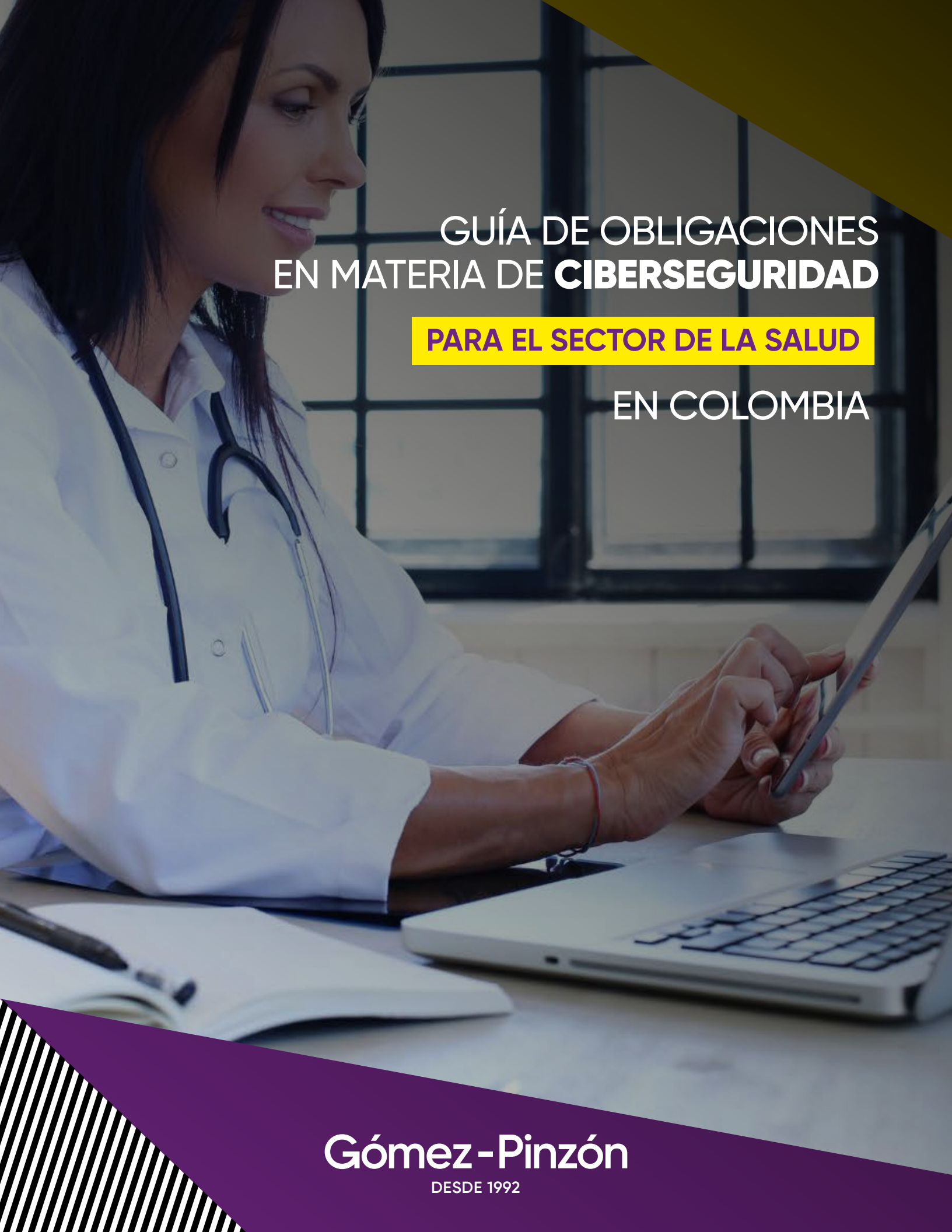


GUÍA DE OBLIGACIONES EN MATERIA DE **CIBERSEGURIDAD**

PARA EL SECTOR DE LA SALUD

EN COLOMBIA

Gómez-Pinzón

DESDE 1992

Introducción:

