I

(Resoluciones, recomendaciones y dictámenes)

RECOMENDACIONES

CONSEJO

RECOMENDACIÓN DEL CONSEJO

de 8 de diciembre de 2022

sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas

(Texto pertinente a efectos del EEE)

(2023/C 20/01)

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114 y su artículo 292, frases primera y segunda,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

(1) Con el fin de garantizar el funcionamiento del mercado interior, redunda en interés de todos los Estados miembros y de la Unión en su conjunto identificar con claridad y proteger las infraestructuras críticas pertinentes que prestan servicios esenciales dentro de dicho mercado, especialmente en sectores clave como la energía, la infraestructura digital, el transporte y el espacio, así como las infraestructuras críticas con una importancia transfronteriza significativa ([1]), cuya perturbación podría afectar de manera considerable a otros Estados miembros.

(2) La presente Recomendación, que es un acto no vinculante, demuestra la voluntad política de los Estados miembros de cooperar y su compromiso con las medidas recomendadas, que se destacan en un plan de cinco puntos publicado por la presidenta de la Comisión Europea, al tiempo que respeta plenamente las competencias de los Estados miembros. La presente Recomendación no afecta a la protección de los intereses esenciales de la seguridad nacional, la seguridad pública o la defensa de los Estados miembros y ninguno de estos últimos deberá compartir información que menoscabe de dichos intereses.

(3) Si bien la responsabilidad principal de garantizar la seguridad y la prestación de servicios esenciales a través de infraestructuras críticas corresponde a los Estados miembros y a los operadores de sus infraestructuras críticas, una mayor coordinación a escala de la Unión es adecuada especialmente a la luz de amenazas cambiantes que pueden afectar a varios Estados miembros a la vez, como la guerra de agresión rusa contra Ucrania y las campañas híbridas contra los Estados miembros, o afectar a la resiliencia y el buen funcionamiento de la economía, el mercado único y la sociedad de la Unión en su conjunto. Debe prestarse especial atención a las infraestructuras críticas situadas fuera del territorio de los Estados miembros, como las infraestructuras críticas submarinas o las infraestructuras energéticas en alta mar.

([1]) Los Estados miembros deben evaluar dicha importancia en consonancia con sus prácticas nacionales y pueden hacerlo basándose, entre otros factores, en una evaluación del riesgo y en el impacto o la naturaleza del acontecimiento.

(4) El Consejo Europeo, en sus Conclusiones de los días 20 y 21 de octubre de 2022, condenó con firmeza los actos de sabotaje contra infraestructuras críticas, como los llevados a cabo contra los gasoductos Nord Stream, y señaló que la Unión está decidida a dar respuesta a cualquier perturbación deliberada de infraestructuras críticas u otras acciones híbridas con una respuesta unida y decidida.

(5) En vista de la rápida evolución del panorama de amenazas, deben adoptarse medidas de mejora de la resiliencia con carácter prioritario en sectores clave, como la energía, la infraestructura digital, el transporte y el espacio, y en otros sectores pertinentes definidos por los Estados miembros. Dichas medidas deben centrarse en mejorar la resiliencia de las infraestructuras críticas, teniendo en cuenta los riesgos pertinentes, especialmente los efectos en cascada, la perturbación de la cadena de suministro, la dependencia, los efectos del cambio climático, los proveedores y socios poco fiables y las amenazas y campañas híbridas, incluida la manipulación de la información y las injerencias extranjeras. En lo que respecta a las infraestructuras críticas nacionales, habida cuenta de las posibles consecuencias, debe darse prioridad a las infraestructuras críticas de importancia transfronteriza significativa. Se anima a los Estados miembros a que, cuando proceda, adopten con carácter de urgencia dichas medidas de mejora de la resiliencia, manteniendo al mismo tiempo el enfoque establecido en el marco jurídico en evolución.

(6) La protección de las infraestructuras críticas europeas en los sectores de la energía y el transporte está actualmente regulada por la Directiva 2008/114/CE del Consejo ([2]), y la seguridad de las redes y sistemas de información en toda la Unión, centrada en las amenazas cibernéticas, está garantizada por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([3]). Con vistas a garantizar un mayor nivel común de resiliencia y protección de las infraestructuras críticas, la ciberseguridad y el mercado financiero, se está modificando y completando el marco jurídico vigente mediante la adopción de nuevas normas aplicables a las entidades críticas (la «Directiva REC»), normas reforzadas para un elevado nivel común de ciberseguridad en toda la Unión (la «Directiva SRI 2») y nuevas normas aplicables a la resiliencia operativa digital del sector financiero.

(7) Los Estados miembros, de conformidad con el Derecho de la Unión y el Derecho nacional, deberían utilizar todas las herramientas disponibles para avanzar y ayudar a reforzar la resiliencia física y cibernética. A este respecto, debe entenderse que las infraestructuras críticas comprenden las infraestructuras críticas pertinentes definidas por un Estado miembro a nivel nacional o las designadas como infraestructuras críticas europeas en virtud de la Directiva 2008/114/CE, así como las entidades críticas que deben definirse en virtud de la Directiva REC o, en su caso, las entidades en virtud de la Directiva SRI 2. El concepto de resiliencia debe entenderse como la capacidad de prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación o recuperación de una infraestructura crítica frente a acontecimientos que perturben o puedan perturbar significativamente la prestación de servicios esenciales en el mercado interior, es decir, servicios que son fundamentales para mantener las funciones sociales y económicas vitales, la seguridad y la protección públicas, la salud de la población o el medio ambiente.

