COMISIÓN
EUROPEA

Bruselas, 13.9.2017
C(2017) 6100 final

RECOMENDACIÓN DE LA COMISIÓN

de 13.9.2017

sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala

RECOMENDACIÓN DE LA COMISIÓN

de 13.9.2017

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 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[4] 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

---

[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, relativa a la seguridad de las redes y sistemas de información (en lo sucesivo, «Directiva SRI»), sobre medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[4] Documento 14540/16, de 15 de noviembre de 2016.

Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC)[5]; la Comisión utilizará el proceso de coordinación de crisis intersectoriales de alto nivel ARGUS[6]. 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)[7].

(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, 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, ya se definen 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 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

[5] 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.

[6] Ibídem.

[7] Ibídem.

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[8].

(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[9].

(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[10] o el protocolo de actuación para contrarrestar las amenazas híbridas[11], dependiendo del incidente.

---

8 En fase de elaboración; adopción prevista para finales de 2017.

9 Está previsto que las directrices estén terminadas para finales de 2017.

10 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.

11 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 5.7.2016.

(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.

(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[12] 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/

[12] ST 15283/16, de 6 de diciembre de 2016.

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.

(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 13.9.2017

Por la Comisión
Mariya GABRIEL
Miembro de la Comisión

AMPLIACIÓN CERTIFICADA CONFORME
Por el Secretario General,

Jordi AYET PUIGARNAU
Director de la Secretaría
COMISIÓN EUROPEA