CONTROL DE CAMBIOS					
VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	20/02/2020	Se crea documento y se incluyen los lineamientos para la Política de Gestión de Contraseñas	COORDINADOR SGI	COMITÉ DE POLÍTICAS Y SEGURIDAD	GERENTE GENERAL
02	07/03/2024	SE REVISA LA POLITICA SIN GENERAR CAMBIOS, SE ACTUALIZA FIRMA DEL GERENTE GENERAL	COORDINADOR SGI	COMITÉ DE POLÍTICAS Y SEGURIDAD	GERENTE GENERAL

1. OBJETIVO

Proteger la información confidencial y mantener la privacidad de los datos en las aplicaciones o servicios de PKI SERVICES

2. ALCANCE

Esta política aplica para la generación de sus claves de forma segura, para establecer una conexión privada y segura en cualquier aplicación, herramienta o servicio.

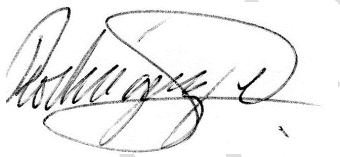
3. CONDICIONES GENERALES

a. Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas, minúsculas y símbolos) y numéricos.
b. Su longitud debe ser mínimo de 8 caracteres.
c. La protección de la contraseña es responsabilidad del Usuario. Al comprometer una cuenta se puede estar comprometiendo la información del sistema.
d. La contraseña se debe cambiar cada 60 días.
e. Es responsabilidad del usuario el manejo apropiado a las claves asignadas, a través de las herramientas aprobadas.
f. En caso de olvido de contraseñas debe reportar el evento a Seguridad de la Información y a tecnología para que se definan las acciones a tomar.
g. Las contraseñas o llaves de la CA raíz de PKI SERVICES son generadas por un procedimiento denominado “ceremonia de llaves”. Estas llaves son generadas en multifactor M de N, cuyos n son almacenados en sobre de seguridad y custodiados en la caja fuerte. Como contingencia, se genera copia de las llaves en otro HSM idéntico, el cual es retirado del pc en modo transporte, almacenado en sobre se seguridad y custodiado en la caja fuerte.

h. El gerente es la única persona de PKI SERVICIES que tiene acceso a la caja fuerte que tiene control dual (clave + biométrico).
i. El acceso a las llaves de la CA raíz de PKI SERVICIES es autorizado por el gerente.

PROHIBICIONES

a. Compartir las contraseñas.
b. Escribir la contraseña en sitios visibles, sin seguridad.
c. contraseñas en una conversación.
d. Mantener una contraseña indefinidamente.
e. Acceder a la CA raíz de PKI SERVICES sin autorización del gerente.



Roberto Rodríguez
Gerente General
Bogotá D.C. 07-03-2024