(8) Debe convocarse a expertos nacionales para coordinar el trabajo encaminado a lograr un nivel común más elevado de resiliencia y protección de las infraestructuras críticas que introducirán las nuevas normas aplicables a las entidades críticas. Ese trabajo coordinado posibilitaría la cooperación entre los Estados miembros y el intercambio de información relativa a actividades como la elaboración de metodologías para definir los servicios esenciales prestados por las infraestructuras críticas. La Comisión ya ha comenzado a convocar a estos expertos y a facilitar su trabajo, y tiene la intención de proseguir esta labor. Una vez que la Directiva REC haya entrado en vigor y se haya creado un Grupo de Resiliencia de las Entidades Críticas en virtud de esa Directiva, dicho grupo deberá proseguir este trabajo anticipatorio de conformidad con sus funciones.

(9) Reconociendo el cambio en el panorama de amenazas, debe seguir desarrollándose el potencial de realizar pruebas de resistencia de las infraestructuras críticas a nivel nacional, ya que esas pruebas podrían ser útiles para mejorar la resiliencia de las infraestructuras críticas. En lo que se refiere a la importancia específica del sector de la energía y a las consecuencias a escala de la Unión derivadas de su posible perturbación, ese sector podría ser el que más se beneficiara de la realización de pruebas de resistencia basadas en principios establecidos de común acuerdo. Dichas pruebas de resistencia son competencia de los Estados miembros, que deben animar y apoyar a los operadores de infraestructuras críticas para que lleven a cabo esas pruebas cuando se consideren beneficiosas, de conformidad con sus marcos jurídicos nacionales.

([2]) Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008, p. 75).

([3]) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

(10) A fin de garantizar una respuesta coordinada y eficaz a las amenazas actuales y previstas, se anima a la Comisión a prestar apoyo adicional a los Estados miembros, en particular facilitando la información pertinente en forma de sesiones informativas, manuales no vinculantes y directrices. El Servicio Europeo de Acción Exterior (SEAE), en particular a través del Centro de Inteligencia y de Situación de la UE y su Célula de Fusión contra las Amenazas Híbridas, con el apoyo de la Dirección de Inteligencia del Estado Mayor de la Unión Europea (EMUE) en el marco de la Capacidad Única de Análisis de Inteligencia (SIAC), debe proporcionar evaluaciones de las amenazas. También se invita a la Comisión a que, en cooperación con los Estados miembros, promueva la adopción de proyectos de investigación e innovación financiados por la Unión.

(11) Con la creciente interdependencia de las infraestructuras físicas y digitales, es posible que las actividades informáticas malintencionadas dirigidas a ámbitos críticos den lugar a perturbaciones o daños en las infraestructuras físicas, o que el sabotaje de infraestructuras físicas haga que los servicios digitales queden inaccesibles. Se invita a los Estados miembros a que aceleren lo antes posible los trabajos preparatorios para la transposición y aplicación del nuevo marco jurídico aplicable a las entidades críticas y el marco jurídico reforzado para la ciberseguridad, sobre la base de la experiencia adquirida en el Grupo de Cooperación establecido por la Directiva (UE) 2016/1148 (el «Grupo de Cooperación SRI»), pero teniendo en cuenta los plazos de transposición y que este trabajo de preparación debe avanzar de forma paralela y coherente.

(12) Además de mejorar la preparación, es importante reforzar las capacidades para responder con rapidez y eficacia en el caso de perturbación de los servicios esenciales prestados a través de infraestructuras críticas. Por consiguiente, la presente Recomendación contiene medidas a nivel de la Unión y nacional, en particular que destacan el papel de apoyo y el valor añadido que puede obtenerse mediante el establecimiento de una cooperación reforzada y el intercambio de información en el contexto del Mecanismo de Protección Civil de la Unión (MPCU), establecido por la Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo ([4]), y que utilizan los recursos pertinentes del Programa Espacial de la Unión establecido por el Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo ([5]).

(13) La Comisión, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (el «Alto Representante») y el Grupo de Cooperación SRI, en cooperación con los organismos y agencias civiles y militares pertinentes y las redes establecidas, como la red de organizaciones de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe), llevarán a cabo una evaluación de riesgos y elaborarán escenarios de riesgo. Por otra parte, tras el llamamiento ministerial conjunto de Nevers, el Grupo de cooperación SRI, con el apoyo de la Comisión y de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), y en colaboración con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), está realizando una evaluación de riesgos. Estos dos ejercicios serán coherentes y estarán coordinados con el ejercicio de elaboración de escenarios en el marco del MPCU, en particular los acontecimientos de ciberseguridad y su impacto en la vida real, que actualmente están desarrollando la Comisión y los Estados miembros. En interés de la eficiencia, la eficacia y la coherencia, y para la correcta aplicación de la presente Recomendación, los resultados de estos ejercicios deberían reflejarse a nivel nacional.

(14) Con el fin de reforzar de forma inmediata la preparación y la capacidad para responder a un incidente de ciberseguridad a gran escala, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros mediante financiación adicional asignada a la ENISA. Los servicios propuestos incluyen, entre otras cosas, actividades de preparación como pruebas de penetración de las entidades con el fin de detectar sus puntos vulnerables. El programa también puede reforzar las posibilidades de asistencia a los Estados miembros en caso de un incidente de ciberseguridad a gran escala que afecte a entidades críticas. Se trata de un primer paso en consonancia con las Conclusiones del Consejo, de 23 de mayo de 2022, sobre la elaboración de la posición de la Unión Europea en materia cibernética (las «Conclusiones del Consejo sobre la posición de la UE en materia de cibernética») que piden a la Comisión que presente una propuesta para un Fondo para Emergencias en materia de Ciberseguridad. Los Estados miembros deben aprovechar plenamente estas oportunidades, de conformidad con los requisitos aplicables, y se les anima a seguir trabajando en el ámbito de la gestión de crisis cibernéticas de la Unión, en particular supervisando periódicamente y haciendo balance de los progresos realizados en la aplicación de la hoja de ruta de gestión de crisis cibernéticas recientemente elaborada en el Consejo. Esa hoja de ruta es un documento vivo y debe revisarse y actualizarse cuando sea necesario.

