II

(Actos no legislativos)

RECOMENDACIONES

RECOMENDACIÓN (EU) 2021/1086 DE LA COMISIÓN

de 23 de junio de 2021

sobre la creación de una Unidad Cibernética Conjunta

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Considerando lo siguiente:

(1) La ciberseguridad es esencial para que la transformación digital de la economía y la sociedad se lleve a cabo con éxito. La UE se ha comprometido a movilizar unos niveles de inversión sin precedentes para apuntalar la confianza de los particulares, las empresas y las autoridades públicas en las herramientas digitales.

(2) La pandemia de COVID-19 ha incrementado la importancia de la conectividad y la dependencia de Europa de unas redes y unos sistemas de información estables, y ha puesto de manifiesto la necesidad de garantizar la protección a lo largo de toda la cadena de suministro. Disponer de redes y sistemas de información fiables y seguros es especialmente importante para las entidades que se encuentran en primera línea de batalla contra la pandemia, como los hospitales, los organismos sanitarios y los fabricantes de vacunas. La coordinación de los esfuerzos de la UE por prevenir, detectar, desalentar, disuadir, mitigar y responder a los ciberataques que tienen una mayor repercusión en dichas entidades podría evitar la pérdida de vidas humanas y neutralizar los intentos de socavar la capacidad de la UE para vencer a la pandemia lo más rápidamente posible. Por otra parte, el refuerzo de la capacidad de la UE para luchar contra los ciberataques contribuye eficazmente a impulsar un ciberespacio mundial, abierto, estable y seguro.

(3) Enfrentados a la naturaleza transfronteriza de las amenazas a la ciberseguridad y al continuo aumento de ataques más complejos, generalizados y específicos ([1]), las instituciones y agentes competentes en el ámbito de la ciberseguridad deben aumentar su capacidad de respuesta a tales amenazas y ataques aprovechando los recursos existentes y coordinando sus esfuerzos de forma más eficaz. Todos los agentes pertinentes de la UE deben estar preparados para ofrecer una respuesta colectiva y para intercambiar información atendiendo a la «necesidad de compartir», en lugar de a la «necesidad de conocer».

(4) Pese a los importantes avances logrados gracias a la cooperación entre los Estados miembros en materia de ciberseguridad, en particular a través del Grupo de cooperación («Grupo de cooperación SRI») y de la red de equipos de respuesta a incidentes de seguridad informática («red CSIRT», por sus siglas en inglés) creados en virtud de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([2]), todavía no existe una plataforma común de la UE en la que la información recopilada en las distintas comunidades de ciberseguridad pueda intercambiarse de manera eficiente y segura y en la que los agentes pertinentes puedan coordinar y movilizar sus capacidades operativas. Como consecuencia de ello, se corre el riesgo de abordar las amenazas e incidentes de seguridad en compartimentos estancos, lo que puede limitar la eficiencia e incrementar la vulnerabilidad. Además, no se dispone a escala de la UE de un canal para la cooperación técnica y operativa con el sector privado, ni en términos de puesta en común de información ni de apoyo a la respuesta ante incidentes.

([1]) Informe «Panorama de amenazas» de ENISA; Europol, Evaluación de 2020 de la amenaza de la delincuencia organizada en internet (IOCTA).

([2]) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a 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).

(5) Los marcos y estructuras en vigor y los recursos y conocimientos especializados de que disponen los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE proporcionan una base sólida para ofrecer una respuesta colectiva ante amenazas, incidentes y crisis de ciberseguridad ([3]). Desde el punto de vista operativo, la arquitectura en vigor incluye el Plan director de respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala («el Plan director») ([4]), la red CSIRT y la red europea de organizaciones de enlace de crisis cibernéticas («EU CyCLONe», por sus siglas en inglés) ([5]), así como el Centro Europeo de Ciberdelincuencia («EC3», por sus siglas en inglés) y el Grupo Conjunto sobre Ciberdelincuencia (J-CAT, por sus siglas en inglés) de la Agencia de la Unión Europea para la Cooperación Policial («Europol»), y el Protocolo de Respuesta Policial ante Emergencias de la UE. El Grupo de cooperación SRI, el Centro de Inteligencia y Situación de la UE («EU INTCEN», por sus siglas en inglés) así como el conjunto de instrumentos de ciberdiplomacia ([6]) y los proyectos relacionados con la ciberdefensa iniciados en el marco de la Cooperación Estructurada Permanente (CEP) ([7]) contribuyen también a la cooperación política y operativa entre las diferentes comunidades de ciberseguridad. La Agencia de la Unión Europea para la Ciberseguridad (ENISA), en virtud de su mandato reforzado, se encarga de apoyar la cooperación operativa ([8]) respecto de la ciberseguridad de las redes y sistemas de información, a los usuarios de dichos sistemas y a otras personas afectadas por amenazas e incidentes de ciberseguridad. A través del Dispositivo de Respuesta Política Integrada a las Crisis (RPIC), la UE es capaz de coordinar su respuesta política ante crisis de gran envergadura, incluso cuando se trata de ciberataques a gran escala.

(6) Sin embargo, todavía no existe un mecanismo para aprovechar los recursos existentes y que permita al conjunto de comunidades cibernéticas responsables de la seguridad de las redes y los sistemas de información prestarse asistencia mutua, con vistas a combatir la ciberdelincuencia, ejercer la ciberdiplomacia y, en su caso, proceder a la ciberdefensa en caso de crisis. Tampoco existe un mecanismo global a escala de la UE para la cooperación técnica y operativa de todas las comunidades en materia de conocimiento de la situación, preparación y respuesta. Además, es preciso lograr sinergias con las comunidades policial y de inteligencia a través de Europol e INTCEN, respectivamente.

(7) La Comisión, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE reconocen la importancia de analizar los puntos fuertes, las deficiencias, las lagunas y los solapamientos de la actual arquitectura de ciberseguridad de la UE, creada en los últimos años. En consulta con los Estados miembros, la Comisión, contando con la participación del Alto Representante, ha desarrollado el concepto de Unidad Cibernética Conjunta como respuesta a este análisis y como un componente importante de la Estrategia para una Unión de la Seguridad ([9]), la Estrategia Digital ([10]) y la Estrategia de Ciberseguridad ([11]).

([3]) La red europea de organizaciones de enlace para la gestión de cibercrisis (CyCLONe UE) fue creada por los Estados miembros en respuesta a la Recomendación del Plan director. Se trata de una red de expertos nacionales operativos y de gestión de crisis que la Comisión ha propuesto regular a través de la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148, COM (2020) 823 final, 2020/0359 (COD) propuesta en diciembre de 2020.

([4]) 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).

([5]) Esta recomendación tiene en cuenta el ejercicio de nivel operacional del Plan director («Blue OLEx», por sus siglas en inglés) 2020 tras el informe de actividades y, en particular, el resumen redactado por la presidencia tras el debate político estratégico sobre la Unidad Cibernética Conjunta.

([6]) Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»), de 19 de junio de 2017 (9916/17).

([7]) En particular, los proyectos de la CEP sobre «equipos de respuesta cibernética rápida y de asistencia mutua en ciberseguridad» coordinados por Lituania y sobre el «centro de coordinación en el ámbito de la ciberseguridad y la información» coordinado por Alemania.

