Consejo de la Unión Europea

**Bruselas, 17 de octubre de 2022**
**(OR. en)**

**13664/22**

**CYBER 327**
**TELECOM 410**
**COSI 247**
**COPEN 354**
**DATAPROTECT 280**
**IND 413**
**RECH 547**
**HYBRID 99**
**JAI 1326**
**POLMIL 225**
**RELEX 1357**

**RESULTADO DE LOS TRABAJOS**

| | |
|---|---|
| De: | Secretaría General del Consejo |
| Fecha: | 17 de octubre de 2022 |
| A: | Delegaciones |
| N.º doc. prec.: | 12930/22 |
| Asunto: | Conclusiones del Consejo sobre la seguridad de las cadenas de suministro de las TIC<br>- Conclusiones del Consejo adoptadas por el Consejo en su sesión del 17 de octubre de 2022 |

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre la seguridad de las cadenas de suministro de las TIC, adoptadas por el Consejo en su sesión celebrada el 17 de octubre de 2022.

**ANEXO**

**Conclusiones del Consejo sobre la seguridad de las cadenas de suministro de las TIC**

EL CONSEJO DE LA UNIÓN EUROPEA,

RECORDANDO sus Conclusiones sobre

– la Comunicación conjunta de 20 de noviembre de 2017 al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»;

– el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE;

– la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G;

– la Estrategia Digital Europea;

– «Una recuperación que haga avanzar en la transición hacia una industria europea más dinámica, resiliente y competitiva»;

– la ciberseguridad de los dispositivos conectados;

– la Estrategia de Ciberseguridad de la UE para la Década Digital;

– el desarrollo de la Unión Europea en materia cibernética;

– el Informe Especial 03/2022 del Tribunal de Cuentas Europeo titulado «Despliegue de la tecnología 5G en la UE: Retrasos en el despliegue de redes y problemas de seguridad que siguen sin resolverse»,

RECORDANDO las Conclusiones del Consejo Europeo sobre:

– la COVID-19, el mercado único, la política industrial, el ámbito digital y las relaciones exteriores de los días 1 y 2 de octubre de 2020;

– la agresión militar rusa contra Ucrania, la seguridad y defensa, la energía, las cuestiones económicas, la COVID-19 y las relaciones exteriores de los días 24 y 25 de marzo de 2022,

– Ucrania, la seguridad alimentaria, la seguridad y defensa, y la energía de los días 30 y 31 de mayo de 2022,

1. Dada la creciente importancia de la geopolítica para la ciberseguridad, HACE HINCAPIÉ en que la Unión Europea y sus Estados miembros deben abordar la ciberseguridad de manera global y estratégica. La agresión militar de Rusia contra Ucrania ha provocado un cambio radical en el entorno estratégico y de seguridad de la Unión Europea y ha puesto de manifiesto la necesidad de una Unión Europea más fuerte y más capaz en el ámbito de la seguridad y la defensa. Ha puesto de relieve que es de suma importancia tener debidamente en cuenta el entorno geopolítico no solo a la hora de reaccionar ante las actividades informáticas malintencionadas, sino también a la hora de desarrollar y mantener la resiliencia de las tecnologías de la información y la comunicación (TIC). Esto reviste especial importancia para las cadenas de suministro de productos y servicios de TIC (cadenas de suministro de las TIC), que podrían verse comprometidas a raíz de una rivalidad geopolítica, como ilustra el ataque a SolarWinds, y afectadas por las tensiones y la inestabilidad geopolíticas, como demuestra la amenaza relacionada con la dependencia de proveedores rusos de TIC en el momento de la agresión militar de Rusia contra Ucrania.

2. SEÑALA que el carácter de los riesgos asociados a las cadenas de suministro de las TIC, formado por un conjunto vinculado de recursos y procesos entre los operadores económicos —tal como se definen en el Reglamento (UE) 2019/1020—, que comienza con el abastecimiento de materias primas y se extiende a lo largo de la fabricación, el procesado, la manipulación y la entrega de productos y servicios de TIC, incluida la prestación de apoyo durante el ciclo de vida de los productos y servicios de TIC, conlleva retos únicos y consecuencias que pueden tener un gran alcance. Además de los riesgos relacionados con la no disponibilidad de productos de TIC —por ejemplo, debido a la escasez de materias primas fundamentales y semiconductores necesarios para su producción—, las cadenas de suministro de productos y servicios de TIC están expuestas a otras amenazas. En particular, pueden ser objeto de ataques o ser utilizadas indebidamente por agentes malintencionados de formas sofisticadas, a menudo encubiertas, que repercuten en la confidencialidad, la integridad y la disponibilidad de los datos delicados transmitidos y almacenados.

