RECOMENDACIONES

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

LA COMISIÓN EUROPEA,

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

Considerando lo siguiente:

(1) La utilización de las tecnologías de la información y la comunicación, así como la dependencia de las mismas, constituyen un elemento esencial en todos los sectores de actividad económica, ya que tanto nuestras empresas como nuestros ciudadanos están más interconectados y son más interdependientes que nunca, en todos los sectores y por encima de todas las fronteras. Los Estados miembros y las instituciones de la UE deben estar bien preparados para el caso de que se produzca un incidente de ciberseguridad que afecte a organizaciones de más de un Estado miembro, o incluso de toda la Unión, con posibles perturbaciones graves del mercado interior y, más en general, de las redes y los sistemas de información en que se basan la economía, la democracia y la sociedad de la Unión.

(2) Un incidente de ciberseguridad puede considerarse una crisis a escala de la Unión cuando la perturbación causada por el incidente sea demasiado fuerte como para que el Estado miembro interesado lo resuelva por sí mismo o cuando afecte a dos o más Estados miembros con un impacto tan amplio de relevancia técnica o política que requiera una coordinación y una respuesta oportuna a nivel político de la Unión.

(3) Los incidentes de ciberseguridad pueden desencadenar una crisis más generalizada, que afecte a sectores de actividad más allá de las redes y los sistemas de información y las redes de comunicaciones; cualquier respuesta adecuada debe basarse en actividades de mitigación tanto de carácter cibernético como de otro tipo.

(4) Los incidentes de ciberseguridad son imprevisibles y a menudo se producen y evolucionan en plazos muy breves, por lo que las entidades afectadas y las que tienen responsabilidades en cuanto a la respuesta y a la mitigación de los efectos del incidente deben coordinar su respuesta con rapidez. Por otra parte, los incidentes de ciberseguridad con frecuencia no se limitan a una zona geográfica específica y pueden producirse simultáneamente o extenderse de manera instantánea en muchos países.

(5) Una respuesta eficaz ante los incidentes y crisis de ciberseguridad a gran escala a nivel de la UE requiere una cooperación rápida y eficaz entre todas las partes interesadas pertinentes y se basa en la preparación y en las capacidades de cada uno de los Estados miembros, así como en una acción común coordinada apoyada en las capacidades de la Unión. Una respuesta oportuna y efectiva a los incidentes se basa, por tanto, en la existencia de procedimientos y mecanismos de cooperación previamente establecidos y, en la medida de lo posible, bien ensayados, en los que se hayan definido claramente las funciones y responsabilidades de los agentes clave a nivel nacional y de la Unión.

(6) En sus conclusiones ([1]) sobre la protección de infraestructuras críticas de información, de 27 de mayo de 2011, el Consejo invitaba a los Estados miembros de la UE a «[potenciar] la colaboración entre Estados miembros y [contribuir], basándose en las experiencias y los resultados nacionales en materia de gestión de crisis y en cooperación con la ENISA, al desarrollo de mecanismos europeos de cooperación en caso de incidentes informáticos con vistas a su ensayo en el marco del próximo ejercicio CyberEurope en 2012».

(7) La Comunicación de 2016 «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora» ([2]) animaba a los Estados miembros a sacar el máximo partido de los mecanismos de cooperación de la Directiva SRI ([3]) y a potenciar la cooperación transfronteriza relativa a la

([1]) Conclusiones del Consejo sobre protección de infraestructuras críticas de información «Logros y próximas etapas: hacia la ciberseguridad global», documento 10299/11, Bruselas, 27 de mayo de 2011.
([2]) COM(2016) 410 final, de 5 de julio de 2016.
([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).

preparación ante un ciberincidente a gran escala. Añadía que un enfoque coordinado de la cooperación ante las crisis entre los diferentes elementos del ecosistema cibernético, descrito en un «plan director», mejoraría la preparación y que dicho plan también debería velar por las sinergias y la coherencia con los mecanismos existentes de gestión de crisis.

(8) En las Conclusiones del Consejo ([1]) sobre la citada Comunicación, los Estados miembros invitaban a la Comisión a presentar un plan director de ese tipo para su consideración por los órganos y otras partes interesadas. Sin embargo, la Directiva SRI no contempla un marco de cooperación de la Unión en el caso de incidentes y crisis de ciberseguridad a gran escala.

(9) La Comisión consultó a los Estados miembros en dos talleres de consulta distintos celebrados en Bruselas los días 5 de abril y 4 de julio de 2017 con representantes, procedentes de los Estados miembros, de los equipos de respuesta a incidentes de seguridad informática (CSIRT), el Grupo de cooperación establecido por la Directiva SRI y el Grupo horizontal del Consejo sobre cuestiones cibernéticas, así como representantes del Servicio Europeo de Acción Exterior (SEAE), la ENISA, Europol/EC3 y la Secretaría General del Consejo (SGC).

(10) El Plan director de la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala a nivel de la Unión que se recoge en el anexo de la presente Recomendación es resultado de las consultas mencionadas y complementa la Comunicación sobre «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora».

(11) El Plan director describe y fija los objetivos y los modos de cooperación entre los Estados miembros y las instituciones, órganos y organismos de la UE (en lo sucesivo denominados «instituciones de la UE») en cuanto a la respuesta a incidentes y crisis de ciberseguridad a gran escala y cómo los mecanismos existentes de gestión de crisis pueden hacer pleno uso de las entidades de ciberseguridad existentes a nivel de la UE.

(12) En la respuesta a una crisis de ciberseguridad en el sentido del considerando 2, la coordinación de la respuesta a nivel político de la Unión en el Consejo utilizará el Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC) ([2]); la Comisión utilizará el proceso de coordinación de crisis intersectoriales de alto nivel ARGUS ([3]). Si la crisis tiene una importante dimensión de política exterior o de Política Común de Seguridad y Defensa (PCSD), se activará el Mecanismo de Respuesta a las Crisis (CRM) del Servicio Europeo de Acción Exterior (SEAE) ([3]).

(13) En determinados ámbitos hay mecanismos de gestión de crisis sectoriales a escala de la UE que permiten la cooperación en caso de incidentes o crisis de ciberseguridad. Por ejemplo, en el marco del Sistema Europeo de Radionavegación por Satélite (GNSS), la Decisión 2014/496/PESC del Consejo ([4]) ya define las funciones respectivas del Consejo, el Alto Representante, la Comisión, la Agencia del GNSS Europeo y los Estados miembros dentro de la cadena de competencias operativas establecidas para reaccionar ante una amenaza para la Unión, para los Estados miembros o para el GNSS, también en caso de ciberataques. Por lo tanto, la presente Recomendación debe entenderse sin perjuicio de estos mecanismos.

(14) Los Estados miembros tienen la responsabilidad primaria de la respuesta en caso de incidentes o crisis de ciberseguridad a gran escala que les afecten. La Comisión, el Alto Representante y otras instituciones o servicios de la UE tienen, sin embargo, una función importante, derivada del Derecho de la Unión o de la posibilidad de que los incidentes y crisis de ciberseguridad afecten a todos los sectores de actividad económica dentro del mercado único, a la seguridad y las relaciones internacionales de la Unión, y a las propias instituciones.

(15) A nivel de la Unión, entre los agentes clave que intervienen en respuesta a las crisis de ciberseguridad se incluyen las recientemente establecidas estructuras y mecanismos de la Directiva SRI, en particular la red de equipos de respuesta a incidentes de seguridad informática (CSIRT), así como las agencias y órganos pertinentes, a saber, la Agencia de Seguridad de las Redes y de la Información de la Unión Europa (ENISA), el Centro Europeo de Ciberdelincuencia de Europol (Europol/EC3), el Centro de Análisis de Inteligencia de la UE (INTCEN), la Dirección de Información del Estado Mayor de la Unión Europea (EMUE INT) y la Sala de Guardia (SITROOM) que trabajan conjuntamente como la SIAC (Capacidad Única de Análisis de Inteligencia), la Célula de Fusión de la UE contra las Amenazas Híbridas (dentro del INTCEN), el Equipo de respuesta a emergencias informáticas de las instituciones de la UE (CERT-UE) y el Centro de Coordinación de la Respuesta a Emergencias de la Comisión Europea.

(16) La cooperación entre los Estados miembros a la hora de responder a los incidentes de ciberseguridad a nivel técnico se hace a través de la red de CSIRT establecida por la Directiva SRI. La ENISA se encarga de las labores de

([1]) Documento 14540/16, de 15 de noviembre de 2016.
([2]) Se puede encontrar más información en la sección 3.1 del apéndice sobre gestión de crisis, mecanismos de cooperación y agentes a nivel de la UE.
([3]) Ibídem.
([4]) Decisión 2014/496/PESC del Consejo, de 22 de julio de 2014, relativa a los aspectos del despliegue y utilización del sistema europeo de radionavegación por satélite que afecten a la seguridad de la Unión Europea y por la que se deroga la Acción Común 2004/552/PESC (DO L 219 de 25.7.2014, p. 53).

secretaría de la Red y apoya activamente la cooperación entre los CSIRT. Los CSIRT nacionales y el CERT-UE cooperan e intercambian información de forma voluntaria, también, en caso necesario, en respuesta a incidentes de ciberseguridad que afecten a uno o más Estados miembros. A instancias del representante del CSIRT de un Estado miembro, pueden debatir y, cuando sea posible, determinar una respuesta coordinada a un incidente que se haya detectado dentro de la jurisdicción de ese Estado miembro. Los procedimientos pertinentes se establecerán en los procedimientos de trabajo normalizados de la Red de CSIRT ([1]).

(17) La red de CSIRT también está encargada de debatir, explorar e identificar más formas de cooperación operativa, también en relación con las categorías de riesgos e incidentes, alertas tempranas, asistencia mutua, principios y modalidades de coordinación, cuando los Estados miembros responden a incidentes y riesgos transfronterizos.

(18) El Grupo de cooperación establecido por el artículo 11 de la Directiva SRI está encargado de proporcionar orientación estratégica para las actividades de la red de CSIRT y debatir sobre las capacidades y la preparación de los Estados miembros, así como, de forma voluntaria, de evaluar las estrategias nacionales en materia de seguridad de las redes y sistemas de información y la eficacia de los CSIRT, y de identificar las buenas prácticas.

(19) Una línea de trabajo específica dentro del Grupo de cooperación está preparando directrices sobre la notificación de incidentes, con arreglo al artículo 14, apartado 7, de la Directiva SRI, respecto de las circunstancias en las que los operadores de servicios esenciales deben notificar incidentes de conformidad con el artículo 14, apartado 3, y el formato y el procedimiento de estas notificaciones ([2]).

(20) El conocimiento y la comprensión de la situación en tiempo real, la posición de riesgo y las amenazas, que se obtienen mediante la presentación de informes, las evaluaciones, la investigación y el análisis, son indispensables para que se puedan tomar decisiones bien fundadas. Este «conocimiento de la situación» por todas las partes interesadas pertinentes es esencial para una respuesta coordinada y efectiva. El conocimiento de la situación se refiere a elementos sobre las causas, así como las repercusiones y el origen del incidente. Se reconoce que depende del intercambio y puesta en común de la información entre las partes pertinentes en un formato adecuado, utilizando una taxonomía común para describir el incidente de forma segura y adecuada.