([8]) El artículo 7 del 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) exige que la Agencia apoye la cooperación operativa entre los Estados miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas. Esto incluye el apoyo a los Estados miembros en lo que respecta a la cooperación operativa dentro de la red CSIRT, la elaboración de un informe periódico y detallado sobre la situación técnica de la ciberseguridad en la UE, relativo a los incidentes y amenazas en este ámbito, y la contribución al desarrollo de una respuesta cooperativa a escala de la Unión y de los Estados miembros a los incidentes o crisis transfronterizos a gran escala. Además, ENISA contribuye a las actividades de formación de la Escuela Europea de Seguridad y Defensa (EESD).

([9]) Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, sobre la Estrategia de la UE para una Unión de la Seguridad, COM/2020/605 final.

([10]) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Configurar el futuro digital de Europa, COM/2020/67 final.

([11]) Comunicación conjunta al Parlamento Europeo y al Consejo: La Estrategia de Ciberseguridad de la UE para la Década Digital [JOIN (2020) 18 final].

(8) En caso de crisis, los Estados miembros deben poder confiar en la solidaridad de la UE, que adoptará la forma de asistencia coordinada, y que procederá también de las cuatro comunidades de ciberseguridad, es decir, la civil, la policial ([12]), la diplomática y, en su caso, la de defensa. El grado de intervención de los integrantes de una o varias comunidades puede depender de la naturaleza del incidente o de la crisis a gran escala y, por consiguiente, del tipo de contramedidas necesarias para responder a los mismos. Ante las amenazas, incidentes y crisis que surgen, los expertos con una formación sólida y el equipo técnico suponen unos activos esenciales que pueden contribuir a evitar perjuicios graves y lograr una recuperación eficaz. Por tanto, el núcleo de la Unidad Cibernética Conjunta estará constituido por capacidades técnicas y operativas claramente identificadas, principalmente expertos y equipos, listos para ser desplegados en los Estados miembros en caso de necesidad. Dentro de esa plataforma, los participantes se encontrarán en una posición privilegiada para fomentar y coordinar dichas capacidades a través de los equipos de reacción rápida de la UE en materia de ciberseguridad, garantizando al mismo tiempo las sinergias adecuadas con los proyectos cibernéticos ya existentes ejecutados en el marco de la CEP.

(9) La Unidad Cibernética Conjunta ofrece una plataforma virtual y física y no requiere la creación de un organismo independiente adicional. Su configuración no debe afectar a las competencias y poderes de las autoridades nacionales de ciberseguridad y las entidades pertinentes de la Unión. La Unidad Cibernética Conjunta debe estar fundamentada en memorandos de acuerdo entre sus participantes. Debe aprovechar las estructuras, recursos y capacidades existentes y añadirles valor en su calidad de plataforma para una cooperación operativa y técnica segura y rápida entre las entidades de la UE y las autoridades de los Estados miembros. También debe asociar a todas las comunidades de ciberseguridad, es decir, la civil, la policial, la diplomática y la de defensa. Los participantes en la plataforma deben desempeñar o bien una función operativa o bien una función de apoyo. Entre los participantes operativos deben figurar ENISA, Europol, el Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE (CERT-UE), la Comisión, el Servicio Europeo de Acción Exterior (incluido el INTCEN), la red de CSIRT y EU-CyCLONe. Entre los participantes de apoyo deben figurar la Agencia Europea de Defensa (AED), el presidente del Grupo de cooperación SRI, el presidente del Grupo horizontal sobre cuestiones cibernéticas del Consejo y un representante de los proyectos pertinentes de la CEP ([13]). Dado que los Estados miembros disponen de capacidades operativas y competencias para responder a las ciberamenazas, incidentes y crisis a gran escala, con vistas a alcanzar sus objetivos, los participantes en la plataforma deben recurrir en primer lugar a sus capacidades, aunque cuentan con la ayuda de las entidades de la Unión pertinentes.

(10) La Unidad Cibernética Conjunta debería imprimir un nuevo impulso al proceso iniciado en 2017 con el Plan director. Debería seguir dotando de operatividad a la arquitectura del Plan director y dar un paso decisivo hacia la creación de un marco europeo de gestión de crisis de ciberseguridad que sirva para identificar y mitigar los riesgos y amenazas y responder a ellos de forma coordinada y oportuna. Con este paso, la Unidad Cibernética Conjunta debería ayudar a la UE a responder a las amenazas actuales e inminentes.

(11) Mediante su participación en la Unidad Cibernética Conjunta, los participantes operativos y de apoyo deben poder colaborar con una gama más amplia de partes interesadas dentro del marco de respuesta a las crisis de ciberseguridad de la UE. En el ejercicio de sus funciones y dentro de los límites de sus mandatos, los participantes deben beneficiarse de una mejor preparación y un conocimiento de la situación mayor que abarque todos los aspectos relacionados con las amenazas e incidentes de ciberseguridad, e impulsar la adquisición de conocimientos especializados adicionales en materia de ciberseguridad. Por ejemplo, los participantes deberían tomar parte periódicamente en ejercicios entre las distintas comunidades, adquirir un papel claramente definido en el Plan de la UE de respuesta a las crisis, aumentar la visibilidad de sus acciones a través de una comunicación pública compartida y celebrar acuerdos de cooperación operativa con el sector privado. Paralelamente, la contribución a la Unidad Cibernética Conjunta debería permitir a los participantes reforzar las redes existentes, como por ejemplo la red de CSIRT y EU CyCLONe, al dotarlas de herramientas seguras de intercambio de información y mejores capacidades de detección (es decir, centros de operaciones de seguridad, «COS»), y aprovechar las capacidades operativas de la UE disponibles.

(12) Los participantes en la Unidad Cibernética Conjunta deben centrarse en la cooperación técnica y operativa, incluidas las operaciones conjuntas. Los participantes deben contribuir a dicha cooperación en la medida en que lo permitan sus mandatos. La cooperación debe desarrollarse a partir de los actuales esfuerzos y complementarlos. En función del tipo de cooperación que se ponga en práctica, podrán adherirse otros participantes.

([12]) También pertinente para la cooperación judicial.

([13]) Véase la nota 5 a pie de página. El SEAE y la AED, a través de la función de Secretaría de la CEP que desempeñan, colaborarán con los coordinadores de los proyectos pertinentes de la CEP.

(13) La plataforma debe reunir a expertos técnicos y operativos en el ámbito de la gestión de crisis de los Estados miembros y de las entidades de la UE con el fin de coordinar las respuestas a las amenazas, incidentes y crisis de ciberseguridad haciendo uso de las capacidades y los conocimientos técnicos disponibles. Los expertos que participen en la Unidad Cibernética Conjunta podrán vigilar y proteger una superficie de ataque mucho más extensa mediante la utilización tanto de la plataforma física como de la virtual. A tal fin, los participantes deben coordinar sus esfuerzos en caso de incidentes y crisis transfronterizos, así como la prestación de asistencia a los países afectados a través de la plataforma.