3. Tomando constancia de que es necesario un enfoque que abarque todos los peligros para garantizar los activos de las TIC, RECONOCE la pertinencia de la propuesta de Directiva relativa a la resiliencia de las entidades críticas a fin de mejorar la seguridad física de las entidades críticas, y HACE HINCAPIÉ en que, además de aumentar la resiliencia ante los ataques a las cadenas de suministro llevados a cabo por medios cibernéticos, es igualmente importante reforzar la resiliencia y la seguridad generales de las cadenas de suministro de las TIC frente a todo tipo de factores de amenaza, como los sucesos naturales, los fallos de los sistemas, las amenazas internas o los errores humanos. En este sentido, RECONOCE que la seguridad de las cadenas de suministro de las TIC incluye garantizar la protección de los productos y servicios de TIC producidos, suministrados, adquiridos y utilizados en dichas cadenas de suministro, en particular protegiendo los componentes individuales y los datos transmitidos.

4. A partir de las lecciones extraídas de las consecuencias de las dependencias estratégicas de la Unión Europea en los combustibles fósiles rusos, así como de las repercusiones de las perturbaciones en las cadenas de suministro durante la pandemia de COVID-19, especialmente las relativas a los productos farmacéuticos y los semiconductores, cuando quedaron al descubierto las dependencias estratégicas de la UE, ANIMA a los Estados miembros a trabajar con el objetivo de evitar situaciones similares de dependencias estratégicas externas no deseadas en relación con los productos y servicios de TIC. Debido a la creciente digitalización de la sociedad y al uso cada vez mayor de las TIC en infraestructuras críticas, las dependencias estratégicas externas relacionadas con los productos y servicios de TIC y sus cadenas de suministro deben evaluarse de forma continua y, en su caso, resolverse.

5. RECUERDA que alcanzar la autonomía estratégica al tiempo que se mantiene una economía abierta es un objetivo clave de la Unión, que incluye detectar y reducir las dependencias estratégicas y aumentar la resiliencia en los entornos industriales y los ámbitos específicos más delicados, en particular en el ámbito digital. Esto incluye desarrollar e implantar capacidades e infraestructuras digitales estratégicas, así como reforzar de la capacidad de tomar decisiones tecnológicas autónomas y, como uno de los pilares principales, garantizar unas infraestructuras, productos y servicios resilientes y seguros para generar confianza en el mercado único digital y en la sociedad europea, manteniendo al mismo tiempo la apertura, la cooperación mundial con socios afines y la competitividad, y aprovechando las ventajas que puedan derivarse de esto último. Los valores fundamentales de la Unión Europea protegen, en particular, la privacidad, la seguridad, la igualdad, la dignidad humana, el Estado de Derecho y una internet abierta, todos ellos elementos indispensables para lograr una sociedad, una economía y una industria digitalizadas y centradas en el ser humano.

6. OBSERVA que, debido a la evolución del panorama de las ciberamenazas —como demuestra la tendencia de los últimos años de perpetrar sofisticados ataques de gran repercusión a las cadenas de suministro, por ejemplo, los ataques a SolarWinds, Mimecast o Kaseya, que va unida a la externalización de servicios esenciales de TIC y se ve intensificada por la dependencia general de productos y servicios de TIC fabricados, suministrados o atendidos por terceros—, es muy probable que en el futuro se produzcan más ataques a las cadenas de suministro con daños sustanciales para la economía y la sociedad. En vista de ello, HACE HINCAPIÉ en la importancia de mejorar la seguridad y la resiliencia de las cadenas de suministro de TIC para el funcionamiento del mercado único, junto con la necesidad de garantizar la disponibilidad, la seguridad y la diversidad de productos y servicios de TIC en el mercado único. Por lo tanto, RECONOCE la necesidad de aumentar al máximo y racionalizar el uso de los instrumentos y enfoques existentes de la UE para alcanzar estos objetivos, así como la necesidad de adaptarse continuamente al panorama variable de las ciberamenazas mediante la introducción de medidas y mecanismos adicionales adecuados, en particular en relación con los posibles riesgos para la seguridad que plantean las tecnologías emergentes y disruptivas. ANIMA a los Estados miembros a seguir, a este respecto, un planteamiento basado en el riesgo para hacer frente a los nuevos avances tecnológicos.

