2024/1366

24.5.2024

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

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de la electricidad ([1]), y en particular su artículo 59, apartado 2, letra e),

Considerando lo siguiente:

(1) La gestión de riesgos para la ciberseguridad es crucial para mantener la seguridad del suministro de electricidad y garantizar un alto nivel de ciberseguridad en el sector de la electricidad.

(2) La digitalización y la ciberseguridad son decisivas para prestar servicios esenciales y, por tanto, de importancia estratégica para las infraestructuras energéticas críticas.

(3) La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([2]) establece medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. El Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo ([3]) completa la Directiva (UE) 2022/2555 garantizando que los incidentes de ciberseguridad en el sector de la electricidad estén adecuadamente considerados como un riesgo y que las medidas adoptadas para abordarlos se reflejen adecuadamente en los planes de preparación frente a los riesgos. El Reglamento (UE) 2019/943 completa la Directiva (UE) 2022/2555 y el Reglamento (UE) 2019/941 estableciendo normas específicas para el sector de la electricidad a nivel de la Unión. Además, el presente Reglamento Delegado completa las disposiciones de la Directiva (UE) 2022/2555 relativas al sector de la electricidad, siempre que se trate de flujos transfronterizos de electricidad.

(4) En un contexto de sistemas eléctricos digitalizados e interconectados, la prevención y gestión de crisis de electricidad relacionadas con ciberataques no puede considerarse una tarea exclusivamente nacional. Deben desarrollarse medidas más eficientes y menos costosas a través de la cooperación regional y de la Unión para aprovechar todo su potencial. Por lo tanto, es necesario un marco común de normas y procedimientos mejor coordinados para garantizar que los Estados miembros y otros agentes puedan cooperar eficazmente a través de las fronteras, en un espíritu de mayor transparencia, confianza y solidaridad entre los Estados miembros y las autoridades competentes responsables de la electricidad y la ciberseguridad.

(5) La gestión de riesgos para la ciberseguridad dentro del ámbito de aplicación del presente Reglamento requiere un proceso estructurado que incluya, entre otras cosas, la determinación de los riesgos para los flujos transfronterizos de electricidad a raíz de ciberataques, los procesos operativos y los perímetros conexos, y los correspondientes controles y mecanismos de verificación de la ciberseguridad. Si bien el calendario de todo el proceso comprende varios años, cada etapa debe contribuir a un elevado nivel común de ciberseguridad en el sector y a la mitigación de los riesgos para la ciberseguridad. Todos los participantes en el proceso deben hacer todo lo posible por desarrollar y acordar las metodologías lo antes posible sin demora indebida y, en cualquier caso, a más tardar en los plazos definidos en el presente Reglamento.

([1]) DO L 158 de 14.6.2019, p. 54.

([2]) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).

([3]) Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE (DO L 158 de 14.6.2019, p. 1).

(6) Las evaluaciones de riesgos para la ciberseguridad a nivel de la Unión, de los Estados miembros, de las regiones y de las entidades contempladas en el presente Reglamento se limitarán a los resultantes de ciberataques, tal como se definen en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([4]); así pues, quedarán excluidos los ataques físicos, las catástrofes naturales y los cortes debidos a la pérdida de instalaciones o recursos humanos, por ejemplo. Los riesgos regionales y a escala de la Unión relacionados con ataques físicos o catástrofes naturales en el ámbito de la electricidad ya están cubiertos por otra legislación vigente de la Unión, incluidos el artículo 5 del Reglamento (UE) 2019/941 y el Reglamento (UE) 2017/1485 de la Comisión ([5]), por el que se establece una directriz sobre la gestión de la red de transporte de electricidad. Asimismo, la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo ([6]), relativa a la resiliencia de las entidades críticas, tiene por objeto reducir las vulnerabilidades y reforzar la resiliencia física de dichas entidades, y abarca todos los riesgos naturales y de origen humano pertinentes que pueden afectar a la prestación de servicios esenciales, incluidos los accidentes, las catástrofes naturales, las emergencias de salud pública como las pandemias y las amenazas híbridas u otras amenazas antagónicas, incluidos los delitos de terrorismo, la infiltración delictiva y el sabotaje.

(7) El concepto de «entidades de impacto alto y de impacto crítico» en el presente Reglamento es fundamental para definir el alcance de las entidades que estarán sujetas a las obligaciones descritas en él. El enfoque basado en el riesgo descrito en las distintas disposiciones pretende determinar los procesos, los activos de apoyo y las entidades que los explotan que afectan a los flujos transfronterizos de electricidad. Dependiendo del grado de impacto de los posibles ciberataques en sus operaciones de flujos eléctricos transfronterizos, pueden considerarse «de impacto alto» o «de impacto crítico». El artículo 3 de la Directiva (UE) 2022/2555 establece los conceptos de entidades esenciales e importantes y los criterios para determinar qué entidades pertenecen a esas categorías. Si bien muchas entidades se considerarán simultáneamente como «esenciales» en el sentido del artículo 3 de la Directiva (UE) 2022/2555 y «de impacto alto o de impacto crítico» con arreglo al artículo 24 del presente Reglamento, los criterios establecidos en este último se refieren únicamente al papel e impacto de las entidades en los procesos eléctricos que afectan a los flujos transfronterizos, sin tener en cuenta los criterios definidos en el artículo 3 de la Directiva (UE) 2022/2555.

(8) Las entidades incluidas en el ámbito de aplicación del presente Reglamento, consideradas de impacto alto o de impacto crítico con arreglo al artículo 24 del presente Reglamento y sujetas a las obligaciones en él establecidas, son principalmente las que tienen un impacto directo en los flujos transfronterizos de electricidad en la UE.

(9) El presente Reglamento hace uso de los mecanismos e instrumentos existentes, ya establecidos en otros actos legislativos, para garantizar la eficiencia y evitar duplicaciones en la consecución de los objetivos.

(10) Al aplicar el presente Reglamento, los Estados miembros, las autoridades pertinentes y los gestores de redes deben tener en cuenta las normas y especificaciones técnicas europeas acordadas de las organizaciones europeas de normalización y actuar en consonancia con la legislación de la Unión relativa a la introducción en el mercado o la puesta en servicio de productos cubiertos por dicha legislación de la Unión.

([4]) Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (DO L 333 de 27.12.2022, p. 1).

([5]) Reglamento (UE) 2017/1485 de la Comisión, de 2 de agosto de 2017, por el que se establece una directriz sobre la gestión de la red de transporte de electricidad (DO L 220 de 25.8.2017, p. 1).

([6]) Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164).

(11) Con vistas a mitigar los riesgos para la ciberseguridad, es necesario establecer un código normativo detallado que regule las acciones de las partes interesadas pertinentes y la cooperación entre ellas, cuyas actividades se refieran a los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad, a fin de garantizar la seguridad del sistema. Dichas normas organizativas y técnicas deben garantizar que la mayoría de los incidentes de electricidad cuyas causas raíz tengan que ver con la ciberseguridad se aborden eficazmente a nivel operativo. Es necesario establecer qué deben hacer las partes interesadas pertinentes para prevenir tales crisis y las medidas que pueden adoptar cuando las normas de gestión de la red no sean suficientes por sí solas. Por lo tanto, es necesario establecer un marco común de normas sobre cómo prevenir las crisis simultáneas de electricidad cuyas causas raíz tengan que ver con la ciberseguridad, cómo prepararse para ellas y cómo gestionarlas. De este modo se aumenta la transparencia en la fase de preparación y durante una crisis simultánea de electricidad y se garantiza que las medidas se adopten de manera coordinada y eficaz junto con las autoridades competentes en materia de ciberseguridad en los Estados miembros. Los Estados miembros y las entidades pertinentes deben estar obligados a cooperar, a nivel regional y, cuando proceda, bilateralmente, en un espíritu de solidaridad. Esta cooperación y estas normas tienen por objeto lograr una mejor preparación frente a los riesgos para la ciberseguridad a un coste menor, también en consonancia con los objetivos de la Directiva (UE) 2022/2555. También parece necesario reforzar el mercado interior de la electricidad aumentando la confianza en todos los Estados miembros, en particular mitigando el riesgo de reducciones indebidas de los flujos transfronterizos de electricidad, mermando así el riesgo de efectos colaterales negativos en los Estados miembros vecinos.

(12) La seguridad del suministro eléctrico implica la existencia de una cooperación efectiva entre Estados miembros, instituciones de la Unión, organismos, oficinas y agencias, y partes interesadas pertinentes. Los gestores de redes de distribución y los gestores de redes de transporte desempeñan un papel clave por lo que respecta a garantizar que la red eléctrica sea segura, fiable y eficiente de conformidad con los artículos 31 y 40 de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo ([7]). Las distintas autoridades reguladoras y otras autoridades nacionales competentes pertinentes también desempeñan un papel importante por lo que respecta a garantizar y supervisar la ciberseguridad en el suministro de electricidad, como parte de las tareas que les atribuyen las Directivas (UE) 2019/944 y (UE) 2022/2555. Los Estados miembros deben designar a una entidad existente o nueva como su autoridad nacional competente para ejecutar el presente Reglamento, a fin de garantizar la participación transparente e inclusiva de todos los agentes implicados, la preparación eficiente y la correcta ejecución del Reglamento, la cooperación entre las distintas partes interesadas pertinentes y las autoridades competentes en el ámbito de la electricidad y la ciberseguridad, y para facilitar la prevención y la evaluación *ex post* de las crisis de electricidad cuyas causas raíz tengan que ver con la ciberseguridad, así como los intercambios de información al respecto.

(13) Cuando una entidad de impacto alto o de impacto crítico preste servicios en más de un Estado miembro, o tenga su sede u otro establecimiento o un representante en un Estado miembro, pero sus redes y sistemas de información estén situados en otro u otros Estados miembros, dichos Estados miembros deben incitar a sus respectivas autoridades competentes a hacer todo lo posible por cooperar y ayudarse mutuamente según sea necesario.

(14) Los Estados miembros deben velar por que las autoridades competentes dispongan de las facultades necesarias, en relación con las entidades de impacto alto y de impacto crítico, para promover el cumplimiento del presente Reglamento. Dichas facultades deben permitir a las autoridades competentes llevar a cabo inspecciones *in situ* y supervisión a distancia. Esto puede comprender la realización de controles aleatorios, auditorías periódicas y auditorías de seguridad específicas basadas en evaluaciones del riesgo o en la información disponible relacionada con el riesgo, así como análisis de seguridad basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes, en los que se solicite la información necesaria para evaluar las medidas de ciberseguridad adoptadas por la entidad. Dicha información debe incluir políticas de ciberseguridad documentadas, el acceso a datos, documentos o cualquier información necesaria para el desempeño de sus funciones de supervisión, y pruebas de la ejecución de las políticas de ciberseguridad, como por ejemplo los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las correspondientes pruebas subyacentes.

([7]) Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre normas comunes para el mercado interior de la electricidad y por la que se modifica la Directiva 2012/27/UE (versión refundida) (DO L 158 de 14.6.2019, p. 125).

(15) A fin de evitar lagunas y duplicaciones entre las obligaciones de gestión de riesgos de ciberseguridad impuestas a las entidades de impacto alto y de impacto crítico, las autoridades nacionales contempladas en la Directiva (UE) 2022/2555 y las autoridades competentes con arreglo al presente Reglamento deben cooperar con respecto a la aplicación de las medidas para la gestión de riesgos para la ciberseguridad y la supervisión del cumplimiento de dichas medidas a nivel nacional. Las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 podrían considerar que el cumplimiento por parte de una entidad de los requisitos de gestión de riesgos para la ciberseguridad establecidos en el presente Reglamento garantiza el cumplimiento de los requisitos correspondientes establecidos en dicha Directiva, o viceversa.

(16) Un planteamiento común de la prevención y gestión de las crisis simultáneas de electricidad requiere de un entendimiento común entre los Estados miembros de lo que constituye una crisis simultánea de electricidad y el momento en que un ciberataque es un factor importante en estas crisis. En particular, debe facilitarse la coordinación entre los Estados miembros y las entidades pertinentes para hacer frente a las situaciones en las que exista un riesgo potencial, presente o inminente, de penuria significativa de electricidad o de imposibilidad de suministrar electricidad a los clientes, y ello se deba a un ciberataque.

(17) El considerando 1 del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([8]) reconoce el papel vital de las redes y los sistemas de información y las redes y servicios de comunicaciones electrónicas para sustentar el funcionamiento de la economía en sectores clave como la energía, mientras que el considerando 44 explica que la Agencia de la Unión Europea para la Ciberseguridad (ENISA) debe permanecer en contacto con la Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (ACER).

(18) El Reglamento (UE) 2019/943 asigna responsabilidades específicas con respecto a la ciberseguridad a los gestores de redes de transporte (GRT) y a los gestores de redes de distribución (GRD). Sus asociaciones europeas, a saber, la Red Europea de Gestores de Redes de Transporte de Electricidad («REGRT de Electricidad») y la entidad europea de los gestores de redes de distribución («entidad de los GRD de la UE»), con arreglo a los artículos 30 y 55 de dicho Reglamento, respectivamente, promoverán la ciberseguridad en cooperación con las autoridades y entidades reguladas pertinentes.

(19) Un planteamiento común para la prevención y la gestión de las crisis simultáneas de electricidad cuyas causas raíz tengan que ver con la ciberseguridad exige también que todas las partes interesadas pertinentes utilicen métodos y definiciones armonizados para determinar los riesgos relacionados con la ciberseguridad del suministro de electricidad. Asimismo, requiere estar en condiciones de comparar eficazmente su rendimiento y el de sus vecinos en ese ámbito. Por consiguiente, es necesario establecer los procesos y las funciones y responsabilidades para desarrollar y actualizar metodologías de gestión de riesgos, escalas de clasificación de incidentes y medidas de ciberseguridad adaptadas a los riesgos para la ciberseguridad que afectan a los flujos transfronterizos de electricidad.

(20) Los Estados miembros, a través de la autoridad competente designada para el presente Reglamento, son responsables de indicar las entidades que cumplen los criterios para considerarse entidades de impacto alto y de impacto crítico. A fin de eliminar las divergencias entre los Estados miembros en ese sentido y garantizar la seguridad jurídica para todas las entidades pertinentes en lo que se refiere a las medidas para la gestión de riesgos para la ciberseguridad y las obligaciones de notificación, debe establecerse un conjunto de criterios que determine las entidades que están incluidas en el ámbito de aplicación del presente Reglamento. Este conjunto de criterios debe definirse y actualizarse periódicamente mediante el proceso de elaboración y adopción de las condiciones y metodologías establecidas en el presente Reglamento.

(21) Las disposiciones del presente Reglamento deben entenderse sin perjuicio del Derecho de la Unión por el que se establecen normas específicas sobre la certificación de productos, servicios y procesos de tecnologías de la información y la comunicación (TIC), en particular sin perjuicio del Reglamento (UE) 2019/881 en lo que respecta al marco para el establecimiento de esquemas europeos de certificación de la ciberseguridad. En el contexto del presente Reglamento, los productos de TIC también deben incluir los dispositivos técnicos y programas informáticos que permiten la interacción directa con la red electrotécnica, en particular los sistemas de control industrial que pueden utilizarse para el transporte, la distribución y la producción de energía, así como para la recogida y transmisión de información conexa. Las disposiciones deben garantizar que los productos, servicios y procesos de TIC que se contraten cumplan los objetivos de seguridad pertinentes del artículo 51 del Reglamento (UE) 2019/881.

([8]) Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (DO L 151 de 7.6.2019, p. 15).

(22) Los recientes ciberataques muestran que las entidades son cada vez más el blanco de ataques a la cadena de suministro. Estos ataques a la cadena de suministro no solo afectan a las entidades individuales incluidas en su radio de alcance, sino que también pueden tener un efecto en cascada en ataques de mayor envergadura contra entidades a las que están conectadas en la red eléctrica. Por lo tanto, se han añadido disposiciones y recomendaciones para ayudar a mitigar los riesgos para la ciberseguridad asociados a los procesos relacionados con la cadena de suministro, en particular la contratación, con repercusiones en los flujos transfronterizos de electricidad.

(23) Dado que la explotación de las vulnerabilidades de las redes y los sistemas de información puede causar perturbaciones energéticas significativas y daños a la economía y los consumidores, estas vulnerabilidades deben detectarse y remediarse rápidamente para reducir los riesgos. A fin de facilitar la ejecución efectiva del presente Reglamento, las entidades pertinentes y las autoridades competentes deben cooperar para llevar a cabo y probar las actividades que se consideren adecuadas a tal fin, incluidos el intercambio de información sobre ciberamenazas, ciberataques, vulnerabilidades, herramientas y métodos, tácticas, técnicas y procedimientos, preparación para la gestión de crisis de ciberseguridad y otros ejercicios. Dado que la tecnología está en constante evolución y que la digitalización del sector de la electricidad avanza rápidamente, la aplicación de las disposiciones adoptadas no debe ir en detrimento de la innovación ni constituir un obstáculo para el acceso al mercado de la electricidad y el consiguiente uso de soluciones innovadoras que contribuyan a la eficiencia y la sostenibilidad del sistema eléctrico.

(24) La información recogida con vistas a la supervisión de la ejecución del presente Reglamento debe limitarse razonablemente según el principio de la necesidad de conocer. Debe concederse a las partes interesadas plazos viables y efectivos para la presentación de dicha información. Ha de evitarse la doble notificación.

(25) La protección de la ciberseguridad no se detiene en las fronteras de la Unión. Un sistema seguro requiere la participación de terceros países vecinos. La Unión y sus Estados miembros deben esforzarse por ayudar a los terceros países vecinos cuya infraestructura eléctrica esté conectada a la red europea a aplicar normas de ciberseguridad similares a las establecidas en el presente Reglamento.

(26) Con el fin de mejorar la coordinación de la seguridad en una fase temprana y de probar futuras condiciones y metodologías vinculantes, la REGRT de Electricidad, la entidad de los GRD de la UE y las autoridades competentes deben empezar a elaborar orientaciones no vinculantes inmediatamente después de la entrada en vigor del presente Reglamento. Estas orientaciones servirán de base para el desarrollo de las futuras condiciones y metodologías. Paralelamente, las autoridades competentes deben señalar entidades como candidatas a ser consideradas entidades de impacto alto y de impacto crítico para empezar, de forma voluntaria, a cumplir las obligaciones.

(27) El presente Reglamento ha sido elaborado en estrecha cooperación con la ACER, la ENISA, la REGRT de Electricidad, la entidad de los GRD de la UE y otras partes interesadas, con vistas a la adopción transparente y participativa de normas eficaces, equilibradas y proporcionadas.

(28) El presente Reglamento completa y mejora las medidas para la gestión de crisis establecidas en el Marco de respuesta a las crisis de ciberseguridad de la UE, tal como se establece en la Recomendación (UE) 2017/1584 de la Comisión ([9]). Un ciberataque también podría causar una crisis de electricidad, contribuir a su aparición o coincidir con una de estas crisis, tal como se definen en el artículo 2, punto 9, del Reglamento (UE) 2019/941, que afecte a los flujos transfronterizos de electricidad. Dicha crisis de electricidad podría dar lugar a una crisis simultánea de electricidad, tal como se define en el artículo 2, punto 10, del Reglamento (UE) 2019/941. Un incidente de este tipo también podría repercutir en otros sectores dependientes de la seguridad del suministro de electricidad. En caso de que pasara a ser un incidente de ciberseguridad a gran escala a efectos del artículo 16 de la Directiva (UE) 2022/2555, deben aplicarse las disposiciones de dicho artículo por las que se establece la red europea de organizaciones de enlace para las crisis de ciberseguridad («EU-CyCLONe»). De cara a la gestión de crisis a nivel de la Unión, las partes pertinentes deben recurrir al Dispositivo de la UE de Respuesta Política Integrada a las Crisis («Dispositivo RPIC») con arreglo a la Decisión de Ejecución (UE) 2018/1993 del Consejo ([10]).