(14) La creación de la Unidad Cibernética Conjunta exige un proceso gradual que aproveche y consolide los marcos y estructuras existentes mencionados en la presente Recomendación, como por ejemplo los mecanismos de colaboración establecidos en los foros dirigidos por los Estados miembros (por ejemplo, la red de CSIRT, EU CyCLONe, el Grupo horizontal sobre cuestiones cibernéticas del Consejo, el J-CAT y los proyectos pertinentes de la CEP), y, por parte de las instituciones, órganos y organismos de la UE, la cooperación estructurada entre ENISA y el CERT-UE, así como el Grupo Interinstitucional de Intercambio de Información sobre Ciberseguridad. Debe hacerse participar de forma adecuada a las estructuras para las amenazas híbridas, para la protección civil ([14]) y sectoriales ([15]). Del mismo modo, debe establecerse un vínculo estructurado con el Dispositivo de Respuesta Política Integrada a las Crisis (RPIC) ([16]). Con ello se logrará que, en caso de crisis, tenga lugar una transmisión rápida y eficaz de la información a los responsables políticos reunidos en el Consejo.

(15) Así pues, la creación de la Unidad Cibernética Conjunta debe seguir un proceso gradual y transparente que se completará a lo largo de los próximos dos años. Por esta razón, los objetivos establecidos en la presente Recomendación deben alcanzarse mediante un proceso en cuatro etapas, que se describe en el anexo de la presente Recomendación. En las dos primeras etapas, debería iniciarse y llevarse a cabo, en el marco de un grupo de trabajo que creará la Comisión, un proceso de preparación organizado y apoyado por ENISA en el que tomen parte participantes operativos y de apoyo a escala de la UE y de los Estados miembros. Los trabajos preparatorios deben guiarse por los principios de compromiso mutuo, inclusión y creación de consenso. Debe fomentarse la implicación de todos los participantes, de modo que puedan expresarse diversas opiniones y posiciones y que se procure hallar soluciones que reciban el mayor apoyo posible. En función de las necesidades existentes y en circunstancias oportunamente justificadas, podrá adaptarse el calendario de las distintas etapas indicadas en la presente Recomendación.

(16) En la primera etapa, el proceso preparatorio debe comenzar con la identificación de las capacidades operativas pertinentes disponibles en la UE y la puesta en marcha de una evaluación de las funciones y responsabilidades de los participantes en la plataforma. La segunda etapa debe abarcar el desarrollo del Plan de la UE de respuesta a incidentes y crisis, que deberá estar en consonancia con el Plan director ([17]) y el Protocolo de Respuesta Policial ante Emergencias de la UE, el despliegue de las actividades relacionadas con la preparación y el conocimiento de la situación, en consonancia con el Reglamento de Ciberseguridad y el Reglamento Europol ([18]), y la conclusión de la evaluación de las funciones y responsabilidades de los participantes en la plataforma. El grupo de trabajo debe presentar los resultados de dicha evaluación a la Comisión y al Alto Representante, quienes a continuación los compartirán con el Consejo. La Comisión y el Alto Representante deben colaborar, en el marco de sus respectivas competencias, en la elaboración de un informe conjunto basado en dicha evaluación e invitar al Consejo a refrendarlo a través de conclusiones del Consejo.

(17) Tras este refrendo, la Unidad Cibernética Conjunta entrará en funcionamiento, de modo que puedan completarse las dos etapas restantes del proceso. En la tercera etapa, los participantes deben poder desplegar equipos de reacción rápida de la UE en el seno de la Unidad Cibernética Conjunta, de acuerdo con los procedimientos definidos en el Plan de la UE de respuesta a incidentes y crisis, sirviéndose tanto de la plataforma física como de la virtual y contribuyendo a diversos aspectos de la respuesta a incidentes (desde la comunicación pública hasta la recuperación tras el incidente). Por último, en la cuarta etapa, se invitará a las partes interesadas del sector privado, incluidos tanto los usuarios como los proveedores de soluciones y servicios de ciberseguridad, a colaborar con la plataforma, lo que permitirá a los participantes mejorar el intercambio de información y reforzar la respuesta coordinada de la UE ante amenazas e incidentes de ciberseguridad.

([14]) En este contexto, la Unidad Cibernética Conjunta debe establecer sinergias con el Mecanismo de Protección Civil de la UE (MPCU) a fin de mejorar la preparación y la respuesta europeas en caso de catástrofes y emergencias múltiples que incluyan un elemento cibernético.

([15]) Como, por ejemplo, el del sector financiero, contemplado en el Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo* [DORA].

([16]) Véase el considerando 5.

([17]) Véase la nota a pie de página 3.

([18]) Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).

(18) Al concluir este proceso, los participantes deberán elaborar un informe de actividad sobre los progresos realizados en la aplicación de las cuatro etapas previstas en la Recomendación, en el que se describan los logros y los retos, que deberá presentarse a la Comisión y al Alto Representante. Basándose en el informe, la Comisión y el Alto Representante deben llevar a cabo una evaluación de dichos resultados y extraer conclusiones para el futuro de la Unidad Cibernética Conjunta.

(19) La Comisión, ENISA, Europol y el CERT-UE deben prestar apoyo administrativo, financiero y técnico a la Unidad Cibernética Conjunta, tal como se establece en la sección IV de la presente Recomendación, en función del presupuesto y de los recursos humanos disponibles. El refuerzo de las capacidades operativas de ciberseguridad de las instituciones, órganos y organismos pertinentes de la UE será clave para garantizar una preparación y una sostenibilidad efectivas de la Unidad Cibernética Conjunta. La Comisión tiene la intención de garantizar que el próximo Reglamento sobre normas comunes vinculantes en materia de ciberseguridad destinadas a las instituciones, órganos y organismos de la UE (previsto para octubre de 2021) constituya la base jurídica para esta contribución en el caso del CERT-UE.

(20) Habida cuenta de que goza de un mandato reforzado en virtud del Reglamento (UE) 2019/881 («Reglamento sobre Ciberseguridad»), ENISA se encuentra en una posición privilegiada para organizar y apoyar la preparación de la Unidad Cibernética Conjunta, así como para contribuir a su puesta en funcionamiento. En consonancia con lo dispuesto en el Reglamento sobre Ciberseguridad, ENISA está implantado una oficina en Bruselas para apoyar su cooperación estructurada con el CERT-UE. Esa cooperación estructurada, que abarca el establecimiento de oficinas adyacentes, proporciona un marco útil para facilitar la creación de la Unidad Cibernética Conjunta, en particular mediante la implantación de un espacio físico en el que alojarla, que debe ponerse a disposición de los participantes en caso de necesidad, así como del personal de otras instituciones, órganos y organismos pertinentes de la UE. La plataforma física debe combinarse con una plataforma virtual compuesta por herramientas de colaboración y de puesta en común segura de la información. Estas herramientas aprovecharán la abundante información recopilada a través del Escudo Cibernético Europeo ([19]), en particular de los centros de operaciones de seguridad y de los centros de puesta en común y análisis de la información (CPCAI).

