CONTROL DE CAMBIOS					
VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	10-03-2020	Se crea documento y se incluyen los lineamientos para la Política de seguridad de Información para proveedores	COORDINADOR SGI	COMITÉ DE POLITICAS 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 POLITICAS Y SEGURIDAD	GERENTE GENERAL

1. OBJETIVO

Definir los lineamientos, políticas, que debe cumplir el Proveedor y/o Tercero que presta cualquier servicio en PKI SERVICE.

2. ALCANCE

Esta política aplica todos los contratistas y Proveedores de PKI SERVICES.

3. CONDICIONES GENERALES

a. Todo proveedor y/o Contratista debe ser registrado por PKI SERVICES, aportando la documentación solicitada, para su verificación.

b. Todo proveedor y/o Contratista debe conocer la Política de Seguridad de Información.

c. El proveedor y/o Contratista debe tener identificados los servicios que va a prestar.

d. El área Administrativa debe autorizar a que información debe tener acceso.

e. El proveedor y/o Contratista debe contar con los requisitos exigidos para la aprobación de equipos de cómputo, capacidad de Internet, y demás requisitos establecidos para el desarrollo su labor.

f. El proveedor y/o Contratista debe contar con requisitos para la Seguridad de sus Equipos, debe disponer de Antivirus.

g. Debe tener definidos normas para acceso a sus equipos de cómputo.

h. El proveedor y/o Contratista es responsable de la Información de PKI SERVICES que maneje

i. El proveedor y/o Contratista es responsable de la disponibilidad de la Información cuando PKI SERVICES lo requiera.

j. El proveedor y/o Contratista debe tener disposición en capacitaciones y toma de conciencia.

k. Las condiciones y requisitos deben quedar documentadas y firmadas como acuerdo de ambas partes.

l. El proveedor y/o Contratista deben proteger la información confidencial de toda revelación no autorizada, modificación, destrucción o uso incorrecto.

m. El proveedor y/o Contratista deberán tomar precauciones posibles para proteger físicamente los sistemas y prevenirlos frente al robo o destrucción

n. El proveedor y/o Contratista deberá asegurarse la confidencialidad de la información almacenada, tanto en formato electrónico como no electrónico.

o. El proveedor y/o Contratista deberá contar con un Backup de la información propia de PKI SERVICE

p. El proveedor y/o Contratista deberá informa a PKI SERVICES sobre cualquier anomalía de seguridad que observe.

4. PROHIBICIONES

a. Destruir, dañar o eliminar datos o información de la Empresa sin previa autorización.

b. Divulgar información de la Empresa, sin previa autorización.

c. Hacer uso indebido de la información de PKI SERVICES.

5. SUPERVISIÓN Y REVISIÓN

El propietario del contrato debe revisar y controlar periódicamente (según contrato) el nivel de los servicios y cumplimiento de las cláusulas de seguridad de parte de los proveedores o socios y los informes y registros generados por ellos.

Todos los incidentes de seguridad relacionados con el trabajo del proveedor o socio deben ser elevados inmediatamente al oficial de seguridad o quien haga sus veces

6. CAPACITACIÓN Y CONCIENCIACIÓN

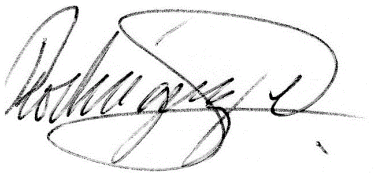
El propietario del contrato decide qué empleados del proveedor o socio necesita concienciación y capacitación sobre seguridad.

El oficial de seguridad o quien haga sus veces, es responsable de suministrar toda la capacitación y de realizar la concienciación a esos empleados.

7. ELIMINACIÓN DE DERECHO DE ACCESO Y DEVOLUCIÓN DE ACTIVOS

Cuando se modifica o finaliza un contrato, se deben eliminar los derechos de acceso para el proveedor, sus los empleados y/o socio de acuerdo a la Política de control de acceso.

Además, cuando se cambia o finaliza un contrato, el propietario del contrato debe asegurarse de que todo el equipamiento, software o información en formato electrónico o papel sea devuelto.



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