

	PROCEDIMIENTO GESTION DE USUARIOS RMS SAS	Código SG-SI-24
		Página 1 de 4
		Versión: 1.1
		Vigente a partir de: 2024/02/01

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, dominio y correo corporativo de RMS SAS.

3. DEFINICIONES

3.1. Cuentas de usuarios: Identificador usado por una persona real para conectarse a un sistema de información o servicio. Tiene asociada una contraseña para la autenticación 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 autenticación 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 basadas 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

4.2. Documentos relacionados

	PROCEDIMIENTO GESTION DE USUARIOS RMS SAS	Código SG-SI-24
		Página 2 de 4
		Versión: 1.1
		Vigente a partir de: 2024/02/01

- 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 RMS SAS 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.

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. 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.

6.3. 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 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 el mantenimiento de una matriz de roles y privilegios configurados o asignados en todos los sistemas que gestione usuarios.

- Los cambios de adición o retiro de privilegios de acceso son realizados mediante una solicitud formal del líder o jefe inmediato, mediante los procedimientos vigentes.
- 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.

	PROCEDIMIENTO GESTION DE USUARIOS RMS SAS	Código SG-SI-24
		Página 3 de 4
		Versión: 1.1
		Vigente a partir de: 2024/02/01

- 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.

7. ROLES Y RESPONSABILIDADES

7.1. 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 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.
- 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.

8. PROCEDIMIENTO

8.1. Solicitud de canales de atención

Únicamente el superior inmediato es responsable 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.

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.

	PROCEDIMIENTO GESTION DE USUARIOS RMS SAS	Código SG-SI-24
		Página 4 de 4
		Versión: 1.1
		Vigente a partir de: 2024/02/01

- 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 las solicitudes para las creaciones de cuentas de correo corporativo.
- El Jefe de Sistemas realiza seguimiento de los avances del caso.
- El Jefe de Sistemas 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 Jefe de Sistemas

8.3. Cierre a la solicitud

Es responsabilidad del jefe de sistemas, realizar el cambio de estado de la solicitud cuando la gestión del mismo haya terminado.

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
CARGO:	Consultor	Gerencia	Gerencia
NOMBRE:	Ing. Enith E. Gustin	Diego Córdoba	Diego Córdoba
Fecha:	2024-01-27	2024-01-28	2024-02-01

CONTROL DE CAMBIOS		
VERSIÓN No.	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO
1	2024-02-01	Creación del documento