(21) El Protocolo de Respuesta Policial ante Emergencias de la UE para los ciberataques transfronterizos a gran escala, adoptado por el Consejo en 2018, otorga un papel clave al Centro Europeo de Lucha contra la Ciberdelincuencia de Europol («EC3») ([20]) como parte de la estructura del «Plan director». Dicho Protocolo permite a las autoridades policiales de la UE dar respuesta a los ataques transfronterizos a gran escala de carácter supuestamente malintencionado veinticuatro horas al día y siete días a la semana mediante una reacción y una evaluación rápidas, así como mediante el intercambio seguro y oportuno de información crítica para la coordinación eficaz de las respuestas a incidentes transfronterizos. El Protocolo desarrolla en mayor medida la colaboración con otras instituciones de la UE y los protocolos de crisis a escala de la UE, así como la cooperación con el sector privado en caso de crisis. La comunidad policial, con el apoyo de Europol cuando proceda, debe contribuir a la Unidad Cibernética Conjunta adoptando las medidas necesarias a lo largo del ciclo completo de investigación, en consonancia con los requisitos del marco para la justicia penal y los procedimientos aplicables en materia de tratamiento electrónico de pruebas. Europol viene prestando apoyo operativo y facilitando la cooperación operativa contra las ciberamenazas desde el inicio del EC3 en 2013. Europol debe apoyar a la plataforma de acuerdo con su mandato y con un enfoque policial basado en los servicios de inteligencia, aprovechando al mismo tiempo los conocimientos especializados, productos, instrumentos y servicios internos de todo tipo que sean útiles para dar respuesta al incidente o a la crisis.

(22) La Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, también exige a los Estados miembros que garanticen que disponen de un punto de contacto nacional operativo veinticuatro horas al día y siete días a la semana para el intercambio de información sobre las infracciones mencionadas en dicha Directiva. La red de puntos de contacto nacionales operativos también debe contribuir a la Unidad Cibernética Conjunta garantizando la participación, cuando proceda, de las autoridades policiales y judiciales de los Estados miembros.

(23) La comunidad de ciberdiplomacia de la UE contribuye a promover y proteger un ciberespacio mundial, abierto, estable y seguro, y a prevenir, disuadir y responder a las actividades informáticas malintencionadas a este respecto. En 2017, la UE estableció un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»). Este marco se integra en una política más amplia de la UE en materia de ciberdiplomacia. Contribuye a la prevención de conflictos y a una mayor estabilidad de las relaciones internacionales. Permite a la UE y a los Estados miembros, en cooperación con sus socios internacionales cuando proceda, aplicar todas las medidas de la Política Exterior y de Seguridad Común («PESC»), en consonancia con los respectivos procedimientos para su consecución, a fin de fomentar la cooperación, mitigar las amenazas e influir en los comportamientos malintencionados actuales y futuros, en su caso, en el ciberespacio. La comunidad de ciberdiplomacia debe cooperar en el marco de la Unidad Cibernética Conjunta utilizando y apoyando el recurso a toda la gama de medidas diplomáticas disponible, en particular en lo que se refiere a la comunicación pública, apoyando el conocimiento de la situación compartido y el compromiso con terceros países en caso de crisis.

([19]) JOIN/2020/18 final, apartado 1.2.
([20]) Establecido mediante el Reglamento (UE) 2016/794.

(24) En consonancia con el marco del Plan director, el Alto Representante, también a través del INTCEN, debe contribuir a la Unidad Cibernética Conjunta proporcionando de forma permanente un conocimiento de la situación compartido y basado en los servicios de inteligencia respecto de las amenazas ya existentes o emergentes, incluido el conocimiento estratégico de la situación necesario en relación con un acontecimiento determinado.

(25) En el seno de la comunidad de ciberdefensa, la UE y los Estados miembros aspiran a reforzar las capacidades de ciberdefensa y a intensificar las sinergias, la coordinación y la cooperación entre las instituciones, órganos y organismos pertinentes de la UE, así como con y entre los Estados miembros, también en lo que respecta a las misiones y operaciones de la Política Común de Seguridad y Defensa (PCSD). Las funciones de esta comunidad se basan en una gobernanza intergubernamental a escala de la UE, en estructuras de mando militar nacionales y en capacidades y activos militares o de doble uso. Habida cuenta de su diferente naturaleza, deben crearse interfaces específicas con la Unidad Cibernética Conjunta para permitir el intercambio de información con la comunidad de ciberdefensa ([21]).

(26) La Cooperación Estructurada Permanente es un marco jurídico introducido por el Tratado de Lisboa ([22]) y establecido en 2017 en el marco de la Unión. La cooperación estructurada ha conducido al establecimiento de una serie de proyectos de CEP en el ámbito de la ciberseguridad, contribuyendo así al cumplimiento del compromiso 11 ([23]) de «garantizar mayores esfuerzos en la cooperación en materia de ciberdefensa, como el intercambio de información, la formación y el apoyo operativo». El SEAE con el Estado Mayor de la UE y la AED asumen la Secretaría de la CEP, que constituye un punto de contacto único dentro del marco de la Unión para todas las cuestiones vinculadas a la CEP, incluidas las funciones de apoyo y coordinación relacionadas con sus proyectos (por ejemplo, la evaluación de nuevas propuestas de proyectos, la preparación de los informes de situación de los proyectos, etc.). Los representantes de los proyectos pertinentes de la CEP deben apoyar a la Unidad Cibernética Conjunta, en particular en relación con el conocimiento de la situación y la preparación.

(27) A través de la Unidad Cibernética Conjunta, los participantes deben integrar de forma apropiada a las partes interesadas del sector privado, incluidos tanto los proveedores como los usuarios de soluciones y servicios de ciberseguridad, a fin de apoyar el marco europeo de gestión de crisis de ciberseguridad, prestando la debida atención al marco jurídico para la puesta en común de datos y la seguridad de la información. Los proveedores de ciberseguridad deben colaborar en la iniciativa mediante la puesta en común de información sobre amenazas y proporcionando expertos en respuesta a incidentes con el fin de ampliar rápidamente la capacidad de la Unidad para responder a los ataques y crisis a gran escala. Los usuarios de bienes y servicios de ciberseguridad, principalmente aquellos incluidos en el ámbito de aplicación de la Directiva SRI, deberían poder solicitar ayuda y asesoramiento a través de canales estructurados, actualmente inexistentes, que estarían vinculados a los centros de puesta en común y análisis de la información (ISAC) a escala de la UE ([24]). La plataforma podría contribuir asimismo a reforzar la cooperación con los socios internacionales.

(28) El desarrollo y mantenimiento del conocimiento de la situación requiere capacidades punteras de detección y prevención de intrusiones. La Unidad Cibernética Conjunta debe basarse en una red de vanguardia capaz de analizar las amenazas e incidentes malintencionados que puedan afectar a los principales sistemas de comunicación e información en la Unión en su conjunto. Esto significa que, a fin de mejorar la evaluación por parte de los participantes de la situación existente en la UE en materia de amenazas, es preciso incorporar a la Unidad Cibernética Conjunta, entre otras fuentes, los conocimientos sobre amenazas extraídos de las redes de comunicación supervisadas por los centros de operaciones de seguridad nacionales, sectoriales y transfronterizos.

(29) Con el fin de apoyar el intercambio de información operativa, posiblemente también la de carácter confidencial, la plataforma debe utilizar canales de comunicación que cumplan las condiciones de seguridad adecuadas. Estos canales también podrían desarrollarse a partir de la infraestructura ya implantada, como la Aplicación de la Red de Intercambio Seguro de Información («SIENA», por sus siglas en inglés) utilizada por Europol y la comunidad policial. Tal como se anunció en la Estrategia de Ciberseguridad, las herramientas utilizados por las instituciones, órganos y organismos de la UE deben respetar las normas sobre seguridad de la información que la Comisión propondrá en breve.

([21]) En particular, a través de la representación del SEAE, a fin de permitir la oportuna implicación de la comunidad de ciberdefensa, mediante contribuciones nacionales voluntarias.

([22]) Artículo 42, apartado 6, artículo 46 y Protocolo n.º 10 del TUE.

