COMISIÓN
EUROPEA

ALTO REPRESENTANTE
DE LA UNIÓN PARA
ASUNTOS EXTERIORES Y
POLÍTICA DE SEGURIDAD

Bruselas, 16.12.2020
JOIN(2020) 18 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

La Estrategia de Ciberseguridad de la UE para la Década Digital

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

La Estrategia de Ciberseguridad de la UE para la Década Digital

I. INTRODUCCIÓN: UNA TRANSFORMACIÓN DIGITAL CIBERSEGURA EN UN ENTORNO COMPLEJO DE AMENAZAS

La ciberseguridad es una parte integrante de la seguridad de los europeos. Ya se trate de dispositivos conectados, redes eléctricas o bancos, aviones, administraciones públicas u hospitales que utilizan o frecuentan, las personas merecen hacerlo con la seguridad de que estarán protegidas de las ciberamenazas. La economía, la democracia y la sociedad de la UE dependen más que nunca de las herramientas digitales fiables y seguras y de la conectividad. Por tanto, la ciberseguridad es esencial para construir una Europa resiliente, ecológica y digital.

El transporte, la energía y la salud, las telecomunicaciones, las finanzas, la seguridad, los procesos democráticos, el espacio y la defensa dependen en gran medida de los sistemas de redes e información que están cada vez más interconectados. Las interdependencias intersectoriales son muy fuertes porque las redes y los sistemas de información, a su vez, dependen de un suministro constante de electricidad para funcionar. Los dispositivos conectados ya superan en número a las personas en el planeta, y se prevé que su número aumente a 25 000 millones para 2025[1]: una cuarta parte de ellos estará en Europa. La digitalización de las pautas de trabajo se ha acelerado por la pandemia COVID-19, durante la cual el 40 % de los trabajadores de la UE se pasaron al teletrabajo, con probables efectos permanentes en la vida cotidiana[2]. Esto aumenta la vulnerabilidad a los ciberataques[3]. Los objetos conectados se envían a menudo al consumidor con vulnerabilidades conocidas, lo que aumenta aún más la superficie de ataque para las actividades cibernéticas maliciosas[4]. El panorama industrial de la UE está cada vez más digitalizado y conectado; esto también significa que los ciberataques pueden tener un impacto mucho mayor que nunca en las industrias y los ecosistemas.

El panorama de amenazas se ve agravado por las tensiones geopolíticas en torno a la internet mundial y abierta y al control de las tecnologías en toda la cadena de

[1] Estimado por la asociación comercial de telecomunicaciones GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). International Data Corporation predijo 42 600 millones de máquinas, sensores y cámaras conectadas; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Según una encuesta realizada en junio de 2020, el 47 % de los líderes empresariales declaró tener la intención de permitir que los empleados trabajen a distancia a tiempo completo, incluso cuando sea posible volver al lugar de trabajo; el 82% declaró tener la intención de permitir el trabajo a distancia al menos una parte del tiempo; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[4] Uno de los programas maliciosos más dañinos hasta la fecha, conocido como Mirai, creó redes infectadas en más de 600 000 dispositivos que perturbaron múltiples sitios web importantes en Europa y Estados Unidos.

suministro[5]. Esas tensiones se reflejan en el creciente número de Estados nacionales que están estableciendo fronteras digitales. Las restricciones de internet y sobre el uso de este amenazan el ciberespacio mundial y abierto, así como el Estado de Derecho, los derechos fundamentales, la libertad y la democracia, que son los valores fundamentales de la UE. El ciberespacio se explota cada vez más con fines políticos e ideológicos, y la creciente polarización a nivel internacional está obstaculizando un multilateralismo eficaz. Las amenazas híbridas combinan campañas de desinformación con ciberataques a la infraestructura, los procesos económicos y las instituciones democráticas, con la posibilidad de causar daños físicos, obtener acceso ilegal a datos personales, robar secretos industriales o de Estado, sembrar la desconfianza y debilitar la cohesión social. Estas actividades socavan la seguridad y la estabilidad internacionales y los beneficios que el ciberespacio aporta al desarrollo económico, social y político.

El ataque malicioso a infraestructuras críticas es un riesgo mundial importante[6]. Internet tiene una arquitectura descentralizada sin una estructura central y una gobernanza de múltiples interesados. Ha logrado mantener aumentos exponenciales en los volúmenes de tráfico, al tiempo que ha sido un objeto constante de intentos maliciosos de interrupción[7]. Al mismo tiempo, existe una mayor dependencia de las funciones básicas de la internet mundial y abierta, como el sistema de nombres de dominio (DNS, por sus siglas en inglés), y de los servicios esenciales de internet para las comunicaciones y el alojamiento, las aplicaciones y los datos. Estos servicios están cada vez más concentrados en manos de unas pocas empresas privadas[8]. Esto hace a la economía y la sociedad europeas vulnerables frente a acontecimientos geopolíticos o técnicos perturbadores que afectan al núcleo de internet o a una o más de esas empresas. El aumento del uso de internet y los cambios en las pautas debido a la pandemia han expuesto aún más la fragilidad de las cadenas de suministro que dependen de esta infraestructura digital.

La preocupación por la seguridad es un gran impedimento para el uso de los servicios en línea[9]**.** Alrededor de dos quintas partes de los usuarios de la UE han experimentado problemas relacionados con la seguridad y tres quintas partes se sienten incapaces de

[5] Incluidos los componentes electrónicos, el análisis de datos, la nube, las redes más rápidas e inteligentes con 5G y más allá, el cifrado, la inteligencia artificial (IA) y los nuevos paradigmas de computación y de tratamiento de datos fiables como la cadena de bloques, computación de la nube hasta el borde y la computación cuántica.

[6] Foro Económico Mundial, Global Risks Report 2020 (Informe sobre los riesgos mundiales 2020).

[7] La pandemia provocó un aumento del 60 % del tráfico de internet según la Organización de Cooperación y Desarrollo Económicos; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. El Organismo de Reguladores Europeos de las Comunicaciones Electrónicas y la Comisión publican periódicamente informes sobre la situación de la capacidad de internet durante las medidas de confinamiento del coronavirus. Según un informe de ENISA, hubo un aumento del 241 % en el número total de ataques distribuidos de denegación de servicios durante el tercer trimestre de 2019 en comparación con el tercer trimestre de 2018. Los ataques distribuidos de denegación de servicios están aumentando en intensidad; el mayor ataque hasta la fecha sucedió en febrero de 2020 y alcanzó un pico de tráfico de 2,3 terabits por segundo. En el «apagón de CenturyLink» de agosto de 2020, un problema de enrutamiento en el proveedor de servicios de internet de EE. UU. provocó una caída del 3,5 % en el tráfico web mundial; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8] Internet Society, «El informe global de Internet: consolidación en la economía de Internet»; https://www.internetsociety.org/es/blog/2019/02/el-informe-global-de-internet-consolidacion-en-la-economia-de-internet/.

[9] https://data.europa.eu/euodp/es/data/dataset/S2249_92_2_499_ENG.

protegerse contra la ciberdelincuencia[10]. En los últimos tres años, un tercio ha recibido correos electrónicos o llamadas telefónicas fraudulentas en las que se le pedían datos personales, pero el 83 % nunca ha denunciado un ciberdelito. Una de cada ocho empresas se ha visto afectada por los ciberataques[11]. Más de la mitad de los ordenadores personales de empresas y consumidores que han sido infectados con programas maliciosos una vez son reinfectados en el mismo año[12]. Cientos de millones de registros se pierden cada año a causa de las violaciones de la seguridad de los datos; el coste medio de una violación en una sola empresa se elevó a más de 3,5 millones EUR en 2018[13]. El impacto de un ciberataque a menudo no se puede aislar, y puede provocar reacciones en cadena en toda la economía y la sociedad, afectando a millones de personas[14].

La investigación de prácticamente todos los tipos de delitos tiene un componente digital. En 2019, se informó de que el número de incidentes interanuales se había triplicado. Se calcula que existen unos 700 millones de nuevos ejemplares de programas maliciosos, el medio más frecuente de promover un ciberataque[15]. El coste anual de la ciberdelincuencia para la economía mundial en 2020 se estima en 5,5 billones EUR, el doble que en 2015[16]. Esto representa la mayor transferencia de riqueza económica de la historia, mayor que el comercio mundial de drogas. Para un solo incidente importante, el ataque del programa de secuestro WannaCry en 2017, el coste para la economía global se estimó en más de 6 500 millones EUR[17].

Los servicios digitales y el sector financiero figuran entre los objetivos más frecuentes de los ciberataques, junto con el sector público y la industria manufacturera, pero la preparación y la sensibilización cibernéticas de las empresas y los particulares siguen siendo limitadas[18], y hay una gran escasez de capacidades en materia de ciberseguridad

[10] Índice 2020 de la Economía y la Sociedad Digitales; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/es/data/dataset/S2249_92_2_499_ENG.

[11] Comunicado de prensa de Eurostat, «ICT security measures taken by vast majority of enterprises in the EU» (Medidas de seguridad de las TIC adoptadas por la gran mayoría de las empresas de la UE), 6/2020 - 13 de enero de 2020. «Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation»(Los ciberataques a infraestructuras críticas se han convertido en la nueva normalidad en sectores como la energía, la sanidad y el transporte); Foro Económico Mundial, Informe sobre los riesgos mundiales 2020.

[12] Fuente: Comparitech.

[13] Informe anual del coste de una violación de la seguridad de los datos, 2020 Ponemon Institute, y basado en el análisis cuantitativo de 524 violaciones recientes en 17 áreas geográficas y 17 industrias; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[14] Informe del Centro Común de Investigación (JRC), «Cybersecurity, our digital anchor» (Ciberseguridad: nuestro pilar digital); https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.

[15] Fuente: AV-TEST, https://www.av-test.org/en/statistics/malware/.

[16] JRC, «Cybersecurity – Our Digital Anchor».

[17] Fuente: Cyence.

[18] La concienciación de las empresas sigue siendo escasa también en lo que respecta al robo cibernético de secretos comerciales, especialmente entre las pymes; PwC, «Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets» (Estudio sobre la escala y la incidencia del espionaje industrial y el robo de secretos comerciales por medios cibernéticos: Informe de divulgación sobre las medidas para hacer frente y prevenir el robo cibernético de secretos comerciales), 2018.

en la mano de obra[19]. En 2019 se produjeron casi 450 incidentes de ciberseguridad relacionados con infraestructuras críticas europeas como las finanzas y la energía[20]. Las organizaciones y los profesionales de la salud se han visto especialmente afectados durante la pandemia. A medida que la tecnología se hace inextricable del mundo físico, los ciberataques ponen en peligro las vidas y el bienestar de los más vulnerables[21]. Más de dos tercios de las empresas, en particular las pymes, se consideran «novatas» en materia de ciberseguridad, y las empresas europeas se consideran menos preparadas que las de Asia y América[22]. Se estima que en Europa quedan por cubrir 291 000 puestos de profesionales de la ciberseguridad. La contratación y formación de expertos en ciberseguridad es un proceso lento que conlleva mayores riesgos de ciberseguridad para las organizaciones[23].

La UE carece de una conciencia colectiva de la situación de las amenazas cibernéticas. Esto se debe a que las autoridades nacionales no reúnen ni comparten sistemáticamente información —como la disponible en el sector privado— que pueda ayudar a evaluar el estado de la ciberseguridad en la UE. Los Estados miembros solo comunican una parte de los incidentes y el intercambio de información no es ni sistemático ni exhaustivo[24]; los ciberataques pueden ser solo un aspecto de los ataques maliciosos concertados contra las sociedades europeas. En la actualidad, solo existe una asistencia operativa mutua entre los Estados miembros limitada y no existe ningún mecanismo operativo entre los Estados miembros y las instituciones, agencias y organismos de la UE en caso de crisis o incidentes cibernéticos transfronterizos a gran escala[25].

Por tanto, la mejora de la ciberseguridad es esencial para que las personas confíen, utilicen y se beneficien de la innovación, la conectividad y la automatización, y para salvaguardar los derechos y libertades fundamentales, incluidos los derechos a la privacidad y a la protección de los datos personales, y la libertad de expresión e información. La ciberseguridad es indispensable para la conectividad de la red y la internet global y abierta que debe sustentar la transformación de la economía y la sociedad en la década de 2020. Contribuye a la creación de más y mejores empleos, a la flexibilización de los lugares de trabajo, a un transporte y una agricultura más eficientes y sostenibles y a un acceso más fácil y justo a los servicios de salud. También es esencial para la transición a una energía más limpia en el marco del Pacto Verde Europeo[26], mediante redes transfronterizas y medidores inteligentes y evitando la duplicación innecesaria del almacenamiento de datos.

[19] Véase «ENISA Threat Landscape» (Panorama de amenazas de ENISA) 2020. Véase también, «Verizon Data Breach Investigations Report» (Informe sobre investigaciones de la violación de la seguridad de los datos) 2020; https://enterprise.verizon.com/resources/reports/dbir/.

