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 Control de Accesos	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

Esta Política determina reglas de acceso a sistemas, servicios, instalaciones, información, documentos y registros.

- Limitar el acceso a información y a instalaciones de procesamiento de información, diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

2. ALCANCE

Sistemas y recursos de información, cuentas del usuario y los derechos y privilegios asociados con ellas, aplicaciones, recursos, bases de datos e información que requiera control de acceso, los usuarios de este documento son todos los empleados y partes relacionadas de PKI SERVICES.

3. RESPONSABILIDADES

- Empleados
- Contratitas
- Proveedores

4. ACCESO A REDES Y SERVICIOS

a. El control de acceso a los Sistemas de Información de PKI SERVICES debe realizarse por medio de asignación de Usuario y Contraseña, las cuales son de uso exclusivo e intransferible.

b. El usuario debe informar, las vulnerabilidades de acceso físicas y lógicas que observe y las mismas no pueden ser explotadas.

c. Para la asignación y/o eliminación de acceso de usuarios se hará de acuerdo con el procedimiento.

d. El uso de contraseñas compartidas está prohibido.

e. Los usuarios deben tener en cuenta para la construcción de sus contraseñas: al menos ocho (8) caracteres. Estos caracteres deben ser caracteres alfabéticos, numéricos y símbolos o caracteres especiales.

f. Los usuarios son responsables de todas las actividades llevadas a cabo con su identificación de usuario y contraseña.

g. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

h. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla.

i. Acceso a plataformas, aplicaciones, servicios áreas y en general cualquier recurso de información de PKI SERVICES, debe ser asignado a los usuarios por el área de tics, de acuerdo con los requerimientos de los responsables de Procesos.

j. Acceso a la RA- Administrador RA, Acceso a la Administración PKI – Administrador Tics, Acceso a la CA- Oficial de Decisión.

k. Los subscriptores ingresan a la RA expuesta en Internet.

l. Es responsabilidad del usuario el manejo apropiado a las claves asignadas.

m. Cambiarse obligatoriamente cada 60 días, o cuando lo establezca el Área de Tecnología y Sistemas de Información.

n. Se deben revisar los derechos de acceso otorgados a los usuarios regularmente.

o. Cuando un empleado deja algún puesto en la organización, los archivos alojados en los computadores y los archivos impresos deben ser revisados por su supervisor o el jefe inmediato.

5. CONTROL DE ACCESO E IDENTIFICACIÓN PERSONAL PARA ÁREAS GENERALES Y ÁREAS RESTRINGIDAS

a. Para el ingreso de personas visitantes, deben diligenciar el formato **CONTROL VISITANTES.**

b. El personal sólo puede acceder a visualizar y/o trabajar aquella información para la que están expresamente autorizado.

c. El acceso al rack y a la oficina quedan registrados en el formato de control de visitantes y control de acceso al Rack.

d. El acceso a oficinas, o áreas de trabajo que contengan información sensible debe estar restringido e identificado; su acceso debe ser autorizado.

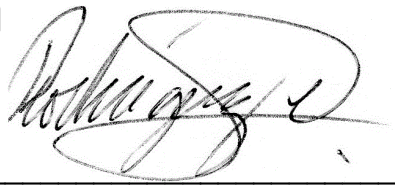
e. Cuando un trabajador termina su relación laboral, sus permisos de acceso deben ser revocados, deben diligenciar el formato de **PAZ Y SALVO**

6. PROHIBICIONES

a. Dejar visibles los Usuarios y contraseñas, de manera de que se permita a personas no autorizadas su conocimiento.

b. Compartir su Clave.

c. Acceder a las áreas restringidas o a la información sin previa autorización



Roberto Rodríguez
Gerente General
Bogotá D.C. 20-02-2020