([4]) Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (DO L 347 de 20.12.2013, p. 924).

([5]) Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo, de 28 de abril de 2021, por el que se crean el Programa Espacial de la Unión y la Agencia de la Unión Europea para el Programa Espacial y por el que se derogan los Reglamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 y (UE) n.º 377/2014 y la Decisión n.º 541/2014/UE (DO L 170 de 12.5.2021, p. 69).

(15) Los cables submarinos de comunicaciones mundiales son fundamentales para la conectividad mundial y dentro de la UE. Dada la gran longitud de estos cables y su instalación en el fondo marino, la vigilancia visual subacuática de la mayoría de las secciones de cable es extremadamente difícil. La jurisdicción compartida y otras cuestiones jurisdiccionales relacionadas con dichos cables constituyen una cuestión específica para la cooperación europea e internacional en materia de protección y recuperación de infraestructuras. Por ello, es necesario completar las evaluaciones de riesgos en curso y previstas relativas a las infraestructuras digitales y físicas que sustentan los servicios digitales con evaluaciones de riesgos específicas y opciones para medidas de mitigación con respecto a los cables submarinos de comunicaciones. Los Estados miembros invitan a la Comisión a llevar a cabo estudios con ese fin y a compartir sus conclusiones con los Estados miembros.

(16) Los sectores de la energía y el transporte también pueden verse afectados por las amenazas relacionadas con las infraestructuras digitales, por ejemplo, en relación con las tecnologías energéticas que incorporan componentes digitales. La seguridad de las cadenas de suministro asociadas es importante para la continuidad de la prestación de servicios esenciales y para el control estratégico de infraestructuras críticas en el sector de la energía. Estas circunstancias deben tenerse en cuenta a la hora de adoptar medidas para mejorar la resiliencia de las infraestructuras críticas de conformidad con la presente Recomendación.

(17) La importancia creciente de las infraestructuras espaciales, de los medios terrestres relacionados con el espacio, incluidas las instalaciones de producción, y de los servicios espaciales para las actividades relacionadas con la seguridad hace que sea esencial garantizar la resiliencia y la protección de los recursos espaciales, de los medios terrestres relacionados con el espacio y de los servicios espaciales de la Unión y dentro de esta. Por las mismas razones, en el marco de la presente Recomendación, también es esencial hacer un uso más estructurado de los datos y servicios espaciales proporcionados por los sistemas y programas espaciales para la vigilancia, el seguimiento y la protección de las infraestructuras críticas en otros sectores. La futura estrategia espacial de la UE para la seguridad y la defensa propondrá medidas adecuadas a este respecto, que deben tenerse en cuenta a la hora de aplicar la presente Recomendación.

(18) La cooperación internacional también es necesaria para abordar eficazmente los riesgos para las infraestructuras críticas, por ejemplo, en aguas internacionales. Por lo tanto, se invita a los Estados miembros a cooperar con la Comisión y el Alto Representante para adoptar determinadas medidas con vistas a lograr dicha cooperación, teniendo en cuenta que tales medidas solo deben adoptarse de conformidad con sus respectivas funciones y responsabilidades recogidas en el Derecho de la Unión, en particular las disposiciones de los Tratados relativas a las relaciones exteriores.

(19) Como se estableció en la Comunicación titulada «Contribución de la Comisión a la defensa europea», de 15 de febrero de 2022, en apoyo del documento «Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales», la Comisión evaluará las líneas de base sectoriales en materia de resiliencia híbrida en cooperación con el Alto Representante y los Estados miembros, detectando las lagunas y necesidades, así como las medidas para subsanarlas de aquí a 2023. Esa iniciativa debe servir de base para el trabajo que se realice en el marco de la presente Recomendación, contribuyendo a reforzar el intercambio de información y la coordinación de las acciones, en relación con un mayor refuerzo de la resiliencia, también de las infraestructuras críticas.

(20) La Estrategia de Seguridad Marítima de la Unión Europea de 2014 y su Plan de Acción revisado instaban a una mayor protección de las infraestructuras marítimas críticas, entre ellas, las submarinas, y en particular las infraestructuras de transporte marítimo, energía y comunicaciones, entre otras cosas aumentando el conocimiento de la situación marítima mediante la mejora de la interoperabilidad y un intercambio de información (obligatorio y voluntario) más ágil. En este momento, esa Estrategia y ese Plan de Acción están siendo actualizados e incluirán medidas reforzadas destinadas a proteger las infraestructuras marítimas críticas. Estas medidas deben completar la presente Recomendación.

(21) Reforzar la resiliencia de las infraestructuras críticas contribuye a la intensificación de los esfuerzos para hacer frente a las amenazas y las campañas híbridas contra la Unión y sus Estados miembros. La presente Recomendación se basa en la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Comunicación conjunta sobre la lucha contra las amenazas híbridas: Una respuesta de la Unión Europea». La medida n.º 1 de la Comunicación conjunta, a saber, el estudio sobre riesgos híbridos, desempeña un papel clave para determinar las vulnerabilidades que puedan afectar a las estructuras y redes nacionales y paneuropeas. Además, la aplicación de las Conclusiones del Consejo, de 21 de junio de 2022, sobre un marco para una respuesta coordinada de la UE a las campañas híbridas, permitirá una acción coordinada más enérgica mediante la aplicación del conjunto de instrumentos de la UE contra las amenazas híbridas en todos los ámbitos afectados.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

CAPÍTULO I: OBJETIVO, ÁMBITO DE APLICACIÓN Y DETERMINACIÓN DE PRIORIDADES

1) La presente Recomendación establece una serie de acciones específicas a escala nacional y de la Unión destinadas a apoyar y mejorar la resiliencia de las infraestructuras críticas, de carácter voluntario, que se centran en las infraestructuras críticas que tienen una importancia transfronteriza significativa y en sectores clave identificados, como la energía, las infraestructuras digitales, el transporte y el espacio. Esas acciones específicas consisten en la mejora de la preparación, la mejora de la respuesta y la cooperación internacional.