([23]) Cada uno de los Estados miembros que participan en la CEP asume 20 compromisos individuales, divididos en los cinco ámbitos clave establecidos en el artículo 2 del Protocolo n.º 10 sobre la Cooperación Estructurada Permanente anejo al Tratado de la Unión Europea.

([24]) Entre los ejemplos destacados de centros de puesta en común y análisis de la información existentes que podrían participar en este intercambio cabe citar el de la energía europea (EE-ISAC) o el las Instituciones Financieras Europeas (FI-ISAC).

(30) La Comisión, principalmente a través del programa Europa Digital, apoyará las inversiones necesarias para crear la plataforma física y virtual y desarrollar y mantener canales de comunicación y capacidades de formación seguros, así como para desarrollar y desplegar las capacidades de detección. Además, el Fondo Europeo de Defensa podría contribuir a financiar tecnologías y capacidades de ciberdefensa clave que reforzarían la preparación nacional en materia de ciberdefensa.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

I. **OBJETIVO DE LA RECOMENDACIÓN**

1) la finalidad de la presente Recomendación es determinar las acciones necesarias para coordinar los esfuerzos de la UE con vistas a la prevención, detección, desaliento, disuasión, mitigación y respuesta a los incidentes y crisis de ciberseguridad a gran escala a través de una Unidad Cibernética Conjunta. Para ello, la presente Recomendación define asimismo el proceso, los hitos y el calendario que deben seguir los Estados miembros y las instituciones, órganos y organismos de la UE pertinentes respecto de la creación y el desarrollo de dicha plataforma.

2) los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE deben garantizar que, en caso de que se produzcan incidentes y crisis de ciberseguridad a gran escala, coordinarán sus esfuerzos a través de una Unidad Cibernética Conjunta que permita la asistencia mutua ([25]) mediante los conocimientos especializados de las autoridades de los Estados miembros y de las instituciones, órganos y organismos pertinentes de la UE. La Unidad Cibernética Conjunta también debe permitir a los participantes cooperar con el sector privado.

II. **DEFINICIONES**

3) A efectos de la presente Recomendación, se entiende por:

a) «Plan de la UE de respuesta a incidentes y crisis de ciberseguridad»: compilación de funciones, modalidades y procedimientos que conduzca a la finalización del Marco de respuesta a las crisis de ciberseguridad de la UE descrito en el punto 1) de la Recomendación de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala («Plan director»).

b) «Comunidades de ciberseguridad»: grupos de colaboración en los ámbitos civil, policial, diplomático, y de defensa, que representan tanto a los Estados miembros como a las instituciones, órganos y organismos pertinentes de la UE, que intercambian información en pos de objetivos, intereses y misiones compartidos en relación con la ciberseguridad.

c) «Participantes del sector privado»: los representantes de entidades del sector privado que ofrecen o utilizan soluciones ([26]) y servicios ([27]) de ciberseguridad.

d) «Incidente a gran escala»: incidente tal como se define en el artículo 4, apartado 7, de la Directiva (UE) 2016/1148 con un impacto significativo en dos Estados miembros, como mínimo.

e) «Informe integrado sobre la situación de la ciberseguridad en la UE»: informe en el que se recogen las aportaciones de los participantes en la Unidad Cibernética Conjunta, basándose en el informe sobre la situación técnica de la ciberseguridad en la UE, definido en el artículo 7, apartado 6, del Reglamento (UE) 2019/881.

f) «Equipo de reacción rápida de la UE en materia de ciberseguridad»: equipo formado por expertos reconocidos en materia de ciberseguridad, procedentes en particular de los CSIRT de los Estados miembros, que cuenta con el apoyo de ENISA, CERT-UE y Europol y que está preparado para asistir a distancia a los participantes afectados por incidentes y crisis a gran escala.

g) «Memorando de acuerdo»: el acuerdo entre los participantes en el que se establecen las modalidades de cooperación necesarias, incluida una definición de los activos y procedimientos necesarios para crear y movilizar a los equipos de reacción rápida de la UE en materia de ciberseguridad, así como para permitir la asistencia mutua.

([25]) En consonancia con el enfoque y los principios establecidos en la Directiva (UE) 2016/1148 y en el artículo 222 del TFUE. Sin perjuicio de lo dispuesto en el artículo 42, apartado 7, del Tratado de la Unión Europea.
([26]) Incluidos los vendedores de programas informáticos.
([27]) Incluida la inteligencia sobre amenazas.

III. OBJETIVO DE LA UNIDAD CIBERNÉTICA CONJUNTA

4) Los Estados miembros y las instituciones, órganos y organismos de la UE pertinentes deben garantizar **una respuesta de la UE coordinada** a los incidentes y crisis de ciberseguridad a gran escala, así como la recuperación a raíz de los mismos. En particular, es preciso que en dicha respuesta se impliquen tanto los participantes operativos, en particular ENISA, Europol, CERT-UE, la Comisión, el Servicio Europeo de Acción Exterior (incluido el INTCEN), la red de CSIRT, EU-CyCLONe, como los participantes de apoyo, en particular la Presidencia del Grupo de Cooperación sobre SRI, la Presidencia del Grupo Horizontal «Cuestiones Cibernéticas» del Consejo, la Agencia Europea de Defensa y un representante de los proyectos pertinentes de la CEP ([28]). Los participantes operativos deben estar en condiciones de movilizar rápida y eficazmente recursos operativos con vistas a la asistencia mutua en el seno de la Unidad Cibernética Conjunta. A tal fin, dentro de la Unidad Cibernética Conjunta, los mecanismos de asistencia mutua deben coordinarse a petición de uno o varios Estados miembros.

5) A fin de que la respuesta coordinada sea efectiva, los participantes operativos y de apoyo enumerados en el punto 4) deben ser capaces de poner en común sus mejores prácticas, valerse de un **conocimiento de la situación compartido y continuo** y garantizar la **preparación** necesaria en la medida en que lo permitan sus respectivos mandatos. Dichos participantes deben tener en cuenta los procesos en curso y los conocimientos especializados de las diferentes comunidades de ciberseguridad.

IV. DEFINICIÓN DEL FUNCIONAMIENTO DE LA UNIDAD CIBERNÉTICA CONJUNTA

6) Los Estados miembro y las instituciones, órganos y organismos pertinentes de la UE, basándose en la contribución de ENISA, de conformidad con el artículo7, apartado 7, del Reglamento (UE) 2019/881, deben garantizar una **respuesta coordinada** a los incidentes y crisis a gran escala, así como la recuperación a raíz de los mismos mediante:

a) La creación, formación, prueba y despliegue coordinado de los **equipos de reacción rápida de la UE en materia de ciberseguridad**, sobre la base del artículo 7, apartado 4, del Reglamento (UE) 2019/881 y de los artículos 3 y 4 del Reglamento (UE) 2016/794;

b) la implantación coordinada de una **plataforma física y virtual,** aprovechando la cooperación estructurada de ENISA y CERT-UE consagrada en el artículo 7, apartado 4, del Reglamento (UE) 2019/881, que debe servir como infraestructura de apoyo para la cooperación técnica y operativa entre los participantes y para reunir el personal pertinente y otros recursos de los participantes;

c) la elaboración y el mantenimiento de un inventario de las **capacidades operativas y técnicas disponibles en la UE** aportadas por todas las comunidades de ciberseguridad ([29]) de la Unión que estén listas para su despliegue en caso de incidentes o crisis de ciberseguridad a gran escala;

d) la presentación de informes a la Comisión y al Alto Representante sobre la experiencia adquirida en el marco de **actividades de cooperación operativa en materia de ciberseguridad** dentro de las comunidades de ciberseguridad y como fruto de la cooperación entre estas.

