

	PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		Fecha de aprobación:	11-12-2024
			Versión:	04
	Nivel: 2	Código: GSI-PRC-013	Página:	1 de 6

1. OBJETIVO

Garantizar la seguridad de la información confidencial al proporcionar un sistema eficiente y confiable para crear, modificar y eliminar cuentas de usuario y contraseñas. Este también asegurará que los usuarios tengan acceso solo a los recursos e información relevantes para su trabajo.

2. ALCANCE

Incluir la gestión de cuentas de usuario y contraseñas para todos los sistemas, aplicaciones y bases de datos de la organización, y se aplicará a todos los usuarios internos y externos con acceso a estos recursos. Incluirá la creación, modificación y eliminación de cuentas, así como los requisitos para la creación y cambio de contraseñas.

3. RESPONSABILIDAD

- Director de Seguridad de la Información
- Coordinador de Infraestructura Tecnológica
- Grupo de Infraestructura Tecnológica

4. TÉRMINOS Y DEFINICIONES

Contraseña. Una contraseña o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa

Procedimiento. Es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias

Usuario. Es una persona que usa habitualmente un servicio.

GLPI: Mesa de ayuda implementado, para dar gestión a las solicitudes que son reportadas al área de infraestructura.

5. POLÍTICAS

La selección, uso y administración de contraseñas como un medio para controlar el acceso a los sistemas debe cumplir necesariamente con las mejores prácticas al respecto definidas por la organización. Particularmente, las contraseñas no deben ser compartidas con otras

Elaboró:	Revisó:	Aprobó:
Diana Karime Cruz Celis Coordinadora de Infraestructura	Jhonathan Smit Reyes Perilla Líder Sistema Integrado de Gestión	José Omar Mayorga Pabón Gerente Administrativo

COPIA CONTROLADA

	PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		Fecha de aprobación:	11-12-2024
			Versión:	04
	Nivel: 2	Código: GSI-PRC-013	Página:	2 de 6

personas por ninguna razón, a menos que la naturaleza del sistema al cual dan acceso lo permita.

6. DESCRIPCIÓN GENERAL

6.1 GENERALIDADES SOBRE LA ADMINISTRACIÓN DE USUARIOS

- Sólo los empleados de **SYSCAFE** pueden tener usuario de red con acceso a los servicios de Infraestructura Tecnológica. Las personas no empleadas deben contar con la autorización de la dirección administrativa.
- El estándar para la creación de usuarios del dominio se basará en la siguiente práctica:
 - ✓ El administrador de infraestructura tecnológica asigna el nombre para la creación del usuario de acuerdo con su disponibilidad, usando los nombres y apellidos de este.
 - ✓ En el caso de existir una similitud para un usuario nuevo, se cambiará al segundo nombre o apellido según corresponda.

El perfil básico de un usuario de la red tiene acceso a los siguientes servicios:

- Dominio de Red LOCAL de **SYSCAFE**.
- Acceso a carpetas compartidas.
- Acceso al servicio de Correo y Navegación Internet
- Acceso al servicio corporativo de Microsoft Teams

Dependiendo del perfil del usuario (desarrollo, comercial, administrativo, soporte técnico), se les da acceso a aplicaciones de usuario:

- Especializadas Contables, administrativas (Gastos, Facturación).
- Aplicaciones de soporte y desarrollo.
- Aplicación CRM-Licencias.
- Acceso a las carpetas de área.
- Bases de datos.

Elaboró:	Revisó:	Aprobó:
Diana Karime Cruz Celis Coordinadora de Infraestructura	Jhonathan Smit Reyes Perilla Líder Sistema Integrado de Gestión	José Omar Mayorga Pabón Gerente Administrativo

COPIA CONTROLADA

SysCafé	PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		Fecha de aprobación:	11-12-2024
			Versión:	04
	Nivel: 2	Código: GSI-PRC-013	Página:	3 de 6

Se utiliza la herramienta GLPI, para gestionar la creación de usuarios. El proceso comienza con una solicitud a través de un formulario llamado "Gestión de Usuarios", en el cual se proporciona la información necesaria para crear el nuevo usuario, ésta solicitud es generada exclusivamente por la Dirección Administrativa.

Cada usuario creado cuenta con permisos divididos por áreas de la empresa, lo que significa que el acceso a los diferentes recursos y datos se asigna de acuerdo con las necesidades de cada departamento o función. Este enfoque de permisos específicos ayuda a garantizar que la información sea segura y solo esté disponible para aquellos que la necesitan.

