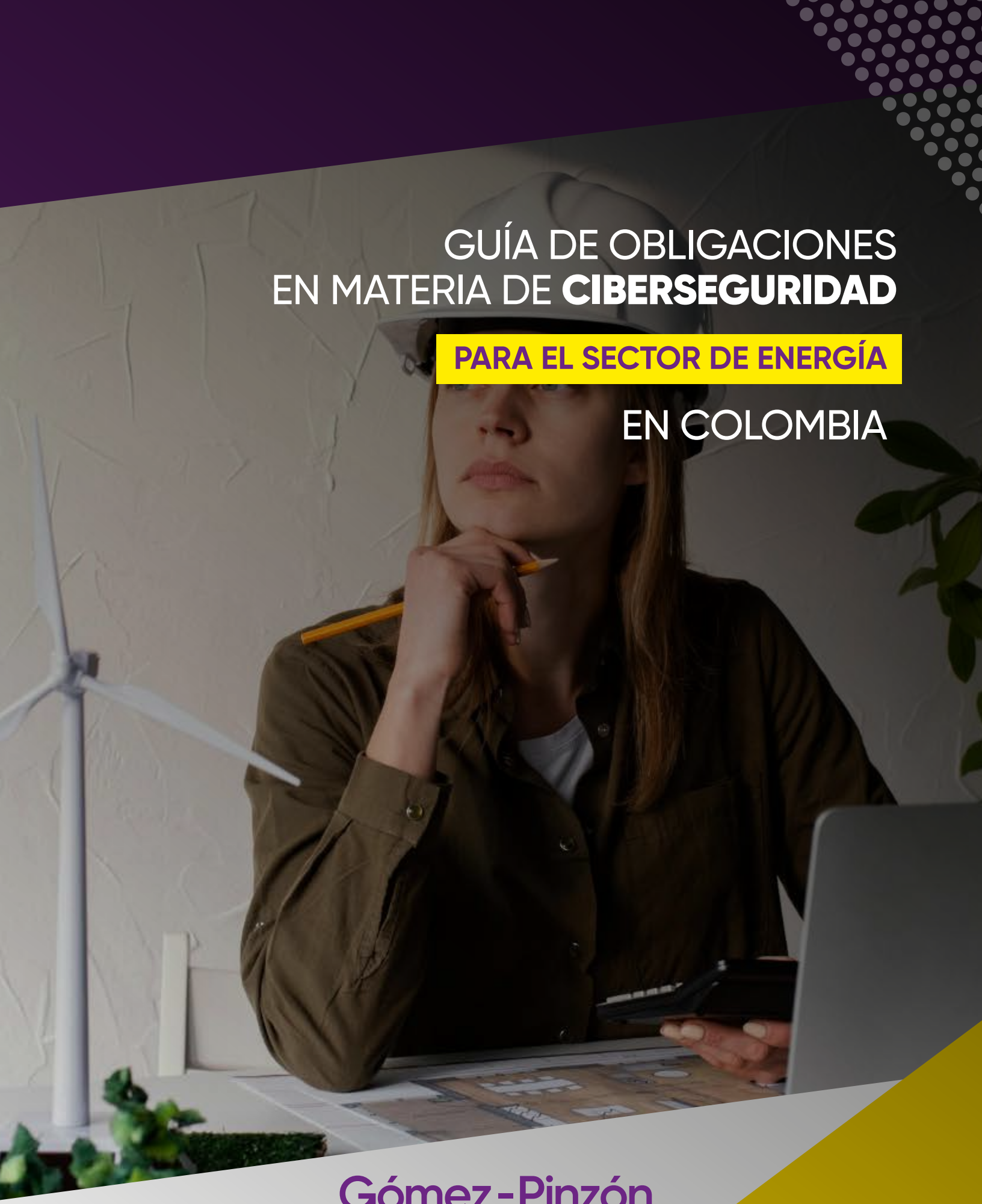
GUÍA DE OBLIGACIONES EN MATERIA DE **CIBERSEGURIDAD**

PARA EL SECTOR DE ENERGÍA

EN COLOMBIA



Gómez-Pinzón

DESDE 1992

Introducción:

En la actualidad cualquier sector de la economía es vulnerable a ataques cibernéticos, y las empresas que hacen parte del sector energético no son la excepción. Por ello, con el objetivo de cuidar su operación, las empresas energéticas deben catalogar los riesgos cibernéticos como riesgos empresariales fundamentales. Además, los actores del sector deben cooperar para evaluar, comprender y crear una fuerte resistencia a estos riesgos, los cuales amenazan la continuidad del servicio, su reputación, su información propia y de terceros, así como sus sistemas.

