología
004	23-12-2021	12-10-2023	Se actualizaron los nombres de las coordinaciones de los grupos y de la Dirección, acorde con la nueva estructura funcional.	Director de Tecnología de la Información y las Comunicaciones.
005	13-10-2023		Se realiza actualización de las actividades de atención de aprovisionamiento de los accesos, se ajustan políticas, monitoreo, se incluye los apartados sobre gestión de contraseñas, gestión de tokens, se incluye el formato de aceptación de condiciones como usuario. Se unifica dentro del procedimiento con la GINT-G-001 Guía de contraseña segura	Director de Tecnología de la Información y las Comunicaciones.