Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales

Bruselas, 16 de diciembre de 2020

La Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentan hoy la nueva Estrategia de Ciberseguridad de la UE. Como elemento clave de la Configuración del futuro digital de Europa, el Plan de Recuperación para Europa y la Estrategia de la Unión de la Seguridad de la UE, la Estrategia reforzará la resiliencia colectiva europea contra las ciberamenazas y ayudará a garantizar que todos los ciudadanos y las empresas puedan beneficiarse plenamente de unos servicios y herramientas digitales fiables y de confianza. Tanto si se trata de dispositivos conectados, la red eléctrica o servicios bancarios, aviones, administraciones públicas y hospitales, los europeos merecen poder utilizarlos o recurrir a ellos con la certeza de estar protegidos frente a ciberamenazas.

La nueva Estrategia de Ciberseguridad también permite a la UE reforzar su liderazgo en el ámbito de las normas internacionales del ciberespacio y potenciar su cooperación con socios de todo el mundo, con el fin de promover un ciberespacio global, abierto, estable y seguro, basado en el Estado de Derecho, los derechos humanos, las libertades fundamentales y los valores democráticos.

Asimismo, la Comisión está presentando propuestas que abordan tanto la resiliencia física como la ciberresiliencia de entidades críticas y redes: una Directiva sobre las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (la Directiva SRI revisada o «SRI 2») y una nueva Directiva sobre la resiliencia de entidades críticas. Estas abarcan una amplia gama de sectores con el objetivo de hacer frente, de un modo coherente y complementario, a los riesgos actuales y futuros existentes dentro y fuera de Internet, ya sea en forma de ciberataques, delitos o desastres naturales.

Confianza y seguridad, protagonistas en la Década Digital de la UE

La nueva Estrategia de Ciberseguridad tiene por objeto salvaguardar una Internet global y abierta, y ofrecer, al mismo tiempo, protección tanto para garantizar la seguridad, como para defender los valores europeos y los derechos fundamentales de todas las personas. Sobre la base de los logros alcanzados en los últimos meses y años, la estrategia incluye propuestas concretas de iniciativas reguladoras, estratégicas y de inversión en los tres ámbitos de acción de la UE:

1. **Resiliencia, soberanía tecnológica y liderazgo**

Bajo esta línea de acción, la Comisión propone reformar las normas sobre la seguridad de las redes y los sistemas de información por medio de una Directiva sobre las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (la Directiva SRI revisada o «SRI 2»), con la finalidad de aumentar el nivel de ciberresiliencia de los sectores públicos y privados críticos: los hospitales, las redes de energía, los ferrocarriles, los centros de datos, las administraciones públicas, los laboratorios de investigación y la fabricación de medicamentos y productos sanitarios críticos, así como otras infraestructuras y servicios críticos, deben permanecer protegidos frente a un entorno cada vez más cambiante y de amenazas más complejas.

La Comisión también propone la creación, en toda la UE, de una red de Centros de Operaciones de Seguridad basados en la inteligencia artificial (IA) que reforzará la protección de la Unión en materia de ciberseguridad, capaz de detectar indicios de ciberataques con suficiente antelación y permitiendo adoptar medidas proactivas, antes de que los daños se lleguen a producir. Entre las medidas adicionales se incluirá un apoyo específico destinado a pequeñas y medianas empresas (pymes), por medio de centros de innovación digital, así como un mayor esfuerzo para mejorar las capacidades de la mano de obra, atraer y retener a los mejores talentos en el ámbito de la ciberseguridad e invertir en una investigación e innovación abierta, competitiva y basada en la excelencia.

2. **Desarrollo de la capacidad operativa para prevenir, disuadir y responder**

La Comisión, través de un proceso progresivo e integrador con los Estados miembros, está

preparando una nueva unidad informática conjunta con el fin de reforzar la cooperación entre los organismos de la UE y las autoridades de los Estados miembros encargadas de la prevención, la disuasión y la respuesta a los ciberataques, incluidas las comunidades civiles, policiales, diplomáticas y de ciberdefensa. El Alto Representante ha presentado propuestas para reforzar el «conjunto de instrumentos de ciberdiplomacia de la UE», cuyo objetivo es prevenir, desalentar, disuadir y responder eficazmente a las actividades informáticas malintencionadas y, en particular, aquellas que dañen nuestras infraestructuras críticas, cadenas de suministro, instituciones y procesos democráticos. La UE también se ha fijado el objetivo de seguir mejorando la cooperación en el campo de la ciberdefensa y el desarrollo de capacidades de vanguardia en este campo, a partir del trabajo realizado por la Agencia Europea de Defensa, así como de animar a los Estados miembros a que hagan pleno uso de la Cooperación Estructurada Permanente y del Fondo Europeo de Defensa.

