SUPERINTENDENCIA DE SOCIEDADES

GUIA PARA CONTRASEÑAS SEGURAS

1. INFORMACIÓN GENERAL.

1.1 OBJETIVO	Gestionar el uso de contraseñas seguras en la Entidad
1.2. RESPONSABLE	Coordinador Grupo de Sistemas
1.3. ALCANCE	Aplica para las contraseñas de acceso a los sistemas de información y la administración de todos los equipos y dispositivos de tecnología de la Superintendencia de Sociedades.
1.4. DEFINICIONES	**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 **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. **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. **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 él 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

2. CONDICIONES GENERALES

2.1. *La contraseña es un código único, personal e intransferible, que no debe ser divulgado o compartido con terceras personas, el no observar esta buena práctica constituye una violación a las políticas de seguridad de la entidad.*

2.2. *Un usuario registrado y autorizado en la Entidad, se debe autenticar siempre con su contraseña personal para acceder a los Sistemas de Información y a los servicios de la plataforma tecnológica.*

2.3. *Toda cuenta de usuario de la plataforma tecnológica debe identificar una persona en la vida real, funcionario, contratista o tercero, no se deben permitir el uso de cuentas genéricas o anónimas (ej: pasante).*

2.4. *En caso de requerirse el acceso a las cuenta de un funcionario que se encuentre fuera de las instalaciones de la Entidad, únicamente el jefe inmediato o superior realizará la solicitud escrita a la Coordinación de Sistemas o a la Dirección de Informática y esta autorizará a la mesa de ayuda para asignar una contraseña temporal con una duración especifica, y luego la cuenta será desactivada; el solicitante será responsable de lo que suceda con los activos de información y la seguridad por la duración del evento.*

2.5. *Una vez el funcionario retorne a las oficinas deberá ser informado del cambio de contraseña y solicitará la activación de su cuenta actualizando su contraseña. Manteniendo la confidencialidad de la misma.*

2.6. *El usuario es el responsable de garantizar la seguridad de la información a su cargo, la cual está disponible en medios electrónicos y a través de documentos físicos, utilizando para ello en todo momento las mejores prácticas de manejo documental, contraseñas seguras y dándole a esta el uso adecuado.*

2.7. *Las contraseñas tendrán un periodo de vigencia de noventa días (90) días, fecha en la cual se obligará a cambiarse de acuerdo con las mejores prácticas y políticas de seguridad, de lo contrario se desactiva la cuenta.*

2.8. *Es importante precisar que el usuario y la contraseña, es el mecanismo de identificación de un usuario ante la Entidad para el uso de los recursos tecnológicos y de información, esta identificación, permite manejar los perfiles y permisos de los usuarios, hacer el seguimiento y trazabilidad en caso de problemas de acceso y seguridad.*

2.9. *Únicamente las contraseñas de administración de la plataforma tecnológica deberán ser escritas, protegidas en un sobre debidamente sellado y almacenadas en un lugar seguro, con los datos del remitente, la fecha y el sistema, para ser utilizados en caso de una contingencia o de ausencia del líder del proceso.*

3. GENERALIDADES.

3.1. *CONTRASEÑA SEGURA O FUERTE*

Una contraseña segura, es un código especial para proteger sus recursos informáticos, debe contener letras mayúsculas y minúsculas, con números y caracteres especiales sin espacios, y tiene como finalidad disminuir la posibilidad de acceso no autorizado y que

sea utilizada por un tercero, para suplantarnos ante la organización ocasionando fraude o falsificación.

Para esto se deben observar ciertas recomendaciones al momento de su creación, como por ejemplo no utilizar datos personales, tales como nombres, números de identificación, fechas que puedan ser utilizados por terceros para adivinar nuestra contraseña. Por ejemplo: compartiría la contraseña de su tarjeta debito o crédito, con un extraño? Claro que no, esto podría ocasionarle graves inconvenientes financieros; lo mismo ocurre con los activos tecnológicos, de nuestra Entidad.