Con ocasión de la pandemia derivada del Covid 19, el sector salud se enfrentó a obstáculos y desafíos innumerables, como también a oportunidades como la digitalización y transformación digital. Lo anterior, trajo consigo la ocurrencia de ciberataques y brechas de seguridad de la información. De acuerdo con el estudio "Healthcare breaches on the rise in 2022", referente a los ciber ataques en el sector salud, se indica un aumento del 84% de ciberataques en el sector en los últimos tres años. Teniendo en cuenta la alta exposición y vulnerabilidad en la que se encuentra este sector y la sensibilidad de la información que procesan de los pacientes y otros grupos de interés, a continuación, se expondrán algunas de las obligaciones que deben cumplir los actores del sector, así como buenas prácticas a implementar para intentar mitigar posibles perjuicios a sus sistemas o la información que manejan (Doyle, P, 2022).

Obligaciones:

Con ocasión de la pandemia derivada del Covid 19, el sector salud se enfrentó a obstáculos y desafíos innumerables, como también a oportunidades como la digitalización y transformación digital. Lo anterior, trajo consigo la ocurrencia de ciberataques y brechas de seguridad de la información. De acuerdo con el estudio "Healthcare breaches on the rise in 2022", referente a los ciber ataques en el sector salud, se indica un aumento del 84% de ciberataques en el sector en los últimos tres años. Teniendo en cuenta la alta exposición y vulnerabilidad en la que se encuentra este sector y la sensibilidad de la información que procesan de los pacientes y otros grupos de interés, a continuación, se expondrán algunas de las obligaciones que deben cumplir los actores del sector, así como buenas prácticas a implementar para intentar mitigar posibles perjuicios a sus sistemas o la información que manejan (Doyle, P, 2022).

1. Los actores del sector salud, siendo estos los prestadores de servicios de salud públicos y privados, las Entidades Promotoras de Salud (EPS), las Entidades Adaptadas al Sistema General de Seguridad Social en Salud (SGSSS), las entidades que administren planes voluntarios de salud, las administradoras de riesgos laborales y los fondos de pensiones en sus actividades de salud, las entidades pertenecientes a los regímenes de excepción especial de salud, las secretarías, institutos y unidades administrativas departamentales, distritales y municipales de salud, que accedan a la información de manera innominada y las compañías de seguros que emitan pólizas de accidentes de tránsito, deberán cumplir con las siguientes obligaciones en materia de seguridad de la información (Artículo 19, Resolución 886 de 2021, Ministerio de Salud):

- Adoptar una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la cual deberán desarrollar periódicamente una evaluación del riesgo de seguridad digital.

- Asegurar la infraestructura, sistemas de tecnología de la información y prácticas de negocios que interactúan o implican el uso de cualquier información o dato personal.

- Incorporar prácticas y procesos de desarrollos destinados a salvaguardar la información personal de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.

2. Ahora, los prestadores de servicios de salud públicos y privados deberán tener en cuenta que les aplican las siguientes obligaciones específicas (Artículo 24, Resolución 886 de 2021, Ministerio de Salud):

- Contar con estrategias de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio que permiten el uso de los mecanismos de comunicación y garantizar la confidencialidad, integridad, disponibilidad, autenticación y autorización en el marco de intercambio de datos.

- Adoptar estándares alineados con la Política de Gobierno Digital, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, la cual, en el Manual de Gobierno Digital establece las necesidades y problemáticas que determinan el uso de las Tecnologías y las Comunicaciones (TIC).

3. A su vez, las entidades que sean fabricantes e importadoras de dispositivos médicos o prestadores de Servicios de Salud y profesionales independientes deben diseñar e implementar un programa de tecnovigilancia, en los términos del Decreto 1011 de 2006 del Ministerio de Salud, el cual debe contener como mínimo (Artículo 10, Resolución 4816 de 2008, Ministerio de Salud):

- La designación de un responsable del programa;

- La elaboración de un formato de reportes adversos por utilización de dispositivos médicos;

- La implementación de un sistema de administración de gestión de datos; y

- La elaboración de un Manual de Tecnovigilancia entendido como el documento institucional que define el tipo de dispositivos objeto de vigilancia que asegure un permanente seguimiento de los eventos o incidentes adversos que permitan identificar, registrar, evaluar y gestionar reportes de dispositivos médicos.