7) Los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE deben garantizar que la Unidad Cibernética Conjunta ofrezca un **conocimiento de la situación** compartido y continuo así como **preparación** para hacer frente a las crisis facilitadas por el ciberespacio dirigido a las comunidades de ciberseguridad en su conjunto, así como dentro de cada una de ellas, de acuerdo con los objetivos establecidos en el artículo 7 del Reglamento (UE) 2019/881 y el artículo 3 del Reglamento (UE) 2016/794. A tal fin, los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE, de conformidad con el Reglamento (UE) 2019/881 y el Reglamento (UE) 2016/794, deben permitir la ejecución de las siguientes **operaciones de apoyo**:

a) la elaboración del **informe integrado sobre la situación de la ciberseguridad en la UE** mediante la recopilación y el análisis de toda la información pertinente y de la inteligencia sobre amenazas;

b) la utilización de **herramientas** adecuadas y seguras, de conformidad con el artículo 7, apartado 1, del Reglamento (UE) 2019/881, para el intercambio rápido de información entre los participantes y con otras entidades;

c) el **intercambio de la información y de los conocimientos especializados** necesarios para preparar a la Unión con vistas a la gestión de los incidentes y crisis a gran escala facilitados por el ciberespacio, con el apoyo de ENISA, tal como se establece en el artículo 7, apartado 2, del Reglamento (UE) 2019/881;

d) la adopción y la prueba de los **planes nacionales de respuesta a incidentes y crisis de ciberseguridad** ([30]) de conformidad con el artículo 7, apartados 2, 5 y 7, del Reglamento (UE) 2019/881;

([28]) Centro de Coordinación del Ámbito del Ciberespacio y de la Información (CIDCC) y Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad (CRRT).

([29]) Incluida, cuando proceda, la comunidad de ciberdefensa.

([30]) Propuesto en virtud del artículo 7, apartado 3, de la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 [COM(2020) 823 final, 2020/0359 (COD)].

e) el desarrollo, la gestión y la prueba, también a través de ejercicios y cursos de formación entre las distintas comunidades, del **Plan de la UE de respuesta a incidentes y crisis de ciberseguridad**, de conformidad con la recomendación del Plan director y sobre la base del artículo 7, apartado 3, de la propuesta de la Comisión de una Directiva (UE) 2016/1148 revisada, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión ([31]);

f) la asistencia a los participantes en la celebración de acuerdos de puesta en común de información, así como de acuerdos de cooperación operativa con **entidades del sector privado** que presten, entre otras cosas, servicios de inteligencia sobre amenazas y de respuesta a incidentes, con el apoyo de ENISA, tal como se establece en el artículo 7, apartado 1, del Reglamento (UE) 2019/881;

g) el establecimiento de sinergias estructuradas con las capacidades nacionales, sectoriales y transfronterizas de **seguimiento y detección**, en particular con los centros de operaciones de seguridad;

h) la asistencia a los participantes en la **gestión** de incidentes y crisis a gran escala, en consonancia con la función de apoyo de ENISA establecida en el artículo 7 del Reglamento (UE) 2019/881. Ello incluye la contribución al conocimiento compartido de la situación, el apoyo a la acción diplomática, la atribución política y la atribución en el contexto de investigaciones penales, también a través de Europol ([32]), la armonización de la comunicación pública y la facilitación de la recuperación a raíz de los incidentes.

8) Con vistas a la aplicación de los puntos 6) y 7), los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE deben garantizar:

a) **una definición de los aspectos organizativos de la Unidad Cibernética** Conjunta, y de las **funciones y responsabilidades** de los participantes operativos y de apoyo dentro de la plataforma, que permita un funcionamiento efectivo de la plataforma en consonancia con los aspectos y principios especificados en el anexo de la presente Recomendación;

b) la celebración de **memorandos de acuerdo** en los que se establezcan las modalidades de cooperación necesarias entre los participantes a que se refiere el punto 4).

9) De conformidad con lo dispuesto en el artículo 7 del Reglamento (UE) 2019/881, ENISA debe garantizar la coordinación y el apoyo de los Estados miembros y de las instituciones, órganos y organismos pertinentes de la UE dentro de la Unidad Cibernética Conjunta, por ejemplo, desempeñando funciones de secretaría, organizando reuniones y contribuyendo a la implementación de acciones tanto a escala de los Estados miembros como de la UE. ENISA debe crear una plataforma virtual segura y un espacio físico para acoger reuniones y facilitar las acciones de ejecución necesarias.

V. DESARROLLO DE LA UNIDAD CIBERNÉTICA CONJUNTA

10) los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE deben garantizar que la Unidad Cibernética Conjunta pase a una fase operativa a partir del **30 de junio de 2022**. En ese momento, los participantes operativos deben poner a disposición capacidades operativas y expertos que puedan constituir la base de los equipos de reacción rápida de la UE en materia de ciberseguridad. Los planes para la creación de una plataforma física y virtual deben estar muy avanzados.

11) Los Estados miembros y las instituciones, órganos y organismos pertinentes de la UE deben contribuir al funcionamiento de la Unidad Cibernética Conjunta y garantizar que su puesta en funcionamiento esté plenamente finalizada a más tardar **el 30 de junio de 2023**. Ello se llevará a cabo en cuatro etapas sucesivas, que tendrán por objeto la realización de las siguientes actividades:

a) Etapa 1 - Evaluación de los aspectos organizativos de la Unidad Cibernética Conjunta e identificación de las capacidades operativas de la UE disponibles, a más tardar el **31 de diciembre de 2021**;

b) Etapa 2 - Preparación de Planes de respuesta a incidentes y crisis y puesta en marcha de actividades conjuntas de preparación, a más tardar el **30 de junio de 2022**;

c) Etapa 3 - Puesta en funcionamiento de la Unidad Cibernética Conjunta, a más tardar el **31 de diciembre de 2022**;

d) Etapa 4 - Ampliación de la cooperación en el seno de la Unidad Cibernética Conjunta a las entidades privadas e información sobre los avances realizados, a más tardar el **30 de junio de 2023**.

En el anexo de la presente Recomendación se establecen medidas más detalladas que deberán llevarse a cabo en las cuatro etapas sucesivas.

([31]) COM(2020) 823 final.
([32]) En consonancia con el Reglamento (UE) 2016/794.

12) En las dos primeras etapas, ENISA debe organizar y apoyar la preparación de la Unidad Cibernética Conjunta. Los servicios de la Comisión deben convocar un grupo de trabajo que reunirá a participantes operativos y de apoyo para la finalización de dichos trabajos preparatorios. Los servicios de la Comisión designarán a un copresidente del Grupo de Trabajo; el otro copresidente será designado por el Alto Representante; ambos copresidentes contribuirán a los puntos del orden del día de conformidad con sus respectivas competencias. También habrá un representante elegido por los Estados miembros.