3. **Promover un ciberespacio global y abierto a través de una mayor cooperación**

La UE intensificará su colaboración con socios internacionales con el objeto de fortalecer el orden mundial basado en normas, promover la seguridad y la estabilidad internacionales en el ciberespacio, y proteger los derechos humanos y las libertades fundamentales en línea. También impulsará las normas internacionales que reflejen estos valores fundamentales de la UE a través de la cooperación con sus socios internacionales en las Naciones Unidas y otros foros pertinentes. La UE seguirá reforzando su «conjunto de instrumentos de ciberdiplomacia» y aumentará sus esfuerzos para apoyar a terceros países en este ámbito, mediante un programa destinado al desarrollo de la capacidad cibernética exterior de la UE. Para ello, se intensificarán los diálogos en materia cibernética con terceros países, organizaciones regionales e internacionales, así como con la comunidad multilateral. Asimismo, la UE establecerá una red de ciberdiplomacia en todo el mundo para promover su visión del ciberespacio.

La UE se compromete a apoyar la nueva Estrategia de Ciberseguridad, tal y como refleja su próximo presupuesto a largo plazo, con un nivel de inversiones sin precedentes en la transición digital durante los próximos siete años, en particular a través del Programa Europa Digital, el Horizonte Europa y el Plan de Recuperación para Europa. Así pues, se anima a los Estados miembros a que hagan pleno uso del Mecanismo de Recuperación y Resiliencia de la UE con el fin de impulsar la ciberseguridad y de igualar los esfuerzos de inversión de la UE en este ámbito. El objetivo es alcanzar una inversión conjunta de 4 500 millones EUR entre la Unión, los Estados miembros y la industria, en especial a través del Centro de Competencias en Ciberseguridad y la Red de Centros de Coordinación, así como garantizar que las pymes reciben una parte importante de la misma.

La Comisión se propone también reforzar las capacidades industriales y tecnológicas de la UE en materia de ciberseguridad, por ejemplo, mediante proyectos apoyados conjuntamente por los presupuestos nacionales y de la UE. La UE tiene una oportunidad única de compartir sus recursos para mejorar su autonomía estratégica e impulsar su liderazgo en materia de ciberseguridad a lo largo de toda la cadena de suministro digital (incluidos los datos y la nube, las tecnologías de procesadores de próxima generación, la conectividad ultrasegura y las redes 6G), en consonancia con sus valores y prioridades.

Ciberresiliencia y resiliencia física de las redes, los sistemas de información y las entidades críticas

Es necesario actualizar las medidas existentes a escala de la Unión destinadas a proteger los servicios e infraestructuras clave contra los riesgos cibernéticos y físicos. Los riesgos de ciberseguridad siguen evolucionando con el aumento de la digitalización y la interconexión. Los riesgos físicos también son cada vez más complejos desde la adopción, en 2008, de las normas de la UE sobre infraestructuras críticas, que en la actualidad se aplica exclusivamente a los sectores de la energía y el transporte. El objetivo de las revisiones es actualizar las normas según la lógica de la Estrategia de la UE para una Unión de la Seguridad, superar la falsa dicotomía entre lo que está en línea y fuera de ella, así como romper con el enfoque compartimentado.

Para hacer frente al incremento de las amenazas derivadas de la digitalización y la interconexión, la propuesta **Directiva sobre las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (la Directiva SRI revisada o «SRI 2»)** se aplicará a entidades medianas y grandes de más sectores, en función de su importancia crítica para la economía y la sociedad. La SRI 2 refuerza los requisitos de seguridad que se imponen a las empresas, se ocupa de la seguridad de las cadenas de suministro y las relaciones con los proveedores, simplifica las obligaciones de notificación, introduce medidas de supervisión más estrictas para las autoridades nacionales, requisitos de ejecución más estrictos y tiene por objeto armonizar los regímenes de sanciones entre los Estados miembros. La propuesta SRI 2 contribuirá a aumentar el intercambio de información y la cooperación en el ámbito de la gestión de cibercrisis a nivel nacional y de la UE.

La propuesta **Directiva sobre la resiliencia de las entidades críticas (REC)** amplía el ámbito de aplicación y la profundidad de la Directiva sobre infraestructuras críticas europeas de 2008. Se incluyen diez nuevos sectores: la energía, el transporte, la banca, las infraestructuras de los mercados financieros, la sanidad, el agua potable, las aguas residuales, las infraestructuras digitales, la administración pública y el espacio. En el marco de la directiva propuesta, los Estados miembros podrían adoptar una estrategia nacional con el objetivo de reforzar la resiliencia de las entidades críticas y efectuar evaluaciones periódicas sobre el riesgo. Estas evaluaciones también ayudarían a identificar un grupo más reducido de entidades críticas que estarían sujetas a obligaciones destinadas a mejorar su resiliencia frente a riesgos no cibernéticos, incluidas las evaluaciones de riesgos a nivel de las entidades, la adopción de medidas técnicas y organizativas o la notificación de incidentes. Por su parte, la Comisión prestaría apoyo complementario a los Estados miembros y a las entidades críticas, por ejemplo, mediante el desarrollo de una visión general a escala de la Unión de los riesgos transfronterizos e intersectoriales, y la aplicación de mejores prácticas, metodologías, actividades de formación transfronterizas y ejercicios para poner a prueba la resiliencia de las entidades críticas.

Asegurar la nueva generación de redes: la 5G y otras innovaciones

En el marco de la nueva Estrategia de Ciberseguridad, se anima a los Estados miembros, con el apoyo de la Comisión y de la ENISA (Agencia de la UE para la Ciberseguridad), a que finalicen la aplicación del conjunto de instrumentos de la UE de las redes 5G, un enfoque global y objetivo basado en los riesgos para la seguridad de la 5G y las generaciones futuras de redes.

Según indica un informe publicado hoy, relativo al impacto de la Recomendación de la Comisión sobre la ciberseguridad de las redes 5G y los avances en la aplicación del conjunto de medidas paliativas de la UE, desde el informe de situación de julio de 2020, la mayoría de los Estados miembros va por buen camino en lo que respecta a la aplicación de las medidas recomendadas. Ahora deben velar por que su aplicación se haya completado antes del segundo trimestre de 2021 y por la reducción adecuada y coordinada de los riesgos identificados, sobre todo con vistas a minimizar la exposición a proveedores de alto riesgo y evitar la dependencia respecto de estos proveedores. Asimismo, la Comisión establece hoy objetivos y acciones clave destinados a proseguir con el trabajo coordinado a escala de la UE.

Declaraciones de los miembros del Colegio de Comisarios:

La vicepresidenta ejecutiva para Una Europa Adaptada a la Era Digital, Margrethe **Vestager**, ha declarado: *«Europa está comprometida con la transición digital de nuestra sociedad y nuestra economía. Por lo tanto, tenemos que apoyarla con un nivel de inversiones sin precedentes. La transición digital se está acelerando, pero solo podrá tener éxito si las personas y las empresas pueden confiar en la seguridad de los productos y servicios conectados, de los que dependen».*

Josep **Borrell**, Alto Representante, ha añadido lo siguiente: *«La seguridad y la estabilidad internacionales dependen más que nunca de un ciberespacio global, abierto, estable y seguro en el que se respeten el Estado de Derecho, los derechos humanos, las libertades y la democracia. Mediante la estrategia anunciada hoy, la UE está intensificando sus esfuerzos para proteger a sus gobiernos, ciudadanos y empresas de las ciberamenazas mundiales, y para asumir el liderazgo en el ciberespacio, velando por que todo el mundo pueda aprovechar los beneficios de Internet y el uso de las tecnologías».*

Margaritis **Schinas**, vicepresidente para la Promoción de nuestro Modo de Vida Europeo, ha hecho las siguientes observaciones: *«La ciberseguridad es una parte central de la Unión de la Seguridad. Ya no existe distinción entre amenazas dentro y fuera de línea. Ahora, el mundo digital y el físico se entrelazan inextricablemente. El conjunto de medidas que se anuncian hoy demuestra que la UE está dispuesta a utilizar todos sus recursos y conocimientos técnicos para prepararse y enfrentarse a las ciberamenazas y amenazas físicas con la misma determinación».*

El comisario de Mercado Interior, Thierry **Breton**, ha declarado: *«Las ciberamenazas evolucionan rápidamente, son cada vez más complejas y adaptables. Para garantizar la protección de nuestros ciudadanos e infraestructuras tenemos que ir varios pasos por delante; la protección de la UE en materia de ciberseguridad, resiliente y autónoma, permitirá que podamos utilizar nuestra experiencia y nuestros conocimientos para identificar y reaccionar con mayor rapidez, limitar los posibles daños, así como aumentar nuestra resiliencia. Invertir en ciberseguridad significa hacerlo en un futuro saludable de nuestros entornos en línea y en nuestra autonomía estratégica».*

Ylva **Johansson**, comisaria europea de Asuntos de Interior, ha declarado: *«Nuestros hospitales, sistemas de tratamiento de aguas residuales o infraestructuras de transporte solo son igual de fuertes que su eslabón más débil. Las perturbaciones en una parte de la Unión pueden afectar a la prestación de servicios esenciales en otro lugar. Para garantizar el buen funcionamiento del mercado*

interior y los medios de subsistencia de las personas residentes en Europa, nuestra infraestructura clave debe ser resiliente frente a riesgos como catástrofes naturales, atentados terroristas, accidentes y pandemias como la que hoy vivimos. Ese es precisamente el objetivo de mi propuesta relativa a las infraestructuras críticas».

Próximas etapas

La Comisión Europea y el Alto Representante se han comprometido a aplicar la nueva Estrategia de Ciberseguridad en los próximos meses. Se elaborarán informes periódicos sobre los progresos realizados y se mantendrá al Parlamento Europeo, al Consejo de la Unión Europea y a las partes interesadas totalmente informados e involucrados en todas las acciones pertinentes.

Ahora, corresponde al Parlamento Europeo y al Consejo examinar y adoptar la propuesta de Directiva SRI 2 y la Directiva sobre la resiliencia de las entidades críticas. Cuando las propuestas se hayan acordado y adoptado en consecuencia, los Estados miembros dispondrán de un plazo de 18 meses a partir de su entrada en vigor para incorporarlas a su ordenamiento jurídico.

La Comisión revisará periódicamente la Directiva SRI 2 y la Directiva sobre la resiliencia de las entidades críticas, e informará sobre su funcionamiento.

Antecedentes

La ciberseguridad es una de las principales prioridades de la Comisión y la piedra angular de una Europa digital y conectada. El aumento de los ciberataques producidos durante la crisis del coronavirus ha puesto de manifiesto la importancia de proteger los hospitales, los centros de investigación y otras infraestructuras. Por tanto, es necesario adoptar medidas firmes en este ámbito, para que la economía y la sociedad de la UE estén preparadas para el futuro.

La nueva Estrategia de Ciberseguridad propone integrar la ciberseguridad en todos los elementos de la cadena de suministro y concentrar aún más las actividades y los recursos de la UE en torno a las cuatro comunidades de ciberseguridad: mercado interior, aplicación de la ley, diplomacia y defensa. Está basada en la Configuración del futuro digital de Europa y en la Estrategia de la UE para una Unión de la Seguridad, así como en una serie de actos legislativos, acciones e iniciativas aplicadas por la UE con el fin de reforzar las capacidades de ciberseguridad y garantizar la ciberresiliencia de Europa. Ello incluye la Estrategia de Ciberseguridad de 2013, revisada en 2017, y la Agenda Europea de Seguridad de la Comisión de 2015-2020. Asimismo, reconoce la creciente interconexión entre seguridad interior y exterior, en particular, por medio de la política exterior y de seguridad común.

La Directiva SRI, en vigor desde el 2016, es la primera ley en materia de ciberseguridad a escala de la Unión y contribuyó a alcanzar de manera uniforme un elevado nivel común de seguridad de las redes y los sistemas de información en toda la UE. Como parte de su objetivo político clave de hacer una Europa adaptada a la era digital, la Comisión anunció la revisión de la Directiva SRI en febrero de este año. El Reglamento de Ciberseguridad, en vigor desde 2019, dotó a la UE de un marco de certificación de la ciberseguridad de los productos, procesos y servicios, y reforzó el mandato de la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

En lo que concierne a la ciberseguridad de las redes 5G, los Estados miembros, con el apoyo de la Comisión y de la ENISA, y sobre la base del conjunto de instrumentos de la UE de las redes 5G, adoptaron en enero de 2020 un enfoque global y objetivo basado en el riesgo. La revisión de la Comisión de su Recomendación de marzo de 2019 sobre la ciberseguridad de las redes 5G reveló los progresos de la mayoría de los Estados miembros en lo que respecta a la aplicación del conjunto de instrumentos.

Desde la aplicación de la Estrategia de Ciberseguridad de 2013, la UE ha desarrollado una política internacional coherente y holística en materia de ciberseguridad. En colaboración con sus socios a nivel bilateral, regional e internacional, la UE ha promovido un ciberespacio global, abierto, estable y seguro, sobre la base de los valores fundamentales de la UE y del Estado de Derecho. La UE ha apoyado a terceros países en el aumento de su ciberresiliencia y su capacidad para enfrentarse a la ciberdelincuencia, y ha utilizado su «conjunto de instrumentos de ciberdiplomacia» de 2017 para seguir contribuyendo a la seguridad y la estabilidad internacionales en el ciberespacio. Un ejemplo de ello es la aplicación, por primera vez, de su régimen de sanciones cibernéticas de 2019 y la inclusión de ocho personas y cuatro entidades y organismos en su lista de sancionados. La UE también ha realizado avances significativos en la cooperación en materia de ciberdefensa, en particular en lo que se refiere a las capacidades al respecto, sobre todo, en su marco político de ciberdefensa, así como en el contexto de la Cooperación Estructurada Permanente (CEP) y la labor de la Agencia Europea de Defensa.

La ciberseguridad es una prioridad que también se refleja en el próximo presupuesto a largo plazo de la UE (2021-2027). En el marco del Programa Europa Digital, la UE cooperará con la investigación, la

innovación y las infraestructuras en materia de ciberseguridad, la ciberdefensa y su industria de ciberseguridad. Además, como respuesta a la crisis del coronavirus, en la que se produjo un aumento de los ciberataques durante el confinamiento, se garantizan inversiones adicionales en ciberseguridad en el marco del Plan de Recuperación para Europa.

La UE viene reconociendo desde hace mucho tiempo la necesidad de garantizar la resiliencia de las infraestructuras críticas destinadas a la prestación servicios esenciales, ya que son fundamentales para el correcto funcionamiento del mercado interior, así como para las vidas y los medios de subsistencia de los ciudadanos europeos. Por este motivo, la UE creó el Programa Europeo de Protección de Infraestructuras Vitales (PEPIC) en 2006, y adoptó en 2008 la Directiva sobre infraestructuras críticas europeas, aplicable a los sectores de la energía y el transporte. Estas medidas se complementaron en años posteriores con diversas medidas sectoriales e intersectoriales sobre aspectos específicos, como la protección contra el cambio climático, la protección civil o la inversión extranjera directa.

Más información

Ficha informativa sobre la nueva Estrategia de Ciberseguridad.

Ficha informativa sobre la propuesta de Directiva sobre las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (la Directiva SRI revisada)

Ficha informativa sobre la Ciberseguridad Acción exterior de la UE

Preguntas y respuestas: Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales

Propuesta de Directiva sobre las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (la Directiva SRI revisada o «SRI 2»)

Propuesta de Directiva sobre la resiliencia de entidades críticas (véase también el Anexo I de la propuesta, así como la evaluación de impacto y su resumen).

Unión Europea de la Seguridad

Evaluación de impacto sobre la Directiva SRI revisada (o «SRI 2»)

Más información sobre la ciberseguridad

Más información sobre la Directiva SRI

IP/20/2391

Personas de contacto para la prensa:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

Solicitudes del público en general: Europe Direct por teléfono 00 800 67 89 10 11 , o por e-mail