(21) La respuesta a incidentes de ciberseguridad puede adoptar muchas formas, desde identificar medidas técnicas que pueden implicar a dos o más entidades que investiguen conjuntamente las causas técnicas del incidente (por ejemplo, análisis de programas informáticos maliciosos) o identificar métodos mediante los cuales las organizaciones puedan evaluar si se han visto afectadas (por ejemplo, indicadores de compromiso), hasta tomar decisiones operativas sobre la aplicación de tales medidas y, a nivel político, decidir sobre el uso de otros instrumentos tales como el marco para una respuesta conjunta a las actividades cibernéticas malintencionadas ([3]) o el protocolo de actuación para contrarrestar las amenazas híbridas ([4]), dependiendo del incidente.

(22) La confianza de los ciudadanos y empresas europeos en los servicios digitales es esencial para que prospere el mercado único digital. Por lo tanto, la comunicación de las crisis desempeña un papel especialmente importante para mitigar los efectos negativos de los incidentes y crisis de ciberseguridad. La comunicación puede utilizarse también en el contexto del marco para una respuesta diplomática conjunta como medio para influir en el comportamiento de los agresores (potenciales) que actúen desde terceros países. La adaptación de la comunicación al público a fin de paliar los efectos negativos de los incidentes y crises de ciberseguridad y de la comunicación al público para influir en un agresor es indispensable a efectos de una respuesta política eficaz.

(23) La prestación de información a los ciudadanos sobre cómo pueden reducir a nivel de usuario y de organización los efectos de un incidente (por ejemplo, aplicando un parche o adoptando acciones complementarias para evitar la amenaza, etc.) podría ser una medida eficaz para atenuar un incidente o crisis de ciberseguridad a gran escala.

(24) La Comisión, a través de la infraestructura de servicios digitales sobre ciberseguridad del Mecanismo «Conectar Europa» (MCE), está elaborando un mecanismo de cooperación de plataforma central de servicios, conocido como MeliCERTes, entre los CSIRT de los Estados miembros participantes, para mejorar sus niveles de preparación, cooperación y respuesta a las amenazas e incidentes cibernéticos emergentes. La Comisión, a través de convocatorias de propuestas competitivas para la concesión de las subvenciones en virtud del MCE está cofinanciando los CSIRT de los Estados miembros, con vistas a mejorar sus capacidades operativas a nivel nacional.

([1]) En fase de elaboración; adopción prevista para finales de 2017.
([2]) Está previsto que las directrices estén terminadas para finales de 2017.
([3]) Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»), Doc. 9916/17.
([4]) Documento de trabajo conjunto sobre el protocolo de actuación de la UE para contrarrestar las amenazas híbridas [*Joint Staff Working Document EU operational protocol for countering hybrid threats, «EU Playbook»*], SWD(2016) 227 final de 5 de julio de 2016.

(25) Los ejercicios de ciberseguridad a nivel de la UE son esenciales para estimular y mejorar la cooperación entre los Estados miembros y el sector privado. A tal fin, desde 2010 la ENISA organiza regularmente ejercicios de incidentes cibernéticos paneuropeos (CyberEurope).

(26) Las Conclusiones del Consejo ([1]) sobre la ejecución de la declaración conjunta del presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte, piden que se siga reforzando la cooperación en los ejercicios cibernéticos a través de la participación recíproca del personal en los ejercicios correspondientes, entre ellos, en particular, en el marco de Cyber Coalition y CyberEurope.

(27) La continua evolución del panorama de las amenazas y los recientes incidentes de ciberseguridad son una indicación del aumento del riesgo al que se enfrenta la Unión. Los Estados miembros deben actuar sobre la presente Recomendación sin más dilación, y en cualquier caso antes de finales de 2018.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

(1) Los Estados miembros y las instituciones de la UE deben crear un Marco de respuesta a las crisis de ciberseguridad de la UE donde se integren los objetivos y las modalidades de la cooperación que se presentan en el Plan director siguiendo los principios rectores allí descritos.

(2) El Marco de respuesta a las crisis de ciberseguridad de la UE debe identificar en especial a los agentes, instituciones de la UE y autoridades de los Estados miembros que sean pertinentes, a todos los niveles necesarios (técnico, operativo y estratégico/político) y elaborar, en caso necesario, procedimientos de trabajo normalizados que definan cómo han de colaborar en el contexto de los mecanismos de gestión de crisis de la UE. Debe hacerse hincapié en permitir el intercambio de información, sin demoras indebidas, y en coordinar la respuesta durante incidentes y crisis de ciberseguridad a gran escala.

(3) A tal fin, las autoridades competentes de los Estados miembros deben trabajar juntas en el sentido de especificar en mayor medida los protocolos de cooperación y de intercambio de información. El Grupo de cooperación debe intercambiar sus experiencias sobre estas cuestiones con las instituciones pertinentes de la UE.

(4) Los Estados miembros deben velar por que sus mecanismos nacionales de gestión de crisis den la respuesta adecuada a los incidentes de ciberseguridad y establezcan los procedimientos necesarios para la cooperación a nivel de la UE en el contexto del Marco de la UE.

(5) Por lo que se refiere a los mecanismos existentes de gestión de crisis de la UE, en consonancia con el Plan director, es conveniente que los Estados miembros, junto con los servicios de la Comisión y el SEAE, establezcan directrices para la aplicación práctica por lo que respecta a la integración de sus entidades y procedimientos nacionales en materia de gestión de crisis y ciberseguridad en los mecanismos existentes de gestión de crisis de la UE, a saber, el DIRPC y el CRM del SEAE. En particular, los Estados miembros deben velar por la existencia de estructuras apropiadas que permitan el flujo eficiente de información entre sus autoridades nacionales de gestión de crisis y sus representantes a nivel de la UE en el contexto de los mecanismos de crisis de la UE.

(6) Los Estados miembros deben hacer pleno uso de las oportunidades que ofrece el programa de infraestructuras de servicios digitales (ISD) del Mecanismo «Conectar Europa» (MCE), y cooperar con la Comisión para que el mecanismo de cooperación de plataforma central de servicios, actualmente en elaboración, aporte todas las funcionalidades necesarias y cumpla sus requisitos para la cooperación también durante las crisis de ciberseguridad.

(7) Los Estados miembros, con la ayuda de la ENISA y sobre la base de los trabajos realizados anteriormente en este ámbito, deben cooperar en la elaboración y la adopción de una taxonomía y un formato comunes para los informes de situación a fin de describir las causas técnicas y las consecuencias de los incidentes de ciberseguridad y reforzar su cooperación técnica y operativa durante las crisis. A este respecto, los Estados miembros deben tener en cuenta el trabajo en curso del Grupo de cooperación en relación con las directrices sobre notificación de incidentes, y en particular los aspectos relacionados con el formato de las notificaciones nacionales.

(8) Los procedimientos establecidos en el Marco deben someterse a prueba y, en caso necesario, modificarse tras las lecciones aprendidas de la participación de los Estados miembros en los ejercicios de ciberseguridad a escala nacional, regional y de la Unión, así como en los de la ciberdiplomacia y de la OTAN. En particular, deben someterse a prueba en el contexto de los ejercicios de CyberEurope organizados por la ENISA. CyberEurope 2018 representa la primera de tales oportunidades.

([1]) ST 15283/16, de 6 de diciembre de 2016.

(9) Los Estados miembros y las instituciones de la UE deben practicar regularmente su respuesta a los incidentes y crisis de ciberseguridad a gran escala a nivel nacional y europeo, incluida su respuesta política, cuando sea necesario y con la participación de entidades del sector privado según proceda.

Hecho en Bruselas, el 13 de septiembre de 2017.

Por la Comisión

Mariya GABRIEL

Miembro de la Comisión

ANEXO

Plan director de la respuesta coordinada a los incidentes y crisis de ciberseguridad transfronterizos a gran escala

INTRODUCCIÓN

El presente Plan director se aplica a los incidentes de ciberseguridad que causen perturbaciones demasiado fuertes como para que el Estado miembro afectado lo resuelva por sí mismo o cuando afecten a dos o más Estados miembros o instituciones de la UE con un impacto tan amplio y de tanta relevancia técnica o política que requieran una coordinación y una respuesta oportuna a nivel político de la Unión.

Los incidentes de ciberseguridad a gran escala de este tipo se consideran «crisis» de ciberseguridad.

En caso de crisis a escala de la UE con elementos cibernéticos, el Consejo, utilizando el Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC), coordinará la respuesta a nivel político de la Unión.

Dentro de la Comisión, la coordinación se llevará a cabo de conformidad con el sistema de alerta rápida ARGUS.

Si la crisis tiene una importante dimensión de política exterior o de Política Común de Seguridad y Defensa (PCSD), se activará el Mecanismo de Respuesta a las Crisis del SEAE.

El Plan director describe cómo estos mecanismos bien establecidos de gestión de crisis deben hacer pleno uso de las entidades de ciberseguridad existentes a nivel de la UE, así como de los mecanismos de cooperación entre los Estados miembros.

De este modo, el Plan director tiene en cuenta una serie de principios rectores (principios de proporcionalidad, subsidiariedad, complementariedad y confidencialidad de la información), presenta los objetivos centrales de la cooperación (respuesta eficaz, conocimiento compartido de la situación, mensajes de comunicación al público) a tres niveles (estratégico/político, operativo y técnico), los mecanismos y los agentes implicados, así como las actividades destinadas a cumplir dichos objetivos centrales.

El Plan director no abarca la totalidad del ciclo de gestión de las crisis (prevención/mitigación, preparación, respuesta y recuperación), sino que se focaliza en la respuesta. No obstante, se abordan en él algunas otras actividades, en particular las relacionadas con la consecución de un conocimiento compartido de la situación.

También es importante señalar que los incidentes de ciberseguridad pueden encontrarse en el origen o formando parte de una crisis más amplia que afecte a otros sectores. Dado que se espera que las crisis de ciberseguridad tengan en su mayoría efectos sobre el mundo físico, toda respuesta adecuada debe basarse en actividades de mitigación de carácter tanto cibernético como no cibernético. Las actividades de respuesta a las crisis cibernéticas deben coordinarse con otros mecanismos de gestión de crisis a nivel de la UE, nacional o sectorial.

Por último, el Plan director no sustituye a los mecanismos, dispositivos o instrumentos existentes específicos de un sector o de una política, como el establecido para el Sistema Europeo de Radionavegación por Satélite (GNSS) ([1]), y debe entenderse sin perjuicio de tales elementos.

Principios rectores

Al trabajar en pos de los objetivos, al identificar las actividades necesarias y asignar funciones y responsabilidades a los agentes o mecanismos respectivos, se han aplicado los principios rectores siguientes, que también deben respetarse a la hora de preparar las futuras directrices de aplicación.