(29) El presente Reglamento se entiende sin perjuicio de la competencia de los Estados miembros para adoptar las medidas necesarias para garantizar la protección de los intereses esenciales de su seguridad, preservar el orden y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales, con arreglo al Derecho de la Unión. De conformidad con el artículo 346 del TFUE, ningún Estado miembro debe estar obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad.

([9]) Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36).

([10]) Decisión de Ejecución (UE) 2018/1993 del Consejo, de 11 de diciembre de 2018, sobre el dispositivo de la UE de respuesta política integrada a las crisis (DO L 320 de 17.12.2018, p. 28).

(30) Aunque el presente Reglamento se aplica, en principio, a las entidades que realizan actividades de producción de electricidad en centrales nucleares, algunas de esas actividades pueden tener vinculación con la seguridad nacional.

(31) El Derecho de la Unión en materia de protección de datos y de la intimidad debe aplicarse a todo tratamiento de datos personales realizado con arreglo al presente Reglamento. En particular, el presente Reglamento se entiende sin perjuicio del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([11]), de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([12]) y del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([13]). Por consiguiente, el presente Reglamento no debe afectar, en particular, a los cometidos y competencias de las autoridades competentes para supervisar el cumplimiento del Derecho de la Unión en materia de protección de datos y de la intimidad aplicables.

(32) Dada la importancia de la cooperación internacional en materia de ciberseguridad, las autoridades competentes responsables de llevar a cabo las tareas que les encomienda el presente Reglamento y que hayan sido designadas por los Estados miembros deben poder participar en las redes de cooperación internacional. Por consiguiente, a efectos del desempeño de sus funciones, las autoridades competentes deben poder intercambiar información, incluidos datos personales, con las autoridades competentes de terceros países, siempre que se cumplan las condiciones establecidas en la legislación de la Unión en materia de protección de datos para las transferencias de datos personales a terceros países, entre otras las del artículo 49 del Reglamento (UE) 2016/679.

(33) El tratamiento de datos personales, en la medida en que sea necesario y proporcionado para garantizar la seguridad de los activos por parte de las entidades de impacto alto o de las entidades de impacto crítico, podría considerarse lícito sobre la base de que dicho tratamiento cumple una obligación jurídica a la que está sujeto el responsable del tratamiento, de conformidad con los requisitos del artículo 6, apartado 1, letra c), y del artículo 6, apartado 3, del Reglamento (UE) 2016/679. El tratamiento de datos personales también podría ser necesario para la satisfacción de intereses legítimos perseguidos por entidades de impacto alto o de impacto crítico, así como por proveedores de tecnologías y servicios de seguridad que actúen en nombre de dichas entidades, de conformidad con el artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, incluso cuando dicho tratamiento sea necesario para los mecanismos de puesta en común de información sobre ciberseguridad o la notificación voluntaria de información pertinente de conformidad con el presente Reglamento. Las medidas relacionadas con la prevención, la detección, la identificación, la contención y el análisis de ciberataques y la respuesta ante estos, las medidas para incrementar el conocimiento relacionado con ciberamenazas específicas, el intercambio de información en el contexto de la corrección y divulgación coordinada de las vulnerabilidades, el intercambio voluntario de información sobre dichos ciberataques, así como ciberamenazas y vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración pueden requerir el tratamiento de determinadas categorías de datos personales, como direcciones IP, localizadores uniformes de recursos (URL), nombres de dominio, direcciones de correo electrónico y, si revelan datos personales, sellos de tiempo. El tratamiento de datos personales por parte de las autoridades competentes, los puntos de contacto únicos y los CSIRT podría constituir una obligación legal o considerarse necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento de los datos de conformidad con el artículo 6, apartado 1, letras c) o e), y el artículo 6, apartado 3, del Reglamento (UE) 2016/679, o para perseguir un interés legítimo de entidades de impacto alto o de impacto crítico a que se refiere el artículo 6, apartado 1, letra f), de dicho Reglamento. Además, el Derecho nacional podría establecer normas que permitan a las autoridades competentes, los puntos de contacto únicos y los CSIRT, en la medida en que sea necesario y proporcionado a efectos de garantizar la seguridad de los sistemas de redes y de información de las entidades de impacto alto o de impacto crítico, tratar categorías especiales de datos personales de conformidad con el artículo 9 del Reglamento (UE) 2016/679, en particular estableciendo medidas adecuadas y específicas para salvaguardar los derechos e intereses fundamentales de las personas físicas, incluidas limitaciones técnicas a la reutilización de dichos datos y el uso de medidas de última generación en materia de seguridad y protección de la intimidad, como la seudonimización o el cifrado cuando la anonimización pueda afectar significativamente al objetivo perseguido.

([11]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

([12]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([13]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

(34) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de ciberataques. En este contexto, las autoridades competentes deben cooperar e intercambiar información sobre todas las cuestiones pertinentes con las autoridades a que se refieren el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE.

(35) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725, emitió su dictamen el 17 de noviembre de 2023.

HA ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

El presente Reglamento establece un código de red que fija normas sectoriales específicas para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad, incluidas normas sobre los requisitos mínimos comunes, la planificación, la supervisión, la información y la gestión de crisis.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplica a los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad en el marco de las actividades de las siguientes entidades, si se consideran como entidades de impacto alto o de impacto crítico de conformidad con el artículo 24:

a) las empresas eléctricas, tal y como se definen en el artículo 2, punto 57, de la Directiva (UE) 2019/944;

b) los operadores designados para el mercado eléctrico o NEMO, según se definen en el artículo 2, punto 8, del Reglamento (UE) 2019/943;

c) los mercados organizados, según se definen en el artículo 2, punto 4, del Reglamento de Ejecución (UE) n.º 1348/2014 de la Comisión ([14]), que gestionen operaciones sobre productos pertinentes para los flujos transfronterizos de electricidad;

d) los proveedores de servicios de TIC críticos contemplados en el artículo 3, punto 9, del presente Reglamento;

e) la REGRT de Electricidad, creada en virtud del artículo 28 del Reglamento (UE) 2019/943;

f) la entidad de los GRD de la UE, creada en virtud del artículo 52 del Reglamento (UE) 2019/943;

g) los sujetos de liquidación responsables del balance, según se definen en el artículo 2, punto 14, del Reglamento (UE) 2019/943;

h) los operadores de puntos de recarga, según se definen en el anexo I de la Directiva (UE) 2022/2555;

i) los centros de coordinación regionales creados de conformidad con el artículo 35 del Reglamento (UE) 2019/943;

j) los proveedores de servicios de seguridad gestionados, según se definen en el artículo 6, punto 40, de la Directiva (UE) 2022/2555;

k) cualquier otra entidad o tercero en que se hayan delegado responsabilidades o que tenga responsabilidades asignadas con arreglo al presente Reglamento.

2. Las siguientes autoridades son responsables, en el marco de sus mandatos actuales, de llevar a cabo las tareas asignadas por el presente Reglamento:

a) la Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (ACER), creada por el Reglamento (UE) 2019/942 del Parlamento Europeo y del Consejo ([15]);

b) las autoridades nacionales competentes responsables de llevar a cabo las tareas que les hayan sido asignadas con arreglo al presente Reglamento y designadas por los Estados miembros con arreglo al artículo 4, o «autoridades competentes»;

c) las autoridades reguladoras nacionales designadas por cada Estado miembro de conformidad con el artículo 57, apartado 1, de la Directiva (UE) 2019/944;

([14]) Reglamento de Ejecución (UE) n.º 1348/2014 de la Comisión, de 17 de diciembre de 2014, relativo a la comunicación de datos en virtud del artículo 8, apartados 2 y 6, del Reglamento (UE) n.º 1227/2011 del Parlamento Europeo y del Consejo sobre la integridad y la transparencia del mercado mayorista de la energía (DO L 363 de 18.12.2014, p. 121).

([15]) Reglamento (UE) 2019/942 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, por el que se crea la Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (Texto (DO L 158 de 14.6.2019, p. 22).

d) las autoridades competentes en materia de preparación frente a los riesgos establecidas de conformidad con el artículo 3 del Reglamento (UE) 2019/941;

e) los equipos de respuesta a incidentes de seguridad informática («CSIRT») designados o establecidos de conformidad con el artículo 10 de la Directiva (UE) 2022/2555;

f) las autoridades competentes encargadas de la ciberseguridad designadas o establecidas de conformidad con el artículo 8 de la Directiva (UE) 2022/2555;

g) la Agencia de la Unión Europea para la Ciberseguridad, creada en virtud del Reglamento (UE) 2019/881;

h) cualquier otra autoridad o tercero en que se hayan delegado responsabilidades o que tenga responsabilidades asignadas con arreglo al artículo 4, apartado 3.

3. El presente Reglamento se aplicará también a todas las entidades que no estén establecidas en la Unión pero presten servicios a entidades de la Unión, siempre que hayan sido consideradas como entidades de impacto alto o de impacto crítico por las autoridades competentes de conformidad con el artículo 24, apartado 2.

4. El presente Reglamento se entenderá sin perjuicio de las responsabilidades de los Estados miembros de salvaguardar la seguridad nacional y de sus competencias para salvaguardar otras funciones esenciales del Estado, como garantizar la integridad territorial del Estado o mantener el orden público.

5. El presente Reglamento se entenderá sin perjuicio de la responsabilidad de los Estados miembros de salvaguardar la seguridad nacional con respecto a las actividades de producción de electricidad a partir de centrales nucleares, incluidas las actividades dentro de la cadena de valor nuclear, de conformidad con los Tratados.

6. Las entidades, las autoridades competentes, los puntos de contacto únicos a nivel de entidad y los CSIRT tratarán los datos personales en la medida necesaria para los fines del presente Reglamento y de conformidad con el Reglamento (UE) 2016/679; en particular, dicho tratamiento se basará en su artículo 6.

Artículo 3

Definiciones

Se entenderá por:

1) «activo»: toda información, programa o equipo informático de las redes y los sistemas de información, ya sea tangible o intangible, que tenga valor para una persona, una organización o una administración;

2) «autoridad competente en materia de preparación frente a los riesgos»: autoridad competente designada con arreglo al artículo 3 del Reglamento (UE) 2019/941;

3) «equipo de respuesta a incidentes de seguridad informática»: equipo responsable de la gestión de riesgos e incidentes de conformidad con el artículo 10 de la Directiva (UE) 2022/2555;

4) «activo de impacto crítico»: un activo necesario para llevar a cabo un proceso de impacto crítico;

5) «entidad de impacto crítico»: una entidad que lleva a cabo un proceso de impacto crítico y que ha sido designada como tal por las autoridades competentes de conformidad con el artículo 24;

6) «perímetro del impacto crítico»: un perímetro definido por una entidad contemplada en el artículo 2, apartado 1, que contiene todos los activos de impacto crítico y en el que puede controlarse el acceso a dichos activos, y que define el ámbito en que se aplican los controles avanzados de ciberseguridad;

7) «proceso de impacto crítico»: proceso de negocio llevado a cabo por una entidad cuyos índices de impacto en la ciberseguridad de la electricidad superan el umbral del impacto crítico;

8) «umbral del impacto crítico»: los valores de los índices de impacto en la ciberseguridad de la electricidad a que se refiere el artículo 19, apartado 3, letra b), por encima de los cuales un ciberataque a un proceso de negocio causará una perturbación crítica de los flujos transfronterizos de electricidad;

9) «proveedor de servicios de TIC críticos»: una entidad que presta un servicio de TIC o un proceso de TIC que es necesario para un proceso de impacto crítico o de impacto alto que afecte a los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad y que, si se ve comprometido, puede causar un ciberataque con un impacto que supere el umbral del impacto crítico o del impacto alto;

10) «flujo transfronterizo de electricidad»: un flujo transfronterizo según se define en el artículo 2, punto 3, del Reglamento (UE) 2019/943;

11) «ciberataque»: un incidente según se define en el artículo 3, punto 14, del Reglamento (UE) 2022/2554;

12) «ciberseguridad»: la ciberseguridad según se define en el artículo 2, punto 1, del Reglamento (UE) 2019/881;

13) «control de la ciberseguridad»: las acciones o procedimientos llevados a cabo con el fin de evitar, detectar, contrarrestar o minimizar los riesgos para la ciberseguridad;

14) «incidente de ciberseguridad»: un incidente según se define en el artículo 6, punto 6, de la Directiva (UE) 2022/2555;

15) «sistema de gestión de la ciberseguridad»: las políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una entidad, con el fin de proteger sus activos de información frente a las ciberamenazas, que establecen, aplican, gestionan, supervisan, revisan, mantienen y mejoran sistemáticamente la seguridad de las redes y los sistemas de información de una organización;

16) «centro operativo de ciberseguridad»: centro específico en el que un equipo técnico compuesto por uno o más expertos, con el apoyo de sistemas informáticos de ciberseguridad, realiza tareas relacionadas con la seguridad (servicios de centro operativo de ciberseguridad), como la gestión de ciberataques y errores de la configuración de seguridad, la supervisión de la seguridad, el análisis de registros y la detección de ciberataques;

17) «ciberamenaza»: una ciberamenaza según se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881;

18) «gestión de las vulnerabilidades de ciberseguridad»: la práctica de detectar y abordar las vulnerabilidades;

19) «entidad»: una entidad según se define en el artículo 6, punto 38, de la Directiva (UE) 2022/2555;

20) «alerta temprana»: la información necesaria para indicar si se sospecha que el incidente significativo tiene su causa en actos ilícitos o malintencionados o puede tener un impacto transfronterizo;

21) «índice de impacto en la ciberseguridad de la electricidad» («ECII», por sus siglas en inglés): índice o escala de clasificación que establece una jerarquía de las posibles consecuencias de los ciberataques a procesos de negocio que intervienen en los flujos transfronterizos de electricidad;

22) «esquema europeo de certificación de la ciberseguridad»: un esquema según se define en el artículo 2, punto 9, del Reglamento (UE) 2019/881;

23) «entidad de impacto alto»: una entidad que lleva a cabo un proceso de impacto alto y que ha sido designada como tal por las autoridades competentes de conformidad con el artículo 24;

24) «proceso de impacto alto»: todo proceso de negocio llevado a cabo por una entidad cuyos índices de impacto en la ciberseguridad de la electricidad superen el umbral del impacto alto;

25) «activo de impacto alto»: un activo necesario para llevar a cabo un proceso de impacto alto;

26) «umbral del impacto alto»: los valores de los índices de impacto en la ciberseguridad de la electricidad a que se refiere el artículo 19, apartado 3, letra b), por encima de los cuales un ciberataque con éxito dirigido a un proceso causará un nivel alto de perturbación de los flujos transfronterizos de electricidad;

27) «perímetro del impacto alto»: un perímetro definido por cualquier entidad contemplada en el artículo 2, apartado 1, que contiene todos los activos de impacto alto y en el que puede controlarse el acceso a dichos activos, y que define el ámbito en que se aplican los controles mínimos de ciberseguridad;

28) «producto de TIC»: un producto de TIC según se define en el artículo 2, punto 12, del Reglamento (UE) 2019/881;

29) «servicio de TIC»: un servicio de TIC según se define en el artículo 2, punto 13, del Reglamento (UE) 2019/881;

30) «proceso de TIC»: un proceso de TIC según se define en el artículo 2, punto 14, del Reglamento (UE) 2019/881;

31) «sistema heredado»: un sistema de TIC heredado según se define en el artículo 3, punto 3, del Reglamento (UE) 2022/2554;

32) «punto de contacto único nacional»: el punto de contacto único designado o establecido por cada Estado miembro de conformidad con el artículo 8, apartado 3, de la Directiva (UE) 2022/2555;

33) «autoridades de gestión de crisis de ciberseguridad en el ámbito de los SRI»: las autoridades designadas o establecidas de conformidad con el artículo 9, apartado 1, de la Directiva (UE) 2022/2555;

34) «originador»: una entidad que inicia una acción de intercambio, puesta en común o almacenamiento de información;

35) «especificaciones de contratación»: las especificaciones que definen las entidades para la contratación de productos, procesos o servicios de TIC nuevos o actualizados;

36) «representante»: una persona física o jurídica establecida en la Unión designada expresamente para actuar en nombre de una entidad de impacto alto o de impacto crítico no establecida en la Unión, pero que presta servicios a entidades de la Unión y a la que puede dirigirse una autoridad competente o un CSIRT en vez de a la propia entidad de impacto alto o de impacto crítico en relación con las obligaciones de dicha entidad en virtud del presente Reglamento;

37) «riesgo»: un riesgo según se define en el artículo 6, punto 9, de la Directiva (UE) 2022/2555;

38) «matriz de impacto del riesgo»: matriz utilizada durante la evaluación de riesgos para determinar el nivel de impacto resultante de cada riesgo evaluado;

39) «crisis simultánea de electricidad»: una crisis de electricidad según se define en el artículo 2, punto 10, del Reglamento (UE) 2019/941;

40) «punto de contacto único a nivel de entidad»: punto de contacto único a nivel de entidad designado con arreglo al artículo 38, apartado 1, letra c);

41) «parte interesada»: cualquier parte que tenga interés en el éxito y funcionamiento continuo de una organización o proceso, como empleados, directores, accionistas, reguladores, asociaciones, proveedores y clientes;

42) «norma»: una norma según se define en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([16]);

43) «región de operación del sistema»: las regiones de operación del sistema definidas en el anexo I de la Decisión 05-2022 de la ACER, relativa a la definición de regiones de operación del sistema, establecidas de conformidad con el artículo 36 del Reglamento (UE) 2019/943;

44) «gestores de red»: los gestores de redes de distribución (GRD) y los gestores de redes de transporte (GRT) según se definen en el artículo 2, puntos 29 y 35, de la Directiva (UE) 2019/944;

45) «proceso de impacto crítico a escala de la Unión»: todo proceso del sector de la electricidad, en el que posiblemente participen múltiples entidades, respecto del cual pueda considerarse que el posible impacto de un ciberataque es crítico durante la realización de la evaluación de riesgos para la ciberseguridad a escala de la Unión;

46) «proceso de impacto alto a escala de la Unión»: todo proceso del sector de la electricidad, en el que posiblemente participen múltiples entidades, respecto del cual pueda considerarse que el posible impacto de un ciberataque es alto durante la realización de la evaluación de riesgos para la ciberseguridad a escala de la Unión;

47) «vulnerabilidad aprovechada activamente no subsanada»: vulnerabilidad que aún no se ha divulgado públicamente ni se ha subsanado respecto de la cual existen pruebas fiables de la ejecución de un código malicioso en un sistema por parte de un agente sin autorización del propietario del sistema;

48) «vulnerabilidad»: una vulnerabilidad según se define en el artículo 6, punto 15, de la Directiva (UE) 2022/2555.

Artículo 4

Autoridad competente

1. Lo antes posible y, en cualquier caso, a más tardar el 13 de diciembre de 2024, cada Estado miembro designará una autoridad nacional gubernamental o reguladora responsable de llevar a cabo las tareas que le asigna el presente Reglamento («autoridad competente»). Hasta que se haya encomendado a la autoridad competente que lleve a cabo las tareas contempladas en el presente Reglamento, la autoridad reguladora designada por cada Estado miembro con arreglo al artículo 57, apartado 1, de la Directiva (UE) 2019/944 llevará a cabo las tareas de la autoridad competente de conformidad con el presente Reglamento.

2. Los Estados miembros notificarán sin demora a la Comisión, a la ACER, a la ENISA, al Grupo de Cooperación SRI, creado en virtud del artículo 14 de la Directiva (UE) 2022/2555, y al Grupo de Coordinación de la Electricidad, creado en virtud del artículo 1 de la Decisión de la Comisión de 15 de noviembre de 2012 ([17]), y les comunicarán el nombre y los datos de contacto de su autoridad competente designada con arreglo al apartado 1 del presente artículo, así como cualquier modificación posterior de esta información.