13) Al final de la segunda etapa, el grupo de trabajo debe concluir la evaluación de los aspectos organizativos de la Unidad Cibernética Conjunta y de las funciones y responsabilidades de los participantes operativos en dicha plataforma. El grupo de trabajo debe presentar los resultados de dicha evaluación a la Comisión y al Alto Representante, quienes la compartirán, a continuación, con el Consejo. La Comisión y el Alto Representante deben elaborar un informe conjunto sobre la base de dicha evaluación e invitar al Consejo a refrendarlo a través de conclusiones del Consejo.

14) La Unidad Cibernética Conjunta debería estar operativa a partir la tercera fase.

15) ENISA y la Comisión deben garantizar la utilización de los recursos existentes en el marco de los programas de financiación de la UE, principalmente del programa Europa Digital, de conformidad con las normas aplicables para el establecimiento de los respectivos programas de trabajo, a fin de dotar a los participantes en la Unidad Cibernética Conjunta de capacidades de formación adicionales, capacidades de comunicación e infraestructuras seguras de puesta en común de información que permitan el intercambio de información clasificada, incluso entre las distintas comunidades.

VI. **REVISIÓN**

16) los Estados miembros deben cooperar con la Comisión y el Alto Representante, en el marco de sus respectivas competencias, para evaluar la eficacia y eficiencia de la Unidad Cibernética Conjunta, a más tardar, el **30 de junio de 2025**, a fin de extraer conclusiones con vistas al futuro de la Unidad Cibernética Conjunta. Esta evaluación debe tener en cuenta la aplicación de las cuatro etapas mencionadas.

Hecho en Bruselas, el 23 de junio de 2021.

Por la Comisión
Thierry BRETON
Miembro de la Comisión

ANEXO

Etapas para la creación de la Unidad Cibernética Conjunta

El presente anexo detalla las acciones centrales y de apoyo necesarias para crear y poner en funcionamiento la Unidad Cibernética Conjunta.

1. *Etapa 1 - Evaluación de los aspectos organizativos de la Unidad Cibernética Conjunta e identificación de las capacidades operativas de la UE disponibles*

ACCIONES CENTRALES

Los participantes operativos de la Unidad Cibernética Conjunta, reunidos en un grupo de trabajo creado por la Comisión y con el apoyo de la ENISA, deben recopilar información sobre las capacidades operativas existentes, incluida una lista de profesionales reconocidos disponibles, con indicación de sus conocimientos especializados pertinentes, las herramientas, funciones y activos disponibles para la gestión de incidentes, las capacidades disponibles de formación y realización de ejercicios y los productos de análisis de información e inteligencia existentes. Sobre la base de esa información, los participantes operativos deben elaborar una **lista de las capacidades operativas de la UE disponibles** para ser desplegadas en caso de incidentes o crisis de ciberseguridad, en particular a través de los equipos de reacción rápida en materia de ciberseguridad de la UE.

El grupo de trabajo debe poner en marcha una evaluación de los **aspectos organizativos** de la Unidad Cibernética Conjunta y de las **funciones y responsabilidades de los participantes operativos en esa plataforma**.

A efectos de disponer de una visión general de las capacidades y de llegar a un acuerdo sobre los procedimientos, las acciones centrales (y cuando sea posible, las acciones de apoyo) de la etapa 1 deben completarse a más tardar el **31 de diciembre de 2021 [6 meses después de la adopción]**.

2. *Etapa 2 - Preparación de planes de respuesta a incidentes y crisis y puesta en marcha de actividades conjuntas de preparación*

ACCIONES CENTRALES

Los participantes operativos en el grupo de trabajo, en consulta con los participantes de apoyo, deben preparar el **Plan de la UE de respuesta a incidentes y crisis de ciberseguridad** sobre la base de los planes nacionales homólogos. Dicho Plan debe incluir los objetivos de preparación de la UE, los procedimientos identificados y los canales seguros de intercambio de información, incluidas las formas de manejar la información, así como criterios para activar el mecanismo de asistencia mutua sobre la base de una taxonomía de clasificación de incidentes acordada y de la lista de capacidades disponibles en la UE.

Al finalizar la etapa 2, el grupo de trabajo debe concluir su evaluación de los aspectos organizativos de la Unidad Cibernética Conjunta y de las funciones y responsabilidades de los participantes operativos en dicha plataforma. El grupo de trabajo debe presentar los resultados de la evaluación a la Comisión y al Alto Representante quienes, a su vez, deben compartir la evaluación con el Consejo. En el marco de sus respectivas competencias, la Comisión y el Alto Representante deben cooperar para elaborar un informe conjunto basado en dicha evaluación, e invitar al Consejo a refrendarlo en forma de conclusiones del Consejo.

ACCIONES DE APOYO

El Plan de la UE de respuesta a incidentes y crisis de ciberseguridad debe basarse en los principales elementos de los planes nacionales homólogos. En consonancia con la propuesta de Directiva de la Comisión relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión y por la que se deroga la Directiva (UE) 2016/1148 ([1]), los Estados miembros deben adoptar planes nacionales de respuesta ante incidentes y crisis de ciberseguridad. Estos planes, que pueden estar sujetos a revisión inter pares, deben definir objetivos y modalidades en la gestión de los incidentes y crisis de ciberseguridad a gran escala. Los planes nacionales deberán aportar, en particular, los siguientes elementos:

a) los objetivos de las medidas y actividades nacionales en materia de preparación;

b) las tareas y responsabilidades de las autoridades nacionales competentes;

c) los procedimientos de gestión de crisis y los canales para el intercambio de información;

d) las medidas de preparación, incluidos los ejercicios y las actividades de formación;

e) las partes interesadas pertinentes, tanto públicas como privadas, y la infraestructura implicada;

f) los procedimientos y mecanismos nacionales entre las autoridades y los organismos nacionales pertinentes, incluidos los responsables de todas las comunidades cibernéticas, para garantizar la participación efectiva del Estado miembro en la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel de la Unión y el respaldo de ella.

Sobre la base de las aportaciones de los Estados miembros y de las instituciones, órganos y organismos de la UE, los participantes operativos deben llevar a cabo las siguientes acciones de apoyo en el marco de la Unidad Cibernética Conjunta:

a) elaborar el primer informe integrado sobre la situación en la UE sirviéndose de los planes nacionales de respuesta a incidentes y crisis de ciberseguridad;

([1]) COM(2020) 823 final 2020/0359 (COD), Bruselas, 16.12.2020.

b) establecer capacidades de comunicación y herramientas seguras de intercambio de información;

c) facilitar la adopción de protocolos de asistencia mutua entre los participantes;

d) organizar ejercicios y cursos de formación intercomunitarios para expertos incluidos en la lista de capacidades operativas disponibles en la UE;

e) elaborar un plan plurianual para coordinar los ejercicios.

Cuando sea necesario, los participantes operativos deben consultar a los participantes de apoyo. La ENISA, con el apoyo de la Comisión, Europol y el CERT-UE, debe permitir la puesta en común de información mediante el establecimiento de capacidades de comunicación y herramientas seguras a tal efecto.

A fin de garantizar la definición de los planes necesarios y la puesta en marcha de las actividades conjuntas, las acciones centrales (y cuando sea posible, las acciones de apoyo) de la etapa 2 deben completarse a más tardar el **30 de junio de 2022 [6 meses después del final de la etapa 1]**.