2) El intercambio de información a efectos de alcanzar los objetivos de la presente Recomendación, que es confidencial con arreglo al Derecho de la Unión y nacional aplicable, así como de las normas sobre el secreto comercial, se llevará a cabo entre la Comisión y otras autoridades pertinentes únicamente cuando tal intercambio sea necesario para la aplicación de la presente Recomendación. Esta Recomendación no afecta a la protección de los intereses esenciales de la seguridad nacional, la seguridad pública o la defensa de los Estados miembros y ninguno de estos últimos deberá compartir información que sea contraria a dichos intereses.

CAPÍTULO II: MEJORAR LA PREPARACIÓN

Acciones a escala de los Estados miembros

3) Los Estados miembros deben adoptar un enfoque que abarque todos los riesgos cuando actualicen sus evaluaciones de riesgos o sus análisis equivalentes existentes, en consonancia con la naturaleza cambiante de las amenazas actuales para sus infraestructuras críticas, especialmente en sectores clave identificados y, cuando sea posible, en todos los sectores que abarque el próximo nuevo marco jurídico aplicable a las entidades críticas.

4) Se invita a los Estados miembros a acelerar los trabajos preparatorios y adoptar medidas de mejora de la resiliencia, cuando sea posible, según lo dispuesto en el próximo marco jurídico aplicable a las entidades críticas, haciendo especial hincapié en la cooperación y el intercambio de información pertinente entre los Estados miembros y con la Comisión, en la identificación de entidades críticas con una importancia transfronteriza significativa y en el aumento del apoyo a las entidades críticas identificadas con el fin de mejorar su resiliencia.

5) Los Estados miembros deben apoyar la formación de los expertos, así como que realicen ejercicios e intercambien las buenas prácticas y enseñanzas extraídas. Los Estados miembros deben animar a los expertos a participar en las plataformas de formación existentes, tanto nacionales como internacionales, por ejemplo en el marco del Mecanismo de Protección Civil de la Unión.

6) Los Estados miembros deben animar y apoyar a los operadores de infraestructuras críticas, al menos en el sector de la energía, a realizar pruebas de resistencia, siguiendo los principios acordados conjuntamente a escala de la Unión, cuando ello resulte beneficioso. Las pruebas de resistencia deben evaluar la resiliencia de las infraestructuras críticas frente a las amenazas antagónicas de origen humano. Por lo tanto, los Estados miembros deben tratar de identificar las infraestructuras críticas pertinentes que deban someterse a dichas pruebas y consultar lo antes posible a los operadores de infraestructuras críticas pertinentes, a más tardar antes de que finalice el primer trimestre de 2023. Además, los Estados miembros deben ayudar a los operadores de infraestructuras críticas para que realicen esas pruebas lo antes posible e intenten completarlas antes de que finalice 2023, de conformidad con la legislación nacional. El Consejo tiene la intención de evaluar la situación de las pruebas de resistencia antes de finales de abril de 2023.

7) Dado que las amenazas para las infraestructuras críticas evolucionan rápidamente, es de vital importancia mantener el elevado nivel de protección de estas. Se anima a los Estados miembros a que asignen recursos financieros suficientes para reforzar las capacidades de sus autoridades nacionales pertinentes y a apoyarlas, para poder aumentar la resiliencia de las infraestructuras críticas. Asimismo se anima a los Estados miembros a asignar recursos financieros suficientes a las autoridades responsables de la gestión de incidentes de ciberseguridad a gran escala, a apoyarlas y a garantizar que sus equipos de respuesta a incidentes de seguridad informática (CSIRT) y sus autoridades competentes se movilicen plenamente en la red CSIRT y en EU-CyCLONe, respectivamente.

8) Se invita a los Estados miembros a que, de conformidad con los requisitos aplicables, aprovechen para ellos mismos las posibilidades de financiación que existan a nivel nacional y de la Unión para la mejora de la resiliencia de las infraestructuras críticas en la Unión y a que animen también a los operadores de infraestructuras críticas a que aprovechen dichas posibilidades de financiación, por ejemplo las redes transeuropeas, para hacer frente a toda la gama de amenazas significativas, en particular en el marco de los programas financiados por el Fondo de Seguridad Interior, creado mediante el Reglamento (UE) 2021/1149 del Parlamento Europeo y del Consejo ([6]), el Fondo Europeo de Desarrollo Regional, establecido por el Reglamento (UE) n.º 1301/2013 del Parlamento Europeo y del Consejo ([7]), el Mecanismo de Protección Civil de la Unión y el plan REPowerEU de la Comisión. También se anima a los Estados miembros a que hagan el mejor uso posible de los resultados obtenidos de proyectos pertinentes en el marco de programas de investigación, como Horizonte Europa, creado por el Reglamento (UE) 2021/695 del Parlamento Europeo y del Consejo ([8]).

9) En cuanto a la infraestructura de redes y comunicaciones en la Unión, se invita al Grupo de cooperación SRI a que, actuando de conformidad con el artículo 11 de la Directiva (UE) 2016/1148, acelere los trabajos en curso basados en el llamamiento ministerial conjunto de Nevers para realizar una evaluación específica del riesgo y a que presente las primeras recomendaciones lo antes posible. Esta evaluación de riesgos debe aportar información a la evaluación de riesgos cibernéticos intersectoriales en curso y a la elaboración de hipótesis que solicitó el Consejo en sus Conclusiones sobre la posición de la UE en materia cibernética. Además, esta labor debe realizarse garantizando la coherencia y la complementariedad con la labor realizada por el Grupo de Cooperación SRI en su línea de trabajo sobre la seguridad de la cadena de suministro de tecnologías de la información y la comunicación, así como por otros grupos pertinentes.