([16]) Reglamento (UE) n ° 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

([17]) Decisión de la Comisión, de 15 de noviembre de 2012, por la que se crea el Grupo de Coordinación de la Electricidad (2012/C 353/02) (DO C 353 de 17.11.2012, p. 2).

3. Los Estados miembros podrán autorizar a su autoridad competente a delegar en otras autoridades nacionales las tareas asignadas por el presente Reglamento, con excepción de las tareas contempladas en el artículo 5. Cada autoridad competente supervisará la aplicación del presente Reglamento por parte de las autoridades en las que haya delegado tareas. La autoridad competente comunicará a la Comisión, a la ACER, al Grupo de Coordinación de la Electricidad, a la ENISA y al Grupo de Cooperación SRI el nombre de las autoridades en las que se haya delegado una tarea, sus datos de contacto y las tareas asignadas, así como cualquier modificación posterior de esta información.

Artículo 5

Cooperación entre las autoridades y organismos pertinentes a nivel nacional

Las autoridades competentes coordinarán y garantizarán una cooperación adecuada entre las autoridades competentes encargadas de la ciberseguridad, las autoridades de gestión de crisis de ciberseguridad, las autoridades reguladoras nacionales, las autoridades competentes en materia de preparación frente a los riesgos y los CSIRT a efectos del cumplimiento de las obligaciones pertinentes establecidas en el presente Reglamento. Las autoridades competentes también se coordinarán con cualquier otro organismo o autoridad según determine cada Estado miembro para garantizar la eficacia de los procedimientos y evitar la duplicación de tareas y obligaciones. Las autoridades competentes podrán exigir a las respectivas autoridades reguladoras nacionales que soliciten un dictamen a la ACER de conformidad con el artículo 8, apartado 3.

Artículo 6

Condiciones o metodologías, o planes

1. Los GRT elaborarán, en cooperación con la entidad de los GRD de la UE, propuestas de condiciones o metodologías con arreglo al apartado 2, o de planes con arreglo al apartado 3.

2. Las siguientes condiciones o metodologías y sus modificaciones deberán ser aprobadas por todas las autoridades competentes:

a) las metodologías de evaluación de riesgos para la ciberseguridad, de conformidad con el artículo 18, apartado 1;

b) el informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad, de conformidad con el artículo 23;

c) los controles mínimos y avanzados de ciberseguridad, de conformidad con el artículo 29; la cartografía de los controles de ciberseguridad de la electricidad con respecto a las normas, de conformidad con el artículo 34, incluidos los controles mínimos y avanzados de ciberseguridad en la cadena de suministro, de conformidad con el artículo 33;

d) una recomendación sobre contratación en materia de ciberseguridad, de conformidad con el artículo 35;

e) la metodología de la escala de clasificación de los ciberataques, de conformidad con el artículo 37, apartado 8.

3. Las propuestas de planes regionales de mitigación de riesgos para la ciberseguridad con arreglo al artículo 22 estarán sujetas a la aprobación de todas las autoridades competentes de la región de operación del sistema de que se trate.

4. Las propuestas de condiciones o metodologías a que se refiere el apartado 2, o las propuestas de planes a que se refiere el apartado 3, incluirán un calendario propuesto para su aplicación, así como una descripción de su impacto previsto en los objetivos del presente Reglamento.

5. La entidad de los GRD de la UE podrá presentar un dictamen motivado a los GRT correspondientes hasta tres semanas antes de la fecha límite para presentar la propuesta de condiciones o metodologías, o de planes, a las autoridades competentes. Los GRT responsables de la propuesta de condiciones o metodologías, o de planes, tendrán en cuenta el dictamen motivado de la entidad de los GRD de la UE antes de presentarla para la aprobación de las autoridades competentes. Los GRT razonarán los casos en que no tengan en cuenta la opinión de la entidad de los GRD de la UE.

6. Cuando elaboren conjuntamente condiciones y metodologías, y también planes, los GRT participantes cooperarán estrechamente. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, informarán periódicamente a las autoridades competentes y a la ACER sobre los avances en el desarrollo de las condiciones o metodologías, o de los planes.

Artículo 7

Normas de votación en los GRT

1. Si los GRT que decidan sobre las propuestas de condiciones o metodologías no consiguen llegar a un acuerdo, tomarán una decisión por mayoría cualificada. La mayoría cualificada para dichas propuestas se calculará sobre la base de:

a) los GRT que representen al menos el 55 % de los Estados miembros, y

b) los GRT que representen a Estados miembros que reúnan como mínimo el 65 % de la población de la Unión.

2. La minoría de bloqueo para las decisiones sobre las propuestas de condiciones o metodologías a que se refiere el artículo 6, apartado 2, incluirá GRT que representen, por lo menos, a cuatro Estados miembros; de lo contrario, se considerará alcanzada la mayoría cualificada.

3. Si los GRT de una región de operación del sistema que decidan sobre las propuestas de planes a que se refiere el artículo 6, apartado 2, no consiguen llegar a un acuerdo y si la región de operación del sistema en cuestión abarca más de cinco Estados miembros, los GRT tomarán una decisión por mayoría cualificada. La mayoría cualificada para la adopción de las propuestas a que se refiere el artículo 6, apartado 2, será una mayoría en la que:

a) los GRT representen al menos el 72 % de los Estados miembros interesados, y

b) los GRT representen a Estados miembros que reúnan como mínimo el 65 % de la población de la zona de que se trate.

4. La minoría de bloqueo para las decisiones sobre propuestas de planes incluirá, por lo menos, un número mínimo de GRT que representen a más del 35 % de la población de los Estados miembros participantes, más GRT que representen al menos a un Estado miembro interesado adicional; de lo contrario, se considerará alcanzada la mayoría cualificada.

5. Para las decisiones de los GRT sobre las propuestas de condiciones o metodologías con arreglo al artículo 6, apartado 2, se asignará un voto a cada Estado miembro. Si en el territorio de un Estado miembro hay más de un GRT, el Estado miembro deberá repartir los derechos de voto entre los GRT.

6. Si los GRT, en cooperación con la entidad de los GRD de la UE, no presentan una propuesta inicial o modificada de condiciones o metodologías, o de planes, a las autoridades competentes pertinentes en los plazos establecidos en el presente Reglamento, facilitarán a las autoridades competentes pertinentes y a la ACER los proyectos pertinentes de las condiciones o metodologías, o de los planes. Explicarán los motivos que hayan impedido un acuerdo. Las autoridades competentes tomarán conjuntamente las medidas adecuadas para la adopción de las condiciones o metodologías necesarias, o de los planes necesarios. Esto podrá hacerse, por ejemplo, solicitando modificaciones de los proyectos con arreglo al presente apartado, revisando y completando dichos proyectos o, si no se han presentado proyectos, definiendo y aprobando las condiciones o metodologías necesarias, o los planes necesarios.

Artículo 8

Presentación de propuestas a las autoridades competentes

1. Los GRT presentarán las propuestas de condiciones o metodologías, o de planes, a las autoridades competentes pertinentes para su aprobación en los plazos respectivos establecidos en los artículos 18, 23, 29, 33, 34, 35 y 37. Las autoridades competentes podrán prorrogar conjuntamente estos plazos en circunstancias excepcionales, en particular en los casos en que no pueda respetarse un plazo debido a circunstancias externas a la responsabilidad de los GRT o de la entidad de los GRD de la UE.

2. Las propuestas de condiciones o metodologías, o de planes, con arreglo al apartado 1, se presentarán a la ACER a efectos de información al mismo tiempo que se presenten a las autoridades competentes.

3. Previa solicitud conjunta de las autoridades reguladoras nacionales, la ACER emitirá un dictamen sobre la propuesta de condiciones o metodologías, o de planes, en un plazo de seis meses a partir de la recepción de las propuestas de condiciones o metodologías, o de planes, y notificará el dictamen a las autoridades reguladoras nacionales y a las autoridades competentes. Las autoridades reguladoras nacionales, las autoridades competentes encargadas de la ciberseguridad y cualquier otra autoridad designada como autoridad competente se coordinarán entre sí antes de que las autoridades reguladoras nacionales soliciten un dictamen a la ACER. La ACER podrá incluir recomendaciones en dicho dictamen. La ACER consultará a la ENISA antes de emitir un dictamen sobre las propuestas a que se refiere el artículo 6, apartado 2.

4. Las autoridades competentes se consultarán y cooperarán estrechamente, y se coordinarán entre sí para llegar a un acuerdo sobre las condiciones o metodologías propuestas, o los planes propuestos. Antes de aprobar las condiciones o metodologías, o los planes, revisarán y completarán las propuestas cuando sea necesario, previa consulta a la REGRT de Electricidad y a la entidad de los GRD de la UE, a fin de garantizar que las propuestas estén en consonancia con el presente Reglamento y contribuyan a un elevado nivel común de ciberseguridad en toda la Unión.

5. Las autoridades competentes decidirán sobre las condiciones o metodologías, o los planes, en un plazo de seis meses a partir de la fecha en que la autoridad competente pertinente o, en su caso, la última autoridad competente pertinente de que se trate, reciba las condiciones o metodologías, o los planes.

6. Si la ACER emite un dictamen, las autoridades competentes pertinentes lo tendrán en cuenta y tomarán sus decisiones en un plazo de seis meses a partir de la recepción del dictamen de la ACER.

7. Si las autoridades competentes exigen conjuntamente una modificación de las condiciones o metodologías propuestas, o de los planes propuestos, para su aprobación, los GRT elaborarán, en cooperación con la entidad de los GRD de la UE, una propuesta de dicha modificación de las condiciones o metodologías, o de los planes. Los GRT presentarán la propuesta modificada para su aprobación en un plazo de dos meses a partir de la solicitud de las autoridades competentes. Las autoridades competentes decidirán sobre las condiciones o metodologías modificadas, o sobre los planes modificados, en un plazo de dos meses a partir de su presentación.

8. Si las autoridades competentes no han conseguido alcanzar un acuerdo en el plazo mencionado en los apartados 5 o 7, informarán de ello a la Comisión. La Comisión podrá tomar las medidas adecuadas para hacer posible la adopción de las condiciones o metodologías necesarias, o de los planes necesarios.

9. Los GRT, con la asistencia de la REGRT de Electricidad, y la entidad de los GRD de la UE publicarán las condiciones o metodologías, o los planes, en sus sitios web tras la aprobación de las autoridades competentes pertinentes, salvo cuando dicha información se considere confidencial de conformidad con el artículo 47.

10. Las autoridades competentes podrán solicitar conjuntamente a los GRT y a la entidad de los GRD de la UE propuestas de modificación de las condiciones o metodologías aprobadas, o de los planes aprobados, y fijar un plazo para la presentación de dichas propuestas. Los GRT, en cooperación con la entidad de los GRD de la UE, podrán proponer modificaciones a las autoridades competentes también por iniciativa propia. Las propuestas de modificación de las condiciones o metodologías, o de los planes, se elaborarán y aprobarán de conformidad con el procedimiento establecido en el presente artículo.

11. Al menos cada tres años después de la primera adopción de las condiciones o metodologías respectivas, o de los planes adoptados respectivos, los GRT, en cooperación con la entidad de los GRD de la UE, revisarán la eficacia de las condiciones o metodologías adoptadas, o de los planes adoptados, e informarán de las conclusiones de la revisión a las autoridades competentes y a la ACER sin demora indebida.

Artículo 9

Consulta

1. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, consultarán a las partes interesadas, incluidas la ACER, la ENISA y la autoridad competente de cada Estado miembro, sobre los proyectos de propuestas de condiciones o metodologías a que se refiere el artículo 6, apartado 2, y de los planes a que se refiere el artículo 6, apartado 3. La consulta tendrá una duración no inferior a un mes.

2. Las propuestas de condiciones o metodologías a que se refiere el artículo 6, apartado 2, presentadas por los GRT, en cooperación con la entidad de los GRD de la UE, se publicarán y se someterán a consulta a nivel de la Unión. Las propuestas de planes a que se refiere el artículo 6, apartado 3, presentadas a nivel regional por los GRT pertinentes, en cooperación con la entidad de los GRD de la UE, se someterán a consulta al menos a nivel regional.

3. Los GRT, con la asistencia de la REGRT de Electricidad, y la entidad de los GRD de la UE, responsables de la propuesta de condiciones o metodologías, o de planes, tendrán debidamente en cuenta los puntos de vista de las partes interesadas resultantes de las consultas realizadas de conformidad con el apartado 1, antes de su presentación para su aprobación reglamentaria. En todos los casos, deberá incluirse en la presentación una justificación bien razonada de la inclusión o la no inclusión de los puntos de vista resultantes de la consulta, y dicha justificación se publicará con antelación suficiente o al mismo tiempo que la propuesta de condiciones o metodologías.

Artículo 10

Participación de las partes interesadas

La ACER, en estrecha cooperación con la REGRT de Electricidad y la entidad de los GRD de la UE, organizará la participación de las partes interesadas, que implicará reuniones periódicas con las partes interesadas con vistas a detectar problemas y proponer mejoras relacionadas con la ejecución del presente Reglamento.

Artículo 11

Recuperación de costes

1. Los costes soportados por los GRT y los GRD sujetos a la regulación de las tarifas de red y derivados de las obligaciones establecidas en el presente Reglamento, incluidos los costes soportados por la REGRT de Electricidad y la entidad de los GRD de la UE, serán evaluados por la autoridad reguladora nacional pertinente de cada Estado miembro.

2. Los costes evaluados como razonables, eficientes y proporcionados se recuperarán mediante tarifas de red u otros mecanismos adecuados, según determine la autoridad reguladora nacional pertinente.

3. Si así lo solicitan las autoridades reguladoras nacionales pertinentes, los GRT y los GRD a que se refiere el apartado 1 proporcionarán, en un plazo razonable determinado por la autoridad reguladora nacional, la información necesaria para facilitar la evaluación de los costes incurridos.

Artículo 12

Supervisión

1. La ACER supervisará la ejecución del presente Reglamento de conformidad con el artículo 32, apartado 1, del Reglamento (UE) 2019/943 y el artículo 4, apartado 2, del Reglamento (UE) 2019/942. Al realizar esta supervisión, la ACER podrá cooperar con la ENISA y solicitar el apoyo de la REGRT de Electricidad y de la entidad de los GRD de la UE. La ACER informará periódicamente al Grupo de Coordinación de la Electricidad y al Grupo de Cooperación SRI sobre la ejecución del presente Reglamento.

2. La ACER publicará un informe al menos cada tres años después de la entrada en vigor del presente Reglamento a fin de:

a) revisar el estado de aplicación de las medidas de gestión de riesgos para la ciberseguridad aplicables en relación con las entidades de impacto alto y de impacto crítico;

b) determinar si pueden ser necesarias normas adicionales sobre los requisitos comunes, la planificación, la supervisión, la información y la gestión de crisis para prevenir riesgos para el sector de la electricidad, y

c) detectar ámbitos de mejora para la revisión del presente Reglamento, o determinar los ámbitos no cubiertos y las nuevas prioridades que puedan surgir debido a los avances tecnológicos.

3. A más tardar el 13 de junio de 2025, la ACER, en cooperación con la ENISA y previa consulta a la REGRT de Electricidad y a la entidad de los GRD de la UE, podrá publicar orientaciones sobre la información pertinente que deba comunicarse a la ACER a efectos de supervisión, así como sobre el proceso y la frecuencia de la recogida, sobre la base de los indicadores de rendimiento definidos de conformidad con el apartado 5.

4. Las autoridades competentes podrán tener acceso a la información pertinente en poder de la ACER que esta haya recogido de conformidad con el presente artículo.

5. La ACER, en cooperación con la ENISA y con el apoyo de la REGRT de Electricidad y la entidad de los GRD de la UE, emitirá indicadores de rendimiento no vinculantes para la evaluación de la fiabilidad operativa vinculados con los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad.

6. Las entidades contempladas en el artículo 2, apartado 1, del presente Reglamento presentarán a la ACER la información necesaria para que esta lleve a cabo las tareas mencionadas en el apartado 2.

Artículo 13

Análisis comparativo

1. A más tardar el 13 de junio de 2025, la ACER, en cooperación con la ENISA, establecerá una guía de análisis comparativo no vinculante en materia de ciberseguridad. La guía explicará a las autoridades reguladoras nacionales los principios de análisis comparativo de los controles de ciberseguridad aplicados con arreglo al apartado 2 del presente artículo, teniendo en cuenta los costes de aplicación de los controles y la eficacia de la función desempeñada por los procesos, productos, servicios, sistemas y soluciones utilizados para aplicar dichos controles. La ACER tendrá en cuenta los informes de análisis comparativo existentes al establecer la guía de análisis comparativo no vinculante en materia de ciberseguridad. La ACER presentará la guía de análisis comparativo no vinculante en materia de ciberseguridad a las autoridades reguladoras nacionales a efectos de información.

2. En un plazo de 12 meses a partir del establecimiento de la guía de análisis comparativo con arreglo al apartado 1, las autoridades reguladoras nacionales llevarán a cabo un análisis comparativo para evaluar si las inversiones actuales en ciberseguridad:

a) mitigan los riesgos que repercuten en los flujos transfronterizos de electricidad;

b) proporcionan los resultados deseados y generan mejoras de eficiencia para el desarrollo de los sistemas eléctricos;

c) son eficientes y están integradas en la contratación general de activos y servicios.

3. Para el análisis comparativo, las autoridades reguladoras nacionales podrán tener en cuenta la guía de análisis comparativo no vinculante en materia de ciberseguridad establecida por la ACER, y evaluarán en particular:

a) el gasto medio relacionado con la ciberseguridad para mitigar los riesgos que repercuten en los flujos transfronterizos de electricidad, especialmente con respecto a las entidades de impacto alto y de impacto crítico;

b) en cooperación con la REGRT de Electricidad y la entidad de los GRD de la UE, los precios medios de los servicios, sistemas y productos de ciberseguridad que contribuyen en gran medida a mejorar y mantener las medidas para la gestión de riesgos para la ciberseguridad en las diferentes regiones de operación del sistema;

c) la existencia y el nivel de comparabilidad de los costes y funciones de los servicios, sistemas y soluciones de ciberseguridad adecuados para la ejecución del presente Reglamento, determinando las posibles medidas necesarias para fomentar la eficiencia del gasto, en particular cuando puedan ser necesarias inversiones tecnológicas en ciberseguridad.

4. Toda información relacionada con el análisis comparativo se gestionará y tratará con arreglo a los requisitos de clasificación de datos del presente Reglamento, los controles mínimos de ciberseguridad y el informe sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad. El análisis comparativo a que se refieren los apartados 2 y 3 no se hará público.

5. Sin perjuicio de los requisitos de confidencialidad del artículo 47 y de la necesidad de proteger la seguridad de las entidades sujetas a las disposiciones del presente Reglamento, el análisis comparativo a que se refieren los apartados 2 y 3 del presente artículo se compartirá con todas las autoridades reguladoras nacionales, todas las autoridades competentes, la ACER, la ENISA y la Comisión.

Artículo 14

Acuerdos con GRT de fuera de la Unión

1. En un plazo de 18 meses a partir de la entrada en vigor del presente Reglamento, los GRT de una región de operación del sistema que sea vecina de un tercer país procurarán celebrar acuerdos con GRT del tercer país vecino que sean conformes con el Derecho pertinente de la Unión y que establezcan las bases para la cooperación en materia de protección de la ciberseguridad y los acuerdos de cooperación en materia de ciberseguridad con dichos GRT.

2. Los GRT informarán a la autoridad competente de los acuerdos celebrados con arreglo al apartado 1.

Artículo 15

Representantes legales

1. Las entidades que no tengan un establecimiento en la Unión, pero que presten servicios a entidades de la Unión y a las que se haya notificado su condición de entidades de impacto alto o de impacto crítico de conformidad con el artículo 24, apartado 6, designarán por escrito, en un plazo de tres meses a partir de la notificación, a un representante en la Unión e informarán de ello a la autoridad competente notificante.

