1. OBJETIVO

Establecer lineamientos para las buenas prácticas en el uso de mecanismos de autenticación secreta (contraseñas y doble factor de autenticación), para usuarios estándar y usuarios con privilegios de administrador, en los diferentes sistemas de información de la Previsora.

2. ALCANCE

Este documento constituye una guía de los diferentes lineamientos para la gestión de accesos a sistemas como Directorio Activo, Aplicativos o Sistemas de Información, Bases de Datos, Equipos de Cómputo, Elementos de Infraestructura Tecnológica y Redes, y cualquier otro sistema que requiera autenticación.

Aplica para los diferentes funcionarios de la Previsora, contratistas y demás personal que tenga asignado un usuario y una contraseña para el ingreso a alguno de los sistemas y equipos de cómputo implementados en la compañía.

3. DEFINICIONES

- **Administrador de sistema:** Persona responsable de ejecutar, mantener, operar y asegurar el correcto funcionamiento de un sistema informático o de una red.
- **Autenticación:** Si el usuario existe dentro de la plataforma tecnológica y en los sistemas de información, pasa la primera etapa de identificación del usuario, y posteriormente con la contraseña, que solo el usuario conoce, se pasa la segunda etapa de autenticación, si ambas etapas son válidas, el usuario finalmente puede acceder a la información y servicios informáticos permitidos.
- **Contraseña:** Palabra o expresión secreta, utilizada por verificar si una persona está autorizada para tener acceso a ciertos recursos o servicios. Cadena de caracteres cuyo conocimiento se reduce a uno o unos pocos usuarios autorizados.
- **Cuenta de usuario:** Es el registro en el Directorio Activo de Windows que contiene toda la información del nombre real del usuario y sus derechos de acceso.
- **Directorio Activo:** Es un componente central de la plataforma Windows, que proporciona los medios para administrar y gestionar las identidades de los usuarios, los recursos y las relaciones que organizan los entornos de red.
- **Doble factor de autenticación:** Capa adicional de seguridad que complementa el uso de una contraseña. Su objetivo es el de asegurarse de que el usuario no solo conoce la

contraseña para acceder al servicio, sino que además es quien dice ser aportando en el proceso de logueo información, un código, por ejemplo, sobre algo que solo él posee. Dicha información puede se obtenida a través de una llamada de teléfono o SMS enviado por el servicio, uso de una tarjeta inteligente (token) física o virtual, utilizando un dispositivo biométrico, entre otros.

- **Usuario privilegiado:** Un usuario privilegiado es aquel que tiene autorización administrativa completa de un sistema o servicio.

4. POLÍTICA

La compañía controla el acceso seguro a sistemas de información y diferentes dispositivos utilizados a través de mecanismos robustos de autenticación con contraseñas fuertes y en algunos casos el uso de doble factor de autenticación, con el fin de evitar que personas no autorizadas accedan a los sistemas de información de la compañía.

Para el cumplimiento de esta política, se deben cumplir los siguientes lineamientos:

4.1 Lineamientos Generales

- Para el acceso a los recursos tecnológicos de la compañía a través de VPN se debe utilizar doble factor de autenticación.
- Para el acceso a la información de la compañía usando herramientas de Office 365, se debe utilizar doble factor de autenticación.
- Se debe exigir a los usuarios cambiar sus contraseñas cuando ingresan por primera vez al recurso tecnológico o sistema de información.
- Se debe restringir en lo posible la visualización de contraseñas en la pantalla cuando se está ingresando.
- No enviar nunca la contraseña por correo electrónico o en mensaje de texto. En caso de requerirse el envío a través de correo, no podrá ser remitida en texto plano, es decir, se adjuntará al correo un archivo cifrado con la respectiva información.
- La clave tendrá una vigencia máxima de 45 días a partir de la fecha de cambio de contraseña.
- Los métodos de autenticación junto con las credenciales de acceso para los diferentes sistemas de información son de uso personal e intransferible.
- Los usuarios por defecto en los sistemas de información o elementos de la plataforma tecnológica deben ser deshabilitados o renombrados siempre y cuando la plataforma lo permita.
- El nombre del usuario corresponderá a la cadena de caracteres conformada por:
  - ✓ Primer apellido o primera letra del segundo apellido
  - ✓ Primera letra del primer nombre, seguido con la primera letra del segundo nombre.
  - ✓ En la construcción de los nombres claves la letra “Ñ” será remplazada por la “N”.