10) También se invita al Grupo de Cooperación SRI a que, con el apoyo de la Comisión y de la ENISA, prosiga su trabajo sobre la seguridad de la infraestructura digital, también en lo relativo a la infraestructura submarina, a saber los cables submarinos de comunicación. También se le invita a iniciar sus trabajos sobre el sector espacial, por ejemplo, cuando sea necesario, mediante la elaboración de orientaciones políticas y metodologías de gestión de riesgos de ciberseguridad basadas en un enfoque que abarque todos los riesgos y en un enfoque basado en el riesgo, dirigidas a los operadores del sector espacial con vistas a aumentar la resiliencia de las infraestructuras terrestres que dan apoyo a la prestación de servicios espaciales.

11) Los Estados miembros deben hacer pleno uso de los servicios de preparación en materia de ciberseguridad ofrecidos en el programa de apoyo a corto plazo de la Comisión ejecutado junto con la ENISA, por ejemplo las pruebas de penetración para detectar puntos vulnerables, y, en este contexto, se les anima a dar prioridad a las entidades que explotan infraestructuras críticas en los sectores de la energía, la infraestructura digital y el transporte.

12) Los Estados miembros deben hacer pleno uso del Centro Europeo de Competencia en Ciberseguridad. Los Estados miembros deben animar a sus centros nacionales de coordinación a colaborar de forma proactiva con los miembros de la comunidad de la ciberseguridad para desarrollar capacidades a escala de la Unión y nacional con el fin de prestar un mejor apoyo a los operadores de servicios esenciales.

13) Es importante que los Estados miembros logren la aplicación de las medidas recomendadas en el conjunto de instrumentos de la UE sobre ciberseguridad de las redes 5G y, en particular, que los Estados miembros impongan restricciones a los proveedores de alto riesgo, teniendo en cuenta que toda pérdida de tiempo puede aumentar la vulnerabilidad de las redes en la Unión, y también reforzar la protección física y no física de las partes críticas y sensibles de las redes 5G, también mediante estrictos controles de acceso. Además, los Estados miembros, en cooperación con la Comisión, deben evaluar la necesidad de medidas complementarias a fin de garantizar un nivel coherente de seguridad y resiliencia de las redes 5G.

14) Los Estados miembros, junto con la Comisión y la ENISA, deben centrarse en la aplicación de las Conclusiones del Consejo de 17 de octubre de 2022 sobre la seguridad de las cadenas de suministro de las TIC.

([6]) Reglamento (UE) 2021/1149 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se crea el Fondo de Seguridad Interior (DO L 251 de 15.7.2021, p. 94).

([7]) Reglamento (UE) n.º 1301/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, sobre el Fondo Europeo de Desarrollo Regional y sobre disposiciones específicas relativas al objetivo de inversión en crecimiento y empleo y por el que se deroga el Reglamento (CE) n.º 1080/2006 (DO L 347 de 20.12.2013, p. 289).

([8]) Reglamento (UE) 2021/695 del Parlamento Europeo y del Consejo, de 28 de abril de 2021, por el que se crea el Programa Marco de Investigación e Innovación «Horizonte Europa», se establecen sus normas de participación y difusión, y se derogan los Reglamentos (UE) n.º 1290/2013 y (UE) n.º 1291/2013 (DO L 170 de 12.5.2021, p. 1).

15) Los Estados miembros deben tener en cuenta el próximo código de red para los aspectos de ciberseguridad de los flujos transfronterizos de electricidad [...] basándose en la experiencia adquirida con la aplicación de la Directiva (UE) 2016/1148 y las correspondientes orientaciones elaboradas por el Grupo de cooperación SRI, en particular, su documento de referencia sobre medidas de seguridad para operadores de servicios esenciales.

16) Los Estados miembros deben impulsar la utilización de Copernicus, Galileo y el sistema europeo de navegación por complemento geoestacionario (EGNOS) para la vigilancia, a fin de compartir la información pertinente con los expertos convocados de conformidad con el punto 15. Debe hacerse un buen uso de las capacidades que ofrece la comunicación gubernamental por satélite de la Unión (Govsatcom) del Programa Espacial de la Unión, para seguimiento de las infraestructuras críticas y apoyo a la predicción de las crisis y la respuesta a estas.

Acciones a escala de la Unión

17) Debe reforzarse el diálogo y la cooperación entre los expertos designados por los Estados miembros y con la Comisión para contribuir a mejorar la resiliencia física de las infraestructuras críticas, en particular:

a) contribuyendo a la preparación, el desarrollo y la promoción de herramientas comunes de carácter voluntario para ayudar a los Estados miembros a mejorar dicha resiliencia, incluidas metodologías e hipótesis de riesgo;

b) apoyando a los Estados miembros en la aplicación del nuevo marco jurídico aplicable a las entidades críticas, en particular animando a la Comisión a adoptar el acto delegado a su debido tiempo;

c) respaldando la realización de las pruebas de resistencia a que se refiere el punto 6, basadas en principios comunes, comenzando por las pruebas que se centran en las amenazas antagónicas de origen humano en el sector de la energía y posteriormente en otros sectores clave, así como apoyando y asesorando sobre la realización de dichas pruebas de resistencia, a petición de un Estado miembro;

d) haciendo uso de cualquier plataforma segura, una vez establecida por la Comisión, para recopilar, hacer balance y compartir, de forma voluntaria, las mejores prácticas, las enseñanzas extraídas de las experiencias nacionales y otra información relacionada con dicha resiliencia.

