1. OBJETIVO

Establecer las acciones y alcances que se deben ejecutar al momento de crear, modificar o eliminar usuarios de aplicativos, dominio y correo corporativo.

2. ALCANCE

Este procedimiento aplica a toda creación, desactivación o modificación que se realice sobre los usuarios Apolo, Vicidial, dominio y correo corporativo de IGS.

3. DEFINICIONES

3.1. Cuentas de usuarios: Identificador usado por una persona real para conectarse a un sistema de información o servicio (APOLO, VICIDIAL, SFTP, VPN, etc.). Tiene asociada una contraseña para la autentificación un conjunto de privilegios que determina las acciones que tiene permiso de ejecutar.

3.2. Cuenta de súper usuario: son cuentas genéricas de usuarios administradores provistas por, los fabricantes de los sistemas o plataformas, con lo más altos privilegios sobre las mismas.

3.3. Rol: Es la forma de agrupar privilegios para asignarlos, luego a los usuarios.

3.4. Privilegios: Conjunto de permisos otorgados a un rol que determinan las acciones autorizadas que ésta puede desempeñar dentro del sistema de información.

3.5. Bloqueo o cancelación de una cuenta de usuario: se refiere a inhabilitar o eliminar una cuenta de usuario.

3.6. Ausencia Temporal: para efectos de este estándar, se refiere a las ausencias de personal por un tiempo mayor a 5 días hábiles, originado por vacaciones, licencias de cualquier tipo, incapacidades, entre otras

3.7. Contraseña: Es el conjunto de símbolos y/o caracteres alfanuméricos que sirven para la autentificación y control de acceso en los sistemas de información.

3.8. Contraseña robusta: Es aquella contraseña que no puede ser adivinada fácilmente ya que cumple con los estándares de calidad.

3.9. Autenticación: Es el proceso de detectar y comprobar la identidad digital de un usuario, mediante la verificación de las credenciales del usuario.

3.10. AD: Directorio Activo.

3.11. Bloqueo o Inhabilitación de una cuenta de usuario: Se refiere a bloquear o inhabilitar una cuenta de usuario.

3.12. MR&P: Matriz de autorización basado en los roles y perfiles de usuario para los sistemas de información.

3.13. RACI: Matriz de responsabilidades basados en las actividades de los cargos involucrados en un proceso o sistemas de información.

3.14. Logs: Registros o eventos generados desde los sistemas que permiten evidenciar la trazabilidad de las actividades ocurridas.

3.15. Información Confidencial: información que ha sido clasificada como confidencial en el inventario de activos de información, según la Política de clasificación de activos de información.

4. POLÍTICAS APLICABLES

4.1. Gobierno de seguridad de la información

Este estándar complementa la POLÍTICA DE CONTROL DE ACCESO o la política homologada en cada una de las filiales de Integral Group Solution.

4.2. Documentos relacionados

- Política de Control de Acceso
- Estándar de Contraseñas
- Formato solicitud creación usuario
- Matriz de Roles y Perfiles

5. CONFIDENCIALIDAD Este documento es el resultado del trabajo desarrollado por Integral Group Solution y está destinado única y exclusivamente a todos los colaboradores, su contenido no debe ser revelado, duplicado, usado o publicado o parcialmente fuera de la organización, o cualquier otra empresa, sin autorización escrita IGS.

6. CONDICIONES GENERALES

6.1. Gestión de Usuarios

La razón principal para la gestión de cuentas de usuario es verificar la identidad de cada colaborador de la organización que utiliza un sistema de información y permitir la utilización personalizada de recursos y privilegios de acceso.

6.2. Contraseñas

Una contraseña proporciona una forma de probar la autenticidad de la persona que dice ser el usuario con ese nombre de usuario. La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos de la contraseña:

- La confidencialidad de la contraseña.
- La complejidad de adivinar la contraseña.
- La complejidad de la contraseña ante un ataque de ser comprometida.

Las contraseñas que efectivamente toman en cuenta estas pautas se conocen como contraseñas robustas, mientras que aquellas que no, se les llama débiles. Es importante para la seguridad de la organización crear contraseñas robustas, mientras más robustas sean las contraseñas, hay menos posibilidades de que estén comprometidas.

El sistema debe permitir que los usuarios creen sus propias contraseñas, y la aplicación deberá verificar la complejidad de la misma para que sean lo suficientemente robustas.

