Acuerdo 1463 Por el cual se aprueba la actualización de la Guía de Ciberseguridad

Acuerdo Número:	**Fecha de expedición:**	**Fecha de entrada en vigencia:**
1463	19 Octubre, 2021	19 Octubre, 2021

Sustituye Acuerdo:

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

Sustituido por:

02/12/2021 Acuerdo 1502 Por el cual se aprueba la actualización de la Guía de Ciberseguridad y se modifican algunos plazos

El Consejo 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 presencial No. 647 del 19 de octubre de 2021, 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 se expidió el Acuerdo 1241 el 3 de octubre de 2019, por el cual se aprobó la actualización de la Guía de Ciberseguridad.
11	Que desde el pasado 7 de enero de 2020 la OMS declaró el brote del coronavirus COVID19 como una Emergencia de Salud Pública de Importancia Internacional y desde el mes de marzo, debido a la declaratoria de emergencia sanitaria por la pandemia COVID19, el Gobierno Nacional ha expedido reglamentación con el objetivo de adoptar medidas preventivas de aislamiento y cuarentena para todo el territorio nacional, restringiendo el derecho de libre circulación, lo cual ha impactado las actividades logísticas y el cumplimiento de algunos plazos previstos en el Acuerdo 1241 de 2019.
12	Que el Comité de Supervisión y Ciberseguridad en la reunión 26 del 9 de septiembre de 2020 recomendó la expedición del presente Acuerdo, en el que se amplian los plazos de las siguientes actividades a partir del 3 de octubre de 2019, fecha de expedición del Acuerdo 1341, así: Ampliación plazo de 12 a 18 meses: • Actualización de inventario de ciberactivos. • Actualización de análisis de riesgos y vulnerabilidades. • Actualización del nivel de gestión de ciberseguridad. • Definición de los perímetros de seguridad electrónica para los ciberactivos. Ampliación plazo de 18 a 24 meses: • Plan de seguridad electrónica de ciberactivos. • Plan de seguridad física para ciberactivos.
13	Que en la reunión CNO 646 del 7 de octubre de 2021, el Consejo aprobó la creación y las funciones de 2 comités: Supervisión y Ciberseguridad, que reemplazarán el Comité de Supervisión y Ciberseguridad.
14	Que entre otras funciones. El Comité de Ciberseguridad debe: Analizar y hacer comentarios a las normas que en materia de ciberseguridad se expidan por parte de las diferentes autoridades, para consulta o en firme, de forma que se garantice la operación del sistema eléctrico de forma confiable y segura con criterios de eficiencia económica, e Identificar las necesidades y hacer las recomendaciones al CNO sobre aspectos tecnológicos relacionados con la ciberseguridad con criterios de eficiencia económica y en coordinación con el comité de Operación y el Comité de Supervisión.
	ACUERDA:
1	Aprobar la actualización 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 del 3 de octubre de 2019, 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 las siguientes actividades, en los siguientes plazos, según los criterios de la Guía de Ciberseguridad: • Política o lineamiento de ciberseguridad: 12 meses contados a partir del 3 de octubre de 2019. • Actualización de inventario de ciberactivos: 18 meses contados a partir del 3 de octubre de 2019. • Actualización de análisis de riesgos y vulnerabilidades: 18 meses contados a partir del 3 de octubre de 2019. • Actualización del nivel de gestión de ciberseguridad: 18 meses contados a partir del 3 de octubre de 2019. • Plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos: 12 meses contados a partir del 3 de octubre de 2019. • Definición de los perímetros de seguridad electrónica para los ciberactivos: 18 meses contados a partir del 3 de octubre de 2019. • Plan de gestión de incidentes de ciberseguridad: 12 meses contados a partir del 3 de octubre de 2019.
4	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán realizar las siguientes actividades, según los criterios de la Guía de Ciberseguridad, en los siguientes plazos: • Plan de seguridad electrónica de ciberactivos: 36 meses contados a partir del 3 de octubre de 2019. • Plan de seguridad física para ciberactivos: 36 meses contados a partir del 3 de octubre de 2019. • Plan de recuperación para ciberactivos: 18 meses contados a partir del 3 de octubre de 2019. • La primera ejecución del plan de sensibilización y entrenamiento para el personal relacionado con ciberactivos: 36 meses contados a partir del 3 de octubre de 2019.
5	Los agentes generadores, transmisores, distribuidores y el operador del Sistema Interconectado Nacional deberán realizar según los criterios de la Guía de Ciberseguridad, en un plazo máximo de (36) treinta y seis meses contados a partir del 3 de octubre de 2019, 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 (42) cuarenta y dos meses contados a partir del 3 de octubre de 2019 b. Para el 75% de sus ciberactivos críticos, en un plazo máximo de (54) cincuenta y cuatro meses contados a partir del 3 de octubre de 2019 c. Para el 100% de sus ciberactivos críticos, en un plazo máximo de (60) sesenta meses contados a partir del 3 de octubre de 2019.
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 cumplimiento de los aspectos solicitados en la guía deberá demostrarse a través de reportes de auditorías internas. La primera auditoría interna se deberá hacer entre el mes de octubre de 2021 y el mes de abril del 2022. Las siguientes auditorías internas deberan realizarse cada 2 años.
9	

	El Comité de Ciberseguridad hará un informe de seguimiento semestral de los compromisos previstos en este Acuerdo, con base en un formato que se enviará a los agentes para su diligenciamiento. Parágrafo: El informe de seguimiento será presentado al CNO.
10	El presente Acuerdo rige a partir de la fecha de su expedición y sustituye el Acuerdo 1347 de 2021.

Presidente - Juan Carlos Guerrero

Secretario Técnico - Alberto Olarte Aguirre