Proporcionalidad: La gran mayoría de los incidentes de ciberseguridad que afectan a los Estados miembros están muy lejos de poder considerarse «crisis» nacionales, y mucho menos europeas. El fundamento de la cooperación entre los Estados miembros a la hora de responder a estos incidentes es aportado por la red de equipos de respuesta a incidentes de seguridad informática (CSIRT), creada por la Directiva SRI ([2]). Los CSIRT nacionales cooperan e intercambian información diariamente de forma voluntaria, en caso necesario también en respuesta a incidentes de ciberseguridad que afecten a uno o varios Estados miembros, en consonancia con los procedimientos de trabajo normalizados (PTN) de la red de CSIRT. El Plan director debe, por tanto, hacer pleno uso de estos PTN, en los que debe reflejarse toda otra tarea específica de las crisis de ciberseguridad.

([1]) Decisión 2014/496/PESC.
([2]) Directiva (UE) 2016/1148.

Subsidiariedad: El principio de subsidiariedad es clave. Los Estados miembros tienen la responsabilidad primaria de la respuesta en caso de incidentes o crisis de ciberseguridad a gran escala que les afecten. No obstante, la Comisión, el Servicio Europeo de Acción Exterior y otras instituciones, órganos y organismos tienen un papel importante, que está definido claramente en el DIRPC, pero también deriva del Derecho de la Unión o simplemente de la posibilidad de que los incidentes y crisis de ciberseguridad afecten a todos los sectores de actividad económica dentro del mercado único, a la seguridad y las relaciones internacionales de la Unión, así como a las propias instituciones.

Complementariedad: El Plan director tiene plenamente en cuenta los mecanismos existentes de gestión de crisis a nivel de la UE, a saber, el Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC), ARGUS, y el Mecanismo de Respuesta a las Crisis del SEAE, integra en ellos las nuevas estructuras y mecanismos de la Directiva SRI, como la red de CSIRT, así como las agencias y órganos pertinentes, a saber, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), el Centro Europeo de Ciberdelincuencia de Europol (Europol/EC3), el Centro de Análisis de Inteligencia de la UE (INTCEN), la División de Información del Estado Mayor de la Unión Europea (EMUE INT) y la Sala de Guardia (SITROOM) en el INTCEN, que trabajan conjuntamente como la SIAC (Capacidad Única de Análisis de Inteligencia); la Célula de Fusión de la UE contra las Amenazas Híbridas (dentro del INTCEN); y el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE). De esta manera, el Plan director debe garantizar también que su interacción y cooperación presente la máxima complementariedad y el mínimo solapamiento.

Confidencialidad de la información: Todos los intercambios de información en el contexto del Plan director deben cumplir las normas aplicables sobre seguridad ([1]) y sobre la protección de datos personales, así como el Protocolo TLP para el intercambio de información ([2]). Para el intercambio de información clasificada, con independencia del sistema de clasificación aplicado, se deben utilizar las herramientas acreditadas disponibles ([3]). Por lo que se refiere al tratamiento de datos personales, se respetarán las normas aplicables de la UE, en particular el Reglamento general de protección de datos ([4]), la Directiva sobre la privacidad y las comunicaciones electrónicas ([5]), y el Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos, oficinas y agencias de la Unión y a la libre circulación de estos datos ([6]).

Objetivos centrales

La cooperación en virtud del Plan director sigue el planteamiento antes mencionado de tres niveles: político, operativo y técnico. A cada nivel, la cooperación puede incluir el intercambio de información y acciones comunes, y aspira a lograr los siguientes objetivos centrales.

— Permitir una respuesta eficaz: La respuesta puede adoptar muchas formas, desde identificar medidas técnicas que pueden implicar a dos o más entidades que investigan conjuntamente las causas técnicas del incidente (por ejemplo, análisis de programas informáticos maliciosos) o identificar métodos mediante los cuales las organizaciones pueden evaluar si se han visto afectadas (por ejemplo, indicadores de compromiso), hasta tomar decisiones operativas sobre la aplicación de tales medidas técnicas y, a nivel político, decidir sobre el lanzamiento de otros instrumentos, tales como la respuesta diplomática de la UE a las actividades cibernéticas malintencionadas («conjunto de instrumentos de ciberdiplomacia») o el protocolo de actuación de la UE para contrarrestar las amenazas híbridas, dependiendo del incidente.

— Compartir el conocimiento de la situación: una comprensión suficientemente buena de los acontecimientos, a medida que se vayan produciendo, por todas las partes interesadas pertinentes a los tres niveles (técnico, operativo, político) es esencial para una respuesta coordinada. El conocimiento de la situación puede incluir elementos tecnológicos sobre las causas, así como las repercusiones y el origen del incidente. Como los incidentes de ciberseguridad pueden afectar a una amplia variedad de sectores (finanzas, energía, transporte, sanidad, etc.), es imperativo que la información adecuada, en el formato adecuado, llegue a todas las partes interesadas pertinentes a su debido tiempo.

([1]) Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión (DO L 72 de 17.3.2015, p. 41); Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53); Decisión de la Alta Representante, de 19 de abril de 2013, sobre las normas de seguridad del Servicio Europeo de Acción Exterior (DO C 190 de 29.6.2013, p. 1); Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 274 de 15.10.2013, p. 1).

([2]) https://www.first.org/tlp/

([3]) En junio de 2016, estos canales de transmisión incluyen el CIMS (Sistema de Gestión de la Información Clasificada), el ACID (algoritmo de cifrado), RUE (sistema seguro para crear, intercambiar y almacenar los documentos RESTREINT UE/EU RESTRICTED) y SOLAN. Otros medios de transmisión de información clasificada son, por ejemplo, PGP o S/MIME.

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

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

([6]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1) (en revisión).

— Ponerse de acuerdo sobre los mensajes clave de comunicación al público ([1]): La comunicación de las crisis desempeña un papel importante para mitigar los efectos negativos de los incidentes y crisis de ciberseguridad, pero también puede utilizarse como instrumento para influir en el comportamiento de los agresores (potenciales). Un mensaje apropiado también puede servir para señalar claramente las posibles consecuencias de una respuesta diplomática con el fin de influir en el comportamiento de los agresores. La adaptación de la comunicación al público a fin de paliar los efectos negativos de los incidentes y crises de ciberseguridad y para influir en un agresor es indispensable a efectos de una respuesta política eficaz. En la ciberseguridad es especialmente importante la difusión de información exacta que permita actuar en relación con las posibilidades de que dispongan los ciudadanos para mitigar los efectos de un incidente (por ejemplo, aplicar un parche informático, tomar medidas complementarias para evitar la amenaza, etc.).

COOPERACIÓN ENTRE LOS AGENTES DE LOS ESTADOS MIEMBROS Y ENTRE ESTOS Y LOS DE LA UE A LOS NIVELES TÉCNICO, OPERATIVO Y ESTRATÉGICO/POLÍTICO

La eficacia de la respuesta a los incidentes o crisis de ciberseguridad a gran escala a nivel de la UE depende de la eficacia de la cooperación técnica, operativa y estratégica/política.

A cada nivel, los agentes implicados deben realizar determinadas actividades en lo que respecta a la consecución de tres objetivos centrales:

— Respuesta coordinada

— Conocimiento compartido de la situación

— Comunicaciones al público

A lo largo del incidente o crisis, los niveles inferiores de cooperación han de avisar, informar y apoyar a los niveles superiores, y estos han de ofrecer directrices ([2]) y decisiones a los niveles inferiores, según proceda.

Cooperación a nivel técnico

Gama de actividades

— Gestión de incidentes ([3]) durante una crisis de ciberseguridad

— Control y seguimiento de incidentes, incluido el análisis continuo de las amenazas y riesgos.

Agentes potenciales

A nivel técnico, el mecanismo central para la cooperación en el Plan director es la red de CSIRT, bajo la autoridad de la Presidencia y con la secretaría facilitada por la ENISA.

— Estados miembros

  — Autoridades competentes y puntos de contacto únicos establecidos por la Directiva SRI

  — CSIRT

— Órganos/oficinas/agencias de la UE

  — ENISA

  — Europol/EC3

  — CERT-UE

([1]) En este contexto es importante recordar que la comunicación al público puede referirse tanto a la comunicación sobre el incidente a la totalidad de los ciudadanos, como a la comunicación de información más técnica u operativa a sectores críticos o a los que se han visto afectados. Esto puede exigir la utilización de canales de difusión confidenciales y el uso de herramientas o plataformas técnicas específicas. En cualquiera de los dos casos, la comunicación con los operadores y el público en general en un Estado miembro es competencia y responsabilidad de cada Estado miembro. Por lo tanto, de acuerdo con el principio de subsidiariedad arriba citado, corresponde a los Estados miembros y a los CSIRT nacionales la responsabilidad última de la información que se difunda dentro de su territorio y de su grupo objetivo, respectivamente.

([2]) «Autorizaciones para actuar»: a la luz de una crisis de ciberseguridad, la brevedad de los tiempos de respuesta es de vital importancia para establecer medidas de mitigación adecuadas. Con el fin de conseguir esta brevedad de los tiempos de respuesta, pueden expedirse «autorizaciones para actuar», voluntarias de un Estado miembro a otro, a fin de darle a un Estado miembro autorización para actuar inmediatamente, sin tener que consultar con los niveles superiores o las instituciones de la UE ni tener que recorrer todos los canales oficiales requeridos normalmente, si es que esto no se exige en un determinado incidente (por ejemplo, un CSIRT no debería tener que consultar con los niveles superiores para transmitir información valiosa a un CSIRT de otro Estado miembro).

([3]) Por «gestión de incidentes» se entienden todos los procedimientos seguidos para detectar, analizar y limitar un incidente y darle respuesta.

— Comisión Europea

  — El CECRE (servicio operativo 24/7 situado en la DG ECHO), y el servicio responsable designado (elegido entre la DG CNECT y la DG HOME, en función del tipo concreto de incidente), la Secretaría General (Secretaría de ARGUS), la DG HR (Dirección de Seguridad), la DG DIGIT (Operaciones de Seguridad de las Tecnologías de la Información).

  — Para otras agencias de la UE ([1]), la respectiva DG de tutela de la Comisión o el SEAE (primer punto de contacto).

— SEAE

  — SIAC (Capacidad Única de Análisis de Inteligencia: INTCEN y EMUE INT

  — La Sala de Guardia de la UE y el servicio geográfico o temático designado.

  — Célula de Fusión de la UE contra las Amenazas Híbridas (parte del INTCEN, ciberseguridad en un contexto híbrido)

Conocimiento compartido de la situación

— Como parte de la cooperación regular a nivel técnico para contribuir al conocimiento de la situación de la Unión, la ENISA debe preparar periódicamente el informe de la situación técnica de ciberseguridad de la UE en cuanto a incidentes y amenazas, sobre la base de la información públicamente disponible, su propio análisis y los informes compartidos con ella por los CSIRT de los Estados miembros (de forma voluntaria) o los puntos de contacto únicos de la Directiva SRI, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, el CERT-UE y, en su caso, el Centro de Inteligencia de la Unión Europea (INTCEN) en el Servicio Europeo de Acción Exterior (SEAE). El informe debe ponerse a disposición de las instancias pertinentes del Consejo, la Comisión, el AR/VP y la red de CSIRT.