2. Se estipulará que contacte con dicho representante, además de con la entidad de impacto alto o de impacto crítico o en lugar de con ella, cualquier autoridad competente o un CSIRT de la Unión, con respecto a las obligaciones de la entidad en virtud del presente Reglamento. La entidad de impacto alto o de impacto crítico proporcionará a su representante legal las facultades necesarias y los recursos suficientes para garantizar su cooperación eficiente y oportuna con las autoridades competentes o los CSIRT pertinentes.

3. El representante deberá estar establecido en uno de los Estados miembros en los que la entidad ofrece los servicios. La entidad se considerará sometida a la jurisdicción del Estado miembro en el que esté establecido su representante. Las entidades de impacto alto o de impacto crítico notificarán el nombre, el domicilio postal, la dirección de correo electrónico y el número de teléfono de su representante legal a la autoridad competente del Estado miembro en el que dicho representante legal resida o esté establecido.

4. El representante legal designado podrá ser considerado responsable por el incumplimiento de las obligaciones en virtud del presente Reglamento, sin perjuicio de la responsabilidad de la propia entidad de impacto alto o de impacto crítico y de las acciones legales que pudiesen iniciarse contra ella.

5. En ausencia de un representante dentro de la Unión designado con arreglo al presente artículo, cualquier Estado miembro en el que la entidad preste servicios podrá emprender acciones legales contra la entidad por incumplimiento de las obligaciones recogidas en el presente Reglamento.

6. La designación de un representante legal en la Unión con arreglo al apartado 1 no constituirá un establecimiento en la Unión.

Artículo 16

Cooperación entre la REGRT de Electricidad y la entidad de los GRD de la UE

1. La REGRT de Electricidad y la entidad de los GRD de la UE cooperarán en la realización de evaluaciones de riesgos para la ciberseguridad con arreglo al artículo 19 y al artículo 21, y en particular en las siguientes tareas:

a) desarrollo de las metodologías de evaluación de riesgos para la ciberseguridad, de conformidad con el artículo 18, apartado 1;

b) desarrollo del informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad, de conformidad con el artículo 23;

c) desarrollo del marco común de ciberseguridad de la electricidad, de conformidad con el capítulo III;

d) desarrollo de la recomendación sobre contratación en materia de ciberseguridad, de conformidad con el artículo 35;

e) desarrollo de la metodología de la escala de clasificación de los ciberataques, de conformidad con el artículo 37, apartado 8;

f) desarrollo del índice provisional de impacto en la ciberseguridad de la electricidad, de conformidad con el artículo 48, apartado 1, letra a);

g) elaboración de la lista provisional consolidada de entidades de impacto alto y de impacto crítico, de conformidad con el artículo 48, apartado 3;

h) elaboración de la lista provisional de procesos de impacto alto y de impacto crítico a escala de la Unión, de conformidad con el artículo 48, apartado 4;

i) elaboración de la lista provisional de normas y controles europeos e internacionales, de conformidad con el artículo 48, apartado 6;

j) realización de la evaluación de riesgos para la ciberseguridad a escala de la Unión, de conformidad con el artículo 19;

k) realización de las evaluaciones regionales de riesgos para la ciberseguridad, de conformidad con el artículo 21;

l) definición de los planes regionales de mitigación de riesgos para la ciberseguridad, de conformidad con el artículo 22;

m) elaboración de orientaciones sobre los esquemas europeos de certificación de la ciberseguridad para productos, servicios y procesos de TIC, de conformidad con el artículo 36;

n) elaboración de directrices para la ejecución del presente Reglamento en consulta con la ACER y la ENISA.

2. La cooperación entre la REGRT de Electricidad y la entidad de los GRD de la UE podrá adoptar la forma de un grupo de trabajo sobre riesgos para la ciberseguridad.

3. La REGRT de Electricidad y la entidad de los GRD de la UE informarán periódicamente a la ACER, a la ENISA, al Grupo de Cooperación SRI y al Grupo de Coordinación de la Electricidad sobre los avances en la aplicación de las evaluaciones de riesgos para la ciberseguridad a escala de la Unión y las evaluaciones regionales de riesgos para la ciberseguridad con arreglo a los artículos 19 y 21.

Artículo 17

Cooperación entre la ACER y las autoridades competentes

La ACER, en cooperación con cada autoridad competente:

1) supervisará la aplicación de las medidas de gestión de riesgos para la ciberseguridad con arreglo al artículo 12, apartado 2, letra a), y las obligaciones de notificación con arreglo a los artículos 27 y 39, y

2) supervisará el proceso de adopción y la aplicación de las condiciones, metodologías o planes con arreglo al artículo 6, apartados 2 y 3. La cooperación entre la ACER, la ENISA y cada autoridad competente podrá adoptar la forma de un organismo de supervisión de riesgos para la ciberseguridad.

CAPÍTULO II

EVALUACIÓN DE RIESGOS Y DETERMINACIÓN DE LOS RIESGOS PARA LA CIBERSEGURIDAD PERTINENTES

Artículo 18

Metodologías de evaluación de riesgos para la ciberseguridad

1. A más tardar el 13 de marzo de 2025, los GRT, con la asistencia de la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y previa consulta con el Grupo de Cooperación SRI, presentarán una propuesta de metodologías de evaluación de riesgos para la ciberseguridad a nivel de la Unión, regional y de los Estados miembros.

2. Las metodologías de evaluación de riesgos para la ciberseguridad a nivel de la Unión, regional y de los Estados miembros incluirán:

a) una lista de ciberamenazas que deben tenerse en cuenta, en la que figuren, como mínimo, las siguientes amenazas a la cadena de suministro:

   i) una corrupción grave e inesperada de la cadena de suministro,

   ii) la indisponibilidad de productos, servicios o procesos de TIC de la cadena de suministro,

iii) ciberataques iniciados a través de agentes de la cadena de suministro,

iv) filtración de información sensible a lo largo de la cadena de suministro, incluido el seguimiento a lo largo de la cadena de suministro,

v) la introducción de deficiencias o puertas traseras en los productos, servicios o procesos de TIC a través de agentes de la cadena de suministro;

b) los criterios para evaluar el impacto de los riesgos para la ciberseguridad como alto o crítico utilizando umbrales definidos para las consecuencias y la probabilidad;

c) un enfoque para analizar los riesgos para la ciberseguridad derivados de los sistemas heredados, los efectos en cascada de los ciberataques y la naturaleza en tiempo real de los sistemas que funcionan en la red;

d) un enfoque para analizar los riesgos para la ciberseguridad derivados de la dependencia de un único proveedor de productos, servicios o procesos de TIC.

3. Las metodologías de evaluación de riesgos para la ciberseguridad a nivel de la Unión, regional y de los Estados miembros evaluarán los riesgos para la ciberseguridad utilizando la misma matriz de impacto del riesgo. La matriz de impacto del riesgo:

a) medirá las consecuencias de los ciberataques sobre la base de los siguientes criterios:

i) pérdida de carga,

ii) reducción de la generación de electricidad,

iii) pérdida de capacidad en la reserva primaria de frecuencia,

iv) pérdida de capacidad para restablecer el funcionamiento de una red eléctrica sin depender de la red de transporte externa al objeto de recuperarse tras un paro total o parcial (también denominado «reposición del servicio»),

v) la duración prevista de un corte de electricidad que afecte a los clientes combinada con la magnitud del corte en términos de número de clientes,

vi) cualquier otro criterio cuantitativo o cualitativo que pueda actuar razonablemente como indicador del efecto de un ciberataque en los flujos transfronterizos de electricidad;

b) medirá la probabilidad de que se produzca un incidente como la frecuencia de ciberataques al año.

4. Las metodologías de evaluación de riesgos para la ciberseguridad a nivel de la Unión describirán cómo se definirán los valores ECII para los umbrales del impacto alto y del impacto crítico. El ECII permitirá a las entidades estimar, con ayuda de los criterios a que se refiere el apartado 2, letra b), el impacto de los riegos sobre su proceso de negocio durante las evaluaciones del impacto sobre la actividad que realicen con arreglo al artículo 26, apartado 4, letra c), inciso i).

5. La REGRT de Electricidad, en coordinación con la entidad de los GRD de la UE, informará al Grupo de Coordinación de la Electricidad sobre las propuestas de metodologías de evaluación de riesgos para la ciberseguridad que se elaboren con arreglo al apartado 1.

Artículo 19

Evaluación de riesgos para la ciberseguridad a escala de la Unión

1. En un plazo de nueve meses a partir de la aprobación de las metodologías de evaluación de riesgos para la ciberseguridad con arreglo a lo dispuesto en el artículo 8 y posteriormente cada tres años, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y en consulta con el Grupo de Cooperación SRI, llevará a cabo, sin perjuicio de lo dispuesto en el artículo 22 de la Directiva (UE) 2022/2555, una evaluación de riesgos para la ciberseguridad a escala de la Unión, y elaborará un proyecto de informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión. A tal fin, utilizará las metodologías desarrolladas con arreglo al artículo 18, y aprobadas con arreglo al artículo 8, para determinar, analizar y evaluar las posibles consecuencias de los ciberataques que afecten a la seguridad operativa del sistema eléctrico y perturben los flujos transfronterizos de electricidad. La evaluación de riesgos para la ciberseguridad a escala de la Unión no tendrá en cuenta los daños de los ciberataques desde el punto de vista jurídico o financiero, ni tampoco los daños a la reputación.

2. El informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión incluirá los siguientes elementos:

a) los procesos de impacto alto a escala de la Unión y los procesos de impacto crítico a escala de la Unión;

b) una matriz de impacto del riesgo que las entidades y las autoridades competentes utilizarán para evaluar los riesgos para la ciberseguridad señalados en la evaluación de riesgos para la ciberseguridad a nivel de Estado miembro, realizada con arreglo al artículo 20, y en la evaluación de riesgos para la ciberseguridad a nivel de entidad, realizada con arreglo al artículo 26, apartado 2, letra b).

3. Con respecto a los procesos de impacto alto y de impacto crítico a escala de la Unión, el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión incluirá:

a) una evaluación de las posibles consecuencias de un ciberataque utilizando los parámetros definidos en la metodología de evaluación de riesgos para la ciberseguridad desarrollada con arreglo al artículo 18, apartados 2, 3, y 4, y aprobada con arreglo al artículo 8;

b) los umbrales ECII y del impacto alto e impacto crítico que las autoridades competentes utilizarán con arreglo al artículo 24, apartados 1 y 2, para determinar las entidades de impacto alto y de impacto crítico que intervienen en los procesos de impacto alto a escala de la Unión y en los procesos de impacto crítico a escala de la Unión.

4. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, presentará a la ACER el proyecto de informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con los resultados de la evaluación de riesgos para la ciberseguridad a escala de la Unión, con vistas a que la ACER emita un dictamen. La ACER emitirá un dictamen sobre el proyecto de informe en un plazo de tres meses a partir de su recepción. La REGRT de Electricidad y la entidad de los GRD de la UE tendrán en cuenta el dictamen de la ACER en la mayor medida posible al finalizar el informe.

5. En un plazo de tres meses a partir de la recepción del dictamen de la ACER, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, notificará el informe final de evaluación de riesgos para la ciberseguridad a escala de la Unión a la ACER, a la Comisión, a la ENISA y a las autoridades competentes.

Artículo 20

Evaluación de riesgos para la ciberseguridad del Estado miembro

1. Cada autoridad competente someterá todas las entidades de impacto alto y de impacto crítico de su Estado miembro a una evaluación de riesgos para la ciberseguridad del Estado miembro, utilizando las metodologías desarrolladas con arreglo al artículo 18 y aprobadas con arreglo al artículo 8. La evaluación de riesgos para la ciberseguridad del Estado miembro determinará y analizará los riesgos de ciberataques que afecten a la seguridad operativa del sistema eléctrico y perturben los flujos transfronterizos de electricidad. La evaluación de riesgos para la ciberseguridad del Estado miembro no tendrá en cuenta los daños de los ciberataques desde el punto de vista jurídico o financiero, ni tampoco los daños a la reputación.

2. En un plazo de 21 meses a partir de la notificación de las entidades de impacto alto y de impacto crítico con arreglo al artículo 24, apartado 6, y cada tres años a partir de esa fecha, y previa consulta a la autoridad competente encargada de la ciberseguridad que sea responsable de la electricidad, cada autoridad competente, apoyada por el CSIRT, presentará a la REGRT de Electricidad y a la entidad de los GRD de la UE un informe sobre la evaluación de riesgos para la ciberseguridad del Estado miembro, que contendrá la siguiente información sobre cada proceso de negocio de impacto alto y de impacto crítico:

a) el estado de aplicación de los controles mínimos y avanzados de ciberseguridad, de conformidad con el artículo 29;

b) una lista de todos los ciberataques notificados en los tres años anteriores, de conformidad con el artículo 38, apartado 3;

c) un resumen de la información sobre ciberamenazas comunicada en los tres años anteriores, de conformidad con el artículo 38, apartado 6;

d) para cada proceso de impacto alto o de impacto crítico a escala de la Unión, una estimación de los riesgos de que la confidencialidad, integridad y disponibilidad de la información y los activos pertinentes se vean comprometidas;

e) en caso necesario, una lista de entidades adicionales consideradas como entidades de impacto alto o de impacto crítico, de conformidad con el artículo 24, apartados 1, 2, 3 y 5.

3. El informe sobre la evaluación de riesgos para la ciberseguridad del Estado miembro tendrá en cuenta el plan de preparación frente a los riesgos del Estado miembro, establecido con arreglo al artículo 10 del Reglamento (UE) 2019/941.

4. La información contenida en el informe sobre la evaluación de riesgos para la ciberseguridad del Estado miembro con arreglo al apartado 2, letras a) a d), no estará vinculada a entidades o activos específicos. El informe sobre la evaluación de riesgos para la ciberseguridad del Estado miembro también incluirá una evaluación de riesgos de las excepciones temporales concedidas por las autoridades competentes de los Estados miembros con arreglo al artículo 30.

5. La REGRT de Electricidad y la entidad de los GRD de la UE podrán solicitar información adicional a las autoridades competentes en relación con las tareas especificadas en el apartado 2, letras a) y c).

6. Las autoridades competentes velarán por que la información que faciliten sea exacta y correcta.

Artículo 21

Evaluaciones regionales de riesgos para la ciberseguridad

1. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y en consulta con el centro de coordinación regional pertinente, llevará a cabo una evaluación regional de riesgos para la ciberseguridad en cada región de operación del sistema utilizando las metodologías desarrolladas con arreglo al artículo 19, y aprobadas con arreglo al artículo 8, para determinar, analizar y evaluar los riesgos de ciberataques que afecten a la seguridad operativa del sistema eléctrico y perturben los flujos transfronterizos de electricidad. Las evaluaciones regionales de riesgos para la ciberseguridad no tendrán en cuenta los daños de los ciberataques desde el punto de vista jurídico o financiero, ni tampoco los daños a la reputación.

2. En un plazo de 30 meses a partir de la notificación de las entidades de impacto alto y de impacto crítico con arreglo al artículo 24, apartado 6, y cada tres años a partir de entonces, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y en consulta con el Grupo de Cooperación SRI, elaborará un informe sobre la evaluación regional de riesgos para la ciberseguridad en cada región de operación del sistema.

3. El informe sobre la evaluación regional de riesgos para la ciberseguridad tendrá en cuenta la información pertinente contenida en los informes sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión y en los informes sobre las evaluaciones de riesgos para la ciberseguridad de los Estados miembros.

4. La evaluación regional de riesgos para la ciberseguridad tendrá en cuenta los escenarios de crisis de electricidad regionales relacionados con la ciberseguridad determinados con arreglo al artículo 6 del Reglamento (UE) 2019/941.

Artículo 22

Planes regionales de mitigación de riesgos para la ciberseguridad

1. En un plazo de 36 meses a partir de la notificación de las entidades de impacto alto y de impacto crítico con arreglo al artículo 24, apartado 6, y a más tardar el 13 de junio de 2031, y cada tres años después de esa fecha, los GRT, con la asistencia de la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y en consulta con los centros de coordinación regionales y el Grupo de Cooperación SRI, elaborarán un plan regional de mitigación del riesgo para la ciberseguridad en cada región de operación del sistema.

2. Los planes regionales de mitigación de riesgos para la ciberseguridad incluirán:

a) los controles mínimos y avanzados de ciberseguridad que las entidades de impacto alto y de impacto crítico aplicarán en la región de operación del sistema;

b) los riesgos residuales para la ciberseguridad en las regiones de operación del sistema tras aplicar los controles a que se refiere la letra a).

3. La REGRT de Electricidad presentará los planes regionales de mitigación de riesgos a los gestores de redes de transporte pertinentes, a las autoridades competentes y al Grupo de Coordinación de la Electricidad. El Grupo de Coordinación de la Electricidad podrá recomendar modificaciones.

4. Los GRT, con la asistencia de la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y en consulta con el Grupo de Cooperación SRI, actualizarán los planes regionales de mitigación de riesgos cada tres años, salvo que las circunstancias exijan actualizaciones más frecuentes.

Artículo 23

Informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad

1. En un plazo de 40 meses a partir de la notificación de las entidades de impacto alto y de impacto crítico con arreglo al artículo 24, apartado 6, y posteriormente cada tres años, los GRT, con la asistencia de la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE y en consulta con el Grupo de Cooperación SRI, presentarán al Grupo de Coordinación de la Electricidad un informe sobre el resultado de la evaluación de riesgos para la ciberseguridad en relación con los flujos transfronterizos de electricidad («informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad»).

2. El informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad se basará en el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión, en los informes sobre la evaluación de riesgos para la ciberseguridad del Estado miembro y en los informes sobre las evaluaciones regionales de riesgos para la ciberseguridad, e incluirá la siguiente información:

a) la lista de procesos de impacto alto y de impacto crítico a escala de la Unión señalados en el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión de conformidad con el artículo 19, apartado 2, letra a), incluida la estimación de la probabilidad y el impacto de los riesgos para la ciberseguridad evaluados durante los informes sobre la evaluación regional de riesgos para la ciberseguridad con arreglo al artículo 21, apartado 2, y al artículo 19, apartado 3, letra a);

b) las ciberamenazas actuales, prestando especial atención a las amenazas emergentes y los riesgos para el sistema eléctrico;

c) los ciberataques durante el período anterior a nivel de la Unión, proporcionando una visión general crítica de cómo dichos ciberataques pueden haber tenido un impacto en los flujos transfronterizos de electricidad;

d) el estado general de aplicación de las medidas de ciberseguridad;

e) el estado de aplicación de los flujos de información con arreglo a los artículos 37 y 38;

f) la lista de información o criterios específicos para la clasificación de la información con arreglo al artículo 46;

g) los riesgos detectados y destacados que pueden derivarse de una gestión precaria de la cadena de suministro;

h) los resultados y las experiencias acumuladas de los ejercicios de ciberseguridad regionales y transregionales organizados con arreglo al artículo 44;

i) un análisis de la evaluación del conjunto de riesgos transfronterizos para la ciberseguridad en el sector de la electricidad desde las últimas evaluaciones regionales de riesgos para la ciberseguridad;

j) cualquier otra información que pueda ser útil para detectar posibles mejoras del presente Reglamento o la necesidad de revisar el presente Reglamento o cualquiera de sus instrumentos, y

k) información agregada y anonimizada de las excepciones concedidas con arreglo al artículo 30, apartado 3.

3. Las entidades contempladas en el artículo 2, apartado 1, podrán contribuir al desarrollo del informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad, respetando la confidencialidad de la información de conformidad con el artículo 47. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, consultarán a estas entidades desde una fase temprana.