El trabajo de estos expertos designados debe prestar especial atención a las dependencias intersectoriales y a las infraestructuras críticas con una importancia transfronteriza significativa, y debe tener continuación en el Consejo y la Comisión, cuando proceda.

18) Se anima a los Estados miembros a hacer uso de cualquier apoyo ofrecido por la Comisión, por ejemplo mediante la elaboración de manuales y directrices, como un manual sobre la protección de las infraestructuras críticas y los espacios públicos contra los sistemas de aeronaves no tripuladas, y herramientas para la evaluación de riesgos. Se invita al SEAE, en particular a través del Centro de Inteligencia y de Situación de la UE y de su Célula de Fusión contra las Amenazas Híbridas, con el apoyo de la Dirección de Inteligencia del Estado Mayor de la Unión Europea (EMUE) en el marco de la Capacidad Única de Análisis de Inteligencia (SIAC), a realizar sesiones informativas sobre las amenazas a las infraestructuras críticas en la Unión con el fin de mejorar el conocimiento de la situación.

19) Los Estados miembros deben apoyar las acciones emprendidas por la Comisión para asimilar los resultados de los proyectos sobre la resiliencia de las infraestructuras críticas financiados en el marco de los programas de investigación e innovación de la Unión. El Consejo toma nota de la intención de la Comisión de aumentar, dentro del presupuesto asignado a Horizonte Europa en el marco financiero plurianual 2021-2027, la financiación destinada a dicha resiliencia, sin perjuicio de la financiación de otros proyectos de investigación e innovación relacionados con la seguridad civil en el marco de Horizonte Europa.

20) Respondiendo a la tarea encomendada en las Conclusiones del Consejo sobre la posición de la UE en materia cibernética, se invita a la Comisión, el Alto Representante y el Grupo de cooperación SRI a que, de conformidad con sus respectivas funciones y responsabilidades en virtud del Derecho de la Unión, intensifiquen los trabajos con las correspondientes redes y organismos civiles y militares para realizar evaluaciones de riesgos y elaborar hipótesis de riesgo de ciberseguridad, teniendo en cuenta en particular la importancia del sector de la energía, la infraestructura digital, el transporte y la infraestructura espacial y en las interdependencias entre sectores y Estados miembros. Este ejercicio debe tener en cuenta los riesgos conexos para las infraestructuras de las que dependen esos sectores. Cuando resulte beneficioso, la evaluación de riesgos y las hipótesis pueden realizarse de forma periódica y basarse en las evaluaciones de riesgos existentes o previstos en esos sectores y complementarlas evitando la duplicación, así como servir de base para los debates sobre cómo puede fortalecerse la resiliencia general de las entidades que explotan infraestructuras críticas y abordarse sus puntos vulnerables.

21) Se invita a la Comisión a que acelere, de conformidad con sus respectivas tareas en el marco de la gestión de crisis cibernéticas, sus actividades sobre el apoyo a la preparación y la respuesta de los Estados miembros frente a los incidentes de ciberseguridad a gran escala y, en particular a que:

a) lleve a cabo, con el fin de complementar las evaluaciones de riesgos pertinentes en el contexto de la seguridad de las redes y de la información, un estudio exhaustivo ([9]) que haga inventario de la infraestructura submarina, a saber los cables submarinos de comunicación, que conectan a los Estados miembros y a Europa a escala mundial, cuyos resultados deben compartirse con los Estados miembros;

b) apoye la preparación y la respuesta de los Estados miembros y las instituciones, órganos y organismos de la Unión frente a incidentes de ciberseguridad a gran escala o a incidentes graves, de conformidad con el marco jurídico reforzado en materia de ciberseguridad y otras normas pertinentes aplicables ([10]);

c) acelere el desarrollo del concepto principal del Fondo de Emergencia Cibernética a través de un debate adecuado con los Estados miembros.

22) Se anima a la Comisión a intensificar los trabajos relacionados con las medidas anticipatorias de cara al futuro, también en colaboración con los Estados miembros en virtud de los artículos 6 y 10 de la Decisión 1313/2013/UE, y en forma de planes de contingencia para apoyar la preparación operativa del Centro de Coordinación de la Repuesta a Emergencias (CECRE) y la respuesta a las interrupciones en las infraestructuras críticas; a aumentar las inversiones en enfoques preventivos y en la preparación de la población y a aumentar el apoyo relacionado con el desarrollo de capacidades en el marco de la Red de Conocimientos sobre Protección Civil de la Unión.

23) La Comisión debe fomentar el uso de los recursos de vigilancia de la Unión (Copernicus, Galileo y EGNOS) para ayudar a los Estados miembros en la vigilancia de infraestructuras críticas y, cuando proceda, a sus vecinos inmediatos, y para respaldar otras opciones de vigilancia previstas en el Programa Espacial de la Unión, como el conocimiento situacional espacial y los marcos de vigilancia y seguimiento espacial de la UE.

24) Cuando sea pertinente y, de conformidad con sus respectivos mandatos, se invita a las agencias de la Unión y a otros órganos pertinentes a que presten apoyo en cuestiones relacionadas con la resiliencia de las infraestructuras críticas, en particular, de la siguiente manera:

a) la Agencia de la Unión Europea para la Cooperación Policial (Europol), en relación con la recopilación de información, el análisis en materia penal y el apoyo a las investigaciones en las acciones policiales transfronterizas y, cuando proceda y sea pertinente, la puesta en común de los resultados con los Estados miembros;

b) la Agencia Europea de Seguridad Marítima (AESM), en cuestiones relacionadas con la seguridad y la protección del sector marítimo en la Unión, incluidos los servicios de vigilancia marítima para asuntos relacionados con la seguridad y protección marítimas;

c) la Agencia de la Unión Europea para el Programa Espacial (EUSPA) y el Centro de Satélites de la Unión Europea (Satcen) pueden prestar asistencia mediante operaciones en el marco del Programa Espacial de la Unión;

d) el Centro Europeo de Competencia en Ciberseguridad, en relación con las actividades relativas a la ciberseguridad, también en cooperación con la Agencia de la Unión Europea para la Ciberseguridad (ENISA), podría fomentar la innovación y la política industrial en materia de ciberseguridad.

