

La CNMC aprueba las metodologías de evaluación de riesgos y clasificación de ciberataques en el sector eléctrico

Las metodologías de evaluación de riesgos de ciberseguridad y de clasificación de ciberataques establecen criterios comunes para identificar, analizar y evaluar los riesgos de ciberseguridad y clasificar los ciberataques según su gravedad e impacto. Estas metodologías se establecen en el marco del código de red europeo de ciberseguridad sobre flujos transfronterizos . (DCOOR/DE/002/25).

Esta normativa europea establece requisitos específicos destinados a reforzar la ciberseguridad del sistema eléctrico y la cooperación entre los Estados miembros frente a los riesgos por los ciberataques.

Propuesta europea

La Red Europea de Gestores de Redes de Transporte de Electricidad (ENTSO-E), en colaboración con la entidad europea de operadores de redes de distribución (DSO Entity), ha elaborado las propuestas de metodologías.

Estas propuestas han sido objeto de un proceso de consulta y cooperación entre las autoridades competentes de los Estados miembros. En el caso de España, la CNMC es la autoridad competente por defecto, ya que aún no se ha producido la designación de la autoridad conforme a lo previsto por el código de red.

Dos metodologías sobre ciberseguridad

Tras el proceso anterior en el ámbito europeo, la CNMC ha aprobado, en su rol de autoridad competente para la aplicación del código de red de ciberseguridad:

- La metodología de evaluación de riesgos, que proporciona la base para las evaluaciones de ciberseguridad a escala nacional, regional y de la Unión Europea previstas en el código de red, que permitirán identificar las amenazas existentes y valorar sus posibles consecuencias sobre la seguridad operativa del sistema eléctrico y los flujos transfronterizos de electricidad.
- La metodología de clasificación de ciberataques que permite evaluar de forma armonizada la gravedad de los ciberataques y determinar cuáles son objeto de notificación, mejorando así la coordinación entre los agentes y las autoridades competentes.

Entidades de impacto alto y crítico

La evaluación de riesgos a escala de la Unión Europea permitirá, entre otros, establecer los índices y umbrales que se usarán para identificar, entre las empresas que actúan en el sistema eléctrico español (tales como el operador del sistema, operador del mercado, transportista, distribuidoras, productores, comercializadores, agregadores, etc.), a aquellas que son consideradas como entidades de impacto alto y crítico en el ámbito del código de red.

Estas entidades serán designadas por las autoridades competentes y deberán cumplir, en los plazos y términos establecidos por el código de red, diferentes obligaciones en función de su clasificación. Entre otras, evaluar sus riesgos, aplicar controles y establecer un sistema de gestión de la ciberseguridad, así como cumplir obligaciones de intercambio de información y de preparación y gestión de crisis de ciberseguridad.

Las metodologías suponen un avance para la ciberseguridad del sistema eléctrico europeo, cada vez más digitalizado e interconectado, donde las amenazas pueden tener consecuencias transnacionales, y sientan las bases para mejorar la resiliencia del sistema, la seguridad del suministro, la prevención y la detección y respuesta ante los ciberataques.

1 Reglamento Delegado (UE) 2024/1366 de la Comisión, de 11 de marzo de 2024, por el que se completa el Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo mediante el establecimiento de un código de red sobre normas sectoriales específicas para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad.

Fuente: CNMC