4. El informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad estará sujeto a las normas sobre protección del intercambio de información con arreglo al artículo 46. Sin perjuicio de lo dispuesto en el artículo 10, apartado 4, y en el artículo 47, apartado 4, la REGRT de Electricidad y la entidad de los GRD de la UE emitirán una versión pública de dicho informe que no contendrá información que pueda causar daños a las entidades contempladas en el artículo 2, apartado 1. La versión pública de este informe solo se emitirá con el acuerdo del Grupo de Cooperación SRI y del Grupo de Coordinación de la Electricidad. La REGRT de Electricidad, en coordinación con la entidad de los GRD de la UE, será responsable de la compilación y emisión de la versión pública del informe.

Artículo 24

Determinación de entidades de impacto alto y de impacto crítico

1. Cada autoridad competente determinará, utilizando los umbrales ECII y del impacto alto e impacto crítico incluidos en el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 3, letra b), las entidades de impacto alto e impacto crítico de su Estado miembro que intervienen en los procesos de impacto alto e impacto crítico a escala de la Unión. Las autoridades competentes podrán solicitar información a una entidad de su Estado miembro para determinar los valores ECII de dicha entidad. Si el ECII determinado de una entidad supera el umbral del impacto alto o del impacto crítico, la entidad determinada se incluirá en el informe sobre la evaluación de riesgos para la ciberseguridad del Estado miembro contemplado en el artículo 20, apartado 2.

2. Cada autoridad competente determinará, utilizando los umbrales ECII y del impacto alto e impacto crítico incluidos en el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 3, letra b), las entidades de impacto alto e impacto crítico no establecidas en la Unión en la medida en que estas operen dentro de la Unión. La autoridad competente podrá solicitar información a una entidad no establecida en la Unión para determinar los valores ECII de dicha entidad.

3. Cada autoridad competente podrá considerar otras entidades de su Estado miembro como entidades de impacto alto o de impacto crítico si se cumplen los siguientes criterios:

a) la entidad forma parte de un grupo de entidades que corren un riesgo significativo de verse afectadas simultáneamente por un ciberataque;

b) el ECII agregado del grupo de entidades supera el umbral del impacto alto o del impacto crítico.

4. Si una autoridad competente determina más entidades de conformidad con el apartado 3, todos los procesos de dichas entidades para las que el ECII agregado del grupo supere el umbral del impacto alto se considerarán procesos de impacto alto, y todos los procesos de dichas entidades para las que el ECII agregado del grupo supere los umbrales del impacto crítico se considerarán procesos de impacto crítico.

5. Si una autoridad competente determina entidades contempladas en el apartado 3, letra a), en más de un Estado miembro, informará de ello a las demás autoridades competentes, a la REGRT de Electricidad y a la entidad de los GRD de la UE. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, basándose en la información recibida de todas las autoridades competentes, facilitará a las autoridades competentes un análisis de la agregación de entidades en más de un Estado miembro que pueda crear una perturbación distribuida en los flujos transfronterizos de electricidad y dar lugar a un ciberataque. Cuando un grupo de entidades de varios Estados miembros se considere como una agregación cuyo ECII supera el umbral del impacto alto o de impacto crítico, todas las autoridades competentes afectadas considerarán las entidades de dicho grupo como entidades de impacto alto o de impacto crítico para su respectivo Estado miembro, basándose en el ECII agregado del grupo de entidades, y las entidades determinadas se incluirán en el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión.

6. En un plazo de nueve meses a partir de la fecha en que la REGRT de Electricidad y la entidad de los GRD de la UE notifiquen el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 5, y, en cualquier caso, a más tardar el 13 de junio de 2028, cada autoridad competente notificará a las entidades incluidas en la lista que han sido consideradas como entidades de impacto alto o de impacto crítico en su Estado miembro.

7. Cuando se señale a una autoridad competente que un proveedor de servicios es un proveedor de servicios de TIC críticos con arreglo al artículo 27, letra c), dicha autoridad competente lo notificará a las autoridades competentes de los Estados miembros en cuyo territorio esté situada la sede o el representante. Esta última autoridad competente notificará al proveedor de servicios que ha sido considerado como proveedor de servicios críticos.

Artículo 25

Sistemas nacionales de verificación

1. Las autoridades competentes podrán establecer un sistema nacional de verificación para comprobar que las entidades de impacto crítico determinadas con arreglo al artículo 24, apartado 1, han implementado el marco legislativo nacional incluido en la matriz cartográfica contemplada en el artículo 34. El sistema nacional de verificación podrá basarse en una inspección realizada por la autoridad competente, en auditorías de seguridad independientes o en revisiones mutuas por pares realizadas por entidades de impacto crítico del mismo Estado miembro supervisadas por la autoridad competente.

2. Si una autoridad competente decide establecer un sistema nacional de verificación, se asegurará de que la verificación se realice de conformidad con los siguientes requisitos:

a) cualquier parte que realice la revisión por pares, la auditoría o la inspección será independiente de la entidad de impacto crítico que se esté verificando y no tendrá conflictos de intereses;

b) el personal que realice la revisión por pares, la auditoría o la inspección tendrá conocimientos demostrables de:

   i) ciberseguridad en el sector de la electricidad,

   ii) sistemas de gestión de la ciberseguridad,

   iii) los principios de auditoría,

   iv) la evaluación de riesgos para la ciberseguridad,

   v) el marco común de ciberseguridad de la electricidad,

   vi) el marco legislativo y reglamentario nacional y las normas europeas e internacionales que aborde la verificación,

   vii) los procesos de impacto crítico que aborde la verificación;

c) la parte que realice la revisión por pares, la auditoría o la inspección dispondrá de tiempo suficiente para llevar a cabo estas actividades;

d) la parte que realice la revisión por pares, la auditoría o la inspección tomará las medidas adecuadas para proteger la información recogida durante la verificación, de acuerdo con su nivel de confidencialidad, y

e) las revisiones por pares, las auditorías o las inspecciones se realizarán al menos una vez al año y abarcarán el alcance completo de la verificación al menos cada tres años.

3. Si una autoridad competente decide establecer un sistema nacional de verificación, informará anualmente a la ACER sobre la frecuencia con la que ha llevado a cabo inspecciones en el marco de dicho sistema.

Artículo 26

Gestión de riesgos para la ciberseguridad a nivel de entidad

1. Cada entidad de impacto alto y de impacto crítico determinada por las autoridades competentes con arreglo al artículo 24, apartado 1, llevará a cabo una gestión de riesgos para la ciberseguridad de todos sus activos en sus perímetros del impacto alto y de impacto crítico. Cada entidad de impacto alto y de impacto crítico realizará una gestión de riesgos que incluya las fases del apartado 2 cada tres años.

2. Cada entidad de impacto alto y de impacto crítico basará su gestión de riesgos para la ciberseguridad en un enfoque que tenga por objeto proteger sus redes y sistemas de información y que comprenda las siguientes fases:

a) establecimiento del contexto;

b) evaluación de los riesgos para la ciberseguridad a nivel de entidad;

c) gestión de los riesgos para la ciberseguridad;

d) aceptación de los riesgos para la ciberseguridad.

3. Durante la fase de establecimiento del contexto, cada entidad de impacto alto y de impacto crítico:

a) definirá el alcance de la evaluación de riesgos para la ciberseguridad, incluidos los procesos de impacto alto y de impacto crítico determinados por la REGRT de Electricidad y la entidad de los GRD de la UE, y otros procesos que puedan ser objeto de ciberataques con un impacto alto o un impacto crítico en los flujos transfronterizos de electricidad, y

b) definirá los criterios para la evaluación y aceptación de los riesgos de conformidad con la matriz de impacto del riesgo que las entidades y las autoridades competentes utilizarán para evaluar los riesgos para la ciberseguridad en las metodologías de evaluación de riesgos para la ciberseguridad a nivel de la Unión, regional y de los Estados miembros desarrolladas por la REGRT de Electricidad y la entidad de los GRD de la UE de conformidad con el artículo 19, apartado 2.

4. Durante la fase de evaluación de riesgos para la ciberseguridad, cada entidad de impacto alto y de impacto crítico:

a) detectará riesgos para la ciberseguridad teniendo en cuenta:

i) todos los activos que sirvan de apoyo a los procesos de impacto alto y de impacto crítico a escala de la Unión, con una evaluación del posible impacto en los flujos transfronterizos de electricidad si el activo se ve comprometido,

ii) las posibles ciberamenazas, teniendo en cuenta las ciberamenazas señaladas en el último informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad contemplado en el artículo 23 y las amenazas a la cadena de suministro,

iii) las vulnerabilidades, incluidas las vulnerabilidades de los sistemas heredados,

iv) posibles escenarios de ciberataques, incluidos los ciberataques que afecten a la seguridad operativa del sistema eléctrico y perturben los flujos transfronterizos de electricidad,

v) las evaluaciones de riesgos pertinentes realizadas a nivel de la Unión, incluidas las evaluaciones coordinadas de los riesgos de las cadenas de suministro críticas de conformidad con el artículo 22 de la Directiva (UE) 2022/2555, y

vi) los controles aplicados existentes;

b) analizará la probabilidad y las consecuencias de los riesgos para la ciberseguridad señalados en la letra a) y determinará el nivel de riesgo para la ciberseguridad valiéndose de la matriz de impacto del riesgo utilizada para evaluar los riesgos para la ciberseguridad en las metodologías de evaluación de riesgos para la ciberseguridad a nivel de la Unión, regional y de los Estados miembros desarrolladas por los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, de conformidad con el artículo 19, apartado 2;

c) clasificará los activos en función de las posibles consecuencias cuando la ciberseguridad se vea comprometida y determinará el perímetro del impacto alto y del impacto crítico siguiendo los siguientes pasos:

i) realizará, para todos los procesos que abarque la evaluación de riesgos para la ciberseguridad, una evaluación de impacto sobre la actividad utilizando el ECII,

ii) clasificará un proceso como de impacto alto o de impacto crítico si su ECII supera el umbral del impacto alto o del impacto crítico, respectivamente,

iii) determinará todos los activos de impacto alto y de impacto crítico como activos necesarios para los procesos de impacto alto y de impacto crítico, respectivamente,

iv) definirá los perímetros del impacto alto y del impacto crítico que contengan todos los activos de impacto alto y de impacto crítico respectivamente, de modo que pueda controlarse el acceso a los perímetros;

d) evaluará los riesgos para la ciberseguridad priorizándolos a través de los criterios de evaluación de los riesgos y los criterios de aceptación de los riesgos a que se refiere el apartado 3, letra b).

5. Durante la fase de gestión de los riesgos para la ciberseguridad, cada entidad de impacto alto y de impacto crítico establecerá un plan de mitigación de riesgos a nivel de entidad seleccionando opciones de gestión de riesgos adecuadas para manejar los riesgos y detectar los riesgos residuales.

6. Durante la fase de aceptación de los riesgos para la ciberseguridad, cada entidad de impacto alto y de impacto crítico decidirá si acepta el riesgo residual sobre la base de los criterios de aceptación de los riesgos establecidos en el apartado 3, letra b).

7. Cada entidad de impacto alto y de impacto crítico registrará los activos señalados en el apartado 1 en un inventario de activos. Dicho inventario de activos no formará parte del informe sobre la evaluación de riesgos.

8. La autoridad competente podrá examinar los activos del inventario durante las inspecciones.

Artículo 27

Presentación de informes sobre la evaluación de riesgos a nivel de entidad

Cada entidad de impacto alto y de impacto crítico presentará a la autoridad competente, en un plazo de 12 meses a partir de la notificación de las entidades de impacto alto y de impacto crítico con arreglo al artículo 24, apartado 6, y posteriormente cada tres años, un informe que contenga la siguiente información:

1) una lista de controles seleccionados para el plan de mitigación del riesgo a nivel de entidad con arreglo al artículo 26, apartado 5, con el estado actual de aplicación de cada control;

2) para cada proceso de impacto alto o de impacto crítico a escala de la Unión, una estimación del riesgo de que la confidencialidad, integridad y disponibilidad de la información y los activos pertinentes se vean comprometidas; la estimación de este riesgo se realizará de conformidad con la matriz de impacto del riesgo contemplada en el artículo 19, apartado 2;

3) una lista de proveedores de servicios de TIC críticos para sus procesos de impacto crítico.

CAPÍTULO III

MARCO COMÚN DE CIBERSEGURIDAD DE LA ELECTRICIDAD

Artículo 28

Composición, funcionamiento y revisión del marco común de ciberseguridad de la electricidad

1. El marco común de ciberseguridad de la electricidad estará compuesto por los siguientes controles y sistema de gestión de la ciberseguridad:

a) los controles mínimos de ciberseguridad, desarrollados de conformidad con el artículo 29;

b) los controles avanzados de ciberseguridad, desarrollados de conformidad con el artículo 29;

c) la matriz cartográfica, elaborada de conformidad con el artículo 34, para cartografiar los controles a que se refieren las letras a) y b) con respecto a una selección de normas europeas e internacionales y marcos legislativos o reglamentarios nacionales;

d) el sistema de gestión de la ciberseguridad, establecido de conformidad con el artículo 32.

2. Todas las entidades de impacto alto aplicarán los controles mínimos de ciberseguridad con arreglo al apartado 1, letra a), dentro de su perímetro del impacto alto.

3. Todas las entidades de impacto crítico aplicarán los controles avanzados de ciberseguridad con arreglo al apartado 1, letra b), dentro de su perímetro del impacto crítico.

4. En un plazo de siete meses a partir de la presentación del primer proyecto de informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 4, el marco común de ciberseguridad de la electricidad a que se refiere el apartado 1 se completará con los controles mínimos y avanzados de ciberseguridad en la cadena de suministro desarrollados con arreglo al artículo 33.

Artículo 29

Controles mínimos y avanzados de ciberseguridad

1. En un plazo de siete meses a partir de la presentación del primer proyecto de informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 4, los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, elaborarán una propuesta de controles mínimos y avanzados de ciberseguridad.

2. En un plazo de seis meses a partir de la elaboración de cada informe sobre la evaluación regional de riesgos para la ciberseguridad con arreglo al artículo 21, apartado 2, los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, propondrán a la autoridad competente una modificación de los controles mínimos y avanzados de ciberseguridad. La propuesta se realizará de conformidad con el artículo 8, apartado 10, y tendrá en cuenta los riesgos señalados en la evaluación regional de riesgos.

3. Los controles mínimos y avanzados de ciberseguridad serán verificables participando en un sistema nacional de verificación de conformidad con el procedimiento establecido en el artículo 31 o sometiéndose a auditorías de seguridad realizadas por terceros independientes de conformidad con los requisitos contemplados en el artículo 25, apartado 2.

4. Los controles mínimos y avanzados de ciberseguridad iniciales desarrollados con arreglo al apartado 1 se basarán en los riesgos señalados en el informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión a que se refiere el artículo 19, apartado 5. Los controles mínimos y avanzados de ciberseguridad modificados desarrollados con arreglo al apartado 2 se basarán en el informe sobre la evaluación regional de riesgos para la ciberseguridad contemplado en el artículo 21, apartado 2.

5. Los controles mínimos de ciberseguridad incluirán controles para proteger la información intercambiada con arreglo al artículo 46.

6. En un plazo de 12 meses a partir de la aprobación de los controles mínimos y avanzados de ciberseguridad con arreglo al artículo 8, apartado 5, o después de cada actualización con arreglo al artículo 8, apartado 10, las entidades contempladas en el artículo 2, apartado 1, y consideradas de impacto crítico y de impacto alto con arreglo al artículo 24 aplicarán, durante el establecimiento del plan de mitigación de riesgos a nivel de entidad con arreglo al artículo 26, apartado 5, los controles mínimos de ciberseguridad dentro del perímetro del impacto alto y los controles avanzados de ciberseguridad dentro del perímetro del impacto crítico.

Artículo 30

Excepciones a los controles mínimos y avanzados de ciberseguridad

1. Las entidades contempladas en el artículo 2, apartado 1, podrán solicitar a la autoridad competente respectiva que conceda una excepción a su obligación de aplicar los controles mínimos y avanzados de ciberseguridad contemplados en el artículo 29, apartado 6. La autoridad competente podrá conceder tal excepción por alguno de los motivos siguientes:

a) en circunstancias excepcionales, cuando la entidad pueda demostrar que los costes de aplicar los controles de ciberseguridad adecuados superan significativamente los beneficios. La ACER y la REGRT de Electricidad, en cooperación con la entidad de los GRD, podrán elaborar conjuntamente orientaciones para estimar los costes de los controles de ciberseguridad a fin de ayudar a las entidades;

b) cuando la entidad presente un plan de gestión de riesgos a nivel de entidad que mitigue los riesgos para la ciberseguridad utilizando controles alternativos hasta alcanzar un nivel aceptable de conformidad con los criterios de aceptación de los riesgos a que se refiere el artículo 26, apartado 3, letra b).

2. En un plazo de tres meses a partir de la recepción de la solicitud a que se refiere el apartado 1, cada autoridad competente decidirá si debe concederse una excepción a los controles mínimos y avanzados de ciberseguridad. Las excepciones a los controles mínimos o avanzados de ciberseguridad se concederán por un período máximo de tres años, con posibilidad de renovación.

3. La información agregada y anonimizada sobre las excepciones concedidas se incluirá como anexo del informe exhaustivo sobre la evaluación de riesgos para la ciberseguridad de los flujos transfronterizos de electricidad contemplado en el artículo 23. La REGRT de Electricidad y la entidad de los GRD de la UE actualizarán conjuntamente la lista, cuando sea necesario.

Artículo 31

Verificación del marco común de ciberseguridad de la electricidad

1. A más tardar 24 meses después de la adopción de los controles a que se refiere el artículo 28, apartado 1, letras a), b) y c), y del establecimiento del sistema de gestión de la ciberseguridad a que se refiere la letra d) de dicho artículo, cada entidad de impacto crítico determinada de conformidad con el artículo 24, apartado 1, deberá poder demostrar su conformidad con el sistema de gestión de la ciberseguridad y con los controles mínimos o avanzados de ciberseguridad a petición de la autoridad competente.

2. Cada entidad de impacto crítico cumplirá la obligación a que se refiere el apartado 1 sometiéndose a auditorías de seguridad realizadas por terceros independientes de conformidad con los requisitos del artículo 25, apartado 2, o participando en un sistema nacional de verificación de conformidad con el artículo 25, apartado 1.

3. La verificación de que una entidad de impacto crítico cumple el sistema de gestión de la ciberseguridad y los controles mínimos o avanzados de ciberseguridad abarcará todos los activos dentro del perímetro del impacto crítico de la entidad de impacto crítico.

4. La verificación de que una entidad de impacto crítico cumple el sistema de gestión de la ciberseguridad y los controles mínimos o avanzados de ciberseguridad se repetirá periódicamente a más tardar 36 meses después de que finalice la primera verificación, y posteriormente cada tres años.

5. Cada entidad de impacto crítico definida de conformidad con el artículo 24 demostrará su conformidad con los controles a que se refiere el artículo 28, apartado 1, letras a), b) y c), así como con el establecimiento del sistema de gestión de la ciberseguridad mencionado en la letra d) de dicho artículo, notificando el resultado de la verificación del cumplimiento a la autoridad competente.

