Acuerdo 2088 Por el cual se aprueba el procedimiento y formato de reporte de incidentes cibernéticos y la guía de suscripción al MISP

Acuerdo Número:	**Fecha de expedición:**	**Fecha de entrada en vigencia:**
2088	15 Enero, 2026	15 Enero, 2026

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. 821 del 15 de enero de 2026, 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 a la fecha se encuentra vigente el Acuerdo 1960 de 2025 Por el cual se aprueba la actualización de la Guía de Ciberseguridad y se modifican algunos plazos.
11	Que en el marco del Acuerdo 1960 de 2025 Por el cual se aprueba la actualización de la Guía de Ciberseguridad y las directrices establecidas por el Comité de Ciberseguridad del CNO, se identificó la necesidad de crear un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) y establecer lineamientos específicos para su implementación. Lo anterior en línea con la política nacional en materia de ciberseguridad, reflejada en documentos como el CONPES, directivas presidenciales y resoluciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), subraya la importancia de fortalecer la ciberseguridad en todos los sectores, incluyendo el sector eléctrico. A su vez, dentro de las actividades del Comité de Ciberseguridad se promovió la implementación de la Plataforma de Intercambio de Información MISP, como un paso crucial para mejorar la gestión de eventos de ciberseguridad. Sin embargo, la problemática actual radica en la falta de un marco estructurado para realizar el proceso de reporte y gestión de incidentes de origen cibernético, los cuales pueden comprometer la prestación del servicio de energía eléctrica. Bajo ese contexto, el presente Acuerdo tiene como propósito mitigar las deficiencias identificadas y establecer los requisitos específicos para mejorar el proceso de reporte de incidentes cibernéticos, propendiendo así por la confiabilidad, continuidad y seguridad del sistema interconectado nacional.
12	Que el Comité de Ciberseguridad en la reunión 53 del 11 de noviembre de 2025 dio concepto técnico favorable a la expedición del presente Acuerdo.

ACUERDA:

1	Aprobar los siguientes documentos: 1. Procedimiento de Reporte de Incidentes Cibernéticos, como se presenta en el Anexo 1 de este Acuerdo, que hace parte integral del mismo. 2. Formato de Reporte de Incidentes Cibernéticos, como se presenta en el Anexo 2 de este Acuerdo, que hace parte integral del mismo. 3. Guía de suscripción al MISP (Malware Information Sharing Platform), como se presenta en el Anexo 3 de este Acuerdo, que hace parte integral del mismo. 4. Guía de Reporte de Incidentes Cibernéticos mediante correo electrónico seguro, como se presenta en el Anexo 4 de este Acuerdo, que hace parte integral del mismo. 5. Acuerdo de Confidencialidad, como se presenta en el Anexo 5 de este Acuerdo, que hace parte integral del mismo.
2	El presente Acuerdo rige a partir de la fecha de su expedición.

Presidente - German Caicedo

Secretario Técnico - Alberto Olarte Aguirre