Buenas prácticas:

El cumplimiento de las normas de seguridad de la regulación más relevante del sector salud y farmacéuticos en EE. UU., la Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios de 1996 (HIPAA por sus siglas en inglés) se basa en varios principios clave, que deberían ser una guía de buenas prácticas a considerar para los actores relevantes en Colombia:

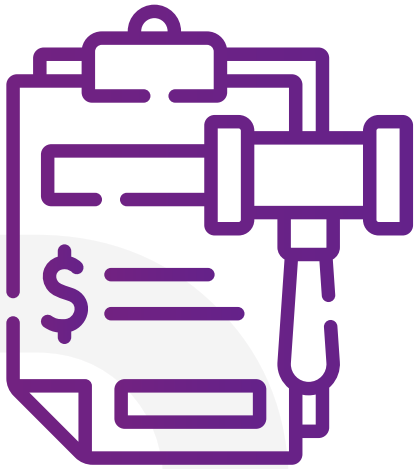
- Implementación de un proceso de gestión de la seguridad, que incluya un análisis de riesgos y medidas de seguridad para mitigar los riesgos potenciales;
- Adopción de los procedimientos ilustrados en su Título II, los cuales incluyen lineamientos de privacidad, reglas transaccionales y de seguridad, y pautas de aplicación para protegerse contra softwares maliciosos;
- Formación de los usuarios sobre los principios de protección contra el software malintencionado; e
- Integración de limitaciones en los controles de acceso y concesión de acceso únicamente a personas que hayan recibido formación en materia de protección de datos.

Más aún, la guía "Protegiendo la Salud Digital – Una Guía de Ciberseguridad en el Sector Salud" del Banco Interamericano de Desarrollo" publicada por el Banco Interamericano de Desarrollo (BID), propone que todos los actores del sector salud deben implementar buenas prácticas para así evitar incidentes de seguridad tales como:

- Incluir la ciberseguridad como prioridad en la gestión estratégica de la organización;
- Definir la estructura organizacional en ciberseguridad;
- Definir los objetivos y las metas de ciberseguridad;
- Realizar un diagnóstico de situación con análisis de brechas o GAP;
- Elaborar un plan de ciberseguridad, el cual sería el instrumento de gestión que se utilizará para cumplir los objetivos y metas de la entidad respecto a ciberseguridad;
- Ejecutar el plan director; y
- Evaluar los resultados y el riesgo remanente.

Posibles Sanciones:

Por el incumplimiento de las obligaciones dirigidas a fabricantes e importadoras de dispositivos médicos, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), podrá iniciar las acciones tanto preventivas como correctivas y/o medidas sanitarias en concordancia con lo establecido en el artículo 579 de la Ley 9 de 1979 y el Decreto 4725 de 2005 del Ministerio de la Protección Social, o las normas que los adicionen, modifiquen o sustituyan. Entre estas se destacan multas, hasta por una suma equivalente a 10.000 salarios mínimos legales diarios vigentes.



Ahora bien, respecto a las obligaciones establecidas en la Resolución 866 de 2021 del Ministerio de Salud, la inspección, vigilancia y control se realizará por parte de la Superintendencia Nacional de Salud, facultada por el artículo 131 de la Ley 1949 de 2019 para imponer sanciones. Entre estas, se destacan multas entre 200 y hasta 8.000 salarios mínimos legales mensuales vigentes para personas jurídicas, y entre 50 y hasta 2.000 salarios mínimos legales mensuales vigentes para las personas naturales, amonestaciones escritas y revocatoria total o parcial de la autorización de funcionamiento.

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