Artículo 32

Sistema de gestión de la ciberseguridad

1. En un plazo de 24 meses a partir de la fecha en que la autoridad competente notifique a las entidades de impacto alto y de impacto crítico que han sido consideradas como entidad de impacto alto o de impacto crítico de conformidad con el artículo 24, apartado 6, cada una de ellas establecerá un sistema de gestión de la ciberseguridad, y posteriormente lo revisará cada tres años, con el fin de:

a) determinar el alcance del sistema de gestión de la ciberseguridad, teniendo en cuenta las interfaces y dependencias con otras entidades;

b) garantizar que todos sus altos directivos estén informados de las obligaciones jurídicas pertinentes y contribuyan activamente a la implementación del sistema de gestión de la ciberseguridad con decisiones oportunas y reacciones rápidas;

c) garantizar que los recursos necesarios para el sistema de gestión de la ciberseguridad estén disponibles;

d) establecer una política de ciberseguridad que se documentará y se comunicará dentro de la entidad y a las partes afectadas por los riesgos de seguridad;

e) asignar y comunicar las responsabilidades de las funciones pertinentes para la ciberseguridad;

f) realizar la gestión de riesgos para la ciberseguridad a nivel de entidad, tal como se define en el artículo 26;

g) determinar y proporcionar los recursos necesarios para la implementación, el mantenimiento y la mejora continua del sistema de gestión de la ciberseguridad, teniendo en cuenta la competencia y el conocimiento necesarios de los recursos de ciberseguridad;

h) determinar la comunicación interna y externa pertinente para la ciberseguridad;

i) crear, actualizar y controlar la información documentada relacionada con el sistema de gestión de la ciberseguridad;

j) evaluar el rendimiento y la eficacia del sistema de gestión de la ciberseguridad;

k) realizar auditorías internas a intervalos planificados para garantizar la implementación y el mantenimiento efectivos del sistema de gestión de la ciberseguridad;

l) revisar la implementación del sistema de gestión de la ciberseguridad a intervalos previstos; y controlar y corregir la no conformidad de los recursos y actividades con las políticas, procedimientos y directrices del sistema de gestión de la ciberseguridad.

2. El sistema de gestión de la ciberseguridad abarcará todos los activos dentro del perímetro del impacto alto y del impacto crítico de la entidad de impacto alto y de impacto crítico.

3. Las autoridades competentes, sin imponer ni discriminar en favor de la utilización de un tipo concreto de tecnología, fomentarán el uso de normas y especificaciones europeas o internacionales relacionadas con los sistemas de gestión y pertinentes para la seguridad de las redes y sistemas de información.

Artículo 33

Controles mínimos y avanzados de ciberseguridad en la cadena de suministro

1. En un plazo de siete meses a partir de la presentación del primer proyecto de informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 4, los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, elaborarán una propuesta de controles mínimos y avanzados de ciberseguridad en la cadena de suministro que mitiguen los riesgos de la cadena de suministro señalados en las evaluaciones de riesgos para la ciberseguridad a escala de la Unión, que completarán los controles mínimos y avanzados de ciberseguridad desarrollados con arreglo al artículo 29. Los controles mínimos y avanzados de ciberseguridad en la cadena de suministro se desarrollarán junto con los controles mínimos y avanzados de ciberseguridad con arreglo al artículo 29. Los controles mínimos y avanzados de ciberseguridad en la cadena de suministro abarcarán el ciclo de vida completo de todos los productos, servicios y procesos de TIC dentro de los perímetros del impacto alto o de impacto crítico de una entidad de impacto alto o de impacto crítico. Se consultará al Grupo de Cooperación SRI durante la elaboración de la propuesta de controles mínimos y avanzados de ciberseguridad en la cadena de suministro.

2. Los controles mínimos de ciberseguridad en la cadena de suministro consistirán en controles para las entidades de impacto alto y de impacto crítico que:

a) incluyan recomendaciones para la contratación de productos, servicios y procesos de TIC referentes a especificaciones de ciberseguridad, que abarquen, como mínimo:

   i) la comprobación de antecedentes del personal del proveedor participante en la cadena de suministro que se ocupa de la información sensible o del acceso a los activos de impacto alto o de impacto crítico de la entidad; la comprobación de antecedentes podrá incluir una verificación de la identidad y el historial del personal o de los contratistas de una entidad de conformidad con la legislación y los procedimientos nacionales y con el Derecho de la Unión pertinente y aplicable, incluidos el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([18]); estas comprobaciones de antecedentes serán proporcionadas y se limitarán estrictamente a lo necesario; se realizarán con el único fin de evaluar un posible riesgo para la seguridad de la entidad de que se trate; deberán ser proporcionales a los requisitos empresariales, a la clasificación de la información a la que se va a acceder y a los riesgos percibidos, y podrán ser realizadas por la propia entidad, por una empresa externa que lleve a cabo un control, o a través de una autorización de la administración,

   ii) los procesos de diseño, desarrollo y producción seguros y controlados de productos, servicios y procesos de TIC, promoviendo el diseño y el desarrollo de productos, servicios y procesos de TIC que incluyan medidas técnicas adecuadas para garantizar la ciberseguridad,

   iii) el diseño de redes y sistemas de información en los que los dispositivos no se consideren fiables, incluso cuando se encuentren dentro de un perímetro seguro, que exijan la verificación de todas las solicitudes recibidas y que apliquen el principio del mínimo privilegio,

   iv) el acceso del proveedor a los activos de la entidad,

([18]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

v) las obligaciones contractuales del proveedor de proteger y restringir el acceso a la información sensible de la entidad,

vi) las especificaciones de contratación en materia de ciberseguridad subyacentes a los subcontratistas del proveedor,

vii) la trazabilidad de la aplicación de las especificaciones de ciberseguridad desde el desarrollo y la producción hasta la entrega de productos, servicios o procesos de TIC,

viii) el apoyo a las actualizaciones de seguridad a lo largo de toda la vida útil de los productos, servicios o procesos de TIC,

ix) el derecho a auditar la ciberseguridad en los procesos de diseño, desarrollo y producción del proveedor, y

x) la evaluación del perfil de riesgo del proveedor;

b) exijan a dichas entidades que tengan en cuenta las recomendaciones sobre contratación a que se refiere la letra a) al celebrar contratos con proveedores, socios colaboradores y otras partes de la cadena de suministro, que cubrirán las entregas ordinarias de productos, servicios y procesos de TIC, así como los acontecimientos y circunstancias no deseados, como la rescisión y la transición de contratos en casos de negligencia del socio contractual;

c) exijan a dichas entidades que tengan en cuenta los resultados de las evaluaciones coordinadas pertinentes de los riesgos de seguridad de las cadenas de suministro críticas realizadas de conformidad con el artículo 22, apartado 1, de la Directiva (UE) 2022/2555;

d) incluyan criterios para seleccionar y contratar a proveedores que puedan cumplir las especificaciones de ciberseguridad establecidas en la letra a) y que posean un nivel de ciberseguridad adecuado a los riesgos para la ciberseguridad del producto, servicio o proceso de TIC que ofrezca el proveedor;

e) incluyan criterios para diversificar las fuentes de suministro de productos, servicios y procesos de TIC y reducir el riesgo de dependencia de un proveedor;

f) incluyan criterios para supervisar, revisar o auditar periódicamente las especificaciones de ciberseguridad de los procesos operativos internos de los proveedores a lo largo de todo el ciclo de vida de cada producto, servicio y proceso de TIC.

3. Para las especificaciones de ciberseguridad de la recomendación de contratación en materia de ciberseguridad a que se refiere el apartado 2, letra a), las entidades de impacto alto o de impacto crítico utilizarán los principios de contratación con arreglo a la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([19]), de conformidad con el artículo 35, apartado 4, o definirán sus propias especificaciones basándose en los resultados de la evaluación de riesgos para la ciberseguridad a nivel de entidad.

4. Los controles avanzados de ciberseguridad en la cadena de suministro incluirán controles para que las entidades de impacto crítico verifiquen, durante la contratación, que los productos, servicios y procesos de TIC que se utilizarán como activos de impacto crítico cumplen las especificaciones de ciberseguridad. El producto, servicio o proceso de TIC se verificará a través de un esquema europeo de certificación de la ciberseguridad contemplado en el artículo 31 o mediante actividades de verificación seleccionadas y organizadas por la entidad. La profundidad y la cobertura de las actividades de verificación serán suficientes para garantizar que el producto, servicio o proceso de TIC puede utilizarse para mitigar los riesgos señalados en la evaluación de riesgos a nivel de entidad. La entidad de impacto crítico documentará las medidas adoptadas para reducir los riesgos detectados.

5. Los controles mínimos y avanzados de ciberseguridad en la cadena de suministro se aplicarán a la contratación de productos, servicios y procesos de TIC pertinentes. Los controles mínimos y avanzados de ciberseguridad en la cadena de suministro se aplicarán a los procesos de contratación de las entidades consideradas como entidades de impacto crítico y de impacto alto con arreglo al artículo 24 que comiencen seis meses después de la adopción o actualización de los controles mínimos y avanzados de ciberseguridad a que se refiere el artículo 29.

([19]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

6. En un plazo de seis meses a partir de la elaboración de cada informe sobre la evaluación regional de riesgos para la ciberseguridad con arreglo al artículo 21, apartado 2, los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, propondrán a la autoridad competente una modificación de los controles mínimos y avanzados de ciberseguridad en la cadena de suministro. La propuesta se realizará de conformidad con el artículo 8, apartado 10, y tendrá en cuenta los riesgos señalados en la evaluación regional de riesgos.

Artículo 34

Matriz cartográfica de los controles de ciberseguridad de la electricidad con respecto a las normas

1. En un plazo de siete meses a partir de la presentación del primer proyecto de informe sobre la evaluación de riesgos para la ciberseguridad a escala de la Unión con arreglo al artículo 19, apartado 4, los GRT, con la asistencia de la REGRT de Electricidad, y en cooperación con la entidad de los GRD de la UE y en consulta con la ENISA, elaborarán una propuesta de matriz para cartografiar los controles establecidos en el artículo 28, apartado 1, letras a) y b), con respecto a una selección de normas europeas e internacionales, así como a las especificaciones técnicas pertinentes («la matriz cartográfica»). La REGRT de Electricidad y la entidad de los GRD de la UE documentarán la equivalencia de los distintos controles con los controles establecidos en el artículo 28, apartado 1, letras a) y b).

2. Las autoridades competentes podrán facilitar a la REGRT de Electricidad y a la entidad de los GRD de la UE una cartografía de los controles establecidos en el artículo 28, apartado 1, letras a) y b), con una referencia a los marcos legislativos o reglamentarios nacionales correspondientes, incluidas las normas nacionales pertinentes de los Estados miembros con arreglo al artículo 25 de la Directiva (UE) 2022/2555. Si la autoridad competente de un Estado miembro facilita dicha cartografía, la REGRT de Electricidad y la entidad de los GRD de la UE integrarán esta cartografía nacional en la matriz cartográfica.

3. En un plazo de seis meses a partir de la elaboración de cada informe sobre la evaluación regional de riesgos para la ciberseguridad con arreglo al artículo 21, apartado 2, los GRT, con la asistencia de la REGRT de Electricidad, y en cooperación con la entidad de los GRD de la UE y en consulta con la ENISA, propondrán a la autoridad competente una modificación de la matriz cartográfica. La propuesta se realizará de conformidad con el artículo 8, apartado 10, y tendrá en cuenta los riesgos señalados en la evaluación regional de riesgos.

CAPÍTULO IV

RECOMENDACIONES SOBRE CONTRATACIÓN EN MATERIA DE CIBERSEGURIDAD

Artículo 35

Recomendaciones sobre contratación en materia de ciberseguridad

1. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, elaborarán, en un programa de trabajo que se establecerá y actualizará cada vez que se adopte un informe sobre la evaluación regional de riesgos para la ciberseguridad, conjuntos de recomendaciones no vinculantes sobre contratación en materia de ciberseguridad que las entidades de impacto alto y de impacto crítico puedan utilizar como base para la contratación de productos, servicios y procesos de TIC en los perímetros del impacto alto y de impacto crítico. Este programa de trabajo incluirá lo siguiente:

a) una descripción y clasificación de los tipos de productos, servicios y procesos de TIC utilizados por las entidades de impacto alto y de impacto crítico en el perímetro del impacto alto y del impacto crítico;

b) una lista de los tipos de productos, servicios y procesos de TIC para los que se elaborará un conjunto de recomendaciones no vinculantes en materia de ciberseguridad sobre la base de los informes pertinentes sobre las evaluaciones regionales de riesgos para la ciberseguridad y de las prioridades de las entidades de impacto alto y de impacto crítico.

2. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, facilitará a la ACER, en un plazo de seis meses a partir de la adopción o actualización del informe sobre la evaluación regional de riesgos para la ciberseguridad, un resumen del programa de trabajo mencionado.

3. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, se esforzarán por garantizar que las recomendaciones no vinculantes sobre contratación en materia de ciberseguridad elaboradas sobre la base de la evaluación regional pertinente de los riesgos para la ciberseguridad sean similares o comparables en todas las regiones de operación del sistema. Los conjuntos de recomendaciones sobre contratación en materia de ciberseguridad abarcarán, como mínimo, las especificaciones a que se refiere el artículo 33, apartado 2, letra a). En la medida de lo posible, las especificaciones se seleccionarán a partir de normas europeas e internacionales.

4. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, velarán por que los conjuntos de recomendaciones sobre contratación en materia de ciberseguridad:

a) cumplan los principios de la contratación con arreglo a la Directiva 2014/24/UE, y

b) sean compatibles con los esquemas europeos de certificación de la ciberseguridad más recientes disponibles pertinentes para el producto, servicio o proceso de TIC, y los tengan en cuenta.

Artículo 36

Orientaciones sobre el uso de los esquemas europeos de certificación de la ciberseguridad para la contratación de productos, servicios y procesos de TIC

1. Las recomendaciones no vinculantes sobre contratación en materia de ciberseguridad elaboradas con arreglo al artículo 35 podrán incluir orientaciones sectoriales específicas sobre el uso de los esquemas europeos de certificación de la ciberseguridad, siempre que se disponga de un esquema adecuado para un tipo de producto, servicio o proceso de TIC utilizado por las entidades de impacto crítico, sin perjuicio del marco para la creación de esquemas europeos de certificación de la ciberseguridad con arreglo al artículo 46 del Reglamento (UE) 2019/881.

2. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, cooperarán estrechamente con la ENISA al proporcionar las orientaciones sectoriales incluidas en las recomendaciones no vinculantes sobre contratación en materia de ciberseguridad con arreglo al apartado 1.

CAPÍTULO V

FLUJOS DE INFORMACIÓN, CIBERATAQUES Y GESTIÓN DE CRISIS

Artículo 37

Normas sobre la puesta en común de información

1. Si una autoridad competente recibe información relacionada con un ciberataque notificable, dicha autoridad competente:

a) evaluará el nivel de confidencialidad de la información e informará a la entidad del resultado de su evaluación sin demora indebida y, a más tardar, en un plazo de veinticuatro horas a partir de la recepción de la información;

b) intentará encontrar otros ciberataques similares en la Unión notificados a otras autoridades competentes, con el fin de correlacionar la información recibida en el contexto del ciberataque notificable con la información facilitada en el contexto de otros ciberataques y enriquecer la información existente, reforzar y coordinar las respuestas en materia de ciberseguridad;

c) será responsable de la eliminación de secretos comerciales y de la anonimización de la información de conformidad con las normas nacionales y de la Unión pertinentes;

d) compartirá la información con los puntos de contacto únicos nacionales, los CSIRT y todas las autoridades competentes designadas con arreglo al artículo 4 en otros Estados miembros sin demora indebida y a más tardar veinticuatro horas después de la recepción de un ciberataque notificable, y facilitará información actualizada periódicamente a dichas autoridades u organismos;

e) difundirá la información sobre el ciberataque, tras la anonimización y eliminación de secretos comerciales con arreglo al apartado 1, letra c), a las entidades de impacto crítico y de impacto alto de su Estado miembro sin demora indebida y a más tardar veinticuatro horas después de recibir la información con arreglo al apartado 1, letra a), y facilitará información actualizada periódicamente, de manera que las entidades puedan organizar su defensa de manera eficaz;

f) podrá solicitar a la entidad de impacto alto o de impacto crítico notificante que difunda la información sobre el ciberataque notificable de manera segura a otras entidades que puedan verse afectadas, a fin de poner al sector de la electricidad en conocimiento de la situación e impedir la materialización de un riesgo que pueda escalar hasta dar lugar a un incidente eléctrico transfronterizo de ciberseguridad;

g) compartirá con la ENISA un informe resumido, tras la anonimización y eliminación de secretos comerciales, con la información sobre el ciberataque.

2. Si un CSIRT tiene conocimiento de una vulnerabilidad aprovechada activamente no subsanada:

a) compartirá este conocimiento sin demora con la ENISA a través de un canal seguro adecuado de puesta en común de información, salvo que se especifique otra cosa en otros actos legislativos de la Unión;

b) ayudará a la entidad de que se trate para que el fabricante o proveedor le proporcione una gestión eficaz, coordinada y rápida de la vulnerabilidad aprovechada activamente no subsanada, o de medidas de mitigación eficaces y eficientes;

c) pondrá en común la información disponible con el vendedor y solicitará al fabricante o proveedor, en la medida de lo posible, que localice una lista de CSIRT de los Estados miembros afectados por la vulnerabilidad aprovechada activamente no subsanada y a los que se informará de ella;

d) pondrá en común la información disponible con los CSIRT determinados en el punto anterior, sobre la base del principio de necesidad de conocer;

e) compartirá, cuando existan, estrategias y medidas de mitigación de la vulnerabilidad aprovechada activamente no subsanada que se haya notificado.

3. Si una autoridad competente tiene conocimiento de una vulnerabilidad aprovechada activamente no subsanada, dicha autoridad competente:

a) compartirá, cuando existan, estrategias y medidas de mitigación de la vulnerabilidad aprovechada activamente no subsanada que se haya notificado, en coordinación con los CSIRT de su Estado miembro;

b) pondrá en común la información con un CSIRT del Estado miembro en el que se haya notificado la vulnerabilidad aprovechada activamente no subsanada.

4. Si la autoridad competente tiene conocimiento de una vulnerabilidad no subsanada, sin pruebas de que se esté aprovechando activamente en ese momento, se coordinará sin demora indebida con el CSIRT a efectos de la divulgación coordinada de vulnerabilidades, tal como se establece en el artículo 12, apartado 1, de la Directiva (UE) 2022/2555.

5. Si un CSIRT recibe información relacionada con ciberamenazas procedente de una o varias entidades de impacto alto o de impacto crítico con arreglo al artículo 38, apartado 6, difundirá dicha información o cualquier otra información importante para prevenir el riesgo relacionado con las ciberamenazas, detectarlo, responder a él o mitigarlo, a las entidades de impacto alto o de impacto crítico de su Estado miembro y, cuando proceda, a todos los CSIRT afectados y a su punto de contacto único nacional sin demora indebida y a más tardar cuatro horas después de recibir la información.

6. Si una autoridad competente tiene conocimiento de información relacionada con ciberamenazas procedente de una o varias entidades de impacto alto o de impacto crítico, transmitirá dicha información al CSIRT a efectos del apartado 5.

7. Las autoridades competentes podrán delegar total o parcialmente las responsabilidades contempladas en los apartados 3 y 4 en relación con una o varias entidades de impacto alto o de impacto crítico que operen en más de un Estado miembro en otra autoridad competente de uno de esos Estados miembros, previo acuerdo entre las autoridades competentes afectadas.

8. Los GRT, con la asistencia de la REGRT de Electricidad y en cooperación con la entidad de los GRD de la UE, desarrollarán una metodología de la escala de clasificación de los ciberataques a más tardar el 13 de junio de 2025. Los GRT, con la asistencia de la REGRT de Electricidad y de la entidad de los GRD de la UE, podrán solicitar a las autoridades competentes que consulten a la ENISA y a sus autoridades competentes encargadas de la ciberseguridad para que presten asistencia en el desarrollo de dicha escala de clasificación. La metodología ofrecerá la clasificación de la gravedad de un ciberataque con arreglo a cinco niveles; los dos niveles más altos serán «alto» y «crítico». La clasificación se basará en la evaluación de los siguientes parámetros:

a) el impacto potencial teniendo en cuenta los activos y perímetros expuestos determinados de conformidad con el artículo 26, apartado 4, letra c), y

b) la severidad del ciberataque.

9. A más tardar el 13 de junio de 2026, la REGRT de Electricidad, en colaboración con la entidad de los GRD de la UE, llevará a cabo un estudio de viabilidad para valorar la posibilidad de crear una herramienta común que permita a todas las entidades compartir información con las autoridades nacionales pertinentes, así como los costes financieros necesarios para desarrollar dicha herramienta.