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

[21] Los programas de secuestro se han utilizado para atacar a hospitales e historias clínicas, por ejemplo, Rumanía (junio de 2020), Düsseldorf (septiembre de 2020) y Vastaamo (octubre de 2020).

[22] PwC, «The Global State of Information Security» (El estado mundial de la seguridad de la información) 2018; ESI Thoughtlab, «The Cybersecurity Imperative» (El imperativo de la ciberseguridad), 2019.

[23] Agencia de la Unión Europea para la Ciberseguridad, «Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database» (Desarrollo de capacidades en materia de ciberseguridad en la UE: la certificación de los títulos de ciberseguridad y la base de datos de la educación superior de ENISA), Diciembre de 2019.

[24] Los Estados miembros deben presentar un informe resumido anual al Grupo de cooperación sobre las notificaciones recibidas en virtud del artículo 10, apartado 3, de la Directiva sobre la seguridad de las redes y los sistemas de información [Directiva (UE) 2016/1148].

[25] Se han establecido procedimientos operativos estándar para la asistencia mutua entre los miembros de la Red de CSIRT.

[26] El Pacto Verde Europeo, COM(2019) 640 final.

Por último, es esencial para la seguridad y la estabilidad internacionales y el desarrollo de las economías, las democracias y las sociedades a nivel mundial. Por consiguiente, los gobiernos, las empresas y los particulares deben utilizar los instrumentos digitales de manera responsable y consciente con respecto a la seguridad. La concienciación acerca de la ciberseguridad y la higiene de la ciberseguridad deben sustentar la transformación digital de las actividades cotidianas.

La nueva Estrategia de Ciberseguridad de la UE para la Década Digital constituye un componente clave de la configuración del futuro digital de Europa[27], el Plan de Recuperación de la Comisión para Europa[28], la Estrategia para una Unión de la Seguridad 2020-2025[29], la Estrategia Global para la Política Exterior y de Seguridad de la UE[30] y la Agenda Estratégica del Consejo Europeo 2019-2024[31]. En ella se establece la forma en que la UE protegerá a su población, empresas e instituciones de las ciberamenazas, y la forma en que fomentará la cooperación internacional y tomará la iniciativa para asegurar una internet mundial y abierta.

II. PENSAR A NIVEL MUNDIAL, ACTUAR A NIVEL EUROPEO

Esta estrategia tiene por objeto garantizar una internet global y abierta con fuertes vallas para hacer frente a los riesgos para la seguridad y los derechos y libertades fundamentales de las personas en Europa. Tras los progresos logrados en el marco de las estrategias anteriores, contiene propuestas concretas para desplegar **tres instrumentos principales —instrumentos normativos, de inversión y de política** —para abordar **tres ámbitos de actuación de la UE: 1) resiliencia, soberanía tecnológica y liderazgo, 2) creación de capacidad operativa para prevenir, disuadir y responder, y 3) fomento de un ciberespacio mundial y abierto.** La UE se ha comprometido a apoyar esta estrategia mediante un **nivel de inversión sin precedentes en la transición digital de la UE durante los próximos siete años** —que podría cuadruplicar los niveles anteriores— como parte de las nuevas políticas tecnológicas e industriales y del programa de recuperación[32].

La ciberseguridad debe integrarse en todas esas inversiones digitales, en particular en tecnologías clave como la inteligencia artificial (IA), el cifrado y la computación cuántica, utilizando incentivos, obligaciones y puntos de referencia. Esto puede estimular el crecimiento de la industria europea de la ciberseguridad y proporcionar la certeza necesaria para facilitar la eliminación gradual de los sistemas heredados. El Fondo Europeo de Defensa (FED) apoyará las soluciones de ciberdefensa europeas, como parte de la base tecnológica e industrial de la defensa europea. La ciberseguridad está incluida en los instrumentos financieros externos de apoyo a nuestros socios, en particular el Instrumento de Vecindad, Desarrollo y Cooperación Internacional. La prevención del uso indebido de las tecnologías, la

[27] Configurar el futuro digital de Europa, COM(2020) 67 final.
[28] El momento de Europa: reparar los daños y preparar el futuro para la próxima generación, COM(2020) 98 final.
[29] Estrategia de la UE para una Unión de la Seguridad 2020-2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en.
[31] https://www.consilium.europa.eu/es/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/.
[32] Las inversiones en toda la cadena de suministro de la tecnología digital, que contribuyan a la transición digital o a abordar los desafíos que se deriven de ella, deben ascender al menos al 20 % —equivalente a 134 500 millones EUR — del Mecanismo de Recuperación y Resiliencia de 672 500 millones EUR, que consiste en subvenciones y préstamos. La financiación de la UE en el marco financiero plurianual 2021-2027 prevista para la ciberseguridad con arreglo al programa Europa Digital, y para la investigación en materia de ciberseguridad en el marco de Horizonte Europa, con especial atención al apoyo a las pymes, podría ascender a un total de 2 000 millones EUR, más las inversiones de los Estados miembros y de la industria.

protección de la infraestructura crítica y la garantía de la integridad de las cadenas de suministro también permiten que la UE se adhiera a las normas, reglas y principios de las Naciones Unidas de comportamiento responsable de los Estados[33].

1. RESILIENCIA, SOBERANÍA TECNOLÓGICA Y LIDERAZGO

La infraestructura crítica y los servicios esenciales de la UE son cada vez más interdependientes y están cada vez más digitalizados. Todas las cosas conectadas a internet en la UE, ya sean automóviles automatizados, sistemas de control industrial o electrodomésticos, y todas las cadenas de suministro que los hacen disponibles, deben ser seguras en el diseño, resistentes a los ciberincidentes, y deben ser rápidamente reparadas cuando se descubran vulnerabilidades. Esto es fundamental para que el sector público y privado de la UE tenga la posibilidad de elegir entre las infraestructuras y servicios más seguros. La próxima década es la oportunidad para la UE de liderar el desarrollo de tecnologías seguras en toda la cadena de suministro. La garantía de la resiliencia y el fortalecimiento de la capacidad industrial y tecnológica en materia de ciberseguridad debe movilizar todos los instrumentos normativos, de inversión y de política necesarios. La ciberseguridad en el diseño para los procesos, operaciones y dispositivos industriales, puede mitigar los riesgos, reducir potencialmente los costes para las empresas así como para la sociedad en general y, por tanto, aumentar la resiliencia.

1.1 Infraestructura resiliente y servicios críticos

Las **normas de la UE sobre la seguridad de las redes y los sistemas de información (SRI)** constituyen el núcleo del mercado único de la ciberseguridad. La Comisión propone reformar esas normas en el marco de una Directiva SRI revisada para aumentar el nivel de **ciberresisiliencia de todos los sectores pertinentes, públicos y privados, que desempeñan una función importante para la economía y la sociedad[34].** La revisión es necesaria para reducir las incoherencias en todo el mercado interior mediante la armonización del ámbito de aplicación, los requisitos de seguridad y de notificación de incidentes, la supervisión y el cumplimiento nacionales y las capacidades de las autoridades competentes.

Una Directiva SRI enmendada proporcionará la base para normas más específicas que también son necesarias para sectores de importancia estratégica, incluida la energía, el transporte y la salud. Con el fin de garantizar un enfoque coherente, como se anunció en la Estrategia para una Unión de la Seguridad 2020-2025, se propone la Directiva enmendada junto con una revisión de la legislación sobre la resiliencia de la infraestructura crítica[35]. Las tecnologías energéticas que incorporan componentes digitales y la seguridad de las cadenas de suministro conexas son importantes para la continuidad de los servicios esenciales y para el control estratégico de la infraestructura energética crítica. Por tanto, la Comisión propondrá medidas, incluido un «código de red» que establezca normas de ciberseguridad en los flujos eléctricos transfronterizos para su adopción a finales de 2022. El sector financiero también debe reforzar la resiliencia operativa digital y garantizar la capacidad de soportar todo tipo de perturbaciones y amenazas relacionadas con las TIC, como ha propuesto la Comisión[36]. En el sector

[33] https://undocs.org/es/A/70/174.
[34] [*Indíquese la referencia a la propuesta SRI*].
[35] [Indíquese la referencia a la *propuesta* de Directiva sobre la resiliencia de las entidades críticas].
[36] Propuesta de Reglamento sobre la resiliencia operativa digital para el sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014, COM/2020/595 final.

del transporte, la Comisión añadió disposiciones sobre la ciberseguridad[37] a la legislación de la UE sobre la seguridad de la aviación y seguirá esforzándose por aumentar la ciberresiliencia en todos los medios de transporte. El fortalecimiento de la ciberresiliencia de los **procesos e instituciones democráticos** es un componente esencial del Plan de Acción para la Democracia Europea para salvaguardar y promover las elecciones libres, y el discurso democrático y la pluralidad de los medios de comunicación[38]. Por último, en lo que respecta a la seguridad de la infraestructura y los servicios en el marco del futuro Programa Espacial, la Comisión seguirá profundizando en la estrategia de ciberseguridad de Galileo para la próxima generación de servicios del sistema global de navegación por satélite y otros nuevos componentes del Programa Espacial[39].

1.2 Construir un escudo cibernético europeo

Con la difusión de la conectividad y la creciente sofisticación de los ciberataques, los Centros de puesta en común y análisis de la información desempeñan una valiosa función, incluso a nivel sectorial, al permitir el intercambio de información entre múltiples partes interesadas sobre las ciberamenazas[40]. Además, las redes y los sistemas informáticos requieren una vigilancia y un análisis constantes para detectar intrusiones y anomalías en tiempo real. Por lo tanto, muchas empresas privadas, organizaciones públicas y autoridades nacionales han creado equipos de respuesta a incidentes de seguridad informática (CSIRT) y centros de operaciones de seguridad (COS).

Los centros de operaciones de seguridad son vitales para recopilar registros[41] y aislar los acontecimientos sospechosos que ocurren en las redes de comunicación que vigilan. Lo hacen mediante la identificación de señales y patrones y la extracción de conocimientos sobre las amenazas a partir de las grandes cantidades de datos que deben ser evaluados. Han contribuido a la detección de las actividades de los ejecutables maliciosos y a su vez han ayudado a contener los ciberataques. La labor que se requiere en estos centros es muy exigente y de ritmo rápido, por lo que la IA y, en particular, las técnicas de aprendizaje automático pueden proporcionar un apoyo inestimable a los profesionales[42].

La Comisión propone crear una **red de centros de operaciones de seguridad en toda la UE[43]** y apoyar la mejora de los centros existentes y el establecimiento de otros nuevos. También apoyará la formación y el desarrollo de capacidades del personal que trabaja en

[37] Reglamento de Ejecución (UE) 2019/1583 de la Comisión.

[38] Comunicación sobre el Plan de Acción para la Democracia Europea COM(2020) 790. Con arreglo al plan, la Red Europea de Cooperación Electoral y las redes electorales de los Estados miembros apoyarán el despliegue de equipos conjuntos de expertos para contrarrestar las amenazas —incluidas las ciberamenazas— a los procesos electorales; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

[39] Esto incluye la nueva iniciativa de comunicación gubernamental por satélite (GOVSATCOM) y residuos espaciales (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[41] De tal manera que las fuerzas y cuerpos de seguridad y el poder judicial puedan utilizarlas como prueba.

[42] Fuente: estudio de Ponemon Institute Research, «Improving the Effectiveness of the SOC, 2019» (Mejorar la eficacia del COS); para los estudios sobre el uso de la IA en los centros de operaciones de seguridad véase, por ejemplo: Khraisat, A., Gondal, I., Vamplew, P. y otros. Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecur* (Estudio de los sistemas de detección de intrusos técnicas, conjuntos de datos y desafíos):2, 20 (2019).

[43] Se elaborarán disposiciones más detalladas sobre la gobernanza, los principios de funcionamiento y la financiación de esos centros, y sobre la forma en que complementarán las estructuras existentes, como los centros de innovación digital.

estos centros. Podría comprometer, sobre la base de un análisis de las necesidades realizado con las partes interesadas pertinentes y con el apoyo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), más de 300 millones EUR para apoyar la cooperación público-privada y transfronteriza en la creación de redes nacionales y sectoriales, en las que participen también las pymes, basándose en disposiciones adecuadas en materia de gobernanza, intercambio de datos y seguridad.

Se alienta a los Estados miembros a que inviertan conjuntamente en este proyecto. De este modo, los centros podrían compartir y correlacionar de manera más eficiente las señales detectadas y crear inteligencia de alta calidad sobre amenazas que se compartirá con los Centros de puesta en común y análisis de la información y las autoridades nacionales, permitiendo así un conocimiento más completo de la situación. El objetivo sería conectar, por fases, el mayor número posible de centros en toda la UE para crear un conocimiento colectivo y compartir las mejores prácticas. Se prestará apoyo a estos centros para mejorar la detección de incidentes, el análisis y las velocidades de respuesta mediante capacidades de IA y aprendizaje automático de última generación, y se complementará con la infraestructura de supercomputación desarrollada en la UE por la Empresa Común de Informática de Alto Rendimiento Europea[44].

Mediante la colaboración y la cooperación sostenidas, esta red proporcionará alertas oportunas sobre incidentes de ciberseguridad a las autoridades y a todas las partes interesadas, incluida la unidad informática conjunta (véase la sección 2.1). **Servirá de verdadero escudo de ciberseguridad para la UE**, proporcionando una red sólida de atalayas, capaces de detectar posibles amenazas antes de que puedan causar daños a gran escala.

1.3 Una infraestructura de comunicación ultrasegura

Las comunicaciones gubernamentales por satélite de la Unión Europea[45], componente del Programa Espacial, proporcionarán capacidades de comunicación seguras y rentables basadas en el espacio para garantizar las misiones y operaciones críticas para la seguridad y la protección gestionadas por la UE y sus Estados miembros, incluidos los agentes de seguridad nacional y las instituciones, órganos y agencias de la UE.

Los Estados miembros se han comprometido a trabajar junto con la Comisión para el despliegue de una infraestructura de comunicación cuántica segura (QCI, por sus siglas en inglés) para Europa[46]. La QCI ofrecerá a las autoridades públicas una nueva manera de transmitir información confidencial utilizando una forma ultrasegura de cifrado para protegerse de los ciberataques, construida con tecnología europea. Tendrá dos componentes principales: las redes de comunicación de fibra terrestre existentes que conectan los sitios estratégicos a nivel nacional y transfronterizo; y satélites espaciales conectados que abarquen toda la UE, incluidos sus territorios de ultramar[47]. Esta iniciativa para desarrollar y aplicar

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking.
[45] GOVSATCOM es un componente del Programa Espacial de la Unión.
[46] La mayoría de los Estados miembros han firmado la Declaración EuroQCI y el desarrollo y el despliegue de la infraestructura tendrán lugar entre 2021 y 2027, con financiación de Horizonte Europa y Europa Digital, y de la Agencia Espacial Europea, sujetos a las disposiciones de gobernanza apropiadas; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.
[47] El desarrollo de un componente espacial es necesario para lograr conexiones punto a punto de larga distancia (>1 000 km) que la infraestructura terrestre no puede soportar. Al explotar las propiedades de la mecánica

formas nuevas y más seguras de cifrado, y para idear nuevas formas de proteger los activos de comunicación y datos críticos, puede ayudar a mantener segura la información sensible y, a su vez, las infraestructuras críticas.

Con esta perspectiva, y yendo más allá, la Comisión explorará el posible despliegue de un sistema de conectividad segura multiorbital. Basándose en GOVSATCOM y en la QCI, este integraría tecnologías de vanguardia (Quantum, 5G, AI, computación en el borde) que se adherirían al marco más restrictivo de la ciberseguridad con el fin de apoyar servicios seguros en el diseño como la conectividad fiable, segura y rentable y la comunicación cifrada para las actividades gubernamentales críticas.

1.4 Protección de la próxima generación de redes móviles de banda ancha

Los ciudadanos y las empresas de la UE que utilizan aplicaciones avanzadas e innovadoras habilitadas por la **5G y las futuras generaciones de redes** deben beneficiarse del más alto nivel de seguridad. Los Estados miembros, junto con la Comisión y con el apoyo de ENISA, han establecido con la caja de herramientas 5G de la UE[48] de enero de 2020 un enfoque amplio y objetivo de la ciberseguridad 5G basado en los riesgos que se apoya en una evaluación de los posibles planes de mitigación y en la identificación de las medidas más eficaces. Además, la UE está consolidando sus capacidades en la 5G y más allá para evitar dependencias y fomentar una cadena de suministro sostenible y diversa.

En diciembre de 2020, la Comisión publicó un informe sobre las repercusiones de la Recomendación del 26 de marzo de 2019 sobre la ciberseguridad de las redes 5G[49] En él se mostraba que se habían realizado avances considerables desde que se acordó la caja de herramientas, y que la mayoría de los Estados miembros están en vías de completar una parte importante de la aplicación de la caja de herramientas en un futuro próximo, aunque con algunas variaciones y lagunas pendientes, como ya se había identificado en el informe sobre los avances publicado en julio de 2020[50].

En octubre de 2020, el Consejo Europeo pidió a la UE y a los Estados miembros «que [aprovechasen] al máximo el conjunto de instrumentos para la ciberseguridad de las redes 5G» y «que [aplicasen] las restricciones pertinentes a los proveedores que se consideren de alto riesgo para recursos clave definidos como críticos y sensibles en la evaluación coordinada de riesgos de la UE [...] atendiendo a criterios objetivos comunes»[51].

De cara al futuro, la UE y sus Estados miembros deben asegurarse de que los riesgos identificados se han mitigado de forma adecuada y coordinada, en particular en lo que

---

cuántica, la QCI permitirá inicialmente a las partes compartir de forma segura claves secretas aleatorias que se utilizarán para cifrar y descifrar mensajes. También incorporará el despliegue de una infraestructura de pruebas y conformidad, para evaluar la conformidad de los dispositivos y sistemas de comunicación cuántica europeos con la infraestructura QCI y su certificación y validación antes de su integración en la QCI. Estará diseñada para soportar aplicaciones adicionales a medida que alcancen el nivel de madurez tecnológica necesario. El actual proyecto piloto OpenQKD (https://openqkd.eu/) es un precursor de esta infraestructura de pruebas y conformidad.

[48]Comunicación de la Comisión sobre el despliegue seguro de la 5G en la UE COM(2020) 50.

[49] Informe de la Comisión sobre las repercusiones de la Recomendación de la Comisión de 26 de marzo de 2019 sobre la ciberseguridad de las redes 5G, de 15 de diciembre de 2020.

[50]Véase el Informe del Grupo de Cooperación SRI sobre la utilización del conjunto de instrumentos, de 24 de julio de 2020.

[51]EUCO 13/20, Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) – Conclusiones.

respecta al objetivo de minimizar la exposición a los proveedores de alto riesgo y de evitar la dependencia de esos proveedores a nivel nacional y de la Unión, y de que se tenga en cuenta cualquier nuevo avance o riesgo significativo. Se invita a los Estados miembros a que utilicen plenamente la caja de herramientas en sus inversiones en capacidades y conectividad digitales.

Sobre la base del informe de las repercusiones de la Recomendación de 2019, la Comisión alienta a los Estados miembros a que aceleren la labor encaminada a completar la aplicación de las principales medidas de la caja de herramientas para el segundo trimestre de 2021. Asimismo, pide a los Estados miembros que sigan supervisando juntos los avances realizados y asegurando una mayor armonización de los enfoques. A escala de la UE, se perseguirán tres objetivos principales para apoyar este proceso: garantizar una mayor convergencia en los enfoques de mitigación de riesgos en toda la UE, apoyar el intercambio continuo de conocimientos y la creación de capacidad, y promover la resiliencia de la cadena de suministro y otros objetivos estratégicos de seguridad de la UE. Las medidas concretas relacionadas con estos objetivos clave se establecen en el anexo específico de la presente Comunicación.

La Comisión seguirá colaborando estrechamente con los Estados miembros para cumplir estos objetivos y medidas con el apoyo de ENISA (véase el anexo).

Además, el enfoque de la caja de herramientas 5G de la UE ha suscitado interés en los países no pertenecientes a la UE que actualmente están desarrollando sus enfoques para proteger sus redes de comunicaciones. Los servicios de la Comisión, junto con el Servicio Europeo de Acción Exterior y la red de delegaciones de la UE, están dispuestos a proporcionar información adicional, si así se solicita, sobre su enfoque integral, objetivo y basado en el riesgo a las autoridades de todo el mundo.

1.5 Una internet de las cosas seguras

Cada cosa conectada contiene vulnerabilidades que pueden ser explotadas con ramificaciones potencialmente extendidas. Las normas del mercado interior incluyen salvaguardias contra los productos y servicios no seguros. La Comisión ya está trabajando para garantizar **soluciones de seguridad transparentes y la certificación en el marco del Reglamento sobre la Ciberseguridad** y para incentivar los productos y servicios seguros sin comprometer el rendimiento[52]. Adoptará su primer programa de trabajo evolutivo de la Unión en el primer trimestre de 2021 (que se actualizará al menos una vez cada tres años) para que la industria, las autoridades nacionales y los organismos de normalización puedan prepararse de antemano para los futuros esquemas europeos de certificación de la ciberseguridad[53]. A

[52] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»). El Reglamento sobre la ciberseguridad promueve la certificación de las TIC a nivel de la UE, con un marco europeo de certificación de la ciberseguridad para el establecimiento de esquemas europeos voluntarios de certificación de la ciberseguridad con el fin de garantizar un nivel adecuado de ciberseguridad para los productos, servicios y procesos de TIC en la Unión, así como para reducir la fragmentación del mercado interior en lo que respecta a los esquemas de certificación de la ciberseguridad en la Unión. Paralelamente, las empresas de «clasificación» de la ciberseguridad tienden a tener su sede fuera de la UE con una transparencia y una supervisión limitadas; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

[53] Según lo dispuesto en el artículo 47, apartado 5, del Reglamento sobre la ciberseguridad.

medida que prolifera la internet de las cosas, es preciso reforzar las normas aplicables, tanto para garantizar la resiliencia general como para impulsar la ciberseguridad.

La Comisión considerará un enfoque integral, incluidas posibles **nuevas normas horizontales para mejorar la ciberseguridad de todos los productos conectados y los servicios asociados que se comercializan en el mercado interior**[54]. Esas normas podrían incluir un **nuevo deber de diligencia para los fabricantes de dispositivos conectados** con el fin de hacer frente a las vulnerabilidades de los programas informáticos, incluida la continuación de las actualizaciones de los programas informáticos y de seguridad, así como la garantía, al final de la vida útil, de la eliminación de datos personales y otros datos sensibles. Estas normas reforzarían la iniciativa «derecho a reparar los programas informáticos obsoletos» presentada en el Plan de acción para la economía circular y complementarían las medidas en curso que abordan tipos específicos de productos, como los requisitos obligatorios que se propondrán para el acceso al mercado de determinados productos inalámbricos (mediante la adopción de un acto delegado en virtud de la Directiva sobre equipos radioeléctricos[55]), y el objetivo de aplicar las normas de ciberseguridad para los vehículos de motor a todos los nuevos tipos de vehículos a partir de julio de 2022[56]. Además, se basarían en la revisión propuesta de las normas generales de seguridad de los productos, que no abordan directamente los aspectos de la ciberseguridad[57].

1.6 Mayor seguridad mundial en internet

Un conjunto de protocolos básicos e infraestructura de apoyo garantiza la funcionalidad e integridad de la internet en todo el mundo[58]. Este conjunto incluye el DNS y su sistema jerárquico y delegado de zonas, comenzando, en la parte superior de la jerarquía, con la zona raíz y los trece servidores raíz del DNS[59] de los que depende la World Wide Web. La Comisión tiene la intención de elaborar **un plan de contingencia, con el apoyo de la financiación de la UE, para hacer frente a escenarios extremos que afecten a la integridad y la disponibilidad del sistema raíz del DNS mundial**. Colaborará con ENISA, los Estados miembros, los dos operadores de servidores raíz de DNS de la UE[60] y la comunidad de múltiples partes interesadas, para evaluar el papel de esos operadores a la hora de garantizar que la internet siga siendo accesible a nivel mundial en cualquier circunstancia.

---

[54] Las conclusiones del Consejo piden que se adopten medidas horizontales sobre la ciberseguridad de los dispositivos conectados; 13629/20, de 2 de diciembre de 2020.

[55] Directiva 2014/53/UE.

[56] Con arreglo al Reglamento de las Naciones Unidas adoptado en junio de 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[57] Revisión de las normas actuales de seguridad general de los productos (Directiva 2001/95/CE); también se prevén propuestas de normas adaptadas sobre la responsabilidad de los productores en el contexto digital en el ámbito de aplicación del marco reglamentario de la UE en materia de responsabilidad.

[58] «El núcleo público de la internet abierta, consistente en sus protocolos e infraestructura principales, que constituyen un bien público mundial, posibilita la funcionalidad esencial de internet en su conjunto, y en él se sustenta su funcionamiento normal. ENISA debe promover la seguridad una internet pública esencial y abierta y la estabilidad de su funcionamiento, lo que incluye, a título meramente enunciativo, sus protocolos esenciales (en particular, DNS, BGP e IPv6), el funcionamiento del sistema de nombres de dominio (incluido el funcionamiento de todos los dominios de nivel superior) y el funcionamiento de la zona raíz»; considerando 23 del Reglamento sobre ciberseguridad.

[59] https://www.iana.org/domains/root/servers.

[60] Los servidores i.root operados por Netnod en Suecia y los servidores k.root operados por RIPE NCC en los Países Bajos.

Para que un cliente acceda a un recurso con un nombre de dominio en particular en internet, su solicitud (generalmente de un localizador uniforme de recursos o URL) debe traducirse o «resolverse» en una dirección IP, mediante referencia a los servidores de nombres DNS. No obstante, las personas y organizaciones de la UE dependen cada vez más de unos pocos resolucionadores de DNS públicos operados por entidades de fuera de la UE. Esta consolidación de la resolución de DNS en manos de escasas empresas[61] hace que el proceso de resolución sea vulnerable en caso de eventos significativos que afecten a un proveedor importante, y dificulta que las autoridades de la UE aborden posibles ciberataques maliciosos e incidentes geopolíticos y técnicos graves[62].

Con vistas a reducir los problemas de seguridad relacionados con la concentración del mercado, la Comisión alentará a las partes interesadas pertinentes, incluidas las empresas de la UE, los proveedores de servicios de Internet y los proveedores de navegadores a adoptar una estrategia de diversificación de la resolución del DNS. La Comisión también tiene la intención de contribuir a la seguridad de la conectividad a internet apoyando el desarrollo de un **servicio público europeo de resolución de DNS**. Esta iniciativa de «DNS4EU» ofrecerá un servicio europeo alternativo para acceder a la internet global. DNS4EU será transparente, se ajustará a las últimas normas y reglas de seguridad, protección de datos y privacidad por diseño y por defecto, y formará parte de la Alianza Industrial Europea para los Datos y la Nube[63].

La Comisión también acelerará, en colaboración con los Estados miembros y la industria, **la adopción de las principales normas de internet, incluidas las relativas al IPv6**[64] **y las normas de seguridad de internet bien establecidas, así como las buenas prácticas del DNS, el enrutamiento y el correo electrónico**[65], sin excluir medidas reglamentarias como una cláusula europea de extinción para el IPv4 para orientar el mercado si no se avanza lo suficiente hacia su adopción. La UE debe promover (como por ejemplo en el marco de la Estrategia de la UE para África[66]) la aplicación de esas normas en los países socios como forma de apoyar el desarrollo de la internet mundial y abierta y de contrarrestar los modelos de internet cerrados y basados en el control. Por último, la Comisión estudiará la necesidad de un mecanismo para supervisar y reunir más sistemáticamente datos agregados sobre el tráfico de internet y asesorar sobre las posibles perturbaciones[67].

---

[61]Consolidation in the DNS resolver market – how much, how fast how dangerous? (Consolidación en el mercado de resolucionadores de DNS: ¿cuánto?, ¿qué rapidez? ¿qué peligrosidad?). (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services (Evidencia de la disminución de la entropía de internet: la falta de redundancia en la resolución del DNS por parte de los principales sitios web y servicios) ( ).

[62] También hay pruebas que muestran que los datos del DNS se pueden utilizar con fines de elaboración de perfiles, con un impacto en los derechos de privacidad y protección de datos.

[63] Declaración conjunta: Building the next generation cloud for businesses and the public sector in the EU (Construcción de la nube de la próxima generación para las empresas y el sector público en la UE); https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe.

[64]El despliegue del IPv6 está más avanzado en la actualidad con el grave agotamiento del suministro y el aumento del coste de las direcciones IPv4. Sin embargo, el despliegue del IPv6 es desigual en toda la UE.

[65]Estas normas incluyen DNSSEC, HTTPS, DNS sobre HTTPS (DoH), DNS sobre TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE y normas de enrutamiento y buenas prácticas, por ejemplo, normas mutuamente acordadas para la seguridad del enrutamiento (MANRS).

[66]Comunicación conjunta «Hacia una estrategia global con África», de 9 de marzo de 209, JOIN(2020) 4 final.

[67] Ese «Observatorio de internet» podría estar dentro del ámbito de actividades del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad; Propuesta de Reglamento por el que

1.7 Una presencia reforzada en la cadena de suministro de tecnología

Con el apoyo financiero previsto para la transformación digital cibersegura a lo largo del marco financiero plurianual 2021-2027, la UE tiene la oportunidad única de poner en común sus activos para impulsar su estrategia industrial[68] y su liderazgo en las tecnologías digitales y la ciberseguridad en toda la cadena de suministro digital (incluidos los datos y la nube, las tecnologías de procesador de próxima generación, la conectividad ultrasegura y las redes 6G), en consonancia con sus valores y prioridades. La intervención del sector público debe basarse en los instrumentos que ofrece el marco normativo de la UE en materia de contratación pública y los proyectos importantes de interés común europeo. Además, puede desbloquear las inversiones privadas mediante asociaciones público-privadas (incluido el aprovechamiento de la experiencia de la asociación contractual público-privada en materia de ciberseguridad y su aplicación a través de la Organización Europea de Ciberseguridad), capital de riesgo en apoyo de las pymes o alianzas industriales y estrategias sobre capacidades tecnológicas.

También se prestará especial atención al Instrumento de Apoyo Técnico[69] y al mejor uso de las últimas herramientas de ciberseguridad por parte de las pymes —especialmente las que no entran en el ámbito de aplicación de la Directiva SRI revisada—, incluso mediante actividades específicas en el marco de los centros de innovación digital del programa Europa Digital. El objetivo es desencadenar una cantidad similar de inversiones por parte de los Estados miembros, que serán igualadas por la industria en el marco de una asociación cogobernada con los Estados miembros en el propuesto **Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (CCCN, por sus siglas en inglés).** El CCCN debe desempeñar un papel fundamental, con aportaciones de la industria y las comunidades académicas, en el desarrollo de la soberanía tecnológica de la UE en materia de ciberseguridad, la creación de capacidad para asegurar infraestructuras sensibles como la 5G y la reducción de la dependencia de otras partes del mundo con respecto a las tecnologías más cruciales.

La Comisión tiene la intención de apoyar, potencialmente con el CCCN, el desarrollo de un programa de máster específico sobre la ciberseguridad, y contribuir a una hoja de ruta europea común de investigación e innovación en materia de ciberseguridad en Europa más allá de 2020. Las inversiones a través del CCCN también se basarían en la cooperación en investigación y desarrollo llevada a cabo por las redes de centros de excelencia en materia de ciberseguridad, reuniendo a los mejores equipos de investigación de Europa con la industria para diseñar y aplicar programas de investigación comunes, de conformidad con la hoja de ruta de la Organización Europea de Ciberseguridad[70]. La Comisión seguirá basándose en la labor de investigación realizada por ENISA y Europol, y también seguirá apoyando, en el marco de Horizonte Europa, a los innovadores particulares de internet que desarrollen tecnologías de comunicación seguras y que mejoren la privacidad, basadas en *software* y *hardware* de código abierto, como se hace actualmente en el marco de la iniciativa Internet de nueva generación.

---

se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación COM(2018) 630 final.

[68] Comunicación sobre un nuevo modelo de industria para Europa, COM/2020/102 final.

[69] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2020:0409:FIN.

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.

1.8 Una población activa cibercualificada de la UE

Los esfuerzos de la UE por mejorar las capacidades de la población activa, desarrollar, atraer y retener a los mejores talentos en materia de ciberseguridad e invertir en investigación e innovación de primer orden constituyen un componente importante de la protección contra las ciberamenazas en general. Este ámbito ofrece un gran potencial. Por tanto, se debe prestar atención específica al desarrollo, la atracción y la retención de un talento más diverso. El Plan de Acción de Educación Digital revisado aumentará la concienciación sobre la ciberseguridad entre los ciudadanos, especialmente los niños y jóvenes, y las organizaciones, particularmente las pymes[71]. También fomentará la participación de las mujeres en la educación en ciencia, tecnología, ingeniería y matemáticas («CTIM») y en los empleos en el ámbito de las TIC para el perfeccionamiento y reciclaje profesional en materia de capacidades digitales. Además, la Comisión, junto con la Oficina de Propiedad Intelectual de la UE en Europol, ENISA, los Estados miembros y el sector privado, desarrollará herramientas de concienciación y directrices para aumentar la resiliencia de las empresas de la UE **contra el robo de propiedad intelectual por medios cibernéticos**[72].

La educación —incluida la formación profesional (FP), la concienciación y los ejercicios— también debe aumentar aún más las capacidades en materia de ciberseguridad y ciberdefensa a nivel de la UE. Para ello, los agentes pertinentes de la UE, como ENISA, la Agencia Europea de Defensa (AED) y la Escuela Europea de Seguridad y Defensa (EESD)[73], deben buscar sinergias entre sus respectivas actividades.

Iniciativas estratégicas

La UE debe garantizar:

- La adopción de la Directiva SRI revisada;
- Medidas reglamentarias para una internet de las cosas seguras
- Mediante la inversión del CCCN en ciberseguridad (en particular a través del programa Europa Digital, Horizonte Europa y el mecanismo de recuperación) que se alcanzan hasta 4 500 millones EUR en inversiones públicas y privadas en el período 2021-2027;
- Una red de la UE de centros de operaciones de seguridad habilitados para la IA y una infraestructura de comunicaciones ultrasegura que aproveche las tecnologías cuánticas;
- La adopción generalizada de tecnologías de ciberseguridad mediante un apoyo específico a las pymes en el marco de los centros de innovación digital;
- El desarrollo de un servicio de resolución de DNS de la UE como alternativa segura y abierta para que los ciudadanos, las empresas y la administración pública de la UE puedan acceder a internet; y
- La finalización de la aplicación de la caja de herramientas 5G para el segundo trimestre de 2021 (véase el anexo).

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_es.
[72] https://ec.europa.eu/commission/presscorner/detail/es/IP_20_2187.
[73] A través de la Plataforma de ejercicios de formación y evaluación de enseñanza cibernética (ETEE).

2. DESARROLLO DE LA CAPACIDAD OPERATIVA PARA PREVENIR, DISUADIR Y CONTRARRESTAR

Los ciberincidentes, ya sean acciones accidentales o deliberadas de delincuentes, agentes públicos o privados, pueden causar enormes daños. Su escala y complejidad, que a menudo están relacionadas con la explotación de servicios, hardware y software de terceros para alcanzar un objetivo final, hacen que el entorno de amenazas colectivo de la UE sea difícil de contrarrestar sin un intercambio de información sistemático y global y cooperación para obtener una respuesta común. La UE se propone alcanzar el objetivo de apoyar a los Estados miembros en la defensa de sus ciudadanos, así como los intereses de su seguridad nacional y económica **mediante la plena aplicación de instrumentos normativos, la movilización y la cooperación**, respetando plenamente los derechos y libertades fundamentales y el Estado de Derecho. Varias comunidades, compuestas de redes, instituciones de la UE, órganos y organismos, así como las autoridades de los Estados miembros, son responsables de prevenir, desalentar, disuadir y contrarrestar las ciberamenazas utilizando sus correspondientes iniciativas e instrumentos[74]. Entre estas comunidades se encuentran: (i) autoridades SRI, como los CSIRT y los responsables de reacción en caso de catástrofe; (ii) autoridades policiales y judiciales; (iii) ciberdiplomacia; y (iv) ciberdefensa.

2.1 Una unidad informática conjunta

Una unidad informática conjunta serviría como plataforma virtual y física para la cooperación entre las diferentes comunidades de ciberseguridad dentro de la UE, con un enfoque centrado en la coordinación operativa y técnica para la lucha contra grandes amenazas y ciberincidentes transfronterizos.

La unidad informática conjunta supondría un importante paso al frente hacia la culminación del **marco europeo de gestión de crisis de ciberseguridad.** Como indica en sus orientaciones políticas la presidenta de la Comisión[75], la unidad debe permitir a los Estados miembros y las instituciones, organismos y agencias de la UE hacer un uso pleno de las estructuras, los recursos y capacidades existentes, y promover una mentalidad de **«necesidad de compartir»**. Proporcionaría los medios para consolidar los avances alcanzados hasta el momento en la aplicación de la recomendación de 2017 sobre una respuesta coordinada frente a incidentes de ciberseguridad y crisis a gran escala (Plan director)[76]. También proporcionaría la oportunidad de reforzar aún más la cooperación en torno a la configuración del Plan director y aprovecharía el progreso alcanzado, sobre todo en el seno del Grupo de Cooperación SRI y la red CyCLONe.

[74]Incluido el apoyo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) para la cooperación operativa y la gestión de las situaciones de crisis; la red de CSIRT; la red de funcionarios de enlace nacionales para la gestión de cibercrisis (CyCLONe, que se convertirá en EU-CyCLONe tal como se propone en la Directiva SRI revisada); El Grupo de Cooperación SRI; «rescEU»; el Centro Europeo de Ciberdelincuencia y Grupo de Acción Conjunta contra la Ciberdelincuencia de Europol y el Protocolo de respuesta policial ante emergencias; el Centro de Inteligencia y de Situación de la Unión Europea (EU INTCEN) y el conjunto de instrumentos de ciberdiplomacia; la Capacidad única de análisis de inteligencia (SIAC); Los ciberproyectos en virtud de la cooperación estructurada permanente (CEP), entre los que destacan los «Equipos de respuesta telemática rápida y de asistencia mutua en el ámbito de la ciberseguridad» (CRRT).

[75]«Una Unión que se esfuerza por lograr más resultados: Mi agenda para Europa», orientaciones políticas para la próxima Comisión Europea 2019-2024, por la candidata a presidenta de la Comisión Europea, Ursula von der Leyen.

[76]Recomendación de Plan director C(2017) 6100 final, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de seguridad a gran escala.

Esto podría abordar **dos carencias importantes** que en la actualidad aumentan las vulnerabilidades y crean ineficiencias en la respuesta frente a las amenazas y los incidentes transfronterizos que afectan a la Unión. En primer lugar, las **comunidades** civiles, policiales, diplomáticas y de ciberdefensa todavía no comparten un espacio común para fomentar una cooperación estructurada y facilitar la cooperación técnica y operativa. En segundo lugar, las partes interesadas en ciberseguridad pertinentes todavía no han sido capaces de aprovechar al máximo todo el **potencial** que ofrece la cooperación operativa y la asistencia mutua dentro de las redes y las comunidades existentes. Esto incluye la ausencia de una plataforma que permita la cooperación operativa con el sector privado. La unidad debe mejorar y acelerar la coordinación, y permitir que la UE pueda hacer frente y responder a las crisis e incidentes cibernéticos a gran escala.

La unidad informática conjunta no sería un organismo adicional independiente, ni tampoco afectaría a las competencias y facultades de las autoridades nacionales de ciberseguridad o de los participantes de la UE. Más bien, la unidad actuaría como mecanismo de protección mediante el cual los participantes pudieran aprovechar el apoyo y la experiencia de los demás, sobre todo en el caso de que varias comunidades de ciberseguridad tuviesen que trabajar en estrecha colaboración. Al mismo tiempo, los acontecimientos recientes muestran la necesidad de que la UE aumente su nivel de ambición y preparación para hacer frente al panorama y las realidades de las ciberamenazas. Por tanto, como parte de su contribución a la unidad informática conjunta, los agentes de la UE (la Comisión y las agencias y organismos de la UE) estarán dispuestos a aumentar considerablemente sus recursos y capacidades, a fin de mejorar su preparación y resiliencia.

La unidad informática conjunta cumpliría tres objetivos principales. En primer lugar, garantizaría la **preparación** en todas las comunidades de ciberseguridad; en segundo lugar, ofrecería un **conocimiento** de la situación continuo y compartido a través del intercambio de información; en tercer lugar, reforzaría la **respuesta** y la recuperación coordinadas. Para lograr estos objetivos, la unidad debe basarse en **bloques y objetivos** bien definidos, como garantizar que la **información se comparta de forma rápida y segura**, mejorar la **cooperación** entre participantes, incluida la interacción entre los Estados miembros y las entidades pertinentes de la UE, establecer **asociaciones estructuradas con una base industrial de confianza** y facilitar un enfoque coordinado para la **cooperación con socios externos**. Con el fin de alcanzarlos, y sobre la base de una descripción de las capacidades disponibles a escala nacional y de la UE, la unidad podría facilitar el desarrollo de un marco de cooperación.

Para que la unidad informática conjunta se convierta en el punto clave de la cooperación operativa de la UE en materia de ciberseguridad, la Comisión trabajará conjuntamente con los Estados miembros y las instituciones, organismos y agencias pertinentes de la UE, incluidos ENISA, CERT-UE y Europol, para promover un **enfoque inclusivo y gradual** que respete plenamente las competencias y los mandatos de todas las partes involucradas. En línea con este enfoque, la unidad podría contribuir a una mayor cooperación entre los componentes de una comunidad cibernética específica, en los ámbitos en que dichos componentes lo consideren necesario.

Se proponen cuatro pasos principales para la creación de la unidad informática conjunta:

- *Definir*, mediante la descripción de las capacidades disponibles a escala nacional y de la UE;

- *Preparar*, mediante el establecimiento de un marco para una cooperación y asistencia estructuradas;

- *Poner en marcha*, mediante la aplicación del marco, aprovechando los recursos que ofrecen los participantes para que la unidad informática conjunta sea operativa;

- *Expandir*, mediante el fortalecimiento de la capacidad de respuesta coordinada con la colaboración de la industria y las partes asociadas.

Sobre la base del resultado de la consulta con los Estados miembros, las instituciones, organismos y agencias de la UE[77], la Comisión, con la participación del Alto Representante, de conformidad con sus competencias, presentarán a más tardar en febrero de 2021 el proceso, los hitos y el calendario para **definir, preparar, poner en marcha y expandir la unidad informática conjunta**.

2.2 Lucha contra la ciberdelincuencia

Nuestra dependencia de las herramientas en línea ha aumentado de forma exponencial la superficie de ataque de los delincuentes cibernéticos y nos ha llevado a una situación en la que la investigación de casi todos los tipos de delitos incluye un componente digital. Por otra parte, algunas partes fundamentales de nuestra sociedad están amenazadas por actores cibernéticos y por aquellos que utilizan herramientas cibernéticas para planificar y ejecutar sus acciones ilegales. Por lo tanto, existen vínculos estrechos con la política general de seguridad de la UE, tal como se refleja en los elementos cibernéticos de la Estrategia de la UE para una Unión de la Seguridad de 2020 y en la agenda de la UE de lucha contra el terrorismo[78].

La lucha efectiva contra la ciberdelincuencia es un factor clave para garantizar la ciberseguridad: la disuasión no se puede alcanzar únicamente mediante la capacidad de recuperación, sino que también requiere la identificación y procesamiento de los infractores. Por lo tanto, es esencial fomentar la cooperación y los intercambios entre los agentes de ciberseguridad y las fuerzas policiales. Por ello, Europol y ENISA ya han iniciado una cooperación sólida a escala de la UE para organizar conferencias y talleres conjuntos, y han proporcionado informes conjuntos a la Comisión, los Estados miembros y otras partes interesadas sobre las amenazas y los desafíos tecnológicos que supone la ciberseguridad. La Comisión continuará apoyando este enfoque integrado para garantizar una respuesta efectiva y coherente basada en una imagen integral de la información.

Como elemento importante de esa respuesta, la UE y las autoridades nacionales necesitan expandir y mejorar la capacidad de las fuerzas policiales para investigar el cibercrimen, respetando plenamente los derechos fundamentales y buscando el equilibrio necesario entre los distintos derechos e intereses. La UE debería ser capaz de hacer frente a la ciberdelincuencia mediante una legislación totalmente aplicada y apta para los fines que persigue, que preste especial atención a la lucha contra el abuso sexual de menores en línea y orientada a las investigaciones digitales, incluida la delincuencia en la Internet profunda. La

[77]Consulta a los Estados miembros (incluso durante el ejercicio Blue OLEx20, que reúne a los responsables de las autoridades nacionales de ciberseguridad), instituciones, organismos y agencias de la UE realizada entre julio y noviembre de 2020.
[78]Comunicación «Agenda de lucha contra el terrorismo de la UE: anticipar, prevenir, proteger, responder», 9.12.2020, COM(2020) 795 final.

aplicación de la ley debe estar completamente preparada para las investigaciones digitales. Por ello, la Comisión presentará un plan de acción para mejorar la capacidad digital de los servicios policiales, proporcionándoles las habilidades y herramientas necesarias. Además, Europol seguirá desarrollando su función como centro de asesoramiento para apoyar a las autoridades policiales nacionales en la lucha contra la delincuencia facilitada por los medios cibernéticos y que depende de ellos, contribuyendo así a la definición de normas forenses comunes (a través del laboratorio y el centro para la innovación de Europol). Todas estas actividades requieren una adecuada difusión por parte de los Estados miembros, a los que se anima a hacer uso de los programas nacionales del Fondo de Seguridad Interior y a proponer proyectos como respuesta a la convocatoria de propuestas en el marco del instrumento temático.

La Comisión utilizará todos los medios adecuados, incluidas las acciones de infracción, para garantizar que la Directiva de 2013 relativa a los ataques contra los sistemas de información[79] se traslade y aplique en su totalidad, incluida la provisión de estadísticas por parte de los Estados miembros. Servirá para evitar el abuso de nombres de dominio, incluida, cuando proceda, la distribución de contenido ilícito, y reivindicar la disponibilidad de datos de registro precisos mediante la continuación del compromiso con la Corporación para la Asignación de Nombres y Números en Internet (ICANN) y otras partes interesadas en el sistema de gobernanza de Internet, especialmente a través del Grupo de Trabajo de Seguridad Pública del Comité Consultivo Gubernamental de ICANN. En consecuencia, la propuesta incluida en la Directiva SRI revisada prevé que existan bases de datos precisas y completas que recojan nombres de dominio y registros de datos o «datos WHOIS» y se ofrezca un acceso legítimo a estos datos como medida esencial para garantizar la seguridad, la estabilidad y la capacidad de recuperación de los sistemas de nombres de dominio.

Asimismo, la Comisión seguirá trabajando para proporcionar canales adecuados y aclarar las normas para obtener acceso transfronterizo a las pruebas electrónicas de las investigaciones penales (necesarias en el 85 % de las investigaciones, con un total de 65 % de las solicitudes dirigidas a los proveedores sobre la base de otra competencia judicial) facilitando la adopción y subsiguiente aplicación del «paquete de pruebas electrónicas» y medidas prácticas[80]. Una adopción rápida por parte del Parlamento Europeo y el Consejo de las propuestas sobre pruebas electrónicas es clave para proporcionar a los profesionales un instrumento eficaz. Las pruebas electrónicas deben ser legibles, por lo tanto, la Comisión seguirá trabajando para apoyar la capacidad policial en el ámbito de las investigaciones digitales, incluidas aquellas que tratan material criptográfico cuando este se encuentra en investigaciones penales, al tiempo que se preserva la integridad de sus funciones con el fin de proteger los derechos fundamentales y la ciberseguridad.

[79]Directiva 2013/40/UE relativa a los ataques contra los sistemas de información.

[80]COM(2018) 225 y 226; C(2020) 2779 final. En concreto, el proyecto SIRIUS ha recibido recientemente fondos adicionales en el marco del Instrumento de Colaboración para mejorar los canales y obtener acceso transfronterizo lícito a las pruebas electrónicas de investigaciones penales (necesarias en el 85 % de las investigaciones de delitos graves, con un total de 65 % de las solicitudes dirigidas a los proveedores sobre la base de otra competencia judicial) y establecer normas compatibles a escala internacional.

2.3 Conjunto de instrumentos de ciberdiplomacia de la UE

La UE ha estado utilizando su **conjunto de instrumentos de ciberdiplomacia**[81] para prevenir, desalentar, disuadir y contrarrestar las actividades cibernéticas maliciosas. Después de la introducción del marco jurídico para las medidas restrictivas dirigidas contra los ciberataques en mayo de 2019[82], la UE enumeró en una lista a seis personas y tres entidades responsables o involucradas en ciberataques que afectaron a la UE y a sus Estados miembros con arreglo al régimen en julio de 2020[83]. Otras dos personas y un organismo se añadieron a la lista en octubre de 2020[84]. Las actividades cibernéticas maliciosas, incluidas aquellas con una naturaleza de combustión lenta, deben abordarse mediante una respuesta diplomática conjunta de la UE, eficaz e integral, mediante el uso de todas las medidas disponibles a escala de la UE.

Una respuesta diplomática conjunta de la UE rápida y eficaz requiere un conocimiento de la situación sólido y compartido, y la capacidad de preparar rápidamente una posición conjunta de la UE. El Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad fomentará y facilitará el establecimiento de un **grupo de trabajo de ciberinteligencia de los Estados miembros de la UE** que resida en el Centro de Análisis de Inteligencia de la UE (INTCEN) para avanzar en la cooperación de inteligencia estratégica sobre actividades y amenazas cibernéticas. Este trabajo seguirá apoyando el conocimiento de la situación de la UE y la toma de decisiones mediante una respuesta diplomática conjunta. El grupo de trabajo se involucrará con las estructuras existentes[85], incluidas, si fuese necesario, aquellas encargadas de amenazas con un abanico más amplio de interferencias híbridas y exteriores para evaluar los conocimientos sobre la situación.

Para fortalecer su capacidad para prevenir, desalentar, disuadir y contrarrestar los comportamientos maliciosos en el ciberespacio, el Alto Representante, con la participación de la Comisión y de conformidad con sus competencias, presentará una propuesta para que la UE siga definiendo su **postura de disuasión cibernética**. Sobre la base del trabajo realizado hasta la fecha en el marco del conjunto de instrumentos de ciberdiplomacia, la postura debe contribuir al comportamiento responsable de los Estados y a la cooperación en el ciberespacio, y debe dar directrices concretas sobre la lucha contra los ciberataques con

[81] https://www.consilium.europa.eu/es/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[82] Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 129I de 17.5.2019, p. 13); y el Reglamento (UE) 2019/796 del Consejo.
de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 129I de 17.5.2019, p. 1).

[83] Decisión (PESC) 2020/1127 del Consejo, de 30 de julio de 2020, por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (ST/9564/2020/INIT) (DO L 246, de 30.7.2020, p. 12); y el Reglamento de Ejecución (UE) 2020/1125 del Consejo, de 30 de julio de 2020, Reglamento de Ejecución (UE) 2019/796 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (ST/9568/2020/INIT) (DO L 246, de 30.7.2020, p. 4).

[84] Decisión (PESC) 2020/1537 del Consejo, de 22 de octubre de 2020, por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 351I, de 22.10.2020, p. 5); Y el Reglamento de Ejecución (UE) 2020/1536 del Consejo, de 22 de octubre de 2020 del Reglamento de Ejecución (UE) 2019/796 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 351I, de 22.10.2020, p. 1).

[85] Al igual que la capacidad única de análisis de inteligencia (SIAC) y, cuando proceda, los proyectos pertinentes establecidos en virtud de CEP, así como el sistema de alerta rápida (RAS) de 2018, que se ha instalado para dar soporte al enfoque general de la UE para hacer frente a la desinformación.

mayor efecto, en particular aquellos que afectan a nuestra infraestructura básica, a las instituciones y procesos democráticos[86], así como contra los ataques a la cadena de suministro y el robo de propiedad intelectual mediante tecnología cibernética. La postura debe describir cómo la UE y los Estados miembros podrían aprovechar sus herramientas políticas, económicas, diplomáticas, legales y de comunicación estratégica para combatir las actividades cibernéticas maliciosas, así como abordar la forma en la que la UE y los Estados miembros podrían avanzar en su capacidad para atribuir actividades cibernéticas maliciosas. Además, junto con el Consejo y la Comisión, el Alto Representante se ha propuesto examinar una serie de **medidas adicionales en el marco del conjunto de instrumentos de ciberdiplomacia**, entre las que se encuentra la posibilidad de ampliar las medidas restrictivas con nuevas opciones, así como explorar la **votación por mayoría cualificada para las listas en el marco del régimen de sanciones horizontales contra los ciberataques.** Además, la UE debería intensificar sus esfuerzos para **reforzar la cooperación con los socios internacionales**, incluida la OTAN, a fin de avanzar en un entendimiento común del panorama de amenazas, desarrollar mecanismos de cooperación e identificar las respuestas diplomáticas cooperativas.

El Alto Representante, con la participación de la Comisión, también propondrá una actualización de las directrices para la **aplicación del conjunto de instrumentos de ciberdiplomacia**[87], incluida en vistas del aumento de la eficiencia del proceso de toma de decisiones, y continuará organizando ejercicios, así como evaluaciones periódicas, del conjunto de instrumentos de ciberdiplomacia. Además, la UE debería seguir **integrando el conjunto de instrumentos de ciberdiplomacia en los mecanismos de crisis de la UE**, esforzarse para buscar sinergias que contrarresten las amenazas híbridas, la desinformación y la interferencia exterior en cumplimiento de la Comunicación conjunta sobre la lucha contra las amenazas híbridas[88] y el Plan de Acción para la Democracia Europea. En este contexto, la UE debería reflexionar sobre la interacción entre el conjunto de instrumentos de ciberdiplomacia y la posible aplicación del artículo 42.7 del TUE y el artículo 222 del TFUE[89].

2.4 Impulsar las capacidades de ciberdefensa

La UE y los Estados miembros necesitan aumentar su capacidad para evitar y contrarrestar las ciberamenazas en consonancia con el nivel de ambición de la UE derivado de la Estrategia Global de la UE de 2016[90]. Con este fin, el Alto Representante, en cooperación con la Comisión, presentará una **revisión del marco político de ciberdefensa** para mejorar aún más la coordinación y la cooperación entre los actores de la UE[91], así como con los Estados miembros y entre ellos, incluidas las misiones y operaciones de la Política Común de Seguridad y Defensa (PCSD). El marco político de ciberdefensa debe informar sobre la

[86] En particular, mediante la búsqueda de sinergias con las iniciativas en el marco del Plan de Acción para la Democracia Europea.
[87] 13007/17.
[88] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018&from=ES.
[89] Respectivamente, la cláusula de defensa mutua, cláusula de solidaridad.
[90] Conclusiones del Consejo (14149/16) sobre la aplicación de la Estrategia Global de la UE en materia de seguridad y defensa.
[91] En particular el SEAE, incluido el Estado Mayor de la Unión Europea (EMUE), la Escuela Europea de Seguridad y Defensa (EESD), la Comisión y las agencias de la UE, en particular la Agencia Europea de Defensa (AED).

próxima brújula estratégica[92] para garantizar que la ciberseguridad y la ciberdefensa se integran aún más en la agenda ampliada de seguridad y defensa.

En 2018, la EU identificó el ciberespacio como un dominio de operaciones[93]. Una próxima **«Visión y estrategia militar en el ciberespacio como un dominio de operaciones»** desarrollada por el Comité Militar de la UE debería definir aún más cómo el ciberespacio como dominio de operaciones permite que se realicen las misiones y operaciones militares de la PCSD de la UE. La **red militar de CERT-UE**[94], creada por la Agencia Europea de Defensa (AED), contribuirá aún más a aumentar de manera significativa la cooperación entre los Estados miembros. Además, para garantizar la ciberseguridad de las infraestructuras espaciales básicas de las que es responsable el Programa Espacial, se reforzarán la Agencia de la Unión Europea para el Programa Espacial y, de manera especial, el Centro de Supervisión de la Seguridad de Galileo y se ampliará su mandato a otros activos críticos del Programa Espacial.

La UE y los Estados miembros deben aportar un nuevo impulso al **desarrollo de las capacidades de ciberdefensa de última generación** a través de diferentes políticas e instrumentos de la UE, en particular el marco político de ciberdefensa, y en su caso, fundamentarse sobre el trabajo de la AED. Esto requiere un hincapié especial en el desarrollo y uso de tecnologías clave, tales como la inteligencia artificial, el cifrado y la computación cuántica. En consonancia con las prioridades de desarrollo de capacidad de la UE de 2018[95] y sobre la base de los resultados del informe de la primera revisión anual coordinada de la defensa (CARD)[96], la UE debería seguir fomentando la cooperación entre los Estados miembros en **investigación sobre ciberdefensa, innovación y desarrollo de la capacidad** y animar a los Estados miembros a que utilicen todo el potencial de la **cooperación estructurada permanente (CEP)**[97] y el **FED**[98]**.**

El próximo **Plan de acción de la Comisión sobre sinergias entre los sectores civil, de defensa y espacial** que se presentará en el primer trimestre de 2021 incluirá medidas para reforzar el apoyo a las sinergias a nivel de programas, tecnologías, innovación y creación de empresas, en consonancia con la gobernanza de los respectivos programas[99].

Además, las sinergias y las interfaces pertinentes deben desarrollarse a partir de las iniciativas de ciberdefensa emprendidas en otros contextos, incluidos los proyectos de colaboración

[92] Conclusiones del Consejo sobre seguridad y defensa de 17 de junio de 2020 (8910/20).
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf.
[94] El establecimiento de una red militar de CERT-UE responde a un objetivo identificado en el marco político de ciberdefensa de 2018 y se propone promover la interacción y el intercambio de información entre los CERT-UE militares de los Estados miembros.
[95] En junio de 2018, los Estados miembros acordaron en la Junta Directiva de la AED dirigir la cooperación en defensa a escala de la UE.
[96] Aprobado por los Ministros de Defensa en la Junta Directiva de la AED en noviembre de 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).
[97] Actualmente existen varios proyectos CEP relacionados con ciberseguridad, en particular la Plataforma de intercambio de información sobre respuestas a ciberamenazas e incidentes de ciberseguridad, los Equipos de respuesta telemática rápida y de asistencia mutua en el ámbito de la ciberseguridad, el Centro de innovación y las instituciones académicas de la UE relacionadas con la cibernética y el Centro de coordinación de los ámbitos de la información y cibernético (CIDCC).
[98] En el marco del FED, la Comisión ya ha identificado oportunidades para emprender posibles medidas de investigación y desarrollo en ciberdefensa colaborativa destinadas a reforzar la cooperación, la capacidad innovadora y la competitividad de la industria de defensa.
[99] Como Horizonte Europa, Europa Digital y el FED.

cibernéticos[100] creados por los Estados miembros en virtud de CEP, así como con las estructuras de ciberseguridad de la UE, para apoyar el intercambio de información y el apoyo mutuo.

Iniciativas estratégicas

La UE debería:

- Completar el marco europeo de gestión de crisis de ciberseguridad y determinar los procesos, hitos y el plazo para el establecimiento de la unidad informática conjunta;
- Continuar aplicando la agenda contra la ciberdelincuencia en cumplimiento de la Estrategia para una Unión de la Seguridad;
- Fomentar y facilitar la creación de un grupo de trabajo de ciberinteligencia de los Estados miembros que resida en el Centro de Análisis de Inteligencia de la UE (INTCEN);
- Avanzar la postura de disuasión cibernética de la UE para prevenir, desalentar, disuadir y contrarrestar las actividades cibernéticas maliciosas;
- Revisar el marco político de ciberdefensa;
- Facilitar el desarrollo de una «Visión y estrategia militar en el ciberespacio como un dominio de operaciones» para las misiones y operaciones militares de la PCSD;
- Apoyar sinergias entre los sectores civil, de defensa y espacial; así como
- Reforzar la ciberseguridad de las infraestructuras espaciales básicas en cumplimiento del Programa Espacial.

3. FOMENTAR UN CIBERESPACIO MUNDIAL Y ABIERTO

La UE debe seguir trabajando con socios internacionales para promover un modelo político y una visión del ciberespacio cimentado sobre el Estado de Derecho, los derechos humanos, las libertades fundamentales y los valores democráticos que contribuyen al desarrollo social, económico y político en todo el mundo, y que contribuyen con una Unión de la Seguridad. La cooperación internacional es esencial para mantener un ciberespacio global, abierto, estable y seguro. Con este fin, la UE debe seguir trabajando con terceros países, organizaciones internacionales, así como con la comunidad de múltiples partes interesadas, para desarrollar y aplicar una política cibernética internacional coherente e integral, teniendo presente la creciente interconexión entre los aspectos económicos de las nuevas tecnologías, la seguridad interior y exterior, y las políticas de defensa y seguridad. La UE, como fuerte bloque económico y comercial, establecida sobre valores democráticos fundamentales, el respeto del Estado de Derecho y los derechos fundamentales, es también un lugar privilegiado desde donde dirigir la definición y promoción de normas y estándares internacionales.

[100] https://pesco.europa.eu/.

3.1. Liderazgo de la UE en materia de estándares, normas y marcos en el ciberespacio

Un paso adelante en la normalización internacional

Con el fin de promover y defender su visión del ciberespacio en el ámbito internacional, la UE necesita **intensificar su participación y liderazgo en los procesos internacionales de normalización y potenciar su representación en los organismos internacionales y europeos de normalización, así como en otras organizaciones de desarrollo de normas**[101]. Con el vertiginoso ritmo de desarrollo de las tecnologías digitales, los estándares internacionales van cobrando cada vez más importancia a la hora de completar los esfuerzos regulatorios tradicionales en ámbitos como la inteligencia artificial, la nube, la computación y la comunicación cuánticas. Los países terceros utilizan cada vez más la normalización internacional para avanzar en su agenda política e ideológica, que a menudo no se corresponde con los valores de la UE. Además, existe un riesgo cada vez mayor de que diferentes marcos compitan por la normalización internacional, lo que llevaría a una fragmentación.

La conformación de las normas internacionales en sectores como las tecnologías emergentes y la arquitectura básica de Internet, en consonancia con los valores de la UE, es esencial para garantizar que Internet siga siendo una herramienta abierta y global, que las tecnologías estén centradas en las personas y la seguridad, y que su uso sea legal, seguro y ético. Como parte de su próxima estrategia de normalización, la UE debería definir sus **objetivos para la normalización internacional** y dirigir una divulgación dinámica y coordinada para promoverlos en el ámbito internacional. Debe buscarse una cooperación más estrecha y el reparto de la carga con socios afines y partes interesadas europeas.

Avances en la actuación responsable de los Estados en el ciberespacio

La UE continúa trabajando con sus socios internacionales para avanzar y promover un ciberespacio global, abierto, estable y seguro en el que se respete el **derecho internacional, en concreto la Carta de las Naciones Unidas**[102], y se **cumplan las normas voluntarias, reglas y principios de conducta responsable de los Estados**[103]. Tras el deterioro del debate multilateral eficaz sobre seguridad internacional en el ciberespacio, existe una necesidad evidente de que la UE y los Estados miembros adopten una postura más dinámica en los debates de la ONU y en otros foros internacionales pertinentes. La UE es la más indicada para **avanzar, coordinar y consolidar las posturas de los Estados miembros en los foros internacionales** y debe **desarrollar una postura de la UE sobre la aplicación del derecho internacional en el ciberespacio**. El Alto Representante, junto con los Estados miembros, también tiene como objetivo impulsar su propuesta inclusiva y basada en el consenso para alcanzar un compromiso político sobre un **Programa de acción para avanzar en la**

[101] Por ejemplo, la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI), la Unión Internacional de Telecomunicaciones (UIT), el Comité Europeo de Normalización(CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC), el Instituto Europeo de Normas de Telecomunicaciones (ETSI), el Grupo Especial sobre Ingeniería de Internet (IETF), el Proyecto de Asociación de Tercera Generación (3GPP) y el Instituto de ingenieros eléctricos y electrónicos (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.

[103] Como se refleja en los informes pertinentes de los Grupos de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (UNGGE), aprobados por la AGNU, en particular los informes de 2015, 2013 y 2010.

actuación responsable de los Estados en el ciberespacio (PoA)[104] en la ONU. Sobre la base del acervo comunitario existente, según lo aprobado por la Asamblea General de las Naciones Unidas[105], el programa PoA ofrece una plataforma para la cooperación y el intercambio de prácticas ejemplares dentro de la ONU y propone establecer un mecanismo para poner en práctica las normas de actuación responsable de los Estados y promover la creación de capacidad. Además, el Alto Representante se ha propuesto reforzar e impulsar la aplicación de **medidas destinadas a fomentar la confianza** entre los Estados, como el intercambio de prácticas ejemplares a escala regional y multilateral, y contribuir a la cooperación entre regiones.

La creciente conectividad global no debe conducir a la censura, la vigilancia masiva, las violaciones de la privacidad de los datos y la represión contra la sociedad civil, las instituciones académicas y los ciudadanos. La UE debería seguir dirigiendo la protección y la promoción de los **derechos humanos y las libertades fundamentales** en línea. Con este fin, la UE debería promover un mayor cumplimiento de las normas y la legislación internacionales de derechos humanos[106], poner en práctica su Plan de Acción para los Derechos Humanos y la Democracia 2020-2024[107] y avanzar en sus orientaciones sobre derechos humanos relativas a la libertad de expresión en línea y fuera de línea[108], **ofreciendo un nuevo impulso para la aplicación práctica de los instrumentos de la UE**. La UE debe mantener los esfuerzos para **proteger a los defensores de los derechos humanos, la sociedad civil y las instituciones académicas que trabajan en cuestiones como la ciberseguridad, la privacidad de los datos, la vigilancia y la censura en línea.** Con este fin, la UE debería proporcionar una mayor orientación práctica, promover prácticas ejemplares e intensificar sus esfuerzos para evitar el mal uso de las tecnologías emergentes, sobre todo mediante el uso de medidas diplomáticas, cuando sea necesario, así como el control de la exportación de este tipo de tecnologías. La UE también debe seguir luchando por la protección en línea de los miembros más vulnerables de la sociedad, proponiendo legislación para proteger mejor a los niños contra el abuso sexual y la explotación de los menores y una Estrategia sobre los Derechos de la Infancia.

Convenio de Budapest sobre la Ciberdelincuencia

La EU sigue apoyando a aquellos países terceros que desean acceder al **Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa** y trabaja para terminar el **Segundo Protocolo adicional al Convenio de Budapest,** que incluye medidas y garantías para mejorar la cooperación internacional entre las autoridades policiales y judiciales, así como entre las autoridades y proveedores de servicios en otros países. Para ello, la Comisión participa en las negociaciones en nombre de la UE[109]. La iniciativa actual para un nuevo instrumento jurídico sobre ciberdelincuencia a escala de la ONU pone en riesgo la ampliación de divisiones y ralentiza reformas nacionales muy necesarias y esfuerzos de creación de

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.
[105] Como se refleja en los informes pertinentes de los Grupos de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (UNGGE), aprobados por la AGNU, en particular: los informes de 2015, 2013 y 2010.
[106] En particular, la Carta de las Naciones Unidas y la Declaración Universal de Derechos Humanos.
[107] https://www.consilium.europa.eu/es/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/.
[108] https://data.consilium.europa.eu/doc/document/ST-9647-2014-INIT/es/pdf.
[109] Decisión del Consejo de junio de 2019 (ref. 9116/19).

capacidad relacionados, que podrían obstaculizar una cooperación internacional eficaz contra la ciberdelincuencia: la UE no ve necesario ningún nuevo instrumento jurídico sobre ciberdelincuencia a escala de la ONU. La UE sigue participando en **intercambios multilaterales sobre ciberdelincuencia** para garantizar el respeto de los derechos humanos y las libertades fundamentales mediante la inclusión y la transparencia, y teniendo en cuenta los conocimientos disponibles, con el objetivo de ofrecer un valor añadido para todos.

3.2 Cooperación con los socios y la comunidad de múltiples partes interesadas

La UE debería **fortalecer y ampliar sus ciberdiálogos con terceros países** para promover sus valores y visión para el ciberespacio, compartir prácticas ejemplares y conseguir una cooperación más eficaz. Asimismo, la UE debe establecer **intercambios estructurados con organizaciones regionales** como la Unión Africana, el Foro Regional de la ASEAN, la Organización de los Estados Americanos y la Organización para la Seguridad y la Cooperación en Europa. Al mismo tiempo, la UE debería tratar de encontrar un terreno común, siempre que sea posible y oportuno, con otros socios basándose en cuestiones de interés común. En colaboración con las delegaciones de la UE y, cuando proceda, con las embajadas de los Estados miembros de todo el mundo, la UE debe formar una **Red de Ciberdiplomacia informal de la UE** para promover la visión de la UE sobre el ciberespacio, el intercambio de información y coordinar periódicamente los avances en materia de ciberespacio[110].

Sobre la base de las declaraciones conjuntas del 8 de julio de 2016[111] y del 10 de julio de 2018[112], la UE debería seguir avanzando en su **cooperación UE-OTAN**, sobre todo en lo que respecta a los requisitos para la interoperabilidad de la ciberdefensa. En este contexto, la UE debe proseguir con la afiliación de las estructuras de la PCSD pertinentes al trabajo en red de las misiones federadas de la OTAN y permitir la interoperabilidad de las redes con la OTAN y sus socios cuando sea necesario. Además, la cooperación entre la UE y la OTAN en materia de educación, formación y ejercicios debe estudiarse más a fondo, como en la búsqueda de sinergias entre la Escuela Europea de Seguridad y Defensa y el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN.

En consonancia con sus valores, la UE apoya firmemente y promueve el **modelo de múltiples partes interesadas para la gobernanza de Internet**. Ninguna entidad, gobierno u organización internacional deben tratar de controlar Internet. La UE debe seguir participando en los foros[113] para mejorar la cooperación y garantizar la protección de los derechos y libertades fundamentales, en particular el derecho a la dignidad, la privacidad y la libertad de expresión e información. Para que la cooperación avance en cuestiones de ciberseguridad entre varias partes interesadas, la Comisión y el Alto Representante, de conformidad con sus respectivas competencias, se han propuesto reforzar los **intercambios regulares y estructurados con las partes interesadas,** incluido el sector privado, las instituciones académicas y la sociedad civil, subrayando que la naturaleza interconectada del ciberespacio requiere que todas las partes interesadas intercambien y asuman sus responsabilidades

[110] Cuando proceda, también podría aprovechar las actividades de la Red de diplomacia digital e incorporar a los ministerios de Asuntos Exteriores de los Estados miembros.
[111] http://www.consilium.europa.eu/es/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/.
[113] Tales como la Corporación para la Asignación de Nombres y Números en Internet (ICANN) y el Foro para la Gobernanza de Internet (IGF).

concretas para mantener un ciberespacio global, abierto, estable y seguro. Estos esfuerzos proporcionarán información valiosa para posibles acciones clave en el ámbito de la UE.

3.3. Fortalecimiento de las capacidades globales para aumentar la capacidad de recuperación mundial

Para asegurar que todos los países sean capaces de aprovechar las ventajas sociales, económicas y políticas que ofrece Internet y el uso de las tecnologías, la UE sigue apoyando a sus socios a fin de que incrementen sus habilidades y su capacidad de adaptación cibernética para investigar y enjuiciar los delitos cibernéticos y abordar las amenazas cibernéticas. Con el fin de asegurar la coherencia global, la UE debería desarrollar una **agenda para el desarrollo de la capacidad cibernética exterior de la UE** y dirigir estos esfuerzos en consonancia con sus directrices para el desarrollo de la capacidad cibernética exterior[114] y la Agenda 2030 para el desarrollo sostenible[115]. La agenda debe aprovechar la experiencia de los Estados miembros y las instituciones, organismos y agencias de la UE, así como las iniciativas, incluida la red para el desarrollo de la capacidad cibernética de la UE[116], en consonancia con sus respectivos mandatos. Debe crearse un **consejo para el desarrollo de la capacidad cibernética de la UE** que incluya a los agentes institucionales pertinentes de la UE y que observe el progreso, así como la identificación de nuevas sinergias y brechas potenciales. Puede apoyar, además, una mayor cooperación con los Estados miembros, así como con los socios del sector público y privado, y otros organismos internacionales pertinentes para asegurar la coordinación de los esfuerzos y evitar duplicidades.

El **desarrollo de la capacidad cibernética de la UE** debe seguir centrándose en los Balcanes Occidentales y en la vecindad de la UE, así como en los países socios que estén experimentando un rápido desarrollo digital. Los esfuerzos de la UE deben apoyar el desarrollo de la legislación y las políticas de los países socios de acuerdo con las políticas y normas diplomáticas relevantes de la UE en materia cibernética. En este contexto, los esfuerzos de desarrollo de la capacidad de la UE en el ámbito de la digitalización deben incluir la ciberseguridad como una característica estándar. Con este fin, la UE debería desarrollar un programa de formación dirigido al personal de la UE encargado de la aplicación de los esfuerzos de desarrollo de la capacidad digital y cibernética exterior. La UE también debería ayudar a esos países a afrontar el desafío creciente de las actividades cibernéticas maliciosas que dañan el desarrollo de sus sociedades y la **integridad y seguridad de los sistemas democráticos**, en consonancia con los esfuerzos que plantea el Plan de Acción para la Democracia Europea. El aprendizaje mutuo entre los Estados miembros de la UE, así como las agencias pertinentes de la UE y terceros países podría ser particularmente útil en este sentido.

Por último, en el contexto del pacto sobre la vertiente civil de la PCSD de 2018[117], las misiones civiles de la PCSD también pueden contribuir a la respuesta general de la UE para hacer frente a los retos de ciberseguridad, en particular mediante el fortalecimiento del Estado de Derecho dentro de los países socios, así como la aplicación de la ley y las capacidades de las administraciones civiles de dichos países.

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.
[116] https://www.eucybernet.eu/.
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/es/pdf.

Iniciativas estratégicas

La UE debería:

- Definir un conjunto de objetivos en los procesos de normalización internacionales y promoverlos en el ámbito internacional;
- Fomentar la seguridad y la estabilidad internacionales en el ciberespacio, especialmente a través de la propuesta de la UE y sus Estados miembros, de un Programa de acción para avanzar en la actuación responsable de los Estados en el ciberespacio (PoA) en las Naciones Unidas;
- Ofrecer una guía práctica sobre la aplicación de los derechos humanos y las libertades fundamentales en el ciberespacio;
- Proteger mejor a los niños contra el abuso sexual y la explotación de menores, así como la Estrategia sobre los Derechos de la Infancia;
- Fortalecer y promover el Convenio de Budapest sobre la Ciberdelincuencia, incluso mediante el trabajo en el Segundo Protocolo adicional al Convenio de Budapest;
- Ampliar el diálogo cibernético de la UE con terceros países, organizaciones regionales e internacionales, incluso a través de una Red de Ciberdiplomacia informal de la UE;
- Reforzar los intercambios con la comunidad de múltiples partes interesadas, en particular mediante intercambios periódicos y estructurados con el sector privado, las instituciones académicas y la sociedad civil; así como
- Proponer una agenda para el desarrollo de la capacidad cibernética exterior de la UE y un consejo para el desarrollo de la capacidad cibernética de la UE.

III. LA CIBERSEGURIDAD EN LAS INSTITUCIONES, AGENCIAS Y ORGANISMOS EUROPEOS

Dado su alto perfil político, sus importantes misiones para coordinar cuestiones sumamente delicadas y su función de gestión de grandes sumas de dinero público, **las instituciones, organismos y agencias de la UE son un blanco habitual de los ciberataques**, en concreto de los espionajes cibernéticos. Sin embargo, la capacidad de recuperación cibernética y la capacidad de detectar y contrarrestar las actividades cibernéticas maliciosas varía de forma significativa en todas estas entidades en cuanto a su madurez. Por tanto, es necesario mejorar el nivel global de seguridad cibernética mediante normas coherentes y homogéneas.

En el ámbito de la seguridad de la información se ha progresado hacia una mayor coherencia de las **normas para la protección de la información clasificada de la UE, así como de la información confidencial no clasificada**. Sin embargo, la interoperabilidad de los sistemas de información clasificada sigue siendo limitada, lo que impide una transferencia de información sin fisuras entre las diferentes entidades. Debe avanzarse más para permitir un enfoque interinstitucional para el manejo de información clasificada de la UE e información confidencial no clasificada, que también pueda servir como modelo de interoperabilidad entre los Estados miembros. También debe establecerse una base de referencia para simplificar los procedimientos con los Estados miembros. La UE también debe seguir desarrollando su capacidad para comunicarse de forma segura con los socios pertinentes y, en la medida de lo posible, basarse en las disposiciones y procedimientos existentes.

Como se anunció en la Estrategia para una Unión de la Seguridad, la Comisión, por lo tanto, hará propuestas de **normas comunes vinculantes sobre seguridad de la información y de normas comunes vinculantes sobre ciberseguridad para todas las instituciones, organismos y agencias de la UE en 2021**, sobre la base de las discusiones interinstitucionales de la UE en curso sobre ciberseguridad[118].

Las tendencias actuales y futuras relacionadas con el teletrabajo también requerirán inversiones adicionales en equipos de seguridad, infraestructuras y herramientas que permitan trabajar a distancia con archivos confidenciales y clasificados.

Además, el panorama de las ciberamenazas, cada vez más hostil, y la cada vez mayor incidencia de ciberataques más sofisticados que afectan a las instituciones, organismos y agencias de la UE impulsa la necesidad de aumentar las inversiones para alcanzar un alto nivel de madurez cibernética. Se está creando un Programa de concienciación cibernética para sensibilizar al personal de todas las instituciones, organismos y agencias de la UE sobre la ciberhigiene y respaldar la cultura común de ciberseguridad.

Es necesario **reforzar el CERT-UE con un mecanismo de financiación mejorado** para aumentar su capacidad de ayuda a las instituciones, organismos y agencias de la UE en la aplicación de las nuevas normas de ciberseguridad y mejorar su capacidad de adaptación cibernética. El mandato del CERT-UE también debe reforzarse para dotarlo de un medio estable para alcanzar estos objetivos.

Iniciativas estratégicas

1. Reglamento sobre la Seguridad de la Información en los organismos y agencias de las instituciones de la UE
2. Reglamento relativo a las normas de ciberseguridad comunes para las instituciones, organismos y agencias de la UE
3. Un nuevo fundamento legal para que el CERT-UE refuerce su mandato y su financiación.

IV. CONCLUSIONES

La aplicación acordada de esta estrategia contribuirá a una década digital de ciberseguridad para la UE, a la consecución de una Unión de la Seguridad y al fortalecimiento de la posición de la UE en el mundo.

La UE debería impulsar estándares y normas para conseguir soluciones de categoría mundial y normas de ciberseguridad aplicables a servicios esenciales e infraestructuras básicas, así como desarrollar y aplicar nuevas tecnologías. Todos los usos de Internet a nivel individual y de organización forman parte de la solución para garantizar una transformación digital segura.

La Comisión y el Alto Representante, de conformidad con sus respectivas competencias, supervisarán el progreso según esta estrategia y desarrollarán criterios para la evaluación. Las aportaciones a esta supervisión deben incluir los informes de ENISA y los informes

[118] El debate interinstitucional habitual de la UE sobre ciberseguridad forma parte de un intercambio mayor sobre las oportunidades y desafíos que presenta la transformación digital para las instituciones de la UE.

periódicos de la Comisión sobre la Unión de la Seguridad. Los resultados contribuirán a los objetivos de la próxima Década Digital[119]. De conformidad con sus respectivas competencias, la Comisión y el Alto Representante seguirán estando en contacto con los Estados miembros para identificar medidas prácticas destinadas a vincular las cuatro comunidades de ciberseguridad en la UE en materia de infraestructura básica y capacidad de adaptación del mercado interior, aplicación de la ley y la justicia, ciberdiplomacia y ciberdefensa, en caso de que fuera necesario. Además, la Comisión y el Alto Representante continuarán trabajando con la comunidad de múltiples partes interesadas, haciendo hincapié en la necesidad de que todo aquel que utiliza Internet desempeñe su función para mantener un ciberespacio global, abierto, estable y seguro, donde todos podamos vivir una vida digital con seguridad.

[119] Como se anunció en el programa de trabajo de la Comisión de 2021.

Apéndice: Próximos pasos en materia de ciberseguridad de las redes 5G

Sobre la base de los resultados de la revisión de la Recomendación de la Comisión sobre la ciberseguridad de las redes 5G[120], los próximos pasos en el trabajo coordinado en el ámbito de la UE deben centrarse en tres objetivos fundamentales y en las principales medidas a corto y medio plazo establecidas en la siguiente tabla, que aplicarán las autoridades de los Estados miembros, la Comisión y ENISA.

La primera prioridad para la siguiente fase consiste en **completar la aplicación del conjunto de instrumentos a escala nacional para hacer frente a los problemas identificados en el informe de situación de julio de 2020.** En este contexto, algunas de las medidas estratégicas del conjunto de instrumentos se beneficiarían de un **trabajo de coordinación mejorado o del intercambio de información** dentro del flujo de trabajo SRI, como ya se ha identificado en el informe de situación, lo que potencialmente podría conducir al desarrollo de **prácticas ejemplares o guías**. En cuanto a las medidas técnicas, ENISA podría ofrecer más apoyo, basándose en el trabajo que ya han realizado e investigando ciertos temas en mayor profundidad, así como **desarrollando una visión global de todas las directrices pertinentes sobre los requisitos de ciberseguridad 5G para los operadores de redes móviles.**

En segundo lugar, los Estados Miembros hicieron hincapié en la importancia de mantenerse al tanto del desarrollo mediante el **seguimiento constante del progreso tecnológico, la arquitectura 5G, las amenazas y los casos y aplicaciones del 5G, así como los factores externos,** con el fin de ser capaces de **identificar y tratar los riesgos nuevos o emergentes.** Por otra parte, es preciso examinar una serie de aspectos en el análisis inicial de riesgos, principalmente para asegurarse de que se ocupan de todo el ecosistema 5G, incluidas todas las partes pertinentes de la infraestructura de red y de la cadena de suministro 5G. Aunque el conjunto de instrumentos se ha diseñado como un instrumento flexible y con capacidad de adaptación, cuando proceda, se podrían adoptar medidas en el medio plazo para ampliarlo o modificarlo, con el fin de asegurar que se mantenga completo y actualizado.

En tercer lugar, se deberían seguir tomando **medidas a escala de la UE** para apoyar y completar los objetivos del conjunto de instrumentos e integrarlos totalmente en las políticas pertinentes de la Unión y de la Comisión, concretamente, realizando un seguimiento de las medidas anunciadas por la Comisión en su Comunicación del conjunto de instrumentos de 29 de enero de 2020[121] en una gran variedad de ámbitos (por ejemplo, la financiación de la UE para redes 5G seguras, inversiones en tecnologías 5G y posteriores al 5G, instrumentos de defensa comercial y competencia, con el fin de evitar distorsiones del mercado de suministro de 5G, etc.).

En su caso, a principios de 2021 los actores principales deberán determinar los hitos y los detalles de los acuerdos de las principales medidas que se exponen a continuación.

Objetivo fundamental 1: Asegurar enfoques nacionales convergentes para la mitigación efectiva

[120] Informe de la Comisión sobre las repercusiones de la Recomendación de la Comisión 2019/534 de 26 de marzo de 2019 sobre la ciberseguridad de las redes 5G.

[121] Comunicación de la Comisión COM (2020)50 sobre la puesta en marcha segura de las redes 5G en la UE: aplicación del conjunto de instrumentos de la UE, 29 de enero de 2020.

de riesgos en toda la UE		
Ámbitos	**Principales medidas a corto y medio plazo**	**Actores principales**
Aplicación del conjunto de instrumentos por los Estados miembros	Completar la aplicación de las medidas recomendadas en las conclusiones del conjunto de instrumentos en el segundo trimestre de 2021, con inventario periódico en el flujo de trabajo SRI.	Autoridades de los Estados miembros
Intercambio de información y prácticas ejemplares sobre medidas estratégicas relacionadas con los proveedores	Intensificar los intercambios de información y considerar las posibles prácticas ejemplares, en concreto sobre: - Restricciones a los proveedores de alto riesgo (ME03) y medidas relacionadas con la prestación de servicios gestionados (ME04); - Seguridad y capacidad de adaptación de la cadena de suministro, en particular, seguimiento de la encuesta realizada por ORECE sobre las ME05-ME06.	Autoridades de los Estados miembros, Comisión
Creación de capacidad y orientación sobre medidas técnicas	Llevar a cabo inmersiones técnicas profundas y desarrollar una guía y herramientas comunes que incluyan: - Una matriz integral y dinámica de los controles de seguridad y las prácticas ejemplares para la seguridad del 5G; La orientación en apoyo a la aplicación de medidas técnicas seleccionadas del conjunto de instrumentos.	ENISA, autoridades de los Estados miembros
Objetivo fundamental 2: Apoyar el intercambio continuo de conocimientos y creación de capacidad		
Ámbitos	**Principales medidas a corto y medio plazo**	**Actores principales**
Creación continua de conocimiento	Organizar actividades de creación de conocimiento sobre tecnología y retos relacionados (arquitecturas abiertas, características 5G como, por ejemplo, la virtualización, la contenedorización, el cortado, etc.), la evolución del panorama de amenazas, incidentes de la vida real, etc.	ENISA, autoridades de los Estados miembros, otras partes interesadas
Evaluaciones de riesgos	Actualización e intercambio de información sobre las evaluaciones de riesgos nacionales actualizadas	Autoridades de los Estados miembros, Comisión, ENISA
Proyectos conjuntos financiados por la UE para apoyar la aplicación del conjunto de instrumentos	Proporcionar ayuda financiera a proyectos de apoyo a la aplicación del conjunto de instrumentos que utilizan fondos de la UE, en particular en el marco del programa Europa Digital (por ejemplo, proyectos de desarrollo de capacidades para las autoridades nacionales, bancos de pruebas u otras capacidades avanzadas, etc.)	Autoridades de los Estados miembros, Comisión
Cooperación entre las partes interesadas	Fomentar la colaboración y la cooperación entre las autoridades nacionales involucradas en la ciberseguridad del 5G (por ejemplo, el Grupo de Cooperación SRI, las autoridades responsables de la ciberseguridad, las autoridades de reglamentación de telecomunicaciones) y con las partes interesadas del sector privado	Autoridades de los Estados miembros, Comisión, ENISA

Objetivo fundamental 3: Promover la capacidad de adaptación de la cadena de suministro y otros objetivos de seguridad estratégicos de la UE		
Ámbitos	**Principales medidas a corto y medio plazo**	**Actores principales**
Normalización	Definir y poner en funcionamiento un plan de acción concreto para mejorar la representación de la UE en los organismos de normalización como parte de los próximos pasos del trabajo del subgrupo SRI para la normalización, con el fin de alcanzar objetivos específicos de seguridad, como la promoción de interfaces interoperables para facilitar la diversificación de los proveedores.	Autoridades de los Estados miembros
Capacidad de adaptación de la cadena de suministro	- Llevar a cabo un análisis en profundidad del ecosistema 5G y la cadena de suministro para identificar y supervisar mejor los activos clave y posibles dependencias básicas - Asegurar el funcionamiento del mercado y la cadena de suministro de 5G es una medida en consonancia con los objetivos y las normas sobre competencia de la UE, tal como se define en la Comunicación de la Comisión de 29 de enero, y que el control de las inversiones extranjeras directas (IED) se aplique a la evolución de las inversiones que pueden afectar a la cadena de valor del 5G, teniendo en cuenta los objetivos del conjunto de instrumentos. - Vigilar las tendencias actuales y predicciones del mercado y evaluar los riesgos y oportunidades en el ámbito de la tecnología «Open RAN», especialmente a través de un estudio independiente	Autoridades de los Estados miembros, Comisión
Certificación	Iniciar los preparativos de los sistemas de certificación de componentes 5G clave y los procesos de los proveedores para contribuir a resolver ciertos riesgos relacionados con las vulnerabilidades técnicas, tal como se define en los planes de mitigación de riesgos del conjunto de instrumentos.	Comisión, ENISA, autoridades nacionales, otras partes interesadas
Capacidades de la UE y puesta en marcha de redes seguras	- Invertir en I+i y en capacidades, en particular mediante la adopción de asociaciones de redes y servicios inteligentes. - Poner en marcha las condiciones de seguridad pertinentes para los programas de financiación de la UE y los instrumentos financieros (internos y externos), tal como se anunció en la Comunicación de la Comisión de 29 de enero.	Estados miembros, Comisión, Partes interesadas del sector del 5G
Aspectos externos	Responder favorablemente a las solicitudes de terceros países que deseen comprender y potencialmente utilizar el enfoque de las herramientas desarrolladas por la UE.	Estados miembros, Comisión SEAE, delegaciones de la UE