Con base en lo anterior, esta sección abordará especialmente el sector de energía eléctrica y los agentes que componen el Sistema Interconectado Nacional (SIN). En ese sentido, es fundamental para los agentes de este sector trabajar de forma coordinada dado que, un ciberataque independiente puede afectar a todos los agentes por igual y la integralidad del sistema, disminuyendo su capacidad de distribuir, transmitir y generar energía eléctrica. Por ello, la regulación sectorial busca crear estrategias de ciberseguridad que preparen a los agentes para enfrentar riesgos asociados con incidentes cibernéticos que puedan afectar la operación del sector y el suministro de energía eléctrica de manera oportuna (Documento de Consulta, CREG - 065)

Obligaciones:

1. Los agentes generadores, transmisores, distribuidores y el Operador del Sistema Interconectado tienen la obligación de:

- Implementar políticas o lineamientos de ciberseguridad.
- Realizar actualizaciones de inventario de ciberactivos[1].
- Adelantar actualizaciones de análisis de riesgos y vulnerabilidades.
- Efectuar actualizaciones del nivel de gestión de ciberseguridad.
- Adoptar planes de sensibilización y entrenamiento para el personal relacionado con ciberactivos.
- Realizar definiciones de los perímetros de seguridad electrónica para los ciberactivos.
- Desarrollar planes de gestión de incidentes de ciberseguridad.
- Implementar planes de seguridad electrónica de ciberactivos.
- Ejecutar planes de seguridad física para ciberactivos.
- Adelantar Planes de recuperación para ciberactivos.
- Nombrar un responsable de ciberseguridad
- Adoptar procesos de verificación y revocatoria de accesos lógicos y físicos a cuentas de usuarios.
- Desarrollar análisis de riesgos y vulnerabilidades
- Revisar, actualizar y conservar toda la documentación de soporte del cumplimiento de las acciones de cara a implementación de medidas de seguridad.
- Acreditar el cumplimiento de las anteriores obligaciones, por medio de auditorías internas que deben efectuarse cada dos años y comunicar su ejecución al Consejo Nacional de Operación (CNO) (Acuerdo 1502 de 2021 del CNO).

[1] El término Ciberactivo refiere a un "dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota"(Aparte 1.2., Anexo Guía de Ciberseguridad, Acuerdo 1502 de 2021, CNO).

2. Los representantes de las fronteras, es decir aquellos agentes cuyo nombre se registra en la frontera comercial en el SIN, tienen la obligación de asegurar que los medidores, tanto el principal como el de respaldo, de las fronteras comerciales con reporte al Administrador del Sistema de Intercambios Comerciales (ASIC) cuenten con un sistema de protección en el que:

- El almacenamiento de las mediciones y parámetros de configuración del medidor se realicen en memoria no volátil (Artículo 17, Resolución 038 de 2014, Comisión de Regulación de Energía y Gas).
- La interrogación local y remota de las mediciones y la configuración de los parámetros del medidor cuente como mínimo dos (2) niveles de acceso y emplear contraseña para cada usuario, entre otros (Artículo 17, Resolución 038 de 2014, Comisión de Regulación de Energía y Gas).

3. Para la transmisión de lecturas desde los medidores, los representantes de las fronteras, los Gestión de Medidas (CGM) y el Administrador del Sistema de Intercambios Comerciales (ASIC) tienen la obligación de (Acuerdo 1043 de 2018, CNO):

- Asegurar que los medidores, tanto el principal como el de respaldo, de las fronteras comerciales con reporte al ASIC cuenten con un sistema de protección de datos (Anexo, Acuerdo 1043 de 2018, CNO).
- Implementar mecanismos que aseguren la confidencialidad, integridad y no repudio de la información por medio de cifrado sobre cualquier tipo de canal o protocolo de comunicación (Anexo, Acuerdo 1043 de 2018, CNO).
- En el intercambio de datos entre el CGM y el ASIC deberá realizarse a través de https sobre redes privadas virtuales (IPSEC o SSL), autenticadas con certificados digitales en doble vía para asegurar la confidencialidad, integridad y no repudio (Anexo, Acuerdo 1043 de 2018, CNO).

Buenas prácticas:

De acuerdo con la cartilla "Ciberseguridad en el Sector Eléctrico" publicada por Deloitte en conjunto con Fortinet, a continuación se señalan algunas recomendaciones para los agentes del sector energético en general, de cara a incrementar sus estándares en la tecnología de gestión de procesos:

- Llevar a cabo segmentación de las redes. Para estos fines, los diferentes agentes deben prever el dinamismo de la segmentación, dado que este no es un proceso dinámico. Además, se sugiere implementar los estándares ISA/IEC-62443 que proveen directrices de segmentación de red, asignando niveles de seguridad de estas.

- Adelantar procesos de monitoreo de tráfico. Tras llevar a cabo la segmentación de las redes, se sugiere generar visibilidad sobre el tráfico circulante en cada segmento, de modo que sea posible alertar tempranamente la existencia de amenazas. De igual forma, se recomienda vigilar cuidadosamente la maquinaria y procesos físicos en las instalaciones de energía.

- Implementar procesos de control de acceso a dispositivos. Se recomienda que se adopten procesos de autenticación antes de obtener permisos de ingreso a usuarios, apps, dispositivos que den acceso a la tecnología operacional.

- Adoptar procesos de protección a puntos de acceso. Se recomienda que los puntos de acceso a la tecnología operacional implementen medidas de seguridad desde su diseño y que sean gestionados desde una interfaz central de manera particular.

Posibles Sanciones:

Ante el eventual incumplimiento de las obligaciones mencionadas, se podrán aplicar las siguientes sanciones: amonestación; multas hasta de 2.000 SMLMV; orden de suspender de inmediato todas o algunas de las actividades del infractor, y cierre de los inmuebles utilizados para desarrollarlas; orden de separar a los administradores o empleados de una empresa de servicios públicos, entre otros (Artículo 81, Ley 142 de 1994).

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