10. El estudio de viabilidad abordará la posibilidad de que dicha herramienta común:

a) apoye a las entidades de impacto crítico y de impacto alto con información relacionada con la seguridad pertinente para las operaciones de flujos transfronterizos de electricidad, como la notificación en tiempo cuasirreal de ciberataques, las alertas tempranas relacionadas con cuestiones de ciberseguridad y las vulnerabilidades no divulgadas de los equipos en uso en el sistema eléctrico;

b) se mantenga en un entorno adecuado y altamente fiable;

c) permita la recogida de datos de las entidades de impacto crítico y de impacto alto y facilite la eliminación de información confidencial y la anonimización de los datos, así como su rápida difusión entre las entidades de impacto crítico y de impacto alto.

11. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE:

a) consultará a la ENISA y al Grupo de Cooperación SRI, a los puntos de contacto únicos nacionales y a los representantes de las principales partes interesadas al evaluar la viabilidad;

b) presentará los resultados del estudio de viabilidad a la ACER y al Grupo de Cooperación SRI.

12. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, podrá analizar y facilitar iniciativas propuestas por entidades de impacto crítico y de impacto alto a fin de evaluar y probar dichas herramientas para la puesta en común de información.

Artículo 38

Papel de las entidades de impacto alto y de impacto crítico en la puesta en común de información

1. Cada entidad de impacto alto y de impacto crítico:

a) establecerá, para todos los activos de su perímetro de ciberseguridad determinado con arreglo al artículo 26, apartado 4, letra c), al menos las capacidades de los centros operativos de ciberseguridad para:

   i) garantizar que las redes y los sistemas y aplicaciones de información pertinentes proporcionen registros de seguridad para la supervisión de la seguridad que permitan la detección de anomalías y recojan información sobre ciberataques,

   ii) supervisar la seguridad, incluida la detección de intrusiones y la evaluación de las vulnerabilidades de las redes y los sistemas de información,

   iii) analizar y, en caso necesario, adoptar todas las medidas necesarias bajo su responsabilidad y capacidad para proteger a la entidad,

   iv) participar en la recogida y puesta en común de información descritas en el presente artículo;

b) tendrá derecho a contratar la totalidad o parte de estas capacidades con arreglo a la letra a) a través de proveedores de servicios de seguridad gestionados; las entidades de impacto crítico y de impacto alto seguirán siendo responsables de los proveedores de servicios de seguridad gestionados y supervisarán sus esfuerzos;

c) designará un punto de contacto único a nivel de entidad para la puesta en común de información.

2. La ENISA podrá publicar orientaciones no vinculantes sobre el establecimiento de dichas capacidades o la subcontratación del servicio a proveedores de servicios de seguridad gestionados, como parte de la tarea definida en el artículo 6, apartado 2, del Reglamento (UE) 2019/881.

3. Cada entidad de impacto crítico y de impacto alto pondrá en común la información pertinente relacionada con un ciberataque notificable con sus CSIRT y su autoridad competente sin demora indebida y a más tardar cuatro horas después de tener conocimiento de que el incidente es notificable.

4. La información relacionada con un ciberataque se considerará notificable cuando este sea evaluado por la entidad afectada y el resultado sea una gravedad entre los niveles «alto» y «crítico» según la metodología de la escala de clasificación de los ciberataques con arreglo al artículo 37, apartado 8. El punto de contacto único a nivel de entidad designado con arreglo al apartado 1, letra c), comunicará la clasificación de incidentes.

5. Cuando las entidades de impacto crítico y de impacto alto notifiquen a un CSIRT información pertinente relacionada con vulnerabilidades aprovechadas activamente no subsanadas, este podrá transmitir dicha información a su autoridad competente. En vista del nivel de sensibilidad de la información notificada, el CSIRT podrá retener la información o retrasar su transmisión por motivos justificados relacionados con la ciberseguridad.

6. Cada entidad de impacto crítico y de impacto alto facilitará sin demora indebida a sus CSIRT cualquier información relacionada con una ciberamenaza notificable que pueda tener un efecto transfronterizo. La información relativa a una ciberamenaza se considerará notificable cuando se cumpla al menos una de las condiciones siguientes:

a) la información proporcionada es pertinente para otras entidades de impacto crítico y de impacto alto a fin de prevenir el impacto del riesgo, detectarlo, responder a él o mitigarlo;

b) las técnicas, tácticas y procedimientos determinados utilizados en el contexto de un ataque generan información como direcciones URL o IP comprometidas, *hashes* o cualquier otro atributo útil para contextualizar y correlacionar el ataque;

c) una ciberamenaza puede evaluarse y contextualizarse más en profundidad con información adicional facilitada por proveedores de servicios o terceros no sujetos al presente Reglamento.

7. Al poner en común información con arreglo al presente artículo, cada entidad de impacto crítico y de impacto alto especificará lo siguiente:

a) que la presentación de la información se realiza con arreglo al presente Reglamento;

b) si la información se refiere a:

   i) un ciberataque notificable contemplado en el apartado 3,

   ii) vulnerabilidades aprovechadas activamente no subsanadas que no son conocidas públicamente contempladas en el apartado 4,

   iii) una ciberamenaza notificable contemplada en el apartado 5;

c) en el caso de un ciberataque notificable, el nivel del ciberataque según la metodología de la escala de clasificación de los ciberataques contemplada en el artículo 37, apartado 8, e información que justifique esta clasificación, incluida al menos la gravedad del ciberataque.

8. Cuando una entidad de impacto crítico o de impacto alto notifique un incidente significativo con arreglo al artículo 23 de la Directiva (UE) 2022/2555 y la notificación del incidente con arreglo a dicho artículo contenga la información pertinente exigida en el apartado 3 del presente artículo, la notificación de la entidad con arreglo al artículo 23, apartado 1, de dicha Directiva constituirá una notificación de información con arreglo al apartado 3 del presente artículo.

9. Cada entidad de impacto crítico y de impacto alto informará a su autoridad competente o CSIRT señalando claramente la información específica que solo se pondrá en común con la autoridad competente o el CSIRT en los casos en que la puesta en común de información pueda ser fuente de un ciberataque. Cada entidad de impacto crítico y de impacto alto tendrá derecho a facilitar una versión no confidencial de la información al CSIRT competente.

Artículo 39

Detección de ciberataques y gestión de la información conexa

1. Las entidades de impacto crítico y de impacto alto desarrollarán las capacidades necesarias para gestionar los ciberataques detectados con el apoyo necesario de la autoridad competente pertinente, la REGRT de Electricidad y la entidad de los GRD de la UE. Las entidades de impacto crítico y de impacto alto podrán contar con el apoyo del CSIRT designado en sus respectivos Estados miembros como parte de la tarea asignada a los CSIRT por el artículo 11, apartado 5, letra a), de la Directiva (UE) 2022/2555. Las entidades de impacto crítico y de impacto alto aplicarán procesos eficaces para detectar los ciberataques que vayan a afectar o puedan afectar a los flujos transfronterizos de electricidad, clasificarlos y responder a ellos, con el fin de minimizar su impacto.

2. Si un ciberataque afecta a los flujos transfronterizos de electricidad, los puntos de contacto únicos a nivel de entidad de las entidades de impacto crítico y de impacto alto afectadas cooperarán para compartir información entre ellas, con la coordinación de la autoridad competente del Estado miembro en el que se haya notificado por primera vez el ciberataque.

3. Las entidades de impacto crítico y de impacto alto:

a) garantizarán que su propio punto de contacto único a nivel de entidad tenga acceso, cuando necesite conocerla, a la información que hayan recibido del punto de contacto único nacional a través de su autoridad competente;

b) a menos que ya se haya hecho con arreglo al artículo 3, apartado 4, de la Directiva (UE) 2022/2555, notificarán a la autoridad competente del Estado miembro en el que estén establecidas y al punto de contacto único nacional una lista de sus puntos de contacto únicos en materia de ciberseguridad a nivel de entidad:

   i) de los cuales dicha autoridad competente y dicho punto de contacto único nacional puedan esperar recibir información sobre ciberataques notificables,

   ii) a los cuales las autoridades competentes y los puntos de contacto únicos nacionales posiblemente tengan que facilitar información;

c) establecerán procedimientos de gestión de ciberataques para los ciberataques, incluidas las funciones y responsabilidades, tareas y reacciones basadas en la evolución observable del ciberataque dentro de los perímetros del impacto crítico y del impacto alto;

d) probarán los procedimientos generales de gestión de ciberataques al menos cada año probando al menos un escenario que afecte directa o indirectamente a los flujos transfronterizos de electricidad. Dicha prueba anual podrá ser realizada por entidades de impacto crítico y de impacto alto durante los ejercicios periódicos contemplados en el artículo 43. Cualquier actividad de respuesta a ciberataques en directo con unas consecuencias clasificadas al menos en la escala 2, según la metodología de la escala de clasificación de los ciberataques contemplada en el artículo 37, apartado 8, y cuyas causas raíz tengan que ver con la ciberseguridad, podrá servir de prueba anual del plan de respuesta a ciberataques.

4. Los Estados miembros también podrán delegar las tareas a que se refiere el apartado 1 en los centros de coordinación regionales, de conformidad con el artículo 37, apartado 2, del Reglamento (UE) 2019/943.

Artículo 40

Gestión de crisis

1. Cuando la autoridad competente determine que una crisis de electricidad está relacionada con un ciberataque que afecta a más de un Estado miembro, las autoridades competentes de los Estados miembros afectados, las autoridades competentes encargadas de la ciberseguridad, las autoridades competentes en materia de preparación frente a los riesgos y las autoridades de gestión de crisis de ciberseguridad en el ámbito de los SRI de los Estados miembros afectados crearán conjuntamente un grupo *ad hoc* de coordinación de crisis transfronterizas.

2. El grupo *ad hoc* de coordinación de crisis transfronterizas:

a) coordinará la recuperación eficiente y la ulterior difusión de toda la información pertinente en materia de ciberseguridad entre las entidades que intervienen en el proceso de gestión de crisis;

b) organizará la comunicación entre todas las entidades afectadas por la crisis y las autoridades competentes, con el fin de reducir los solapamientos y aumentar la eficiencia de los análisis y las respuestas técnicas para subsanar las crisis simultáneas de electricidad cuyas causas raíz tengan que ver con la ciberseguridad;

c) proporcionará, en cooperación con los CSIRT competentes, los conocimientos especializados necesarios, incluido el asesoramiento operativo sobre la aplicación de posibles medidas de mitigación dirigido a las entidades afectadas por el incidente;

d) notificará y proporcionará actualizaciones periódicas sobre el estado del incidente a la Comisión y al Grupo de Coordinación de la Electricidad, con arreglo a los principios de protección establecidos en el artículo 46;

e) recabará el asesoramiento de las autoridades, agencias o entidades pertinentes que puedan ayudar a mitigar la crisis de electricidad.

3. Cuando el ciberataque se considere un incidente de ciberseguridad a gran escala, o cuando se prevea que vaya a considerarse como tal, el grupo *ad hoc* de coordinación de crisis transfronterizas informará inmediatamente a las autoridades nacionales de gestión de crisis de ciberseguridad de conformidad con el artículo 9, apartado 1, de la Directiva (UE) 2022/2555 en los Estados miembros afectados por el incidente, así como a la Comisión y a la EU-CyCLONe. En tal situación, el grupo *ad hoc* de coordinación de crisis transfronterizas apoyará a la EU-CyCLONe en lo que respecta a las especificidades sectoriales.

4. Las entidades de impacto crítico y de impacto alto desarrollarán y tendrán a su disposición capacidades, directrices internas, planes de preparación y personal para participar en la detección y mitigación de crisis transfronterizas. La entidad de impacto crítico o de impacto alto afectada por una crisis simultánea de electricidad investigará las causas raíz de dicha crisis en cooperación con su autoridad competente para determinar en qué medida la crisis está relacionada con un ciberataque.

5. Los Estados miembros también podrán delegar las tareas contempladas en el apartado 4 en los centros de coordinación regionales, de conformidad con el artículo 37, apartado 2, del Reglamento (UE) 2019/943.

Artículo 41

Planes de gestión de crisis de ciberseguridad y de respuesta a estas

1. En un plazo de 24 meses a partir de la notificación a la ACER del informe sobre la evaluación de riesgos a escala de la Unión, la ACER, en estrecha cooperación con la ENISA, la REGRT de Electricidad, la entidad de los GRD de la UE, las autoridades competentes encargadas de la ciberseguridad, las autoridades competentes, las autoridades competentes en materia de preparación frente a los riesgos, las autoridades reguladoras nacionales y las autoridades nacionales de gestión de crisis de ciberseguridad en el ámbito de los SRI, elaborará un plan de gestión de crisis de ciberseguridad y de respuesta a estas a escala de la Unión para el sector de la electricidad.

2. En un plazo de 12 meses a partir de la elaboración por parte de la ACER del plan de gestión de la crisis de ciberseguridad y de respuesta a estas a escala de la Unión para el sector de la electricidad con arreglo al apartado 1, cada autoridad competente elaborará un plan nacional de gestión de crisis de ciberseguridad y de respuesta a estas para los flujos transfronterizos de electricidad teniendo en cuenta el plan de gestión de crisis de ciberseguridad a escala de la Unión y el plan nacional de preparación frente a los riesgos establecido de conformidad con el artículo 10 del Reglamento (UE) 2019/941. Este plan será coherente con el plan de respuesta a incidentes y crisis de ciberseguridad a gran escala con arreglo al artículo 9, apartado 4, de la Directiva (UE) 2022/2555. La autoridad competente se coordinará con las entidades de impacto crítico y de impacto alto y con la autoridad competente en materia de preparación frente a los riesgos de su Estado miembro.

3. El plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala exigido con arreglo al artículo 9, apartado 4, de la Directiva (UE) 2022/2555 se considerará un plan nacional de gestión de crisis de ciberseguridad con arreglo al presente artículo si incluye disposiciones de gestión de las crisis y de respuesta a estas para los flujos transfronterizos de electricidad.

4. Los Estados miembros también podrán delegar las tareas contempladas en los apartados 1 y 2 en los centros de coordinación regionales, de conformidad con el artículo 37, apartado 2, del Reglamento (UE) 2019/943.

5. Las entidades de impacto crítico y de impacto alto garantizarán que sus procesos de gestión de crisis relacionadas con la ciberseguridad:

a) cuenten con procedimientos compatibles de gestión de incidentes de ciberseguridad transfronterizos, tal como se define en el artículo 6, punto 8, de la Directiva (UE) 2022/2555, incorporados formalmente a sus planes de gestión de crisis;

b) formen parte de las actividades generales de gestión de crisis.

6. En un plazo de 12 meses a partir de la notificación de las entidades de impacto alto y de impacto crítico con arreglo al artículo 24, apartado 6, y posteriormente cada tres años, las entidades de impacto crítico y de impacto alto elaborarán un plan de gestión de crisis a nivel de entidad para una crisis relacionada con la ciberseguridad, que se incluirá en sus planes generales de gestión de crisis. El plan incluirá, como mínimo, lo siguiente:

a) las normas de declaración de crisis establecidas en el artículo 14, apartados 2 y 3, del Reglamento (UE) 2019/941;

b) funciones y responsabilidades claras para la gestión de crisis, incluido el papel de otras entidades pertinentes de impacto crítico y de impacto alto;

c) información de contacto actualizada, así como normas para la comunicación y la puesta en común de información durante una situación de crisis, incluida la conexión con los CSIRT.

7. Las medidas para la gestión de crisis con arreglo al artículo 21, apartado 2, letra c), de la Directiva (UE) 2022/2555 se considerarán un plan de gestión de crisis a nivel de entidad para el sector de la electricidad con arreglo al presente artículo si incluyen todos los requisitos mencionados en el apartado 6.

8. Los planes de gestión de crisis se probarán durante los ejercicios de ciberseguridad contemplados en los artículos 43, 44 y 45.

9. Las entidades de impacto crítico y de impacto alto incluirán sus planes de gestión de crisis a nivel de entidad en sus planes de continuidad de las actividades para los procesos de impacto crítico y de impacto alto. Los planes de gestión de crisis a nivel de entidad incluirán:

a) los procesos que dependan de la disponibilidad, integridad y fiabilidad de los servicios informáticos;

b) todas las ubicaciones relacionadas con la continuidad de las actividades, también las de los equipos y programas informáticos;

c) todas las funciones y responsabilidades internas relacionadas con los procesos de continuidad de las actividades.

10. Las entidades de impacto crítico y de impacto alto actualizarán sus planes de gestión de crisis a nivel de entidad al menos cada tres años y siempre que sea necesario.

11. La ACER actualizará el plan de gestión de crisis de ciberseguridad y de respuesta a estas a escala de la Unión para el sector de la electricidad elaborado con arreglo al apartado 1 al menos cada tres años y siempre que sea necesario.

12. Cada autoridad competente actualizará el plan nacional de gestión de crisis de ciberseguridad y de respuesta a estas para los flujos transfronterizos de electricidad elaborado con arreglo al apartado 2 al menos cada tres años y siempre que sea necesario.

13. Las entidades de impacto crítico y de impacto alto probarán sus planes de continuidad de las actividades al menos una vez cada tres años o después de que haya cambios importantes en un proceso de impacto crítico. Se documentará el resultado de las pruebas del plan de continuidad de las actividades. Las entidades de impacto crítico y de impacto alto podrán incluir la prueba de su plan de continuidad de las actividades en los ejercicios de ciberseguridad.

14. Las entidades de impacto crítico y de impacto alto actualizarán su plan de continuidad de las actividades siempre que sea necesario y al menos una vez cada tres años, teniendo en cuenta el resultado de la prueba.

15. Si una prueba detecta deficiencias en el plan de continuidad de las actividades, la entidad de impacto crítico y de impacto alto corregirá dichas deficiencias en un plazo de ciento ochenta días naturales a partir de la prueba y realizará una nueva prueba para demostrar que las medidas correctoras son eficaces.

16. Cuando una entidad de impacto crítico o de impacto alto no pueda corregir las deficiencias en un plazo de ciento ochenta días naturales, incluirá las razones en el informe que debe presentarse a su autoridad competente de conformidad con el artículo 27.

Artículo 42

Capacidades de alerta temprana en materia de ciberseguridad para el sector de la electricidad

1. Las autoridades competentes cooperarán con la ENISA para desarrollar capacidades de alerta temprana en materia de ciberseguridad como parte de la asistencia a los Estados miembros con arreglo al artículo 6, apartados 2 y 7, del Reglamento (UE) 2019/881.

2. Las capacidades de alerta temprana en materia de ciberseguridad permitirán a la ENISA, cuando lleve a cabo las tareas descritas en el artículo 7, apartado 7, del Reglamento (UE) 2019/881:

a) recoger información puesta en común voluntariamente por parte de:

   i) los CSIRT, las autoridades competentes,

   ii) las entidades contempladas en el artículo 2 del presente Reglamento,

   iii) cualquier otra entidad que desee poner en común información pertinente de forma voluntaria;

b) evaluar y clasificar la información recogida;

c) evaluar la información a la que tiene acceso la ENISA para determinar las condiciones de riesgo para la ciberseguridad y los indicadores pertinentes para determinados aspectos de los flujos transfronterizos de electricidad;

d) determinar las condiciones y los indicadores que suelen estar relacionados con los ciberataques en el sector de la electricidad;

e) definir si deben realizarse nuevos análisis y tomarse nuevas medidas preventivas mediante la evaluación y la determinación de los factores de riesgo;

f) informar a las autoridades competentes sobre los riesgos detectados y las medidas preventivas recomendadas específicas para las entidades afectadas;

g) informar a todas las entidades pertinentes contempladas en el artículo 2 sobre los resultados de la información evaluada de conformidad con las letras b), c) y d) del presente apartado;

h) incluir periódicamente la información pertinente en el informe sobre el conocimiento de la situación, emitido de conformidad con el artículo 7, apartado 6, del Reglamento (UE) 2019/881;

i) obtener, cuando sea posible, datos aplicables que indiquen una violación de la seguridad o un ciberataque potenciales («indicadores de compromiso») a partir de la información recogida.