- Las aplicaciones deben almacenar las contraseñas en forma cifrada.
- Las credenciales asociadas a un usuario que se encuentre en periodo de vacaciones deberán ser deshabilitadas durante el periodo que duren las mismas.
- Una vez se finalice la vinculación del usuario con la entidad, sus credenciales de acceso deben ser deshabilitadas.
- Los usuarios se deben autenticar con cuentas que no tuvieran más privilegios que los necesarios para hacer uso del servicio.
- El administrador del Directorio Activo es responsable de asegurar que el mismo sistema solicite el cambio de la contraseña, cada vez que ésta sea reestablecida por medio de una contraseña genérica a un usuario.
- Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.
- La autenticación y acceso de usuarios privilegiados y administradores debe hacerse mediante mecanismos de doble autenticación; adicionalmente deberá quedar traza de qué usuario ha accedido a estos privilegios especiales.
- Los servidores y dispositivos se deben configurar con cuentas separadas para los que tienen privilegios de administración y los que no.
- Sólo se tendrán los privilegios especiales el tiempo que sea estrictamente necesario.
- Los derechos de acceso privilegiado se deben asignar a una identificación de usuario diferente de la usada para las actividades regulares de la entidad y atendiendo el procedimiento interno establecido para tal fin.
- Si un empleado o usuario de una parte externa que deja la empresa tiene contraseñas conocidas de usuarios que continúan activos, se deben cambiar al terminar o cambiar de cargo o empleo, contrato o acuerdo.
- Las áreas Gestión Humana y Recursos Físicos, deben definir un procedimiento que permita controlar el ingreso, suspensión, retiro y/o movimiento dentro de las dependencias de la Previsora, de cualquier funcionario de la compañía.

4.2 Lineamientos para usuarios

Los usuarios de los sistemas de información son responsables de establecer contraseñas seguras, que cumplan al menos con las siguientes características:

- El doble factor de autenticación para los usuarios se utiliza con algo que conocen (pin, contraseña) y algo que no conocen o que tienen token, códigos, etc.
- La longitud de la contraseña debe ser mínimo de 8 caracteres, entre más caracteres tenga la contraseña es más difícil de descifrar por algún atacante cibernético.
- Combinar caracteres numéricos, alfabéticos, mayúsculas, minúsculas y caracteres especiales (si el sistema lo permite).
- No deben tener caracteres idénticos consecutivos, cuando los sistemas permitan su activación y utilización.

- La clave del usuario no podrá ser igual a las tres (3) últimas claves utilizadas anteriormente.
- Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
- Una vez el usuario reciba la contraseña, deberá cambiarla inmediatamente.
- No deben usarse palabras o nombres comunes que aparezcan en los diccionarios.
- No debe haber una relación con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo o asociaciones similares que facilite ser identificada por medio de ingeniería social.

Los usuarios son responsables del buen uso de sus credenciales de acceso a los diferentes sistemas de información, por lo cual deben cumplir con lo siguiente:

- No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
- No se debe almacenar la contraseña en la computadora. Algunos cuadros de dialogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
- Las contraseñas para acceso a los sistemas de información son de uso personal e intransferible.
- Los usuarios no deben pedir, obtener o utilizar contraseñas ni mecanismos de acceso a los sistemas de información o recursos tecnológicos de otros usuarios.
- El funcionario y/o tercero al que se le asigne un usuario, deberá responder por las actividades realizadas, daños intencionales o accidentales que puedan ocurrir y sean imputables a su usuario.
- Las contraseñas no deben, bajo ninguna circunstancia, ser comunicadas a ninguna persona, así esta ostente un cargo jerárquico superior.
- Si se presenta alguna sospecha o indicio para creer que una contraseña ha sido comprometida, esta debe cambiarse inmediatamente.

5. REFERENCIA

- Circular Externa 005 de 2019 de la Superintendencia Financiera de Colombia, Regulación para validación de identidad en la Nube.

- Circular Externa 029 de 2019. Superintendencia Financiera de Colombia, Mecanismos fuertes de autenticación.

- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información,

Requisitos, 2013-12-11, ICONTEC Internacional.

- Norma Técnica Colombiana NTC-ISO-IEC 27002:2013, Guía de Implementación Sistemas de Gestión de la Seguridad de la Información, 2013-12-11, ICONTEC Internacional.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE (S)	<Sandra Cediel Bravo>	Sandra Cediel Bravo	Renato Muñoz Rodrìguez
CARGO (S)	<Especialista>	< Especialista >	Gerente de Riesgos

CONTROL DE CAMBIOS	
VERSIÓN	**CAMBIO REALIZADO**
1	Se actualiza documento – Uso de doble factor de autenticación para acceso a VPN y otras disposiciones.