Acuerdo 1241 Por el cual se aprueba la actualización de la Guía de Ciberseguridad

Acuerdo Número:	Fecha de expedición:	Fecha de entrada en vigencia:
1241	3 Octubre, 2019	3 Octubre, 2019

Sustituye Acuerdo:

03/09/2015 Acuerdo 788

Sustituido por:

16/09/2020 Acuerdo 1347 Por el cual se aprueba la actualización de la Guía de Ciberseguridad

Acuerdos relacionados:

Acuerdo 770 - 06/08/2015

El Conseio Nacional de Operación en uso de sus facultades legales, en especial las conferidas en el Artículo 36 de la Ley 143 de t994, el Anexo general de la Resolución CREG 025 de 1995 y su Reglamento Interno y según lo definido en la reunión No. 573 del 3 de octubre de 2019, y

CONSIDERANDO

1	Que el documento CONPES 3701 del 14 de Julio de 2011 estableció los lineamientos de política para la ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que puedan afectar significativamente al país.
2	Que el documento CONPES 3701, implicaba un compromiso del Gobierno Nacional por garantizar la seguridad de la información y busca sentar las bases de política para los tópicos de ciberseguridad y ciberdefensa, y las entidades públicas y privadas involucradas tendrán la responsabilidad de desarrollar estas bases y generar mecanismos que permitan garantizar la seguridad de la información a nivel nacional, teniendo en cuenta las normas técnicas y los estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad.
3	Que el CNO expidió el Acuerdo 788 del 3 de septiembre de 2015 por el cual se aprobó la Guía de Ciberseguridad, que impulsó el desarrollo de capacidades en los agentes del sector eléctrico para la gestión y respuesta frente al riesgo de ciberataques, ya que se requiere la participación de todos los agentes para una protección adecuada y uniforme del Sistema Interconectado Nacional (SIN).
4	Que el Documento CONPES 3854 del 11 de abril de 2016 estableció la Política Nacional de Seguridad Digital cuyo objetivo es fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.
5	Que la Presidencia de la República y el Ministerio de Defensa establecieron que el sector eléctrico es crítico para el país desde la dimensión digital y lo incluyeron dentro de los sectores estratégicos.
6	Que el Ministerio de Defensa formuló el Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia y el Plan Sectorial de Protección y Defensa de la ICC.

7	Que el CNO ha determinado la seguridad digital como un riesgo para la operación confiable y segura del SIN, dado que la probabilidad de ciberataques de alto impacto ha aumentado, como lo demuestran los datos de incidentes en los últimos años como Wanacry, Petya, la filtración de armas cibernéticas de agencias de inteligencia, el acceso a sistemas de operación en el sector eléctrico de Estados Unidos y los ataques a Gran Bretaña; así como la publicación de vulnerabilidades cada vez más frecuentes y de malware especializado diseñado especialmente para atacar tecnologías de operación y protecciones usadas en el sector.
8	Que el Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética del Sector Electricidad Colombiano establece como línea estratégica de acción a corto plazo la actualización de la Guía de Ciberseguridad adoptada por el sector de acuerdo con las prácticas comúnmente aceptadas para la protección de éste sector.
9	Que los resultados de las encuestas sobre ciberseguridad realizadas por el CNO y los análisis realizados en la mesa sectorial de infraestructura critica realizada por el CCOCI y el CNO permitieron definir la hoja de ruta y los tiempos para la implementación de la actualización de la guía de ciberseguridad por parte de los agentes del SIN.
10	Que el Comité de Supervisión y Ciberseguridad realizó la actualización de la Guía de Ciberseguridad a las nuevas realidades del mercado eléctrico colombiano y al entorno de ciberseguridad, según los lineamientos más actuales de las normas internacionales base y en la reunión 8 del 11 de septiembre de 2019 recomendó la expedición del presente Acuerdo.

ACUERDA:

1	Aprobar la adopción de la Guía de Ciberseguridad que se encuentra en el Anexo del presente Acuerdo y hace parte integral del mismo.
2	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán hacer la actualización y notificación del responsable de ciberseguridad, en un plazo máximo de (6) seis meses contados a partir de la fecha de expedición del presente Acuerdo, de acuerdo con lo previsto en la Guía de Ciberseguridad.
3	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán desarrollar en un plazo máximo de (1) un año contado a partir de la fecha de expedición del presente Acuerdo, según los criterios de la Guía de Ciberseguridad, lo siguiente: • Política o lineamiento de ciberseguridad. • Actualización de inventario de ciberactivos. • Actualización de análisis de riesgos y vulnerabilidades. • Actualización del nivel de gestión de ciberseguridad. • Plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos. • Definición de los perímetros de seguridad electrónica para los ciberactivos. • Plan de gestión de incidentes de ciberseguridad
4	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán realizar en un plazo máximo de (18) dieciocho meses contados a partir de la fecha de expedición del presente Acuerdo, según los criterios de la Guía de Ciberseguridad, lo siguiente: • Plan de seguridad electrónica de ciberactivos. • Plan de seguridad física para ciberactivos. • Plan de recuperación para ciberactivos • La primera ejecución del plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos.
5	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán realizar en un plazo máximo de (24) veinticuatro meses contados a partir de la fecha de expedición del presente Acuerdo, según los criterios de la Guía de Ciberseguridad, lo siguiente: • La implementación de los controles en los perímetros de seguridad electrónicos y físicos en acuerdo a los planes desarrollados. • La implementación de monitoreo básico de eventos sobre los ciberactivos críticos.
6	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán implementar la Guía de Ciberseguridad así:

	a. Para el 50% de sus ciberactivos críticos, en un plazo máximo de (30) treinta meses contados a partir de la fecha de expedición del presente Acuerdo. b. Para el 75% de sus ciberactivos críticos, en un plazo máximo de (42) cuarenta y dos meses contados a partir de la fecha de expedición del presente Acuerdo. c. Para el 100% de sus ciberactivos críticos, en un plazo máximo de (48) cuarenta y ocho meses contados a partir de la fecha de expedición del presente Acuerdo.
7	El CNO desarrollará actividades de sensibilización, comunicación, entrenamiento y socialización de la Guía de Ciberseguridad del CNO y de los procesos de seguridad cibernética.
8	El Comité de Supervisión y Ciberseguridad hará un seguimiento cuatrimestral de los compromisos previstos en este Acuerdo. Parágrafo: El informe de seguimiento será presentado al CNO.
9	El presente Acuerdo rige a partir de la fecha de su expedición y sustituye el Acuerdo 788 de 2015.

Presidente - Diego González

Secretario Técnico - Alberto Olarte Aguirre