3. *Etapa 3 – Puesta en funcionamiento de la Unidad Cibernética Conjunta*

ACCIONES CENTRALES

Tras la aprobación por el Consejo de las conclusiones de la Comisión sobre el informe en la etapa 2, los participantes operativos deben coordinar el despliegue de los **equipos de reacción rápida de la UE en materia de ciberseguridad** de la Unidad Cibernética Conjunta y establecer una **plataforma física** que permita a los equipos llevar a cabo actividades técnicas y operativas. Sobre la base del trabajo preparatorio realizado en el marco de la etapa 2, los participantes deben finalizar el Plan de la UE de respuesta a incidentes y crisis de ciberseguridad. Los participantes operativos deben asegurarse de que los expertos y las capacidades incluidos en la lista de capacidades operativas disponibles de la UE estén disponibles y preparados para contribuir a la actividad de los equipos de reacción rápida de la UE en materia de ciberseguridad.

Con el fin de aplicar el Plan de la UE, los participantes deben definir un programa de trabajo anual.

ACCIONES DE APOYO

La comunidad de ciberdiplomacia podrá utilizar la Unidad Cibernética Conjunta para armonizar la comunicación pública. La plataforma podrá permitir a los participantes contribuir a la atribución política y a la atribución en el marco de la justicia penal empleado a nivel policial y judicial. Además, puede facilitar la recuperación y permitir sinergias estructuradas con las capacidades nacionales y transfronterizas de seguimiento y detección.

A fin de garantizar la puesta en marcha de la Unidad Cibernética Conjunta, las acciones centrales de la etapa 3 (y cuando sea posible, las acciones de apoyo) deben completarse a más tardar el **31 de diciembre de 2022 [6 meses después del final de la etapa 2]**.

4. *Etapa 4 - Ampliación de la cooperación en la Unidad Cibernética Conjunta a las entidades privadas e información sobre los avances realizados*

ACCIONES CENTRALES

Los participantes en la Unidad Cibernética Conjunta deben elaborar un **informe de actividad sobre los avances realizados en la aplicación de las cuatro etapas establecidas en la Recomendación, en el que se describan los logros y los retos**. Dicho informe debe incluir información estadística sobre las actividades de cooperación operativa llevadas a cabo a lo largo de las cuatro etapas. El informe debe presentarse a la Comisión y al Alto Representante.

ACCIONES DE APOYO

Con el fin de ampliar las capacidades y la información de que disponen los equipos de reacción rápida de la UE en materia de ciberseguridad, los participantes deben velar por que la Unidad Cibernética Conjunta asista en la celebración de **acuerdos de puesta en común de información y de cooperación operativa entre participantes y entidades del sector privado** que presten, entre otras cosas, servicios de inteligencia sobre amenazas y de respuesta a incidentes. También deben garantizar, entre otras actividades, que la Unidad apoye el diálogo periódico y las actividades de puesta en común de información sobre amenazas y vulnerabilidades con los usuarios de soluciones de ciberseguridad, principalmente aquellas incluidas en el ámbito de aplicación de la Directiva SRI o recogidas en **centros de puesta en común y análisis de la información a escala de la UE**.

Los Estados miembros deben ayudar a las entidades que operan en su territorio, en particular las incluidas en el ámbito de aplicación de la Directiva SRI, a acceder a los diálogos entre el sector público y el privado con los centros de puesta en común y análisis de la información a escala de la UE y contribuir a ellos.

A fin de garantizar la adecuada implicación del sector privado, las acciones centrales (y cuando sea posible, las acciones de apoyo) deben completarse a más tardar el **30 de junio de 2023 [6 meses después del final de la etapa 3]**.

CÓMO MOVILIZAR RÁPIDAMENTE LAS CAPACIDADES OPERATIVAS DE LA UE

QUIÉN APORTA CAPACIDADES: participantes operativos

QUIÉN GESTIONA LAS CAPACIDADES: participantes, dentro de la Unidad Cibernética Conjunta, de acuerdo con las funciones y responsabilidades acordadas

Etapa	Objetivo	Cometido	Acción central	Acción de apoyo
Etapa 1 - Definición a más tardar el **31 de diciembre de 2021 [6 meses después de la adopción]**	PREPARACIÓN	**Identificación de capacidades**	**Elaboración por los participantes operativos de una lista de capacidades operativas disponibles en la UE**	
Etapa 2 - Preparación a más tardar el **30 de junio de 2022 [6 meses desde la finalización de la etapa 1]**	PREPARACIÓN	**Definición de los procedimientos y mecanismos pertinentes para activar las capacidades en caso de necesidad**	**Preparación por los participantes operativos del Plan de la UE de respuesta a incidentes y crisis de ciberseguridad (marco de respuesta a las crisis de ciberseguridad de la UE en el marco del Plan director), sobre la base de los planes nacionales adoptados**	**Elaboración por los participantes operativos de informes integrados sobre la situación en la UE basados en el informe sobre la situación técnica de la ciberseguridad en la UE**
	PREPARACIÓN	**Capacidad de realización de ejercicios**		**Organización de ejercicios y formación conjuntos por los participantes (intercomunitarios)** **Trabajo en un plan plurianual para coordinar los ejercicios, por parte de los participantes**
	CONOCIMIENTO DE LA SITUACIÓN	**Establecimiento de herramientas para compartir información y solicitudes de apoyo**		**Desarrollo por los participantes de una puesta en común de información segura y rápida**
UNIDAD CIBERNÉTICA CONJUNTA YA OPERATIVA Sobre la base del trabajo preparatorio realizado por los participantes en el marco de un grupo de trabajo que creará la Comisión				
Etapa 3 - Despliegue a más tardar el **31 de diciembre de 2022 [6 meses desde la finalización de la etapa 2]**	PREPARACIÓN	**Adopción de los procedimientos, mecanismos y memorandos de acuerdo pertinentes para activar las capacidades en caso de necesidad**	**Finalización por los participantes del Plan de la UE de respuesta a incidentes y crisis de ciberseguridad y definición de su aplicación a través de programas de trabajo anuales**	**Apoyo de los participantes al establecimiento de capacidades nacionales y transfronterizas de seguimiento y detección, incluido el establecimiento de centros de operaciones de seguridad (COS)**
	RESPUESTA COORDINADA	**Despliegue de capacidades en caso de necesidad**	**Coordinación por los participantes de los equipos operativos de reacción rápida de la UE en materia de ciberseguridad a través de la plataforma virtual y física de la Unidad Cibernética Conjunta en Bruselas**	**Coordinación por los participantes de la comunicación pública y contribución a la atribución política, así como a la atribución en el contexto de la justicia penal**

Etapa 4 - Expansión e informes a más tardar el **30 de junio de 2023 [6 meses desde la finalización de la etapa 3]**	CONOCIMIENTO DE LA SITUACIÓN RESPUESTA COORDINADA	**Garantía de la capacidad de ampliación mediante la participación del sector privado para satisfacer las necesidades emergentes**	**Presentación por los participantes de un informe de actividad sobre los avances realizados, describiendo los logros y los retos con ayuda de información estadística**	**Celebración por los participantes de acuerdos de puesta en común de información, así como acuerdos de cooperación operativa con proveedores de ciberseguridad** **Celebración por los participantes de acuerdos de puesta en común de información con los usuarios de ciberseguridad, principalmente entidades incluidas en el ámbito de aplicación de la Directiva SRI y los centros de puesta en común y análisis de la información a escala de la UE**