6.3. Palabras reconocibles

Muchos ataques contra contraseñas están basados en el hecho de que el usuario generalmente usa contraseñas que pueden recordar. Y para la mayoría de usuarios, las contraseñas más fáciles de recordar son las que contienen palabras reconocibles y poco complejas. Por lo anterior muchos ataques a contraseñas están basados en el diccionario de palabras con el fin de encontrar la palabra o palabras que forman la contraseña.

6.4. Contraseñas robustas

Las secciones siguientes describen funcionalidades que una contraseña robusta debe tener.

6.5. Contraseñas largas

Es recomendable el uso de una la contraseña con varios caracteres, de esta forma disminuye la probabilidad de que un atacante pueda acceder a la cuenta y esta se vea comprometida.

6.6. Conjunto de caracteres expandido

Se debe solicitar como requisito el uso de: contraseñas alfanuméricas, la combinación de mayúsculas y minúsculas, y el uso de un carácter no-alfanumérico "caracteres especiales" para todas las contraseñas:

- t1Te-Bf,te
- Lb@lbh4om

6.7. Administración día a día de cuentas y acceso a recursos.

- **Nuevos colaboradores:** Cuando un nuevo colaborador se integra a la organización se debe realizar una gestión óptima para un ingreso seguro y rápido a la información de la organización.
- **Terminaciones:** En caso de terminación de contrato de algún colaborador se debe realizar las correspondientes notificaciones antes de efectuar la liquidación del colaborador, por motivos de seguridad de la información.
- **Cambios de trabajo:** Cuando un colaborador es asignado a otro cargo laboral y/o área de la organización se debe establecer un periodo de transición donde el colaborador entrega sus antiguas funciones y recibe las nuevas.

6.8. Aprobación de roles, perfiles y privilegios en los accesos a los sistemas

- Debe otorgarse el mínimo de privilegios que sean suficientes para el desempeño de las labores del propietario de la cuenta de usuario, de acuerdo con la Política de Control de Acceso a los Sistemas.
- Los administradores de los sistemas con roles y privilegios de administración (en cualquier plataforma como APOLO.) no deberán ser utilizados en las tareas del día a día, sino solo en ocasiones de contingencia y sus contraseñas deberán ser establecidas y protegidas según el Estándar de Contraseñas. Cuando se requieran los privilegios de estos usuarios o administrador para acceso a los sistemas, éstos deberán ser asignados a un usuario nombrado específico responsable.

- Es responsabilidad del área de Tecnología de IGS el mantenimiento de una matriz de roles y privilegios configurados o asignados en todos los sistemas que gestione usuarios. de acuerdo a la matriz RACI.
- Los cambios de adición o retiro de privilegios de acceso son realizados mediante una solicitud formal del líder o jefe inmediato (gerentes, directores, líderes, coordinadores, supervisores), mediante los procedimientos vigentes de Tecnología.
- El cambio de cargo de un funcionario dentro de la compañía debe tratarse como un retiro y un reingreso, en los cuales sus cuentas de usuario pueden mantenerse de ser necesario, pero todos sus privilegios de acceso deben ser completamente removidos y posteriormente creados.
- Tecnología deberá mantener actualizada la matriz de roles y privilegios con los accesos que están autorizados para los perfiles de las plataformas.
- El área de tecnología valida los roles y perfiles de los usuarios del proceso de acuerdo a las solicitudes radicadas por los canales de atención, para ello valida que lo estipulado en la Matriz de Roles y Perfiles adjunta en el canal de atención corresponda con los permisos asignados a los usuarios, dejando evidencia en el seguimiento del canal de atención.

6.9. Bloqueo o cancelación de cuentas de usuario

- Las cuentas de usuario deberán bloquearse luego de 6 intentos fallidos de conexión.
- Los Jefes inmediatos son los primeros responsables de informar a Tecnología el retiro o ausencias temporales (mayores a 5 días hábiles) de funcionarios, para que sean inhabilitados inmediatamente sus accesos lógicos y físicos.
- En el caso de retiro del funcionario es responsabilidad del jefe inmediato informar a tecnología según los procedimientos establecidos, para inhabilitar las cuentas de usuario y/o eliminación.
- Cuando se presenten ausencias temporales el jefe inmediato deberá solicitar por medio de los canales de atención a tecnología la desactivación temporal del usuario, indicando el motivo y la fecha de inicio de dicha desactivación. Es responsabilidad también del jefe inmediato solicitar a tecnología la reactivación del usuario cuando regrese de su ausencia temporal.
- Así mismo, el jefe inmediato debe solicitar el re-direccionar la información, a la cuenta de la persona que asumirá sus funciones.
- El área de Tecnología con una periodicidad trimestral, deberá eliminar del Directorio Activo todos los usuarios inactivos cuyo último inicio de sesión (last logon) sea superior a un año, previo a realizar el borrado de estos usuarios,

se debe generar un listado con todos los datos del usuario registrados en el DA y salvaguardarla de manera permanente.

