Acuerdo 1960 Por el cual se aprueba la actualización de la Guía de Ciberseguridad y se modifican algunos plazos

Acuerdo Número:	**Fecha de expedición:**	**Fecha de entrada en vigencia:**
1960	3 Abril, 2025	3 Abril, 2025

Sustituye Acuerdo:

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 1994, el Anexo general de la Resolución CREG 025 de 1995 y su Reglamento Interno y según lo definido en la reunión No. 788 del 3 de abril de 2025, 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 Infraestructura Crítica Cibernética - 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. Casos como los apagones registrados en Ucrania en 2015, 2016, 2022 y 2024 producidos por ciberataques, así como los ataques a infraestructuras eléctricas del Reino Unido, Irlanda, Estados Unidos, Israel, India, entre otros han demostrado que los ataques cibernéticos a estas infraestructuras son una parte activa del panorama de riesgos actual y futuro.

8	Que el documento CONPES 3995 de julio de 2020, Política Nacional de Confianza y Seguridad digital, establece medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.
9	Que la creciente interconexión e integración de los sistemas de tecnología operativa (OT) con los sistemas de tecnología de la información (IT), incluida la adopción de tecnologías de nube e IoT en entornos industriales, incrementa la superficie de ataque y requiere una reevaluación continua del enfoque de seguridad para los ciberactivos críticos.
10	Que el 3 de septiembre de 2015 el CNO expidió el Acuerdo 788 "Por el cual se aprueba la Guía de Ciberseguridad", el cual fue sustituido por el Acuerdo 1241 de 2019. El anterior acuerdo fue sustituido por el Acuerdo 1347 de 2020 y el Acuerdo 1463 de 2021. El Acuerdo 1463 fue sustituido por el Acuerdo 1502 de 2021.
11	Que el Comité de Ciberseguridad en la reunión 44 del 11 de marzo de 2025 analizó y recomendó actualizar la Guía de Ciberseguridad, cambiando el enfoque de cumplimiento normativo hacia un enfoque basado en riesgos, lo que permitirá a los agentes del sector eléctrico adaptar sus controles según sus perfiles de riesgo específicos. Así mismo, un enfoque basado en riesgos permitirá optimizar las inversiones en materia de ciberseguridad, priorizando los recursos hacia la protección de aquellos activos con mayor impacto potencial en la operación confiable del Sistema Interconectado Nacional.
	ACUERDA:
1	Aprobar la actualización de la Guía de Ciberseguridad como se presenta en los Anexos del presente Acuerdo y aprobar la modificación de algunos plazos. Los Anexos que hacen parte integral del presente Acuerdo son: • Anexo 1: Guia de Ciberseguridad. • Anexo 2: Criterios de activos críticos. • Anexo 3: Lista de cumplimiento periódico de la Guía de Ciberseguridad PARÁGRAFO: Los requisitos de ciberseguridad que deben cumplir los agentes generadores de plantas menores se encuentran detallados en el Anexo 3.
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. Los agentes generadores, transmisores y distribuidores nuevos y existentes, y el operador del Sistema, deberán cumplir con la obligación de hacer la actualización y notificación del responsable de ciberseguridad, según lo previsto en el numeral 5.2 del Anexo 1 del presente Acuerdo.
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 del Anexo 1 del presente Acuerdo: • Evaluación de riesgos realizado al personal de la entidad: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Certificación por parte de proveedores y contratistas sobre la evaluación de riesgos a su personal: 36 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2028). • Actualización de la evaluación de riesgos cada persona que tenga acceso físico o lógico a activos o ciberactivos críticos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Documento procedimiento para gestión de accesos lógicos y físicos: 12 meses contados a partir de la

fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).

- Evidencias documentales de la verificación periódica: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento evidencia registros de revocación de accesos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Lista del personal con acceso físico no escoltado o acceso lógico a los ciberactivos críticos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia documental de los cambios realizados a las listas de acceso: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento procedimiento para el monitoreo y registro de accesos lógicos a los perímetros de seguridad físicos y lógicos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento de línea base para equipos de punto de acceso al perímetro de seguridad lógica: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento procedimiento de administración de conexiones temporales: 12 meses contados a partir de la fecha de expedición del presente acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia de la revisión periódica del control implementado como sistema de control intermedio: 24 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2027).
- Documento procedimiento de evaluación de vulnerabilidades técnicas: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia de evaluación periódica de vulnerabilidades técnicas: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia de vulnerabilidades técnicas sobre nuevos ciberactivos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Plan de remediación del resultado de análisis de vulnerabilidad técnica: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento procedimiento control transitorio y medios extraíbles: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencias de control periódico de ciberactivos críticos transitorios y medios extraíbles: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento procedimiento de actualización e implementación de parches: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencias de los ciclos de parchado: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Documento procedimiento de monitoreo: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia de controles implementados para identificar y monitorear eventos: 24 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2027).
- Documento plan de recuperación y resiliencia y los procedimientos asociados: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia de pruebas o simulacros, y acciones de mejora de estos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia de los cambios realizados a los procedimientos de recuperación y resiliencia: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia documentada de los respaldos realizados y almacenamiento de la información: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).
- Evidencia documentada de que se realizan pruebas de respaldo y su resultado: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026).

	• Documento con el plan de respuesta ante incidentes: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Evidencia de pruebas o simulacros, y acciones de mejora de estos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Documento plan de seguridad física cumpliendo los requisitos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Evidencia de los controles implementados para protección física del cableado y otros componentes de comunicación: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Alarma o alerta en respuesta a fallas de comunicación detectadas: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Procedimiento documentado de mantenimiento y pruebas periódicas a los sistemas de control relacionados a la seguridad física: 12 meses contados a partir de la expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Evidencia mantenimiento y pruebas periódicas: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Documento y evidencia de la gestión de riesgos de la cadena de suministro que incluya los riesgos identificados y plan de tratamiento de riesgos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Plan de Conciencia y entrenamiento en ciberseguridad de proveedores y contratistas de la cadena de suministro: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Documento con mapa de riesgos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Plan de tratamiento de riesgos con medidas de mitigación, plan de implementación de medidas y asignación de responsabilidades: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). • Evidencia del monitoreo y registro del plan de tratamiento de riesgos: 12 meses contados a partir de la fecha de expedición del presente Acuerdo (fecha de cumplimiento: 3 de abril de 2026). Parágrafo: Los agentes generadores, transmisores y distribuidores nuevos deberán dar cumplimiento a las actividades previstas en el presente artículo en un plazo de doce (12) meses, contados a partir de la fecha del registro como agentes del mercado ante el ASIC.
4	El CNO desarrollará actividades de sensibilización, comunicación, entrenamiento y socialización de la Guía de Ciberseguridad del CNO y de los procesos de seguridad cibernética.
5	El Comité de Ciberseguridad hará un informe de seguimiento semestral de los compromisos previstos en los Anexos de este Acuerdo, con base en el formulario de la encuesta que se envía a los agentes para su diligenciamiento. Parágrafo: El informe de seguimiento será presentado al CNO.
6	El presente Acuerdo rige a partir de la fecha de su expedición y sustituye el Acuerdo 1502 de 2021.

Presidente - German Caicedo

Secretario Técnico - Alberto Olarte Aguirre