

Descripción:

El directorio activo es la puerta de ingreso a la red corporativa y en él solo deben estar incluidos los usuarios de la red autorizados por la dirección. Además, incluye el nivel de acceso, grupo de navegación y control.

Incorporación de usuarios

Existe una sola directriz para que una persona sea incorporada en el directorio activo y es ser empleado de la entidad. La dirección de recursos humanos o el jefe inmediato del colaborador debe solicitar al Departamento de TI la asignación de nuevos usuarios e indicar el perfil (Nivel de acceso, tipo de labor a realizar y navegación) a través de la plataforma de gestión de tickets <https://helpdesk.rstasociados.com.co/> para llevar la correspondiente trazabilidad de manera opcional se podrá enviar un correo al Área de TI.

Para labores de mantenimiento por parte de terceros se crea un perfil de MANTENIMIENTO el cual permitirá el acceso al componente a mantener y una vez terminada la labor deberá ser eliminado este perfil tiene una vida limitada.

El área de TI contara con un perfil de acceso global y sin restricciones para el director del área y para la gerencia general.

Eliminación de usuarios

1. La eliminación de un miembro del directorio activo se hace por instrucción de recursos humanos, gerencia o por terminación de labor de mantenimiento.
2. Se debe eliminar el usuario, el acceso a carpetas y confirmar la eliminación a quien lo solicito.

Usuarios inactivos

Se debe verificar la ocurrencia de usuarios inactivos por largos periodos de tiempo que conserven acceso a la red. En este caso se informa a la parte administrativa para que indique la directriz a seguir. (eliminación o continuar inactivo)

Asignación de contraseñas

Las contraseñas deben ser asignadas en forma provisional para que el usuario realice el cambio al primer uso.

El generador de contraseñas asigna por primera vez el acceso a la red.

Las contraseñas se cambian cada 30 días de manera programada

~~No se permite el uso de claves o contraseñas compartidas, genéricas o para grupos, las cuales son de uso individual, personal e intransferibles entre los usuarios.~~

Elaborado por: Director
administrativo y director de T. I
Fecha: 31/07/2023

Revisado por: Director
administrativo y auditor interno
Fecha: 31/07/2023

Aprobado por: Presidente
Fecha: 31/07/2023

Las contraseñas deben contar con un mínimo de ocho (8) caracteres alfanuméricos.

Las contraseñas caducan de forma automática cada treinta días (30) y no pueden ser repetidas al momento de actualizar la contraseña.

Olvidos de contraseñas

1. Estas solicitudes pueden ocurrir por diferentes causas, para la recuperación se debe seguir el siguiente protocolo:
2. Confirmar con la parte administrativa la solicitud.
3. Confirmar que el solicitante sea el correspondiente del usuario.
4. Generar la contraseña provisional para que el usuario ingrese.
5. Confirmar que el usuario cambie la contraseña de inmediato.

Borrado de contraseñas

1. Esta solicitud puede ser atendida únicamente por parte del Director de IT o alguien del área administrativa con atribuciones y mediante solicitud escrita.
2. Aunque no es mandatorio de ser posible debe indicar el motivo del borrado de la contraseña para que quede registrado.

Súper usuario

Esta es la contraseña maestra la cual será asignada por el usuario mismo y dejará registro en sobre lacrado el cual quedará bajo custodia en un lugar externo de la empresa y por persona calificada para esta labor asignada por la gerencia.

Bloqueo automático a equipos

Se habilita el bloqueo automático de los equipos de cómputo por medio de una gpu o política de directriz de grupo donde se establece un tiempo determinado de inactividad de este y por ende se bloquea, esto para evitar la posible filtración de información o manipulación de terceros en los equipos.

Restricción de descarga de Software: Para realizar el bloqueo de instalación de software se cuenta con un usuario administrador, esto quiere decir que cada vez que el usuario intente realizar la instalación de software el sistema le pedirá usuario y credenciales de administrador.

Se tiene bloqueado el acceso a la opción a las siguientes opciones del sistema operativo: CMD, Ejecutar, Panel de control, Bloqueo de medios extraíbles UBS, Escritorio limpio, Fondos de pantalla, Panel de control, se tiene establecido 1 minuto para el bloqueo automático de pantalla.

	POLITICA DEL DIRECTORIO ACTIVO	Clasificación: 1
		Versión: 8.0
		Fecha de Actualización: 16- Abr -2025

La papelera reciclable se encuentra configurada para que los archivos se quiten inmediatamente al eliminarlos.

Se tiene bloque el acceso a las carpetas compartidas con usuario y contraseña, solo se permite el acceso a personal autorizado.nm

CONTROL DE CAMBIOS		
VERSIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA ACTUALIZACIÓN
1.0	Emisión inicial.	03-Ene-2018
2.0	Inclusión de parte ambiental, clasificación del documento y en control de cambios fecha de actualización.	16-Abr-2018
3.0	Actualización documental.	15-jul-2020
4.0	Actualización documental.	30-Mar-2022
5.0	Actualización documental en el ítem Asignación de contraseñas.	25-Feb-2023
6.0	Se agregan responsables documentales	31-Jul-2023
7.0	Se actualizan Items de actualización de directivas de seguridad	20-ene-2025
8.0	Se actualiza inclusión de solicitud de usuarios en GLPI	16-04-2025

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: Presidente
Fecha: 31/07/2023	Fecha: 31/07/2023	Fecha: 31/07/2023