6.10. Ausencias y/o retiros de colaboradores

El líder inmediato es el primer responsable de informar a Tecnología con copia Seguridad de la información del retiro o ausencias temporales (mayores a 5 días hábiles) de sus colaboradores, con el fin de que sean inhabilitados inmediatamente sus accesos lógicos y físicos.

6.11. Retiro de colaboradores

En el caso de retiro del colaborador, el líder o jefe inmediato debe reportar al área de Tecnología quien inhabilita las cuentas de usuario en los sistemas.

7. ROLES Y RESPONSABILIDADES

7.1. Seguridad de la Información

Validar que las políticas de contraseñas establecidas en IGS estén configuradas en el sistema y se cumplan en la organización.

7.2. Superior Inmediato (gerentes, directores, líderes, coordinadores, supervisores)

Realizar solicitudes de creación, bloqueo o inhabilitación de cuentas de usuario y modificación de privilegios, radicándolas ante el Área de Tecnología, considerando el principio de otorgar el mínimo de privilegios necesarios para el desempeño de las labores de un empleado, en caso de requerirse el superior inmediato valida y aprueba los accesos a navegación de internet escalados por el área de tecnología en los canales de atención.

Informar oportunamente a Seguridad de la información y Tecnología los retiros o ausencias temporales de funcionarios, solicitando el bloqueo o inhabilitación de sus accesos lógicos y físicos, radicando un requerimiento en los canales de atención.

Solicitar la desactivación de usuarios de funcionarios a su cargo ya sea por retiros temporales (licencias, incapacidades, vacaciones o similares) o por retiros definitivos. Cualquier incidente que se presente con usuarios activos de funcionarios retirados o ausentes, será responsabilidad del Jefe Inmediato.

Solicitar nuevamente a Tecnología la reactivación del usuario cuando se reintegre a sus funciones normales, lo cual deberá justificarse dentro de la solicitud de

reactivación. En los casos de reintegro de usuarios que habían sido retirados de las compañías, es responsabilidad del Jefe Inmediato solicitar la creación de un nuevo usuario según los procedimientos establecidos por Tecnología.

Informar a Tecnología las actualizaciones de información en cuanto a cambios de cargo o datos de cada usuario de los funcionarios a su cargo.

Mantener junto con Tecnología, actualizada la matriz de roles y privilegios configurados o asignados en los sistemas.

7.3. Infraestructura tecnológica.

- Realizar las respectivas configuraciones en el sistema de las políticas de contraseñas establecidas en la organización.
- Monitorear las cuentas de los sistemas de acceso remoto de los proveedores mientras estas son utilizadas.
- Crear usuarios en el Directorio Activo y asignar grupo de seguridad de acuerdo a la "Matriz DA", si es requerido.
- Utilizar identificadores de usuario únicos, de manera que se pueda reconocer a los usuarios por sus acciones, evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
- Los nombres de las cuentas de usuario deben conformarse por la inicial del primer nombre y primer apellido (por ej. Mperez). En caso de presentarse homónimos con otra cuenta creada, se puede utilizar la sigla del segundo nombre y primer apellido. Si aun así persiste la situación, se establecerá entre el Jefe Inmediato y Tecnología el usuario a nombrar.
- Bajo ninguna razón se asignarán cuentas de usuario existentes a nuevos funcionarios de la organización. No está permitido heredar cuentas de usuario.
- El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- La creación de cuentas de usuario genéricas no está permitida.
- Las cuentas de servicio deben ser solicitadas por medio de los canales de atención de T.I y estar autorizadas por el gerente o director del área que las solicito, a su vez estas no deben poder realizar login en ningún equipo de IGS. En el caso de sistemas de información administrados por terceros, el funcionario definido como contacto oficial del contrato, será el único autorizado para solicitar la creación de cuentas de usuario, de acuerdo con los perfiles de usuario definidos para el servicio.

