| 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 política sin generar cambios, se actualiza firma del gerente general | COORDINADOR SGI | COMITÉ DE POLITICAS Y SEGURIDAD | GERENTE GENERAL |
| 03 | 26/06/2026 | Actualización a ISO/IEC 27001:2022 (controles 5.19–5.23, 5.14, 6.6, 8.10): se agregan lineamientos de tipificación y evaluación previa de proveedores, contenido mínimo de acuerdos, NDA, transferencia segura, cadena de suministro TIC, nueva sección de servicios en la nube, gestión de cambios en servicios y destrucción certificada al terminar contrato. | 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.

q. PKI SERVICES debe identificar y documentar los tipos de proveedores (servicios TIC, infraestructura, servicios en la nube, logísticos, entre otros) y el nivel de acceso de cada uno a su información, servicios TIC e infraestructura.

r. Todo proveedor debe ser evaluado antes de iniciar la relación contractual, considerando sus controles de seguridad de la información y la sensibilidad de la información a la que accederá. PKI SERVICES definirá los criterios de evaluación y selección según el tipo de proveedor.

s. Los acuerdos con proveedores deben contemplar, según la criticidad del servicio, los riesgos identificados y la información que el proveedor esté dispuesto y autorizado a suministrar, como mínimo: a) la descripción y clasificación de la información de PKI SERVICES a la que el proveedor tendrá acceso, según el esquema de clasificación vigente; b) las obligaciones regulatorias aplicables, incluyendo protección de datos personales e información de identificación personal (IIP); c) los controles de seguridad de la información acordados y la obligación del proveedor de cumplirlos; d) el derecho de PKI SERVICES a auditar los procesos y controles del proveedor relacionados con el acuerdo; e) los plazos y el procedimiento de notificación de incidentes de seguridad de la información por parte del proveedor, así como su obligación de colaborar en su atención.

t. La información de PKI SERVICES que el proveedor maneje debe ser tratada conforme al esquema de clasificación de la organización. Los proveedores de servicios TIC que subcontraten partes del servicio deben propagar los requisitos de seguridad de la información de PKI SERVICES a lo largo de su cadena de suministro.

u. La transferencia de información hacia o desde proveedores debe realizarse bajo acuerdos formales que establezcan los controles necesarios para proteger la información durante la transferencia, independientemente del medio utilizado.

v. Todo proveedor que acceda a información confidencial de PKI SERVICES deberá estar sujeto a obligaciones de confidencialidad formalmente establecidas antes de iniciar actividades, ya sea mediante la suscripción de un acuerdo de confidencialidad (NDA), cláusulas contractuales específicas o los términos y condiciones corporativos del proveedor que contemplen compromisos equivalentes de protección de la información.

## 4. PROVEEDORES DE SERVICIOS EN LA NUBE

Esta sección aplica proveedores de Data Center y Hosting que PKI SERVICES utilice.

a. Las responsabilidades de PKI SERVICES y del proveedor de servicios en la nube deben quedar documentadas conforme al modelo de responsabilidad compartida aplicable al tipo de servicio contratado.

b. Los proveedores de servicios en la nube deben acreditar certificaciones de seguridad vigentes (ISO/IEC 27001, SOC 2 o equivalente) y los contratos deben incluir SLAs de seguridad de la información.

c. Ante la finalización o cambio del proveedor de servicios en la nube, PKI SERVICES debe garantizar la devolución o eliminación verificable de toda la información almacenada, con evidencia del proceso de salida segura.

## 5. 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.

## 6. 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
Los cambios en los servicios de los proveedores (actualizaciones de firmware, cambios de versión de software, cambios de infraestructura) deben ser notificados a PKI SERVICES con antelación y evaluados por su impacto en la seguridad de la información antes de su adopción.

## 7. 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.

## 8. 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.

La información de PKI SERVICES que no sea objeto de devolución debe ser destruida de forma segura por el proveedor al terminar el contrato. PKI SERVICES debe obtener evidencia certificada de dicha destrucción.

**Roberto Rodríguez**
**Gerente General**
**Bogotá D.C. 26-06-2026**