— En caso de incidente grave, el presidente de la Red de CSIRT, con la ayuda de la ENISA, prepara un informe de situación del incidente de ciberseguridad de la UE ([2]) que se presentará a la Presidencia, a la Comisión y al AR/VP a través del CSIRT de la Presidencia de turno.

— *Todas las demás agencias de la UE* informan a sus respectivas direcciones generales de tutela, que a su vez informan al servicio responsable de la Comisión.

— El *CERT-UE* proporciona informes técnicos a la red de CSIRT, instituciones y agencias de la UE (según proceda) y ARGUS (si se ha activado).

— El *Europol/EC3* ([3]) *y el CERT-UE* aportan a la red de CSIRT el análisis forense por expertos de artefactos técnicos y demás información técnica.

— SIAC del SEAE: En nombre del INTCEN, la Célula de Fusión de la UE contra las Amenazas Híbridas informa a los departamentos pertinentes del SEAE.

Respuesta:

— *La red de CSIRT* intercambia datos técnicos y análisis sobre el incidente, tales como, por ejemplo, direcciones IP, indicadores de compromiso ([4]), etc. Esta información debe transmitirse a la ENISA sin demora indebida y a más tardar en el plazo de 24 horas desde el momento en que se detecte el incidente.

— De conformidad con los procedimientos de trabajo normalizados de la Red de CSIRT, sus miembros cooperan en sus esfuerzos por analizar los artefactos técnicos disponibles y demás información técnica relacionada con el incidente, con el fin de determinar la causa y las posibles medidas técnicas de mitigación.

— La ENISA ayuda a los CSIRT en sus actividades técnicas sirviéndose de sus conocimientos y de acuerdo con su mandato ([5]).

([1]) Los organismos o agencias de la UE que participen en cada caso dependerán de la naturaleza y del impacto del incidente en los distintos sectores de actividad (sector financiero, transportes, energía, sanidad, etc.).

([2]) El informe de situación del incidente de ciberseguridad de la UE es una agrupación de los informes nacionales proporcionados por los CSIRT nacionales. El formato del informe debe describirse en los procedimientos de trabajo normalizados de la red de CSIRT.

([3]) Según las condiciones y procedimientos establecidos en el marco jurídico del CE3.

([4]) Indicador de compromiso (IOC): en informática forense es un artefacto observado en una red o en un sistema operativo que indica una intrusión con un nivel de confianza elevado. Los IOC típicos son signaturas de virus y direcciones IP, valores *hash* MD5 de archivos de programas informáticos maliciosos o direcciones URL o nombres de dominio de servidores de mando y control de redes infectadas.

([5]) Propuesta de Reglamento relativo a la ENISA, la Agencia Europea de Ciberseguridad, y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Acto de Ciberseguridad»), de 13 de septiembre de 2017.

— Los CSIRT de los Estados miembros coordinan sus actividades de respuesta técnica con la ayuda de la ENISA y la Comisión.

— SIAC del SEAE: En nombre del INTCEN, la Célula de Fusión de la UE contra las Amenazas Híbridas pone en marcha el proceso de recogida de información para recabar las pruebas iniciales.

Comunicaciones al público:

— Los CSIRT emiten avisos técnicos ([1]) y alertas de vulnerabilidad ([2]) y los difunden entre sus respectivas comunidades y el público, según los procedimientos de autorización aplicables en cada caso.

— La ENISA facilita la elaboración y difusión de comunicaciones comunes de la red de CSIRT.

— La ENISA coordina sus actividades de comunicación al público con la Red de CSIRT y el Servicio del Portavoz de la Comisión.

— La ENISA y el EC3 coordinan sus actividades de comunicación al público sobre la base del conocimiento compartido de la situación concertado entre los Estados miembros. Ambos órganos han coordinado sus actividades de comunicación al público con el Servicio del Portavoz de la Comisión.

— Si la crisis tiene una dimensión de política exterior o de Política Común de Seguridad y Defensa (PCSD), la comunicación al público debe coordinarse con el SEAE y el Servicio del Portavoz del AR/VP.

Cooperación a nivel operativo

Gama de actividades:

— Preparación de la toma de decisiones a nivel político.

— Coordinación de la gestión de las crisis de ciberseguridad (según proceda).

— Evaluación de las consecuencias y del impacto a nivel de la UE, y propuesta de posibles medidas de mitigación.

Agentes potenciales:

— Estados miembros

  — Autoridades competentes y puntos de contacto únicos establecidos por la Directiva SRI.

  — CSIRT y agencias de ciberseguridad.

  — Otras autoridades sectoriales nacionales (en caso de incidente o crisis multisectorial).

— Órganos/oficinas/agencias de la UE

  — ENISA.

  — Europol/EC3.

  — CERT-UE.

— Comisión Europea

  — Secretario General (Adjunto) SG (procedimiento ARGUS).

  — DG CNECT/HOME.

  — Autoridad de Seguridad de la Comisión.

  — Otras DDGG (en caso de incidente o crisis multisectorial).

([1]) Asesoramiento de carácter técnico respecto a las causas del incidente y posibles medidas de mitigación.
([2]) Información sobre la vulnerabilidad técnica que se está aprovechando para afectar negativamente a los sistemas informáticos.

— SEAE

  — Secretario General (Adjunto) encargado de la respuesta a las crisis y SIAC (INTCEN y EMUE INT).

  — Célula de fusión de la UE contra las amenazas híbridas.

— Consejo

  — Presidencia [Presidente del Grupo horizontal sobre cuestiones cibernéticas o del Coreper ([1])] con el apoyo de la SGC, o del CPS ([2]) y —si se activa— con el apoyo del DIRPC.

Conocimiento de la situación:

— Apoyo a la elaboración de informes político-estratégicos de situación (por ejemplo, el informe ISAA en caso de activación del DIRPC).

— El *Grupo horizontal del Consejo sobre cuestiones cibernéticas* prepara la reunión del Coreper o del CPS según proceda.

— En caso de activación del DIRPC,

  — La Presidencia podrá convocar mesas redondas en apoyo de su preparación para el Coreper o el CPS, con la participación de partes interesadas pertinentes de los Estados miembros, las instituciones, las agencias y terceros, tales como países de fuera de la UE y organizaciones internacionales. Se trata de reuniones de crisis para detectar los estrangulamientos y presentar propuestas de acción sobre cuestiones transversales.

  — El *servicio responsable de la Comisión o el SEAE* para dirigir el ISAA elabora el informe ISAA con contribuciones de la ENISA, la red de CSIRT, Europol/EC3, EMUE INT, INTCEN y todos los demás agentes pertinentes. El informe ISAA representa una evaluación a escala de la UE basada en la correlación de evaluaciones de incidentes técnicos y crisis (análisis de amenazas, evaluaciones de riesgos, consecuencias y efectos no técnicos, aspectos no cibernéticos del incidente o crisis, etc.) que se adapta a las necesidades de los niveles político y operativo.

— En caso de activación de ARGUS,

  — El CERT-UE y el EC3 ([3]) contribuyen directamente al intercambio de información dentro de la Comisión.

— En caso de activación del Mecanismo de Respuesta a las Crisis del SEAE,

  — La SIAC intensificará su recogida de información, reunirá la información procedente de todas las fuentes y preparará un análisis y una evaluación del incidente.

Respuesta (a petición del nivel político):

— Cooperación transfronteriza con el punto de contacto único y las autoridades nacionales competentes (Directiva SRI), para mitigar las consecuencias y efectos.

— Activación de todas las medidas técnicas de mitigación y coordinación de las capacidades técnicas necesarias para evitar o reducir el impacto de los ataques a los sistemas de información objeto de los mismos.

— Cooperación y, si así se decide, coordinación de las capacidades técnicas en aras de una respuesta conjunta o en colaboración de conformidad con los ***PTN de la red de CSIRT.***

— Evaluación de la necesidad de cooperar con terceras partes pertinentes.

— Toma de decisiones dentro del procedimiento ARGUS (si se activa).

— Preparación de las decisiones y coordinación de conformidad con el DIRPC (si se activa).

— Apoyo a la toma de decisiones del SEAE (si se activa) mediante el Mecanismo de Respuesta a las Crisis del SEAE, también en lo que se refiere a los contactos con terceros países y organizaciones internacionales, así como cualquier medida destinada a garantizar la protección de las misiones y operaciones de la PCSD y las delegaciones de la UE.

([1]) El Comité de Representantes Permanentes o Coreper (artículo 240 del Tratado de Funcionamiento de la Unión Europea, TFUE) se encarga de preparar los trabajos del Consejo de la Unión Europea.

([2]) El Comité Político y de Seguridad es un comité del Consejo de la Unión Europea que se ocupa de la Política Exterior y de Seguridad Común (PESC), según se menciona en el artículo 38 del Tratado de la Unión Europea.

([3]) Según las condiciones y procedimientos establecidos en el marco jurídico del CE3.

Comunicaciones al público

— Acuerdo sobre los mensajes al público en relación con el incidente.

— Si la crisis tiene una dimensión de política exterior o de Política Común de Seguridad y Defensa (PCSD), la comunicación al público debe coordinarse con el SEAE y el Servicio del Portavoz del AR/VP.

Cooperación a nivel estratégico/político

Agentes potenciales

— Por los Estados miembros, los ministros responsables de la ciberseguridad.

— Por el Consejo Europeo, el Presidente.

— Por el Consejo, la Presidencia de turno.

— En caso de medidas dentro del «conjunto de instrumentos de ciberdiplomacia», el CPS y el Grupo Horizontal.

— Por la Comisión Europea, el Presidente o el Vicepresidente/Comisario delegado.

— El Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad/Vicepresidente de la Comisión.

Gama de actividades: Gestión estratégica y política de los aspectos de la crisis, tanto cibernéticos como no cibernéticos, con inclusión de medidas con arreglo al marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas.

Conocimiento compartido de la situación

— Identificación de los impactos de las perturbaciones causadas por la crisis sobre el funcionamiento de la Unión.

Respuesta:

— Activación de mecanismos e instrumentos adicionales de gestión de crisis, en función de la naturaleza y el impacto del incidente. Puede incluirse, por ejemplo, el Mecanismo de Protección Civil.

— Toma de medidas con arreglo al marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas.

— Ayuda de emergencia puesta a disposición de los Estados miembros afectados, por ejemplo activando el Fondo de Respuesta en casos de Emergencia de Ciberseguridad ([1]) una vez sea aplicable.

— Cooperación y coordinación, cuando proceda, con organizaciones internacionales como las Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y, en particular, la OTAN.

— Evaluación de las consecuencias para la seguridad y la defensa nacionales.