7.4. Jefe de tecnología.

Mensualmente el Jefe de Tecnología realiza la verificación de los usuarios reportados en la planilla de usuarios de Dominio para asegurar que no existen colaboradores retirados en el periodo con usuarios activos, en caso de encontrar algún usuario activo enviará correo a los líderes de área para que se gestione la cancelación.

De la misma manera realizará la validación con los usuarios de dominio realizando el escalamiento de ser necesario.

Revisar la viabilidad y autorizar las solicitudes de creación de usuarios de dominio con cuenta de correo.

7.5 Soporte Técnico- Primer nivel

- Recibir la solicitud y escalar en los tiempos establecidos.
- Realiza la correspondiente validación de la información contenida en la solicitud.
- Validación del formato adjunto.
- Realizar seguimiento en caso que no cumpla con los criterios requeridos.
- Escalamiento a infraestructura tecnológica primer nivel.
- Escalamiento a Vicepresidencia de T.I, cuando el usuario solicita creación de cuenta correo corporativo.
- Creación de usuario dominio
- Creación de usuario para aplicativos autorizados en la matriz de roles y perfiles.
- Asignación y modificación de privilegios solicitadas por el (los) superior(es) inmediato(s) (gerentes, directores, lideres, coordinadores, supervisores)
- Bloquear o cancelar cuentas de usuario de usuarios según las solicitudes del (los) superior(es) inmediato(s) (gerentes, directores, líderes, coordinadores, supervisores).
- Informar al usuario final de los avances correspondiente respecto al caso.
- Cerrar solicitud en los canales de atención.

7.6 Colaborador o propietario de la Cuenta de Usuario

El propietario de la cuenta de usuario es responsable de:

- Mantener la confidencialidad de las contraseñas.
- Evitar conservar registros físicos de las contraseñas.
- No compartir la contraseña de sus cuentas de usuario asignadas.
- Las contraseñas almacenadas deben estar cifradas.
- Esto de acuerdo a la política de control de accesos.

8. PROCEDIMIENTO

8.1. Solicitud de canales de atención

Únicamente el superior inmediato (gerentes, directores, líderes, coordinadores, supervisores) son responsables de solicitar a tecnología la creación de cuentas de usuario que un colaborador requiera, como el siguiente procedimiento lo indica:

- Diligenciar el formato **Creación de usuario**, por el jefe directo del colaborador con la información del usuario para creación de la cuenta.
- Radicar la solicitud por los canales de atención por el jefe directo solicitando la creación del usuario y adjuntar el formato **Creación de usuario.**

Nota: la categoría creación de usuario interno se utiliza para las solicitudes de usuario aplicativos Apolo, Vicidial y dominio, en caso tal de que el colaborador requiera una cuenta de correo corporativo y/o permisos de navegación a internet se debe utilizar la categoría creación de usuario con correo.

8.2. Recepción y atención de solicitudes

- El usuario radica la solicitud mediante el canal de atención de T.I en la categoría creación de usuario interno o creación de usuario con correo y/o permisos de navegación a internet, en este se adjuntará el formato creación de usuario.
- La recepción y revisión de la solicitud la realiza el grupo de soporte de Tecnología - primer nivel, asegurando que el caso contenga la información necesaria, de no estar los datos completos se realizara seguimiento en el caso.
- Una vez validada la información, se escala a la vicepresidencia de T.I, las solicitudes para las creaciones de cuentas de correo corporativo.
- El grupo de soporte de T.I - Primer nivel realiza seguimiento de los avances del caso.
- Por parte del soporte técnico - Primer nivel se realiza la creación del usuario para el ingreso de aplicativos, dominio y navegación.
- Al finalizar la gestión, las contraseñas serán entregadas vía telefónica por parte del grupo de infraestructura – primer nivel.

8.3. Cierre a la solicitud

Es responsabilidad de soporte técnico - primer nivel e infraestructura – primer nivel, realizar el cambio de estado de la solicitud cuando la gestión del mismo haya terminado.

9. ANEXOS

Como adjunto a este documento se encuentran los anexos enunciados a continuación:

- Formato Creación de usuarios.
- Política de Control de Acceso.
- Estándar de Contraseñas.
- Matriz roles y Perfiles.

10. APÉNDICE

N/A

11. HISTORIAL DE CAMBIOS

FECHA	VERSION	NATURALEZA DEL CAMBIO
30-08-2019	1.0	➢ Creación del documento.
12-12-2019	2.0	➢ Adición de Ítem 8.2 y 8.3