Existen algunas guías para crear contraseñas fuertes, ellas son importantes para evitar el uso de su identidad por parte de personal no autorizado (suplantación):

- Elija contraseñas largas, de por lo menos 7 caracteres de longitud, o más, si el sistema lo permite.
- Utilice dos números en los primeros siete caracteres.
- Dentro de su contraseña no utilice un nombre, una cadena de números, su ID de usuario (login o username) ni ninguna palabra común que aparezca en un diccionario.
- Utilizar mayúsculas y minúsculas intercaladas dentro de los 7 caracteres.
- Algunos caracteres especiales pueden ser utilizados. Sin embargo, tenga en cuenta que algunas aplicaciones no pueden aceptar caracteres especiales. Si este problema se encuentra, cambiar su contraseña a una combinación de letras y números debería resolver el problema. Ejemplos de caracteres especiales generalmente permitidos se muestran a continuación: ***$ - . , ! %***
- Uno de los métodos de generación de contraseñas más fáciles de recordar y más difíciles de violar es el de contraseña pseudo-aleatoria. En este caso, la contraseña se genera a partir de una frase fácil de recordar que es importante para el usuario. Esta frase puede ser una frase de un libro que le gusta en especial, las palabras de una canción que siempre recuerde con facilidad, una frase que usted nunca olvidará.

La clave para el éxito de la contraseña es crear una frase que le sea fácil de recordar, pero nadie lo atribuiría a Ud, por ejemplo:

Frase Personal: "Oh Gloria Inmarcesible, Oh Júbilo Inmortal…"
Contraseña: 0glin0j
Método: Elija las dos primeras letras de cada palabra, hasta un total de siete caracteres como resultado y cambie algunos caracteres por números. En el ejemplo, se cambiaron las ‘O’ por ceros (‘0’)

Frase Personal: "Era una noche oscura y tormentosa ...".
Contraseña: E1noyt1

Método: Elija primera letra de cada palabra, seguido por la edad de su sobrino.

Frase Personal: Fecha de Nacimiento de mi Hermano: 25 de Abril del Setenta y Tres
Contraseña: fnh25a7
Método: Elija la primera letra de la mayoría de las palabras, y sustituya algunos números por letras.

3.2. *EVITAR UNA CONTRASEÑA DEBIL*

Al crear contraseñas, evitar el texto siguiente:

- Contraseñas fáciles de adivinar, como contraseñas en blanco o palabras como “contraseña”, “amor”, “super”, etc.
- Su nombre, nombre del cónyuge o de su hijo
- El nombre de su mascota
- Nombres de amigos cercanos o compañeros de trabajo
- Nombres de sus personajes favoritos de fantasía
- El nombre de su jefe
- El nombre, en general, de alguien
- Cadenas de números o letras, al igual que *1234, abcde*
- El nombre de su equipo
- Su número de teléfono o su número de placa
- Cualquier parte de sus documentos de identificación
- Una fecha de nacimiento
- Otros información suya que sea fácil de obtener (por ejemplo, dirección, ciudad, oficina)
- Una palabra en un diccionario de cualquier idioma
- Nombres de lugares o nombres propios
- Las contraseñas con una sola letra repetida como *’aaaa’*
- Patrones simples de letras en el teclado, como *asdf*
- Todo lo anterior escrito hacia atrás
- Cualquiera de las anteriores seguida o precedida de un solo dígito (número)

3.3. *CARACTERES ESPECIALES NO PERMITIDOS*

En este momento, los siguientes caracteres están excluidos de la lista de caracteres especiales por ser incompatibles con algunos sistemas:

- Espacio
- ''Comilla Doble''
- 'Comilla simple'

- `Backtick`
- & Ampersand: &
- Paréntesis (izquierdo o derecho ( )
- | Barra |
- < Inferior a <
- > Superior a >

3.4. *COMO CAMBIAR SU CONTRASEÑA*

- Presionar simultáneamente las teclas CTRL+ALT+SUPR, aparece la pantalla de Seguridad de Windows.
- Seleccione la opción de Cambiar Contraseña.
- Escriba la contraseña anterior.
- Escriba la contraseña nueva dos veces, la segunda vez es para reconfirmar la contraseña.
- Aparece un aviso informando que la contraseña ha sido cambiada con éxito.

  Si necesita ayuda en esta tarea, contacte a la mesa de ayuda y/o al Oficial de Seguridad de la Entidad y ellos le apoyarán.

4. ANEXOS Y REGISTROS

No aplica

5. CONTROL DE CAMBIOS.

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	24-02-2014	13-11-2017	Creación del documento	Director de Informática
002	14-11-2017		Cambio periodo de validez de contraseña	Director de Informática