Comunicaciones al público

Decisión sobre una estrategia común de comunicación al público.

RESPUESTA COORDINADA CON LOS ESTADOS MIEMBROS A NIVEL DE LA UE EN EL MARCO DEL DIRPC

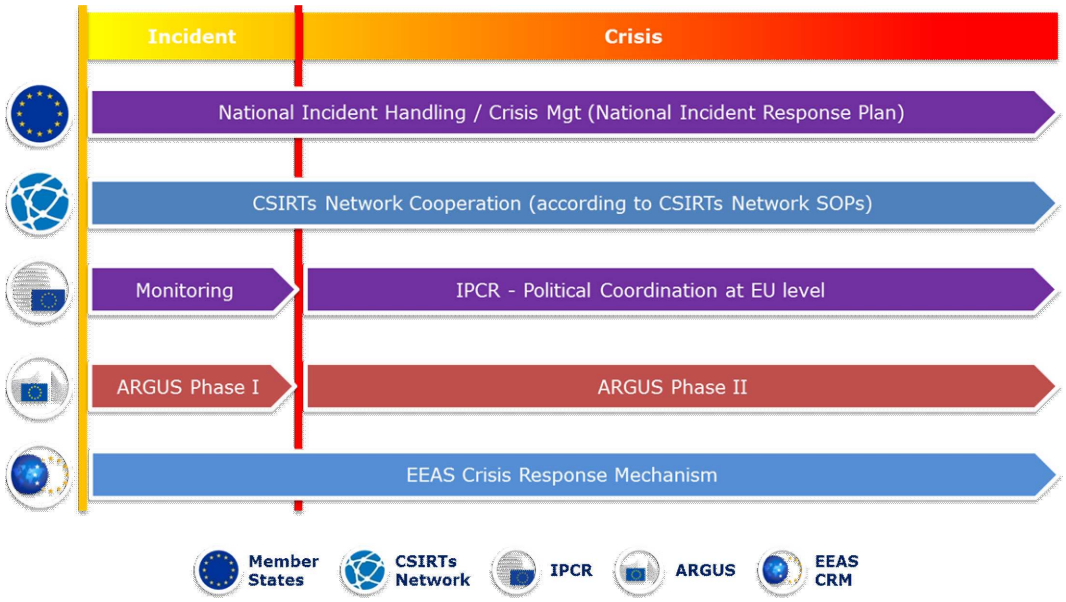
En virtud del principio de complementariedad a nivel de la UE, la presente sección introduce y detalla en particular el objetivo central y las responsabilidades y actividades de las autoridades de los Estados miembros, la red de CSIRT, ENISA, CERT-EU, Europol/EC3, INTCEN, la Célula de Fusión de la UE contra las Amenazas Híbridas y el Grupo horizontal del Consejo sobre cuestiones cibernéticas dentro del proceso del DIRPC. Se supone que los agentes actúan en consonancia con los procedimientos establecidos a nivel nacional o de la UE.

Es fundamental tener en cuenta que, tal como se ilustra en la figura 1, con independencia de la activación de los mecanismos de gestión de crisis de la UE, hay actividades a nivel nacional y también de cooperación en la Red de los CSIRT (en caso necesario) que tienen lugar a lo largo de cualquier crisis/incidente de acuerdo con los principios de subsidiariedad y proporcionalidad.

([1]) El Fondo de Emergencia de Ciberseguridad es una acción propuesta en la Comunicación conjunta «Resiliencia, disuasión y defensa: Reforzar la ciberseguridad de la UE», JOIN(2017) 450/1.

Figura 1

Respuesta a los incidentes/crisis de ciberseguridad a nivel de la UE



Todas las actividades descritas a continuación se deben realizar de conformidad con las normas y procedimientos de trabajo normalizados de los mecanismos de cooperación participantes y de acuerdo con los mandatos y competencias de los distintos agentes e instituciones. Dichos procedimientos y normas pueden necesitar algunas adiciones o modificaciones a fin de lograr la mejor cooperación posible y una respuesta eficaz en caso de crisis e incidentes de ciberseguridad a gran escala.

No todos los agentes que figuran a continuación tienen que tomar medidas durante cualquier incidente particular. No obstante, en el Plan director y en los procedimientos de trabajo normalizados pertinentes de los mecanismos de cooperación debe preverse su posible participación.

Dado el diferente grado de impacto sobre la sociedad que puede tener un incidente o crisis de ciberseguridad, debe haber un alto grado de flexibilidad en cuanto a la participación de los actores sectoriales a todos los niveles, y toda respuesta adecuada habrá de basarse en actividades de mitigación de carácter tanto cibernético como no cibernético.

Gestión de crisis de ciberseguridad — Integración de la ciberseguridad dentro del proceso del DIRPC

El DIRPC, como se describe en sus PTN ([1]), sigue secuencialmente los pasos que se describen a continuación (el uso de algunos de estos pasos dependerá de la situación).

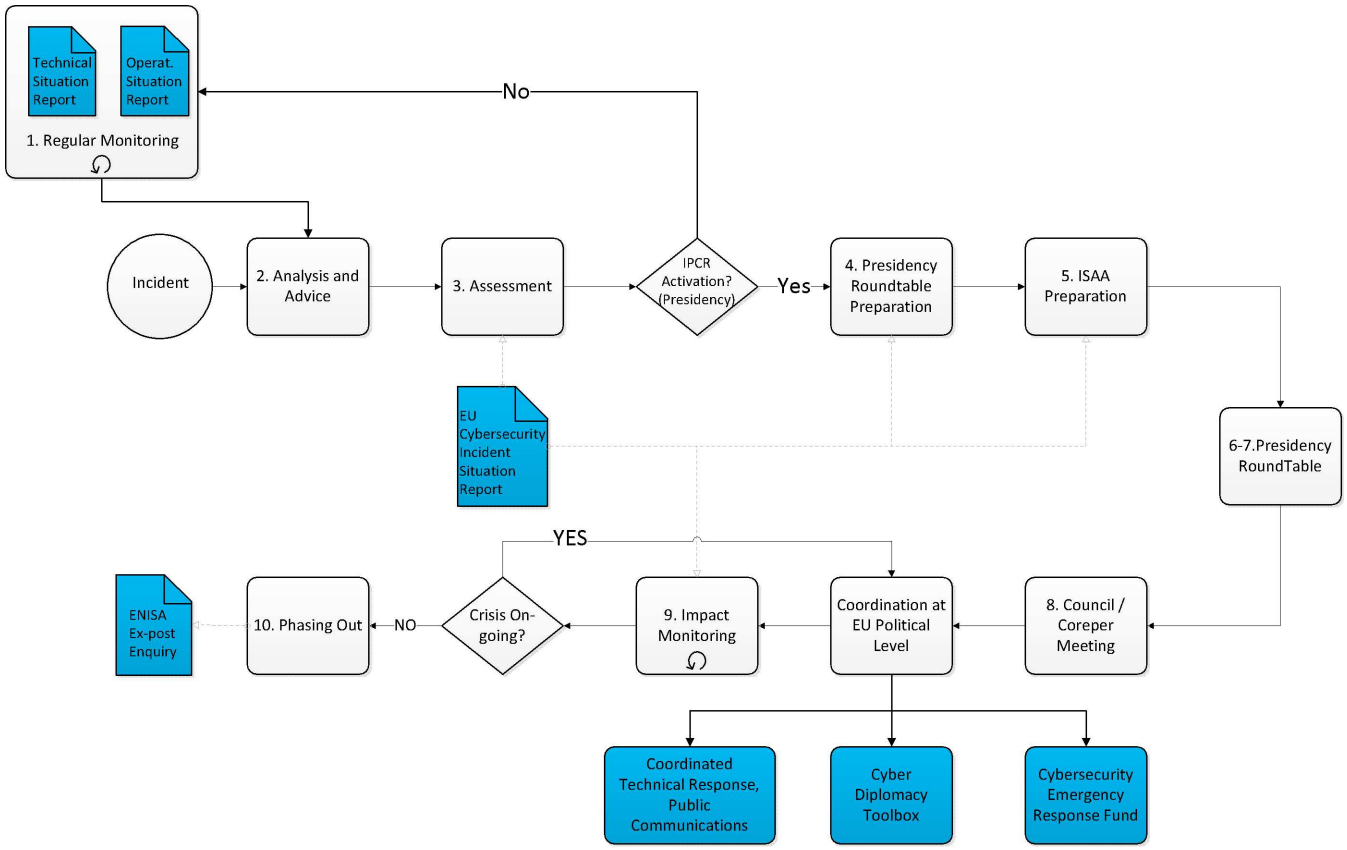
En cada paso se especifican actividades y agentes relacionados con la ciberseguridad. Para facilitar la lectura, en cada paso se presenta el texto de los PTN de la RPC, seguido de las actividades específicas del Plan director. Este enfoque paso a paso también permite una clara identificación de las **deficiencias** existentes en las capacidades y procedimientos necesarios que impiden una respuesta eficaz a las crisis de ciberseguridad.

La figura 2 [a continuación ([2])] es una representación gráfica del proceso del DIRPC en la que los nuevos elementos que se introducen se resaltan en azul.

([1]) Del documento 12607/15 «IPCR Standard Operating Procedures», acordado por el Grupo «Amigos de la Presidencia» y anotado por el Coreper en octubre de 2015.
([2]) En el apéndice se encuentra una versión mayor de la figura.

Figura 2

Elementos específicos de la ciberseguridad del DIRPC



Nota: Dada la naturaleza de las amenazas híbridas en el ciberespacio que están diseñadas para permanecer por debajo del umbral de crisis reconocible, la UE debe tomar medidas preventivas y de preparación. La Célula de Fusión de la UE contra las Amenazas Híbridas tiene la tarea de analizar con rapidez los incidentes pertinentes e informar a las estructuras de coordinación apropiadas. La presentación de informes periódicos de la Célula de Fusión puede contribuir a informar a las instancias que elaboran las políticas sectoriales, a fin de mejorar la preparación.

— **Paso 1 — Vigilancia y alerta sectorial periódica:** Los actuales informes de situación y alertas periódicos por sectores facilitan indicaciones a la Presidencia del Consejo sobre una crisis en desarrollo y su posible evolución.

— **Deficiencia señalada:** En la actualidad no existen informes de situación y alertas periódicos y coordinados sobre la ciberseguridad por lo que se refiere a los incidentes (y amenazas) de ciberseguridad a nivel de la UE.

— **Plan director: Vigilancia/notificación de la situación de ciberseguridad de la UE**

— La ENISA preparará un **informe periódico sobre la situación técnica de ciberseguridad de la UE** en cuanto a incidentes y amenazas de ciberseguridad, sobre la base de la información públicamente disponible, su propio análisis y los informes compartidos con ella por los CSIRT de los Estados miembros (de forma voluntaria) o los puntos de contacto únicos de la Directiva SRI, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, el CERT-UE y el Centro de Inteligencia de la Unión Europea (INTCEN) en el Servicio Europeo de Acción Exterior (SEAE). El informe debe ponerse a disposición de las instancias pertinentes del Consejo, la Comisión y la red de CSIRT.