([9]) En este estudio debe incluirse una cartografía de sus capacidades y duplicaciones, sus puntos vulnerables, las amenazas y los riesgos para la disponibilidad de los servicios, el impacto de la interrupción en el funcionamiento de los cables submarinos (transatlánticos) para los Estados miembros y la Unión en su conjunto y la mitigación de riesgos, teniendo en cuenta al mismo tiempo la sensibilidad de dicha información y la necesidad de protegerla.

([10]) También debe prestarse especial atención a todas las actividades encaminadas a la preparación de una respuesta coordinada eficaz a escala de la Unión en caso de un incidente de ciberseguridad transfronterizo grave o de una amenaza conexa que pudiera tener un impacto sistémico en el sector financiero de la Unión, según lo dispuesto en el nuevo marco jurídico sobre resiliencia operativa digital.

CAPÍTULO III: MEJORAR LA RESPUESTA

Acciones a escala de los Estados miembros

25) Se invita a los Estados miembros a:

a) seguir coordinando su respuesta, cuando proceda, y mantener la perspectiva general de la respuesta intersectorial a las perturbaciones de servicios esenciales prestados por infraestructuras críticas. Esto podría hacerse en el marco de un futuro plan rector sobre una respuesta coordinada a las perturbaciones importantes de infraestructuras críticas con una importancia transfronteriza significativa; mediante los existentes Dispositivos de Respuesta Política Integrada a las Crisis (Dispositivos RPIC), para la coordinación de la respuesta política en lo que se refiere a las infraestructuras críticas con importancia transfronteriza; a través del plan rector sobre incidentes y crisis de ciberseguridad a gran escala con arreglo la Recomendación (UE) 2017/1584 de la Comisión ([11]); mediante EU-CyCLONe; a través del marco para una respuesta coordinada de la UE a las campañas híbridas y el conjunto de instrumentos híbridos de la UE en caso de amenazas y campañas híbridas y con el sistema de alerta rápida en caso de desinformación.

b) aumentar el intercambio de información con el Centro de Coordinación de la Respuesta a Emergencias (CECRE) a nivel operativo, en el contexto del Mecanismo de Protección Civil de la Unión (MPCU), con el fin de mejorar la alerta temprana y coordinar su respuesta mediante dicho Mecanismo en caso de que se produzcan perturbaciones de infraestructuras críticas con importancia transfronteriza significativa, garantizando así una reacción más rápida propiciada por la Unión cuando sea necesario;

c) mejorar su preparación para responder, cuando proceda, a través de instrumentos existentes o que se desarrollen en el futuro, a las perturbaciones significativas a que se refiere la letra a);

d) colaborar para seguir desarrollando las capacidades de respuesta pertinentes en la Reserva Europea de Protección Civil y rescEU;

e) alentar a los operadores de infraestructuras críticas y a las correspondientes autoridades nacionales a mejorar sus capacidades para poder restablecer rápidamente el funcionamiento básico de los servicios esenciales prestados por dichos operadores de infraestructuras críticas;

f) animar a los operadores de infraestructuras críticas a que, cuando reconstruyan su infraestructura crítica, lo hagan de tal modo que esta sea lo más resiliente posible, teniendo en cuenta la proporcionalidad de las medidas respecto de las evaluaciones de riesgos y los costes, y tomando en consideración toda la gama de riesgos significativos que puedan afectarle, incluso en escenarios climáticos adversos.

26) Se invita a los Estados miembros a que, cuando sea posible, aceleren los trabajos preparatorios de conformidad con el marco jurídico reforzado en materia de ciberseguridad, con el objetivo de mejorar las capacidades de los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT), teniendo en cuenta las nuevas tareas de estos equipos y el aumento del número de entidades de nuevos sectores, revisando y actualizando oportunamente sus estrategias de ciberseguridad y adoptando lo antes posible, en caso de que aún no existan, planes nacionales de respuesta a incidentes y crisis de ciberseguridad.

27) Se invita a los Estados miembros a examinar, a nivel nacional, los medios más procedentes para garantizar que las partes interesadas pertinentes sean conscientes de la necesidad de impulsar la resiliencia de las infraestructuras críticas mediante la cooperación con proveedores y socios de confianza. Es importante invertir en capacidad adicional, especialmente en los sectores en los que la infraestructura actual se encuentra al final de su vida útil, por ejemplo, la infraestructura de cables submarinos de comunicaciones, para poder garantizar la continuidad de la prestación de servicios esenciales en caso de perturbaciones y reducir las dependencias no deseadas.

28) Se anima a los Estados miembros a prestar atención a la comunicación estratégica proactiva a nivel nacional en el contexto de la lucha contra las amenazas y campañas híbridas, teniendo en cuenta la posibilidad de que los adversarios puedan optar por la manipulación de información y la injerencia desde el extranjero, configurando los discursos en torno a incidentes dirigidos contra infraestructuras críticas.

Acciones a escala de la Unión

29) Se invita a la Comisión a que colabore estrechamente con los Estados miembros para seguir desarrollando los organismos, los instrumentos y las capacidades de respuesta pertinentes, con vistas a mejorar la preparación operativa para abordar los efectos inmediatos e indirectos de perturbaciones importantes de los servicios esenciales pertinentes prestados por infraestructuras críticas, en particular los expertos y los recursos disponibles a través de la Reserva Europea de Protección Civil y de rescEU en el marco del Mecanismo de Protección Civil de la Unión (MPCU) o futuros equipos de respuesta rápida híbrida.