6.2 REQUERIMIENTOS DE LAS CONTRASEÑAS

Las contraseñas deben cumplir con estos requerimientos mínimos:

Longitud mínima de 8 caracteres. (Obligatorio), y mínimo se deben cumplir 4 reglas de las siguientes:

- ✓ Contener al menos una letra mayúscula.
- ✓ Contener al menos una letra minúscula.
- ✓ Contener al menos un número.
- ✓ Contener al menos un carácter especial.

6.3 USO DE CONTRASEÑAS

El uso de contraseñas en los sistemas de procesamiento de información debe cumplir los siguientes requisitos:

- En el acuerdo de confidencialidad de los empleados y contratistas se establece el compromiso de no divulgación y mantenimiento de confidencialidad de las contraseñas.
- La contraseña inicial segura es asignada por el grupo de infraestructura de forma única para un usuario, comunicada mediante Microsoft Teams o la herramienta GLPI y debe ser modificada por el usuario inmediatamente según instrucciones del sistema.
- La contraseña caduca cada 40 días y debe ser renovada.

Elaboró:	Revisó:	Aprobó:
Diana Karime Cruz Celis Coordinadora de Infraestructura	Jhonathan Smit Reyes Perilla Líder Sistema Integrado de Gestión	José Omar Mayorga Pabón Gerente Administrativo

COPIA CONTROLADA

	PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		Fecha de aprobación:	11-12-2024
			Versión:	04
	Nivel: 2	Código: GSI-PRC-013	Página:	4 de 6

- La contraseña no puede contener el nombre o el apellido del usuario.

6.4 ADMINISTRACIÓN DE CONTRASEÑAS DE ADMINISTRACIÓN DE IT

Todas las contraseñas administrativas usadas en procesos de instalación y configuración de servicios (servidores, bases de datos, aplicaciones corporativas, entre otros), se gestionan en una herramienta que permite guardar todas las credenciales de servidores y aplicaciones críticas de IT de forma segura y de preferencia en la nube.

Se aplican las siguientes condiciones de uso para la contraseña:

- No escriba la contraseña en sitios no protegidos (archivos de papel, correo electrónico, medios removibles).
- No divulgue su contraseña.
- No utilice contraseñas consideradas como no seguras según las siguientes recomendaciones:
 - ✓ Evitar nombres (propio o de familiares), números de teléfono, fechas de cumpleaños.
 - ✓ Mezclar caracteres numéricos y alfanuméricos.
 - ✓ No usar secuencias como 12345678 o ABCDEFGH.
 - ✓ No use contraseñas personales usadas para otras aplicaciones como cuentas de correos personales, bancarios u otras.

6.5 ADMINISTRACIÓN DE CONTRASEÑAS DE SISTEMAS DE INFORMACIÓN PARA USO INTERNO

En aplicaciones de uso interno masivo, la contraseña inicial segura es asignada por el Administrador del sistema con el apoyo del grupo de infraestructura de manera controlada, la cual es comunicada mediante correo electrónico, Aplicación GLPI, Microsoft Teams o directamente al **Director Administrativo** o quien haga sus veces y debe ser modificada por el usuario inmediatamente según instrucciones del sistema.

Elaboró:	Revisó:	Aprobó:
Diana Karime Cruz Celis Coordinadora de Infraestructura	Jhonathan Smit Reyes Perilla Líder Sistema Integrado de Gestión	José Omar Mayorga Pabón Gerente Administrativo

COPIA CONTROLADA

	PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		Fecha de aprobación:	11-12-2024
			Versión:	04
	Nivel: 2	Código: GSI-PRC-013	Página:	5 de 6

Elaboró:	Revisó:	Aprobó:
Diana Karime Cruz Celis Coordinadora de Infraestructura	Jhonathan Smit Reyes Perilla Líder Sistema Integrado de Gestión	José Omar Mayorga Pabón Gerente Administrativo

COPIA CONTROLADA

	PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		Fecha de aprobación:	11-12-2024
			Versión:	04
	Nivel: 2	Código: GSI-PRC-013	Página:	6 de 6

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS						
N° Versión	Fecha de cambio			Descripción de cambios	Numeral(es)	Responsable
	Mes	Día	Año			
1	06	30	2020	Versión inicial del procedimiento	Todo el documento	José Omar Mayorga Pabón, Gerente General
2	01	23	2023	Actualización de objetivo y alcance Eliminación de documentos relacionados	1 y 2	Fabian Barco
3	01	09	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis
4	11	12	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis

Elaboró:	Revisó:	Aprobó:
Diana Karime Cruz Celis Coordinadora de Infraestructura	Jhonathan Smit Reyes Perilla Líder Sistema Integrado de Gestión	José Omar Mayorga Pabón Gerente Administrativo

COPIA CONTROLADA