— En nombre de la SIAC, la Célula de Fusión de la UE contra las Amenazas Híbridas debe elaborar un **informe de situación operativa sobre la ciberseguridad de la UE**. El informe también presta ayuda al marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas.

— Ambos informes se difunden a las partes interesadas nacionales y de la UE a fin de mejorar su propio conocimiento de la situación, contribuir a la toma de decisiones y facilitar la cooperación regional transfronteriza.

Tras la detección de un incidente

— **Paso 2 — Análisis y asesoramiento:** Sobre la base de la vigilancia y alerta disponibles, los servicios de la Comisión, el SEAE y la SGC se mantienen mutuamente informados sobre la posible evolución, a fin de estar preparados para asesorar a la Presidencia en relación con una posible activación (plena o en modo de intercambio de información) del DIRPC.

— **Plan director:**

— Por la Comisión, DG CNECT, DG HOME, DG HR.DS y DG DIGIT, con el apoyo de la ENISA, el EC3 y el CERT-UE.

— SEAE: Basándose en el trabajo realizado por la SITROOM y en fuentes de inteligencia, la Célula de Fusión de la UE contra las Amenazas Híbridas proporciona conocimiento de la situación sobre amenazas híbridas reales y potenciales que afecten a la UE y sus socios, incluidas las amenazas cibernéticas. Por lo tanto, cuando el análisis y valoración de la Célula de Fusión de la UE contra las Amenazas Híbridas indique la existencia de posibles amenazas dirigidas contra un Estado miembro, países socios o una organización, el INTCEN informará (en primera instancia) a nivel operativo, con arreglo a los procedimientos establecidos. El nivel operativo preparará entonces recomendaciones para el nivel estratégico político, incluida la posible activación de mecanismos de gestión de crisis en modo de vigilancia (por ejemplo, el Mecanismo de Respuesta a las Crisis del SEAE o la página de vigilancia del DIRPC).

— El presidente de la Red de CSIRT, con la ayuda de la ENISA, prepara un informe de situación del incidente de ciberseguridad de la UE ([1]) que se presentará a la Presidencia, a la Comisión y al AR/VP a través del CSIRT de la Presidencia de turno.

— **Paso 3 — Evaluación/Decisión sobre la activación del DIRPC:** La Presidencia evalúa la necesidad de coordinación política, intercambio de información o toma de decisiones a nivel de la UE. A tal fin, la Presidencia podrá convocar una mesa redonda informal. La Presidencia efectúa una primera identificación de los ámbitos que requieren la implicación del Coreper o del Consejo. Esto constituirá la base de las directrices para la elaboración de los informes de conocimiento y análisis integrados de la situación (ISAA). La Presidencia decidirá, a la luz de las características de la crisis, sus posibles consecuencias y las necesidades políticas conexas, sobre la conveniencia de convocar reuniones de los grupos pertinentes del Consejo y/o del Coreper y/o del CPS.

— **Plan director:**

— Participantes en la mesa redonda:

— Los servicios de la Comisión y el SEAE asesorarán a la Presidencia sobre sus ámbitos de competencia respectivos.

— Representantes de los Estados miembros en el Grupo horizontal sobre cuestiones cibernéticas apoyados por expertos de las capitales (CSIRT, autoridades competentes en materia de ciberseguridad, otros).

— Orientaciones políticas/estratégicas para los informes ISAA sobre la base del último informe de situación de incidentes de ciberseguridad de la UE e información adicional proporcionada por los participantes en la mesa redonda.

— Grupos de trabajo y comités pertinentes:

— Grupo horizontal cuestiones cibernéticas.

La Comisión, el SEAE y la SGC, en pleno acuerdo y en asociación con la Presidencia, podrán también decidir la activación del DIRPC en modo de intercambio de información a través de la generación de una página de crisis, a fin de preparar el terreno para una posible activación plena.

— **Paso 4 — Activación del DIRPC/recogida e intercambio de información:** Una vez activado (bien plenamente o bien en modo de intercambio de información), se genera una página de crisis en la plataforma web del DIRPC, que permite intercambios específicos de información centrada en los aspectos que contribuirán al ISAA y a preparar el debate a nivel político. El servicio responsable del ISAA (uno de los servicios de la Comisión o el SEAE) dependerá de las circunstancias del caso.

— **Paso 5 — Elaboración de los informes ISAA:** Se pondrá en marcha la elaboración de los informes ISAA. La Comisión o el SEAE publicará los informes ISAA como se indica en los PTN del ISAA y podrá fomentar más el

([1]) El informe de situación del incidente de ciberseguridad de la UE es una agrupación de los informes nacionales proporcionados por los CSIRT nacionales. El formato del informe debe describirse en los procedimientos de trabajo normalizados de la red de CSIRT.

intercambio de información en la plataforma web del DIRPC o lanzar peticiones específicas de información. Los informes ISAA se adaptarán a las necesidades del nivel político (es decir, el Coreper o el Consejo), según defina la Presidencia y recoja en sus directrices, permitiendo así una síntesis estratégica de la situación y un debate con conocimiento de causa sobre los puntos del orden del día definido por la Presidencia. De conformidad con los PTN del ISAA, la naturaleza de la crisis de ciberseguridad determinará si el informe ISAA es elaborado por uno de los servicios de la Comisión (DG CNECT, DG HOME) o por el SEAE.

Tras la activación del DIRPC, la Presidencia indicará los ámbitos específicos de interés para el ISAA a fin de dar apoyo a la coordinación política o al proceso de toma de decisiones en el Consejo. La Presidencia también especificará el calendario del informe, previa consulta con los servicios de la Comisión o el SEAE.

— **Plan director:**

— El informe ISAA contiene contribuciones de los servicios pertinentes, incluyendo los siguientes:

— La red de CSIRT en forma de informe de situación de los incidentes de ciberseguridad de la UE.

— EC3, SITROOM, la Célula de Fusión de la UE contra las Amenazas Híbridas, el CERT-UE. La Célula de Fusión de la UE contra las Amenazas Híbridas apoyará y aportará sus contribuciones al servicio responsable del ISAA y a la mesa redonda del DIRPC, según proceda.

— Agencias y organismos sectoriales de la UE en función de los sectores afectados.

— Autoridades de los Estados miembros (distintas de los CSIRT).

— Reunión de las aportaciones del ISAA ([1]):

— Comisión y agencias de la UE: El sistema informático ARGUS proporcionará la red básica interna para el ISAA. Las agencias de la UE enviarán sus contribuciones a sus respectivas DG de tutela, que a su vez pasarán la información pertinente a ARGUS. Los servicios de la Comisión y las agencias reunirán la información procedente de las redes sectoriales existentes con los Estados miembros y las organizaciones internacionales y de otras fuentes pertinentes.

— Por el SEAE: la Sala de Guardia de la UE, apoyada por el resto de los departamentos pertinentes del SEAE, proporcionará la red básica interior y el punto de contacto único para el ISAA. El SEAE reunirá la información procedente de los terceros países y de las organizaciones internacionales pertinentes.

— **Paso 6 — Preparación de la mesa redonda informal de la Presidencia:** La Presidencia, asistida por la Secretaría General del Consejo, determinará el calendario, el orden del día, los participantes y los resultados esperados (posibles productos concretos) de la mesa redonda informal de la Presidencia. La SGC difundirá en la plataforma web del DIRPC en nombre de la Presidencia la información pertinente y, en concreto, el aviso de la reunión.

— **Paso 7 — Mesa redonda de la Presidencia/medidas preparatorias para la coordinación política/toma de decisiones de la UE:** La Presidencia convocará una mesa redonda informal para revisar la situación, y preparar y revisar los puntos que se vayan a someter a la atención del Coreper o del Consejo. La mesa redonda informal de la Presidencia constituirá también un foro en el que elaborar, revisar y debatir todas las propuestas de medidas que deban presentarse al Coreper/Consejo.

— **Plan director:**

— El Grupo horizontal del Consejo sobre cuestiones cibernéticas debe preparar la reunión del CPS o del Coreper.

— **Paso 8 — Coordinación política y toma de decisiones en el Coreper/Consejo:** Los resultados de las reuniones del Coreper o del Consejo se refieren a la coordinación de las actividades de respuesta a todos los niveles, decisiones sobre medidas excepcionales, declaraciones políticas, etc. Estas decisiones también constituyen unas directrices estratégicas/políticas actualizadas para la elaboración posterior de informes ISAA.

— **Plan director:**

— La decisión política de coordinar la respuesta a la crisis de ciberseguridad es ejecutada a través de las actividades (realizadas por los agentes correspondientes) que se describen arriba, en la sección 1 «Cooperación a los niveles estratégico/político, operativo y técnico» por lo que se refiere a la **Respuesta** y a la **Comunicación al público**.

— La elaboración de informes ISAA continúa sobre la base de la cooperación a los niveles técnico, operativo y político/estratégico en lo que respecta al **Conocimiento de la situación**, como también se describe en la sección 1.

([1]) PTN del ISAA.

— **Paso 9 — Vigilancia del impacto:** El servicio responsable del ISAA, con la ayuda de quienes contribuyen a este, aporta información sobre la evolución de la crisis y sobre el impacto de las decisiones políticas tomadas. Este circuito de realimentación apoyará un proceso dinámico y contribuirá a la decisión de la Presidencia sobre si continuar con la participación del nivel político de la UE o si reducir el DIRPC.

— **Paso 10 — Disminución progresiva:** Siguiendo el mismo proceso que para la activación, la Presidencia podrá convocar una mesa redonda informal para evaluar la conveniencia de mantener activo o no el DIRPC. La Presidencia puede decidir concluir o rebajar la activación.

— **Plan director:**

— La ENISA podrá ser invitada a contribuir a una investigación técnica del incidente *a posteriori*, o a realizarla, de conformidad con lo dispuesto en su mandato.

APÉNDICE

1. GESTIÓN DE CRISIS, MECANISMOS DE COOPERACIÓN Y AGENTES A NIVEL DE LA UE

Mecanismos de gestión de crisis

Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC): El Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC), aprobado por el Consejo el 25 de junio de 2013 ([1]), tiene por objeto facilitar la oportuna coordinación y respuesta a nivel político de la UE en caso de crisis importante. El DIRPC también apoya la coordinación a nivel político de la respuesta a la invocación de la cláusula de solidaridad (artículo 222 del TFUE), como se define en la Decisión 2014/415/UE del Consejo, sobre la aplicación por la Unión de la cláusula de solidaridad, adoptada el 24 de junio de 2014. Los procedimientos de trabajo normalizados (PTN) del DIRPC ([2]) establecen el procedimiento de activación y las medidas posteriores que deban tomarse.

ARGUS: Sistema de coordinación de crisis establecido por la Comisión Europea en 2005 para facilitar un proceso específico de coordinación en caso de crisis multisectorial importante. Está respaldado por un sistema de alerta rápida general (herramienta informática) con el mismo nombre. ARGUS prevé dos fases, de las que la fase II (en caso de crisis multisectorial importante) implica reuniones del Comité de coordinación de crisis (CCC) bajo la autoridad del Presidente de la Comisión o de un Comisario al que se haya atribuido la responsabilidad. El CCC reúne a representantes de las direcciones generales pertinentes de la Comisión, gabinetes, y otros servicios de la UE con el fin de dirigir y coordinar la respuesta de la Comisión a la crisis. Presidido por el Secretario General Adjunto, el CCC evalúa la situación, considera las opciones y toma decisiones que permiten actuar en relación con los instrumentos y herramientas de la UE bajo la responsabilidad de la Comisión, y garantiza la ejecución de las decisiones adoptadas ([3]) ([4]).

Mecanismo de Respuesta a las Crisis del SEAE: El Mecanismo de Respuesta a las Crisis del SEAE (CRM) es un sistema estructurado para que el SEAE responda a las crisis y emergencias que tengan carácter exterior o una importante dimensión exterior, incluidas las amenazas híbridas, que afecten realmente o en potencia a los intereses de la UE o a los de cualquier Estado miembro. Al velar por la participación en sus reuniones de los funcionarios pertinentes de la Comisión y de la Secretaría del Consejo, el CRM facilita la sinergia entre los esfuerzos diplomáticos, de seguridad y de defensa con los instrumentos financieros, comerciales y de cooperación gestionados por la Comisión. La Célula de Crisis puede estar activada mientras dure la crisis.

Mecanismos de cooperación

Red de CSIRT: La red de equipos de respuesta a incidentes de seguridad informática reúne a todos los CSIRT nacionales y gubernamentales y al CERT-UE. El propósito de la red es permitir y mejorar el intercambio de información entre los CSIRT sobre las amenazas e incidentes de ciberseguridad y también cooperar en la respuesta a los incidentes y crisis de ciberseguridad.

Grupo horizontal del Consejo sobre cuestiones cibernéticas: Este Grupo se creó con el fin de garantizar la coordinación estratégica y horizontal de las cuestiones de política cibernética en el Consejo y puede participar en actividades tanto legislativas como no legislativas.

Agentes

ENISA: La Agencia de Seguridad de las Redes y de la Información de la Unión Europea se creó en 2004. Trabaja en estrecha colaboración con los Estados miembros y el sector privado para ofrecer soluciones y asesoramiento sobre cuestiones tales como los ejercicios de ciberseguridad paneuropeos, la elaboración de las estrategias nacionales de ciberseguridad, la cooperación de los CSIRT y el desarrollo de capacidades. La ENISA colabora directamente con los CSIRT en toda la UE y es la Secretaría de la red de CSIRT.

CECRE: El Centro de Coordinación de la Respuesta a Emergencias de la Comisión (dentro de la Dirección General de Protección Civil y Operaciones de Ayuda Humanitaria Europeas, DG ECHO) apoya y coordina una gran variedad de actividades de prevención, preparación y respuesta de forma ininterrumpida (24/7). Inaugurado en 2013, es el eje central de la respuesta de la Comisión a las crisis (enlace con otras salas de crisis de la UE), también en su función de punto de contacto central del DIRPC, de funcionamiento ininterrumpido (24/7).

([1]) Doc. 10708/13 sobre la «Finalización del proceso de revisión del DCC: Dispositivo de respuesta política integrada de la UE a las crisis», aprobado por el Consejo el 24 de junio de 2013.

([2]) Doc. 12607/15 «IPCR Standard Operating Procedures», acordado por el Grupo «Amigos de la Presidencia» y anotado por el Coreper en octubre de 2015.

([3]) Disposiciones de la Comisión sobre el sistema de alerta rápida general «ARGUS», COM(2005) 662 final, de 23 de diciembre de 2005.

([4]) Decisión 2006/25/CE, Euratom de la Comisión, de 23 de diciembre de 2005, por la que se modifica su reglamento interno (DO L 19 de 24.1.2006, p. 20), por la que se crea el sistema de alerta rápida general «ARGUS».

Europol/EC3: El Centro Europeo de Ciberdelincuencia (EC3), creado en 2013 dentro de Europol, apoya la respuesta policial a la ciberdelincuencia en la UE. El EC3 ofrece apoyo analítico y operativo a las investigaciones de los Estados miembros y sirve como nodo central de inteligencia e información de asuntos criminales en apoyo de las operaciones e investigaciones de los Estados miembros con sus análisis operativos, coordinación y conocimientos especializados, así como con sus medios técnicos altamente especializados y ayuda forense digital.

CERT-UE: El Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE tiene mandato para mejorar la protección de las instituciones, órganos y organismos de la UE contra las amenazas cibernéticas. Es miembro de la red de CSIRT. El CERT-UE tiene acuerdos técnicos relativos al intercambio de información sobre las amenazas cibernéticas con el CIRC de la OTAN, algunos terceros países y grandes agentes comerciales en el ámbito de la ciberseguridad.

La Comunidad de Inteligencia de la UE comprende el Centro de Análisis de Inteligencia de la UE (**INTCEN**) y la División de Información del Estado Mayor de la UE (EMUE INT) con arreglo al acuerdo sobre la **Capacidad Única de Análisis de Inteligencia** (SIAC). La misión de la SIAC es aportar análisis de inteligencia, alerta rápida y conocimiento de la situación al Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad y al Servicio Europeo de Acción Exterior (SEAE). La SIAC ofrece sus servicios a los diferentes órganos de toma de decisiones de la UE en los ámbitos de la Política Exterior y de Seguridad Común (PESC), la Política Común de Seguridad y Defensa (PCSD) y lucha contra el terrorismo (CT), así como a los Estados miembros. El INTCEN y el EMUE INT no son agencias operativas y carecen de capacidad de recogida de información. El nivel operativo de inteligencia es responsabilidad de los Estados miembros. La SIAC solo se ocupa de análisis estratégicos.

Célula de Fusión de la UE contra las Amenazas Híbridas: La Comunicación conjunta sobre la lucha contra las amenazas híbridas, de abril de 2016, designa a la Célula de Fusión de la UE contra las Amenazas Híbridas (CFH UE) como punto central para todos los análisis de fuentes sobre las amenazas híbridas en la UE; su mandato fue aprobado en diciembre de 2016 por la Comisión a través de una consulta interservicios. Situada dentro del INTCEN, la Célula de Fusión de la UE contra las Amenazas Híbridas forma parte de la SIAC y, por lo tanto, trabaja conjuntamente con el EMUE INT y tiene asignado un miembro militar permanente. El adjetivo «híbrido» se refiere al uso deliberado por un agente estatal o no estatal de una combinación de múltiples herramientas y resortes de carácter manifiesto/encubierto, militar/civil, tales como ciberataques, campañas de desinformación, espionaje, presión económica, uso de fuerzas afines u otras actividades subversivas. La CFH UE trabaja con una amplia red de puntos de contacto, tanto en el seno de la Comisión como en los Estados miembros, para proporcionar la respuesta integrada o el conjunto del planteamiento gubernamental necesario para hacer frente a diversos retos.

SITROOM UE: La Sala de Guardia de la UE forma parte del Centro de Análisis de Inteligencia de la UE (INTCEN), y aporta al SEAE capacidad operativa a fin de garantizar una respuesta inmediata y eficaz a las crisis. Se trata de un organismo civil-militar disponible permanentemente que facilita la vigilancia mundial y el conocimiento de la situación con un funcionamiento ininterrumpido (24/7).

Instrumentos pertinentes

Marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas: El marco, acordado en junio de 2017, forma parte integrante del enfoque de la UE sobre la ciberdiplomacia, que contribuye a la prevención de conflictos, la mitigación de las amenazas contra la seguridad cibernética y a una mayor estabilidad en las relaciones internacionales. El Marco hace pleno uso de medidas dentro de la Política Exterior y de Seguridad Común, incluyendo, en caso necesario, la adopción de medidas restrictivas. La utilización de las medidas del Marco debe fomentar la cooperación, facilitar la mitigación de las amenazas inmediatas y a largo plazo e influir en el comportamiento del autor responsable y de posibles agresores a largo plazo.

2. COORDINACIÓN ANTE LAS CRISIS DE CIBERSEGURIDAD EN EL DIRPC: CAPA DE COORDINACIÓN HORIZONTAL Y ESCALADA POLÍTICA

El DIRPC puede ser utilizado (y lo ha sido) para hacer frente a cuestiones técnicas y operativas, pero siempre desde un punto de vista político/estratégico.

En términos de escalada, el DIRPC puede utilizarse según el nivel de la crisis, pasando del «modo de vigilancia» al «modo de intercambio de información», que es el primer nivel de activación del DIRPC, y a la «activación plena del DRPIC».

El paso a la activación plena corresponde a una decisión de la Presidencia de turno del Consejo de la UE. La Comisión, el SEAE y la SGC pueden activar el DIRPC en modo de intercambio de información. El modo de vigilancia y el de

intercambio de información corresponden a distintos niveles de información compartida, ya que el modo de intercambio de información implica una petición de elaboración de informes ISAA. La activación plena añade a la caja de herramientas mesas redondas del DIRPC, con participación de la Presidencia (normalmente el presidente del Coreper II, o un experto en el tema a nivel de consejero de las Representaciones Permanentes, pero excepcionalmente se han celebrado mesas redondas a nivel ministerial).

Agentes

Se encarga de la dirección la Presidencia de turno (normalmente, el presidente del Coreper).

Por el Consejo Europeo, el Gabinete del Presidente.

Por la Comisión Europea, el Secretario General Adjunto/a nivel de DG y/o de expertos sobre el tema.

Por el SEAE, el Secretario General Adjunto/a nivel de director ejecutivo y/o de expertos sobre el tema.

Por lo que respecta a la SGC, el Gabinete del Secretario General, el equipo del DIRPC y las Direcciones Generales responsables.

Gama de actividades: Generación de una visión integrada común de la situación y aumento de la sensibilización ante los estrangulamientos o deficiencias a cada uno de los tres niveles, a fin de tratarlos al nivel político, generación de decisiones en la mesa si entran dentro del ámbito de competencias de los participantes, o generación de propuestas de actuación que vayan al Coreper II y hasta el Consejo.

Conocimiento compartido de la situación

(No activado): Pueden generarse páginas de vigilancia del DIRPC para seguir la evolución de las situaciones que puedan escalar hasta una crisis con ramificaciones en la UE.

(Intercambio de información del DIRPC): Los informes ISAA serán redactados por el responsable de este, sobre la base de las contribuciones de los servicios de la Comisión, el SEAE y los Estados miembros (a través de los cuestionarios del DIRPC).

(Activación plena del DIRPC): Además de los informes ISAA, las mesas redondas informales del DIRPC reúnen a los distintos agentes interesados de los Estados miembros, la Comisión, el SEAE, las agencias pertinentes, etc., para debatir las deficiencias y estrangulamientos.

Cooperación y respuesta

Activación/sincronización de mecanismos/instrumentos adicionales de gestión de crisis, en función de la naturaleza y del impacto del incidente. Entre ellos se pueden incluir, por ejemplo, el Mecanismo de Protección Civil, el marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas o el marco común relativo a la lucha contra las amenazas híbridas.

Comunicaciones en caso de crisis

La red del comunicador de crisis del DIRPC puede ser activada por la Presidencia, previa consulta con los servicios pertinentes de la Comisión, la SGC y el SEAE, con el fin de apoyar la creación de mensajes comunes o elaborar los instrumentos de comunicación más eficaces.

3. GESTIÓN DE LAS CRISIS DE CIBERSEGURIDAD EN ARGUS: INTERCAMBIO DE INFORMACIÓN DENTRO DE LA COMISIÓN EUROPEA

Tras enfrentarse a crisis imprevistas que exigieron medidas a nivel europeo, como los atentados terroristas de Madrid (marzo de 2004), el tsunami del sudeste asiático (diciembre de 2004) y los ataques terroristas de Londres (julio de 2005), en 2005 la Comisión creó el sistema de coordinación ARGUS, con el apoyo de un sistema de alerta rápida general del mismo nombre ([1]) ([2]). Su objetivo es ofrecer un **procedimiento específico de coordinación de crisis** en caso de crisis multisectorial importante, a fin de permitir el intercambio en tiempo real de información relacionada con la crisis, y asegurar una rápida toma de decisiones.

ARGUS define dos fases en función de la gravedad del caso:

Fase I: utilizada para «compartir información» sobre una crisis de escala limitada

([1]) Comisión de las Comunidades Europeas, 23 de diciembre de 2005: Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Disposiciones de la Comisión sobre el sistema de alerta rápida general «ARGUS», COM(2005) 662 final.

([2]) Decisión 2006/25/CE, Euratom.

Entre los ejemplos de incidentes notificados recientemente en la fase I se incluyen los incendios forestales de Portugal e Israel, el ataque de Berlín de 2016, las inundaciones de Albania, el huracán Matthew en Haití y la sequía en Bolivia. Cualquier DG puede iniciar un incidente en fase I si considera que una situación en su ámbito de competencia es lo suficientemente grave como para justificar la puesta en común de información o poder beneficiarse de esta. Por ejemplo, la DG CNECT o la DG HOME pueden iniciar un incidente en fase I si consideran que una situación de ciberseguridad en su ámbito de competencia es lo suficientemente grave como para justificar la puesta en común de información o poder beneficiarse de esta.

Fase II: activada en caso de crisis multisectorial importante o amenaza previsible o inminente para la Unión

La fase II desencadena un proceso específico de coordinación que permite a la Comisión tomar decisiones y gestionar una respuesta rápida, coordinada y coherente, al más alto nivel en su ámbito de competencia y en cooperación con las demás instituciones. La fase II está prevista para una crisis multisectorial importante o para una amenaza previsible o inminente de una crisis así. Entre los ejemplos de la vida real de incidentes de la fase II se encuentran la crisis migratoria y de refugiados (iniciada en 2015 y todavía activa), el desastre triple de Fukushima (2011) y la erupción del volcán Eyjafjallajökull en Islandia (2010).

La fase II es activada por el presidente, por propia iniciativa o a petición de un miembro de la comisión. El presidente puede asignar la responsabilidad política de la respuesta de la comisión a un comisario responsable del servicio más afectado por la crisis en cuestión o decidir que retiene él mismo la responsabilidad.

Contempla reuniones de emergencia del Comité de coordinación de crisis (CCC). Estas reuniones se convocan bajo la autoridad del presidente o de un miembro de la Comisión a quien se haya atribuido la responsabilidad. Las reuniones son convocadas por el secretario general a través de la herramienta informática ARGUS. El CCC es una estructura operativa específica de gestión de crisis creada para dirigir y coordinar la respuesta de la Comisión a las crisis, que reúne a representantes de todas las Direcciones Generales de la Comisión, gabinetes y otros servicios de la UE. El CCC, presidido por el secretario general adjunto, evalúa la situación, considera las opciones y toma decisiones, además de velar por que se ejecuten las decisiones y medidas, garantizando al mismo tiempo la coherencia de la respuesta. La SG facilita ayuda al CCC.

4. MECANISMO DE RESPUESTA A LAS CRISIS DEL SEAE

El Mecanismo de Respuesta a las Crisis del SEAE (CRM) se activa en caso de que se presente una emergencia o situación grave relacionada con la dimensión exterior de la UE, o que afecte a esta dimensión de alguna manera. EL CRM es activado por el SGA encargado de la respuesta a las crisis, previa consulta con el AR/VP o el secretario general. También es posible que el SGA reciba del AR/VP, del SG o de otro SGA o director ejecutivo el encargo de iniciar el Mecanismo de Respuesta a las Crisis.

El CRM contribuye a la coherencia de la UE en la respuesta a las crisis dentro de la Estrategia de Seguridad. En particular, el CRM facilita la sinergia entre los esfuerzos diplomáticos, de seguridad y de defensa con los instrumentos financieros, comerciales y de cooperación gestionados por la Comisión.

El CRM está vinculado al sistema general de respuesta a las emergencias de la Comisión (ARGUS) y al Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC), a fin de explotar las sinergias en caso de activación simultánea. La Sala de Guardia del SEAE actúa como plataforma de comunicación entre el SEAE y los sistemas de respuesta a las emergencias del Consejo y de la Comisión.

Normalmente, la primera medida relacionada con la aplicación del CRM es la convocatoria de una **reunión de crisis** entre los altos cargos del SEAE, de la Comisión y del Consejo directamente afectados por la crisis en cuestión. La reunión de crisis evalúa los efectos a corto plazo de la crisis, y puede convenir la adopción de medidas inmediatas, o la activación de la Célula de Crisis, o la convocatoria de la Plataforma de Crisis. Estas vías pueden seguirse en cualquier secuencia temporal.

La **Célula de Crisis** es una pequeña sala de operaciones en la que se reúnen representantes de los servicios del SEAE, de la Comisión y del Consejo que participan en la respuesta a la crisis para vigilar continuamente la situación a fin de ayudar a los responsables de tomar las decisiones en la sede central del SEAE. Cuando se ha activado, la Célula de Crisis está operativa las 24 horas del día, 7 días a la semana.

La **Plataforma de Crisis** reúne a los servicios pertinentes del SEAE, de la Comisión y del Consejo para evaluar los efectos a medio y largo plazo de las crisis y acordar las medidas que deban tomarse. Está presidida por el AR/VP, o el secretario general, o el secretario general adjunto encargado de la respuesta a las crisis. La Plataforma de Crisis evalúa la eficacia de la acción de la UE en la región o país de la crisis, decide sobre eventuales modificaciones o medidas adicionales y debate propuestas de medidas del Consejo. La Plataforma de Crisis es una reunión *ad hoc*; por lo tanto, no está activada de forma permanente.

El **Grupo Operativo** está integrado por representantes de los servicios que participan en la respuesta y puede activarse para seguir y facilitar la ejecución de la respuesta de la UE. Evalúa el impacto de las medidas de la UE, elabora documentos sobre políticas y sobre opciones, contribuye a la preparación del Marco Político para la Gestión de Crisis (PFCA), contribuye a la Estrategia de Comunicación, y adopta cualquier otra disposición que pueda facilitar la ejecución de la respuesta de la UE.

5. DOCUMENTOS DE REFERENCIA

A continuación figura una lista de los documentos de referencia que se han tenido en cuenta en la elaboración del Plan director:

— Marco Europeo de Cooperación ante las Crisis Cibernéticas (*European Cyber Crises Cooperation Framework*), Versión 1, de 17 de octubre de 2012.

— Informe sobre cooperación y gestión de las crisis cibernéticas (*Report on Cyber Crisis Cooperation and Management*), ENISA, 2014.

— Información que permite actuar en relación con la respuesta a los incidentes de seguridad (*Actionable Information for Security Incident Response)*, ENISA, 2014.

— Prácticas comunes de gestión de crisis a escala de la UE y aplicabilidad ante crisis cibernéticas (*Common practices of EU-level crisis management and applicability to cyber crises*), ENISA, 2015.

— Estrategias de respuesta a los incidentes y cooperación ante las crisis de ciberseguridad (*Strategies for Incident Response and Cyber Crisis Cooperation*), ENISA, 2016.

— Procedimientos de trabajo normalizados en cibernética de la UE (*EU Cyber Standard Operating Procedures*), ENISA, 2016.

— Guía de buenas prácticas para el uso de taxonomías en la prevención y detección de incidentes (*A good practice guide of using taxonomies in incident prevention and detection*), ENISA, 2017.

— Comunicación «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora [COM(2016) 410 final], de 5 de julio de 2016.

— Conclusiones del Consejo» Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (15 de noviembre de 2016), doc. 14540/16.

— Decisión 2014/415/UE del Consejo, de 24 de junio de 2014, relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (DO L 192 de 1.7.2014, p. 53).

— Finalización del proceso de revisión del DCC: Dispositivo de respuesta política integrada de la UE a las crisis (DIRPC), doc. 10708/13, de 7 de junio de 2013.

— Conocimiento y análisis integrados de la situación (ISAA). Procedimientos de trabajo normalizados [*Integrated Situational Awareness and Analysis (ISAA)-Standard Operating Procedures*], DS 1570/15, de 22 de octubre de 2015.

— Disposiciones de la Comisión sobre el sistema de alerta rápida general «ARGUS», COM(2005) 662 final, de 23 de diciembre de 2005.

— Decisión 2006/25/CE, Euratom de la Comisión, de 23 de diciembre de 2005, por la que se modifica su reglamento interno (DO L 19 de 24.1.2006, p. 20).

— Modus operandi de ARGUS (*ARGUS Modus Operandi*), Comisión Europea, de 23 de octubre de 2013.

— Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»), Doc. 9916/17.

— Protocolo operativo de la UE para la lucha contra las amenazas híbridas (*EU operational protocol for countering hybrid threats «EU Playbook»*), doc. SWD(2016) 227.

— Mecanismo de respuesta a las crisis del SEAE, de 8 de noviembre de 2016 [Ares(2017)880661]. Documento de trabajo conjunto sobre el protocolo de actuación de la UE para contrarrestar las amenazas híbridas (*Joint Staff Working Document EU operational protocol for countering hybrid threats, «EU Playbook»*), SWD(2016) 227 final de 5 de julio de 2016.

— Comunicación conjunta al Parlamento Europeo y al Consejo: Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. JOIN/2016/018 final, 6 de abril de 2016.

— SEAE(2016) 1674 — Documento de trabajo del Servicio Europeo de Acción Exterior, Célula de Fusión de la UE contra las Amenazas Híbridas — Mandato (*Working Document of the European External Action Service — EU Hybrid Fusion Cell — Terms of Reference*)

6. ELEMENTOS ESPECÍFICOS DE CIBERSEGURIDAD EN EL PROCESO DEL DIRPC