([11]) 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).

30) Teniendo en cuenta la evolución del panorama de amenazas y en cooperación con los Estados miembros, se invita a la Comisión, en el contexto del Mecanismo de Protección Civil de la Unión (MPCU) a que:

a) analice y pruebe continuamente la adecuación y la preparación operativa de las capacidades de respuesta existentes;

b) supervise e identifique periódicamente las deficiencias en la capacidad de respuesta de la Reserva Europea de Protección Civil y de rescEU que pudieran ser importantes;

c) siga intensificando la colaboración intersectorial para garantizar una respuesta adecuada a escala de la Unión y organice cursos de formación o ejercicios periódicos para poner a prueba tal colaboración en cooperación con uno o varios Estados miembros;

d) siga desarrollando el Centro de Coordinación de la Respuesta a Emergencias (CECRE) como centro de emergencia intersectorial a escala de la Unión para la coordinación de la ayuda a los Estados miembros afectados.

31) El Consejo se ha comprometido a iniciar trabajos con vistas a la aprobación de un plan rector de respuesta coordinada a las perturbaciones de las infraestructuras críticas con importancia transfronteriza significativa, que describa y establezca los objetivos y modos de cooperación entre los Estados miembros y las instituciones, órganos y organismos de la Unión en respuesta a incidentes contra tales infraestructuras críticas. El Consejo espera que la Comisión elabore un proyecto de dicho plan rector, sobre la base del apoyo y las contribuciones de las agencias pertinentes de la Unión. El plan rector será plenamente coherente e interoperable con el protocolo revisado de actuación conjunta de la Unión para contrarrestar las amenazas híbridas («EU Playbook»), tendrá en cuenta el actual plan rector de respuesta coordinada a incidentes ([12]) y crisis de ciberseguridad transfronterizos a gran escala y el mandato de EU CyCLONe establecido en la Directiva SRI 2 y evitará la duplicación de estructuras y actividades. Este plan rector deberá respetar plenamente el Dispositivo de Respuesta Política Integrada a las Crisis (Dispositivo RPIC) para la coordinación de la respuesta.

32) Se invita a Comisión a que consulte a las partes interesadas y los expertos pertinentes sobre las medidas adecuadas relativas a potenciales incidentes importantes en relación con las infraestructuras submarinas, que se presentarán junto con el inventario a que se refiere el punto 20, letra a), y a seguir elaborando planes de contingencia, hipótesis de riesgo y objetivos de resiliencia de la Unión ante catástrofes, según se establecen en la Decisión n.º 1313/2013/UE.

CAPÍTULO IV: COOPERACIÓN INTERNACIONAL

Acciones a nivel de los Estados miembros

33) Los Estados miembros deberán cooperar, cuando proceda y de conformidad con el Derecho de la Unión, con terceros países pertinentes en lo que respecta a la resiliencia de las infraestructuras críticas con importancia transfronteriza significativa.

34) Se anima a los Estados miembros a cooperar con la Comisión y el Alto Representante para abordar eficazmente los riesgos para las infraestructuras críticas en aguas internacionales.

35) Se invita a los Estados miembros a que contribuyan, en colaboración con la Comisión y el Alto Representante, al desarrollo y aplicación acelerados del conjunto de instrumentos de la UE contra las amenazas híbridas y las directrices de aplicación a que se refieren las Conclusiones del Consejo de 21 de junio de 2022 sobre un marco para una respuesta coordinada de la UE a las campañas híbridas, y posteriormente a utilizarlos, con el fin de dar pleno efecto al marco para una respuesta coordinada de la Unión a las campañas híbridas, en particular cuando consideren y preparen respuestas globales y coordinadas de la Unión a las campañas y amenazas híbridas, incluidas las dirigidas contra los operadores de infraestructuras críticas.

([12]) 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.

Acciones a escala de la Unión

36) Se invita a la Comisión y al Alto Representante a que apoyen, cuando proceda y de conformidad con sus respectivas funciones y responsabilidades en virtud del Derecho de la Unión, a los terceros países pertinentes para mejorar la resiliencia de infraestructuras críticas en su territorio y, en particular, de infraestructuras críticas que estén físicamente conectadas en su territorio y en el territorio de un Estado miembro.

37) La Comisión y el Alto Representante, en consonancia con sus respectivas funciones y responsabilidades en virtud del Derecho de la Unión, reforzarán la coordinación con la OTAN en materia de resiliencia de las infraestructuras críticas de interés común a través del diálogo estructurado UE-OTAN en materia de resiliencia, respetando plenamente las competencias de la Unión y de los Estados miembros de conformidad con los Tratados y los principios clave que rigen la cooperación UE-OTAN acordados por el Consejo Europeo, en particular la reciprocidad, la inclusividad y la autonomía decisoria. En este contexto, esa cooperación se impulsará en el marco del diálogo estructurado UE-OTAN sobre resiliencia, integrado en el mecanismo existente de interacción del personal para la aplicación de las declaraciones conjuntas, garantizando al mismo tiempo la plena transparencia y la participación de todos los Estados miembros.

38) Se invita a Comisión a considerar la participación de representantes de terceros países pertinentes, cuando sea adecuado y necesario, en el marco de la cooperación y el intercambio de información entre Estados miembros en el ámbito de la resiliencia de las infraestructuras críticas que estén físicamente conectadas al territorio de un Estado miembro y al de un tercer país.

Hecho en Bruselas, el 8 de diciembre de 2022.

Por el Consejo
El Presidente
V. RAKUŠAN