3. Los CSIRT difundirán sin demora la información recibida de la ENISA a las entidades afectadas, en el marco de sus tareas definidas en el artículo 11, apartado 3, letra b), de la Directiva (UE) 2022/2555.

4. La ACER supervisará la eficacia de las capacidades de alerta temprana en materia de ciberseguridad. La ENISA asistirá a la ACER facilitando toda la información necesaria, con arreglo al artículo 6, apartado 2, y al artículo 7, apartado 1, del Reglamento (UE) 2019/881. El análisis de esta actividad de seguimiento formará parte de la supervisión con arreglo al artículo 12 del presente Reglamento.

CAPÍTULO VI

MARCO DEL EJERCICIO DE CIBERSEGURIDAD DE LA ELECTRICIDAD

Artículo 43

Ejercicios de ciberseguridad a nivel de entidad y de Estado miembro

1. A más tardar el 31 de diciembre del año siguiente a la notificación de las entidades de impacto crítico, y posteriormente cada tres años, cada entidad de impacto crítico llevará a cabo un ejercicio de ciberseguridad que incluya uno o varios escenarios con ciberataques que afecten directa o indirectamente a los flujos transfronterizos de electricidad y estén relacionados con los riesgos detectados durante las evaluaciones de riesgos para la ciberseguridad a nivel de Estado miembro y de entidad de conformidad con los artículos 20 y 27.

2. No obstante lo dispuesto en el apartado 1, la autoridad competente en materia de preparación frente a los riesgos, previa consulta a la autoridad competente y a la autoridad de gestión de crisis de ciberseguridad pertinente designada o establecida en la Directiva (UE) 2022/2555 con arreglo al artículo 9, podrá optar por organizar un ejercicio de ciberseguridad a nivel de Estado miembro, tal como se describe en el apartado 1, en lugar de a nivel de entidad. A este respecto, la autoridad competente informará a:

a) todas las entidades de impacto crítico de su Estado miembro, la autoridad reguladora nacional, los CSIRT y las autoridades competentes encargadas de la ciberseguridad a más tardar el 30 de junio del año anterior al ejercicio de ciberseguridad a nivel de entidad;

b) cada entidad que vaya a participar en el ejercicio de ciberseguridad a nivel de Estado miembro a más tardar seis meses antes de que tenga lugar el ejercicio.

3. La autoridad competente en materia de preparación frente a los riesgos, con el apoyo técnico de sus CSIRT, organizará el ejercicio de ciberseguridad descrito en el apartado 2 a nivel de Estado miembro de forma independiente o en el contexto de un ejercicio de ciberseguridad diferente en ese Estado miembro. Para poder agrupar estos ejercicios, la autoridad competente en materia de preparación frente a los riesgos podrá aplazar un año el ejercicio de ciberseguridad a nivel de Estado miembro a que se refiere el apartado 1.

4. Los ejercicios de ciberseguridad a nivel de entidad y de Estado miembro serán coherentes con los marcos nacionales de gestión de crisis de ciberseguridad de conformidad con el artículo 9, apartado 4, letra d), de la Directiva (UE) 2022/2555.

5. A más tardar el 31 de diciembre de 2026, y posteriormente cada tres años, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, facilitará una plantilla de escenarios para la realización de los ejercicios de ciberseguridad a nivel de entidad y de Estado miembro contemplados en el apartado 1. Esta plantilla tendrá en cuenta los resultados de la evaluación de riesgos para la ciberseguridad realizada más recientemente a nivel de entidad y de Estado miembro e incluirá criterios clave de éxito. La REGRT de Electricidad y la entidad de los GRD de la UE invitarán a la ACER y a la ENISA a participar en la elaboración de dicho modelo.

Artículo 44

Ejercicios de ciberseguridad regionales o transregionales

1. A más tardar el 31 de diciembre de 2029, y posteriormente cada tres años, en cada región de operación del sistema, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, organizará un ejercicio de ciberseguridad regional. Las entidades de impacto crítico de la región de operación del sistema participarán en el ejercicio de ciberseguridad regional. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, podrá organizar, en lugar de un ejercicio de ciberseguridad regional, un ejercicio de ciberseguridad transregional en más de una región operativa del sistema en el mismo período. El ejercicio debe tener en cuenta otras evaluaciones y escenarios de riesgos para la ciberseguridad existentes, desarrollados a nivel de la Unión.

2. La ENISA apoyará a la REGRT de Electricidad y a la entidad de los GRD de la UE en la preparación y organización del ejercicio de ciberseguridad regional o transregional.

3. La REGRT de Electricidad, en coordinación con la entidad de los GRD de la UE, informará a las entidades de impacto crítico que participarán en el ejercicio de ciberseguridad regional o transregional seis meses antes de la realización del ejercicio.

4. El organizador de un ejercicio periódico de ciberseguridad a nivel de la Unión con arreglo al artículo 7, apartado 5, del Reglamento (UE) 2019/881, o de cualquier ejercicio de ciberseguridad obligatorio relacionado con el sector de la electricidad dentro del mismo perímetro geográfico, podrá invitar a participar a la REGRT de Electricidad y a la entidad de los GRD de la UE. En tales casos no se aplicará la obligación del apartado 1, siempre que todas las entidades de impacto crítico de la región de operación del sistema participen en el mismo ejercicio.

5. Si la REGRT de Electricidad y la entidad de los GRD de la UE participan en el ejercicio de ciberseguridad contemplado en el apartado 4, podrán aplazar un año el ejercicio de ciberseguridad regional o transregional contemplado en el apartado 1.

6. A más tardar el 31 de diciembre de 2027, y posteriormente cada tres años, la REGRT de Electricidad, en coordinación con la entidad de los GRD de la UE, pondrá a disposición un modelo de ejercicio para la realización de los ejercicios de ciberseguridad regionales y transregionales. Esta plantilla tendrá en cuenta los resultados de la evaluación de riesgos para la ciberseguridad realizada más recientemente a nivel regional e incluirá criterios clave de éxito. La REGRT de Electricidad consultará a la Comisión y podrá recabar asesoramiento de la ACER, la ENISA y el Centro Común de Investigación sobre la organización y ejecución de los ejercicios de ciberseguridad regionales y transregionales.

Artículo 45

Resultado de los ejercicios de ciberseguridad a nivel de entidad, de Estado miembro, regional o transregional

1. A petición de una entidad de impacto crítico, los proveedores de servicios críticos participarán en los ejercicios de ciberseguridad contemplados en el artículo 43, apartados 1 y 2, y el artículo 44, apartado 1, cuando presten servicios para la entidad de impacto crítico en el ámbito correspondiente al alcance del ejercicio de ciberseguridad pertinente.

2. Los organizadores de los ejercicios de ciberseguridad contemplados en el artículo 43, apartados 1 y 2, y en el artículo 44, apartado 1, con el asesoramiento de la ENISA, si lo solicitan, y con arreglo al artículo 7, apartado 5, del Reglamento (UE) 2019/881, analizarán y finalizarán el ejercicio de ciberseguridad pertinente a través de un informe que resuma las lecciones aprendidas, dirigido a todos los participantes. El informe incluirá:

a) los escenarios de los ejercicios, los informes de las reuniones, las principales posiciones, los éxitos y las lecciones aprendidas en cualquier nivel de la cadena de valor de la electricidad;

b) si se cumplieron los criterios clave de éxito;

c) una lista de recomendaciones para que las entidades participantes en el ejercicio de ciberseguridad pertinente corrijan, adapten o modifiquen los procesos y procedimientos de las crisis de ciberseguridad, los modelos de gobernanza asociados y cualquier compromiso contractual existente con proveedores de servicios críticos.

3. Si así lo solicita la red de CSIRT o el Grupo de Cooperación SRI o la EU-CyCLONe, los organizadores de los ejercicios de ciberseguridad contemplados en el artículo 43, apartados 1 y 2, y en el artículo 44, apartado 1, compartirán el resultado del ejercicio de ciberseguridad pertinente. Los organizadores pondrán en común con cada entidad que participe en los ejercicios la información a que se refiere el apartado 2, letras a) y b), del presente artículo. Los organizadores compartirán la lista de recomendaciones a que se refiere dicho apartado, letra c), exclusivamente con las entidades destinatarias de las recomendaciones.

4. Los organizadores de los ejercicios de ciberseguridad contemplados en el artículo 43, apartados 1 y 2, y en el artículo 44, apartado 1, realizarán un seguimiento periódico con las entidades que participen en los ejercicios sobre la aplicación de las recomendaciones con arreglo al apartado 2, letra c), del presente artículo.

CAPÍTULO VII

PROTECCIÓN DE LA INFORMACIÓN

Artículo 46

Principios para la protección de la información intercambiada

1. Las entidades contempladas en el artículo 2, apartado 1, velarán por que la información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento solo sea accesible cuando sea necesario conocerla y de conformidad con las normas nacionales y de la Unión pertinentes en materia de seguridad de la información.

2. Las entidades contempladas en el artículo 2, apartado 1, velarán por que la información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento se trate y sea objeto de seguimiento durante su ciclo de vida completo, y por que solo pueda divulgarse al final de su ciclo de vida una vez anonimizada.

3. Las entidades contempladas en el artículo 2, apartado 1, velarán por que se adopten todas las medidas de protección de carácter organizativo y técnico necesarias para salvaguardar y proteger la confidencialidad, integridad, disponibilidad y no rechazo de la información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento, independientemente de los medios utilizados. Las medidas de protección:

a) serán proporcionadas;

b) tendrán en cuenta los riesgos para la ciberseguridad relacionados con amenazas conocidas pasadas y emergentes a las que pueda estar sujeta dicha información en el contexto del presente Reglamento;

c) en la medida de lo posible, se basarán en normas y mejores prácticas nacionales, europeas o internacionales;

d) estarán documentadas.

4. Las entidades contempladas en el artículo 2, apartado 1, velarán por que toda persona a la que se conceda acceso a la información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento sea informada de las normas de seguridad aplicables a nivel de entidad y de las medidas y procedimientos pertinentes para la protección de la información. Dichas entidades se asegurarán de que la persona en cuestión reconozca la responsabilidad de proteger la información siguiendo las instrucciones de la sesión informativa.

5. Las entidades contempladas en el artículo 2, apartado 1, velarán por que el acceso a la información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento se limite a las personas:

a) que estén autorizadas a acceder a dicha información según sus funciones y que se ciñan a la ejecución de las tareas asignadas;

b) cuyos principios éticos y de integridad haya podido evaluar la entidad, y para quienes no haya pruebas de resultados negativos en una comprobación de antecedentes realizada para evaluar la fiabilidad de la persona de conformidad con las mejores prácticas y los requisitos estándar de seguridad de la entidad y, en caso necesario, con las disposiciones legales y reglamentarias nacionales.

6. Las entidades contempladas en el artículo 2, apartado 1, deberán contar con el acuerdo escrito de la persona física o jurídica que haya creado o facilitado originalmente la información, antes de facilitar dicha información a un tercero que no entre en el ámbito de aplicación del presente Reglamento.

7. Una entidad contemplada en el artículo 2, apartado 1, podrá considerar que esta información deberá ponerse en común sin cumplir lo dispuesto en los apartados 1 y 4 del presente artículo para evitar una crisis simultánea de electricidad cuyas causas raíz tengan que ver con la ciberseguridad o cualquier crisis transfronteriza dentro de la Unión en otro sector. En tal caso:

a) consultará a la autoridad competente y esta deberá autorizarla a poner en común dicha información;

b) anonimizará dicha información sin perder los elementos necesarios para informar al público de un riesgo inminente y grave para los flujos transfronterizos de electricidad, así como de las posibles medidas de mitigación;

c) salvaguardará la identidad del originador y de las entidades que hayan tratado dicha información con arreglo al presente Reglamento.

8. No obstante lo dispuesto en el apartado 6 del presente artículo, las autoridades competentes podrán proporcionar la información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento a un tercero no contemplado en el artículo 2, apartado 1, sin el consentimiento previo por escrito del originador de la información, pero informándole lo antes posible. Antes de divulgar cualquier información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento a un tercero no contemplado en el artículo 2, apartado 1, la autoridad competente interesada se asegurará razonablemente de que el tercero interesado tenga conocimiento de las normas de seguridad vigentes, y recibirá garantías razonables de que el tercero en cuestión puede proteger la información recibida de conformidad con los apartados 1 a 5 del presente artículo. La autoridad competente anonimizará dicha información sin perder los elementos necesarios para informar al público de un riesgo inminente y grave para los flujos transfronterizos de electricidad, así como de las posibles medidas de mitigación, y salvaguardará la identidad del originador de la información. En tal caso, el tercero no contemplado en el artículo 2, apartado 1, protegerá la información recibida de conformidad con las disposiciones ya vigentes a nivel de entidad o, cuando ello no sea posible, con las disposiciones e instrucciones proporcionadas por la autoridad competente pertinente.

9. El presente artículo no se aplicará a las entidades no contempladas en el artículo 2, apartado 1, a las que se facilite información con arreglo al apartado 6 del presente artículo. En este caso, se aplicará el apartado 7 del presente artículo, o la autoridad competente podrá facilitar a dicha entidad disposiciones por escrito para su aplicación en los casos en que se reciba información con arreglo al presente Reglamento.

Artículo 47

Confidencialidad de la información

1. Toda información facilitada, recibida, intercambiada o transmitida con arreglo al presente Reglamento estará sujeta al secreto profesional establecido en los apartados 2 a 5 del presente artículo y a los requisitos establecidos en el artículo 65 del Reglamento (UE) 2019/943. Toda información facilitada, recibida, intercambiada o transmitida entre las entidades contempladas en el artículo 2 del presente Reglamento, a efectos de la ejecución del presente Reglamento, estará protegida teniendo en cuenta el nivel de confidencialidad de la información que aplique el originador.

2. La obligación de secreto profesional se aplicará a las entidades contempladas en el artículo 2.

3. Las autoridades competentes encargadas de la ciberseguridad, las autoridades reguladoras nacionales, las autoridades competentes en materia de preparación frente a los riesgos y los CSIRT intercambiarán toda la información necesaria para llevar a cabo sus tareas.

4. Toda información recibida, intercambiada o transmitida entre las entidades contempladas en el artículo 2, apartado 1, a efectos de la aplicación del artículo 23, será anonimizada y agregada.

5. La información recibida por cualquier entidad o autoridad sujeta al presente Reglamento en el ejercicio de sus funciones no podrá divulgarse a ninguna otra entidad u autoridad, sin perjuicio de los casos contemplados por el Derecho nacional, otras disposiciones del presente Reglamento, u otra legislación pertinente de la Unión.

6. Sin perjuicio de la legislación nacional o de la Unión, una autoridad, entidad o persona física que reciba información con arreglo al presente Reglamento no podrá utilizarla para fines distintos del ejercicio de sus funciones con arreglo al presente Reglamento.

7. La ACER, previa consulta a la ENISA, a todas las autoridades competentes, a la REGRT de Electricidad y a la entidad de los GRD de la UE, emitirá, a más tardar el 13 de junio de 2025, directrices que aborden mecanismos para que todas las entidades contempladas en el artículo 2, apartado 1, intercambien información, y en particular los flujos de comunicación previstos, así como métodos para anonimizar y agregar la información a efectos de la aplicación del presente artículo.

8. La información que sea confidencial con arreglo a las normas de la Unión y nacionales se intercambiará con la Comisión y otras autoridades pertinentes únicamente cuando ese intercambio sea necesario para la aplicación del presente Reglamento. La información que se intercambie se limitará a aquella que resulte necesaria y proporcionada para la finalidad del intercambio. El intercambio de información preservará la confidencialidad de esta y protegerá la seguridad y los intereses comerciales de las entidades de impacto crítico o de impacto alto.

CAPÍTULO VIII

DISPOSICIONES FINALES

Artículo 48

Disposiciones temporales

1. Hasta la aprobación de las condiciones o metodologías mencionadas en el artículo 6, apartado 2, o de los planes mencionados en el artículo 6, apartado 3, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, elaborará orientaciones no vinculantes sobre las siguientes cuestiones:

a) un índice provisional de impacto en la ciberseguridad de la electricidad con arreglo al apartado 2 del presente artículo;

b) una lista provisional de procesos de impacto alto y de impacto crítico a escala de la Unión con arreglo al apartado 4 del presente artículo, y

c) una lista provisional de las normas y controles europeos e internacionales exigidos por la legislación nacional pertinentes para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad con arreglo al apartado 6 del presente artículo.

2. A más tardar el 13 de octubre de 2024, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, elaborará una recomendación de un ECII provisional. La REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, notificará a las autoridades competentes el ECII provisional recomendado.

3. Cuatro meses después de la recepción del ECII provisional recomendado, o a más tardar el 13 de febrero de 2025, las autoridades competentes determinarán los candidatos a entidades de impacto alto e impacto crítico en su Estado miembro sobre la base del ECII recomendado, y elaborarán una lista provisional de entidades de impacto alto y de impacto crítico. Las entidades de impacto alto y de impacto crítico incluidas en la lista provisional pueden cumplir voluntariamente sus obligaciones establecidas en el presente Reglamento sobre la base de un principio de precaución. A más tardar el 13 de marzo de 2025, las autoridades competentes notificarán a las entidades incluidas en la lista provisional que han sido consideradas como entidades de impacto alto o de impacto crítico.

4. A más tardar el 13 de diciembre de 2024, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, elaborará una lista provisional de procesos de impacto alto y de impacto crítico a escala de la Unión. Las entidades notificadas con arreglo al apartado 3 que decidan voluntariamente cumplir sus obligaciones establecidas en el presente Reglamento sobre la base de un principio de precaución utilizarán la lista provisional de procesos de impacto alto y de impacto crítico para determinar los perímetros provisionales del impacto alto y del impacto crítico y los activos que deben incluirse en la primera evaluación de riesgos para la ciberseguridad a nivel de entidad.

5. A más tardar el 13 de septiembre de 2024, cada autoridad competente con arreglo al artículo 4, apartado 1, facilitará a la REGRT de Electricidad y a la entidad de los GRD de la UE una lista de su legislación nacional pertinente para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad.

6. A más tardar el 13 de junio de 2025, la REGRT de Electricidad, en cooperación con la entidad de los GRD de la UE, elaborará una lista provisional de las normas y controles europeos e internacionales exigidos por la legislación nacional pertinentes para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad, teniendo en cuenta la información facilitada por las autoridades competentes.

7. La lista provisional de normas y controles europeos e internacionales incluirá:

a) normas europeas e internacionales y la legislación nacional que proporcionen orientaciones sobre metodologías para la gestión de riesgos para la ciberseguridad a nivel de entidad, y

b) controles de ciberseguridad equivalentes a los controles que se espera formen parte de los controles mínimos y avanzados de ciberseguridad.

8. La REGRT de Electricidad y la entidad de los GRD de la UE tendrán en cuenta los puntos de vista aportados por la ENISA y la ACER al finalizar la lista provisional de normas. La REGRT de Electricidad y la entidad de los GRD de la UE publicarán en sus sitios web la lista transitoria de normas y controles europeos e internacionales.

9. La REGRT de Electricidad y la entidad de los GRD de la UE consultarán a la ENISA y a la ACER sobre las propuestas de orientaciones no vinculantes elaboradas con arreglo al apartado 1.

10. Hasta que los controles mínimos y avanzados de ciberseguridad se desarrollen con arreglo al artículo 29 y se adopten con arreglo al artículo 8, todas las entidades contempladas en el artículo 2, apartado 1, se esforzarán por aplicar progresivamente las orientaciones no vinculantes elaboradas con arreglo al apartado 1.

Artículo 49

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 11 de marzo de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN