POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA RELACIONES CON PROVEEDORES

SECRETARÍA DE EDUCACIÓN DEL DISTRITO

BOGOTÁ – COLOMBIA

2022

Versión 1.0

Av. Eldorado No. 66 – 63
PBX: 324 10 00 Fax: 315 34 48
Código postal: 111321
www.educacionbogota.edu.co
Información: Línea 195

ALCALDÍA MAYOR DE BOGOTÁ D.C.

1. OBJETIVO

Establecer controles y requerimientos de que ayuden a salvaguardar la información implicada entre la Secretaría de Educación del Distrito (SED) y sus proveedores y terceros, que puedan afectar la integridad, disponibilidad y confidencialidad de la información.

2. ALCANCE

La presente política de seguridad aplica para todos los proveedores y terceros que requieran acceder a la información de la SED, para el cumplimiento de sus labores de acuerdo con objetos contractuales establecidos. Así como también, aplica a todo el personal de la SED que esté involucrado laboralmente con proveedores y terceros.

3. DEFINICIONES

- **Activo de Información:** Es todo aquello que en el Ministerio de Educación Nacional es considerado importante o de alta validez para la entidad, porque contiene información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.

- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

- **Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **SGSI:** Sistema de Gestión de Seguridad de la Información.

- **Seguridad digital:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

- **Vulnerabilidad:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

4. RESPONSABLES

- Proveedores y terceros de la SED.
- Supervisores de Contrato
- Equipo de Gobierno y Seguridad Digital.

5. GENERALIDADES

La Secretaría de Educación del Distrito instaura mecanismos de control en sus relaciones con proveedores de bienes y servicios, así como también con terceros, con el propósito de proteger la información de la SED a la que tengan acceso, y que

sea necesaria para el cumplimiento de sus objetos contractuales; con este fin la SED difunde y requiere del acatamiento de sus políticas y procedimientos de seguridad de la información.

Estas políticas, procedimientos, y demás requisitos de seguridad, necesarios para la mitigación de los posibles riesgos asociados con el acceso a proveedores a los activos de información de la entidad, deben ser documentados y publicados por parte de la SED para conocimiento de proveedores y terceros, de tal manera que se asegure la protección de los activos de información de la SED.

Los proveedores que requieran acceder a información sensible, reservada y/o confidencial, deberán acatar las políticas de seguridad, a fin de garantizar la no divulgación y/o modificación de la información antes mencionada, de lo contrario, solo tendrán acceso limitado a la información de la SED.

En caso de que los proveedores y terceros necesiten acceder a zonas o áreas donde se encuentre información sensible, reservada y/o confidencial, se debe solicitar la autorización al jefe de oficina o director del área donde se desea ingresar, con la previa validación del alcance contractual por el servicio contratado y debe contar con la supervisión del equipo de Seguridad Digital de la SED.

5.1. Normas de seguridad para todo el personal

Para establecer las directrices que deberán cumplir los proveedores de la SED en relación con la seguridad de la información y dar cumplimiento al tratamiento definido para los activos de información se deberá acoger lo siguiente:

- Se deberá generar Acuerdos de Confidencialidad, Acuerdos de Niveles de Servicio y Acuerdos de Intercambio de información (cuando sean necesarios), los cuales deberán cumplir los proveedores de servicios. Estos acuerdos deben contener una responsabilidad tanto civil como penal para la tercera parte contratada.
- Se deberá identificar, mitigar y monitorear los riesgos relacionados con los proveedores de servicios, incluidos en la cadena de suministro de los servicios de tecnología o comunicaciones.
- Se deberá divulgar las políticas y procedimientos de seguridad de la información de la SED a los proveedores, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de esta, por parte de los terceros se realice de acuerdo con las políticas y procedimientos de seguridad de la información.
- Se deberá evaluar y aprobar de manera formal los accesos a la información de la SED requeridos por terceras partes.

- Se deberá establecer y monitorear las condiciones de conexión para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la SED.
- Se deberá establecer y monitorear las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- Se deberá establecer y monitorear las condiciones de seguridad física y ambiental de los terceros que prestan servicio a la SED en sus propias instalaciones.
- Se deberá monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad y Acuerdos de Intercambio de información de parte de los terceros proveedores de servicios.

5.2. Normas de seguridad para todos los proveedores

- Deberán cumplir todas las políticas de seguridad de la información de la SED.
- Reportar los incidentes de seguridad que se puedan presentar al equipo de Seguridad de la Información.
- Realizar el aseguramiento de los dispositivos móviles propiedad de los proveedores que almacenen o procesen información de la SED.
- Cifrar la información catalogada como Pública Confidencial y Pública Reservada que sea suministrada por la SED.
- Proteger sus equipos de cómputo en todo momento.
- Portar identificación corporativa todo el tiempo, en un lugar visible.
- Mantener actualizados los equipos móviles que contengan información de la SED, tanto en antivirus como en parches de seguridad.
- Analizar los riesgos de seguridad vinculados a los proyectos en los que se requiere su participación, al igual que los requerimientos y necesidades de seguridad de la información.
- Los controles de acceso físico o lógicos con los cuales los proveedores de la SED deben cumplir, tendrán que estar documentados y aprobados, además de ser de conocimiento de ambas partes.
- Los proveedores, dependiendo de su clasificación, deberán reportar los incidentes de seguridad de la información al director de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).
- Para la adquisición de software a la medida, el proveedor deberá realizar las pruebas pertinentes siguiendo los parámetros establecidos en política de desarrollo seguro de la SED.

- La SED podrá realizar o solicitar auditorias sobre los sistemas informáticos del proveedor, dependiendo de su clasificación para garantizar el cumplimiento de los parámetros establecidos en las políticas de desarrollo seguro.
- Toda información reservada o confidencial suministrada por parte de la SED, deberá ser tratada de acuerdo con la política de protección de datos de la SED y/o ley 1581 de 2012
- Todo proveedor que trate información confidencial y/o sensible, que haya sido suministrada por la SED, al finalizar la relación contractual, deberá ejecutar un procedimiento de borrado seguro, contando con la participación de los colaboradores que sean designados por la SED.

6. CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

- Para toda adquisición de software y hardware que la SED realice, es responsabilidad del equipo de Gobierno y Seguridad Digital de la OTIC definir los requisitos de seguridad, de acuerdo con el procedimiento de compras.
- Los proveedores clasificados de impacto crítico que contratan externamente servicios de otras compañías, y que estén relacionados con el suministro de tecnología de información y comunicación que prestan a la SED, deben asegurar que los requisitos y buenas prácticas de seguridad implementadas por la SED, sean extensivos a sus terceros que intervengan directamente con los servicios prestados a la entidad.

7. GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES

Cuando se presentan modificaciones, la SED establece y notifica los cambios que se generaron o se proyecten realizar con respecto a los acuerdos contractuales iniciales, de acuerdo con lo establecido en el Procedimiento de evaluación de proveedores

8. INCUMPLIMIENTO

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad,

incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

La presente política se basa en la norma ISO 27002 Control A15 Relación con Proveedores.

WILSON ADIEL RODRÍGUEZ RODRÍGUEZ
Jefe Oficina de Tecnologías de Información y las Comunicaciones

Elaboró: Duber Jair Rocha Botero. Profesional Universitario OTIC

Revisó: Equipo de Gobierno y Seguridad Digital OTIC