GUÍA DE OBLIGACIONES EN MATERIA DE **CIBERSEGURIDAD**

PARA EL SECTOR DE LAS TELECOMUNICACIONES

EN COLOMBIA

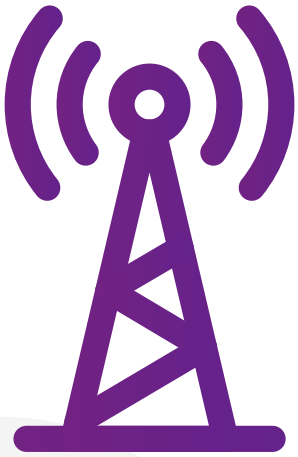
Gómez-Pinzón

DESDE 1992

Introducción:

La ciberseguridad, entendida como el conjunto de herramientas y políticas, conceptos de seguridad, salvaguardas de seguridad, seguros y tecnologías que puedan ser utilizados para proteger los activos de las organizaciones y los usuarios (Numeral 1.47, Título I, Resolución 5050 de 2016, Comisión de Regulación de las Comunicaciones), es crítica para las empresas en el sector de las telecomunicaciones. Lo anterior, debido a los riesgos intrínsecos que conllevan las actividades que desempeñan, tales como el intercambio constante de información y su capacidad de transportar datos, convirtiendo a todo tipo de dispositivos en blancos altamente accesibles para los ciberdelincuentes. Por ende, es pertinente que los actores principales del sector cumplan con los lineamientos y medidas principales relativas a ciberseguridad y seguridad de la información establecidas por la normativa relevante, como también la adopción de buenas prácticas.

Obligaciones:



1. Los proveedores de redes y servicios de telecomunicaciones ("PRST") deben cumplir con las siguientes obligaciones en materia de seguridad de la información (Artículo 2.1.4.1., Resolución 5050 de 2016, Comisión de Regulación de las Comunicaciones):

- Garantizar que los datos personales suministrados al usuario sean utilizados para la correcta prestación del servicio.
- Abstenerse de utilizar los datos personales de los usuarios para la elaboración de bases de datos con fines distintos a los directamente relacionados con los fines para los que fueron entregados, al menos de contar con la autorización expresa.
- Implementar procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor.

2. Asimismo, los PRST que ofrezcan acceso a internet deben acatar los siguientes lineamientos (Artículo 5.1.2.3, Resolución 5050 de 2016, Comisión de Regulación de las Comunicaciones):

- Informar al usuario, en todo momento, los riesgos relativos a la seguridad de la red en cuanto al servicio de acceso a Internet contratado y las acciones que debe adelantar el usuario para preservar la seguridad de la red.
- Publicar en su página web sobre las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención de spam, phishing y malware, entre otras.

3. Ahora, los operadores de servicios postales (Artículo 2.2.3.1, Resolución 5050 de 2016, Comisión de Regulación de las Comunicaciones), deben cumplir con las siguientes obligaciones:

- Garantizar la seguridad de la red postal con el fin de asegurar la inviolabilidad de los envíos postales de los usuarios, la información que curse a través de ella y los datos personales de los usuarios.

- Prohibir, ni por acción ni por omisión, la interceptación o violación de los envíos postales que cursen por sus redes.

- Desarrollar el manejo confidencial, la integridad y disponibilidad de los datos de sus usuarios, los cuales sólo podrán ser requeridos por autoridad judicial.

Buenas prácticas:

Además de las obligaciones referidas, en el sector de las telecomunicaciones desde una perspectiva nacional, la CCIT publicó en el 2022 el documento "Ciber – Seguridad en la Era de la Movilidad Digital" en el que identificó múltiples buenas prácticas en materia de seguridad de la información que pueden considerarse para efectos de sus sistemas y lineamientos de seguridad tales como:

- Analizar en tiempo real el tráfico de autenticación en los sistemas para detectar comportamientos anómalos; e

- Identificar los accesos válidos que un usuario hace desde dispositivos que no se han usado previamente.

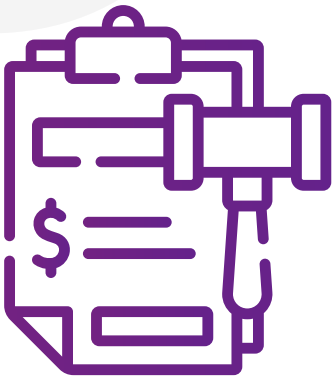
Asimismo, existen distintos instrumentos que permiten identificar los objetivos de la seguridad de la información, considerado a través de los estándares y los marcos de referencia utilizados a nivel mundial como los consignados en el documento "Mejores Prácticas para la ciberseguridad en las empresas", publicado por la CCI en el 2020. Así, se permitirá involucrar la gestión de riesgos, el entorno de los ciberataques, atender los requisitos legales, poner en marcha las prácticas de intercambio de información e implementar los requerimientos de la ciberseguridad, a través de las siguientes recomendaciones:

- Identificación de recursos en el sistema de información, tangibles e intangibles y determinar los procesos necesarios para que la empresa funcione.
- Evaluación con valor cualitativo y cuantitativo de los procesos de negocio.
- Identificar las amenazas que pueden comprometer los activos de información.
- Determinar el impacto en caso de un ciberataque y si afectaría un activo.
- Identificación de medidas de seguridad existentes dentro de la organización y así evaluar los riesgos.

Más aún, desde la perspectiva internacional, el Network Information Systems Directive, NISD, por sus siglas en inglés, legislación implementada en el Reino Unido, se dirige a los operadores de "servicios esenciales" y determinados "proveedores de servicios digitales" y exige adoptar medidas políticas y reglamentarias de un alto nivel de seguridad de las redes y los sistemas de información, así como cuando se produzcan incidentes de seguridad en los sectores afectados.

Posibles Sanciones:

El incumplimiento de las obligaciones descritas anteriormente dirigidas a los PRST puede conllevar a la imposición de sanciones por parte del Ministerio de Tecnologías de la Información y las Comunicaciones. Entre ellas se destacan multas hasta de 2.000 SMLMV, suspensión de la operación al público hasta por 2 meses, caducidad del contrato o cancelación de la licencia, autorización o permiso y amonestaciones.



Ahora bien, el incumplimiento de las obligaciones dirigidas a los operadores de servicios postales puede conllevar a la imposición de sanciones por parte del Ministerio de Tecnologías de la Información y las Comunicaciones. Entre estas se destacan, multas que oscilan entre 60 y 200 salarios mínimos legales mensuales vigentes, cancelación del título habilitante para la prestación de servicios postales, conforme a la graduación de las sanciones descrita en el artículo 39 de la Ley 1369 de 2009.

Más información

Mauricio Jaramillo Campuzano
Socio
Tecnología, Comunicaciones & Protección de Datos
mjaramillo@gomezpinzon.com

Andrés Fernández de Castro
Director
Tecnología, Comunicaciones & Protección de Datos
afernandezdecastro@gomezpinzon.com

Gómez-Pinzón
DESDE 1992

Canal GP 30
Gómez-Pinzón
@GPALegal

BOGOTÁ
Calle 67 # 7-35 Of. 1204
Edificio Caracol
Bogotá, Colombia
Tel: +57 601 319 2900

MEDELLÍN
Cra. 43A # 1- 50 Of. 209
San Fernando Plaza
Medellín, Colombia
Tel: +57 604 444 3815