7. RECONOCE que comprender el panorama en constante evolución de las ciberamenazas, así como la complejidad de los ataques a las cadenas de suministro, es esencial para mitigar eficazmente los riesgos asociados a las cadenas de suministro de las TIC. A este respecto, DESTACA la necesidad de adaptarse a las nuevas amenazas mediante el seguimiento, el análisis y la evaluación activos y continuos del panorama de amenazas a las cadenas de suministro, de sensibilizar y mejorar el conocimiento sobre las amenazas y las vulnerabilidades, así como de poner sobre aviso de manera proactiva a las entidades pertinentes de manera personalizada. ACOGE CON SATISFACCIÓN el trabajo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en relación con la seguridad de las cadenas de suministro de las TIC, en particular su Informe sobre el panorama de las amenazas de ataque a las cadenas de suministro.

INSTRUMENTOS Y ENFOQUES INTERSECTORIALES

8. REAFIRMA la importancia de que los Estados miembros consideren la necesidad de diversificar los proveedores de TIC críticas para evitar o limitar que se genere una gran dependencia de un único proveedor, y en particular de proveedores considerados de alto riesgo, ya que aumenta la exposición a las consecuencias de posibles perturbaciones. RECONOCE que evitar la dependencia de un solo proveedor y la diversificación de proveedores de TIC es uno de los elementos importantes para garantizar la estabilidad y la seguridad del mercado interior. DESTACA la necesidad de promover y aplicar estrategias adecuadas que faciliten la diversificación de los proveedores y la competitividad de manera tecnológicamente neutra. Además, ANIMA a integrar en la legislación de la UE aspectos relativos a la prevención de la dependencia de un solo proveedor. A este respecto, TOMA CONSTANCIA de la propuesta de Reglamento sobre normas armonizadas para un acceso justo a los datos y su utilización, cuyo objetivo es aumentar la interoperabilidad de los servicios de tratamiento de datos y eliminar los obstáculos al cambio de proveedor de servicios de tratamiento de datos.

9. RECONOCE el vínculo entre la seguridad de la cadena de suministro de las TIC y la adjudicación de contratos públicos. HACE HINCAPIÉ en la necesidad de que los procedimientos de adjudicación de contratos públicos tengan debidamente en cuenta la importancia de la seguridad de la cadena de suministro de las TIC, mediante la imposición, cuando proceda, de criterios de selección objetivos y basados en el riesgo en lo que respecta a la capacidad de los licitadores para garantizar un alto nivel de seguridad de los servicios prestados. PIDE que se encuentre el equilibrio adecuado entre el interés público por hacer el uso más eficiente y justo posible de los fondos públicos, por una parte, y el interés público por asegurar los sistemas de información y garantizar el buen funcionamiento del mercado único, por otra. Para facilitar la aplicación de las normas pertinentes de adjudicación de contratos públicos a la luz del aumento de la ciberseguridad, INVITA a la Comisión a que elabore directrices metodológicas, para el tercer trimestre de 2023, con el fin de alentar a los poderes adjudicadores a prestar la debida atención a las prácticas de ciberseguridad de los licitadores y sus subcontratistas, y a evaluar y, en caso necesario, presentar propuestas para revisar o complementar la legislación pertinente en materia de adjudicación de contratos públicos.

10. TOMA CONSTANCIA de que las inversiones extranjeras directas relacionadas con productos y servicios de TIC, si bien proporcionan beneficios económicos y sociales a los Estados miembros, las empresas y los ciudadanos, podrían implicar riesgos para la seguridad y el orden público, y SEÑALA que el mecanismo de control de las inversiones extranjeras directas de la UE —junto con sus respectivos sistemas de control nacionales, que proporcionan medios para hacer frente a tales riesgos— también podría aplicarse como herramienta útil para salvaguardar la seguridad y la resiliencia de la cadena de suministro de las TIC, al contribuir a la eliminación de las inversiones de alto riesgo que puedan afectar a dicha seguridad y resiliencia. RECONOCE que la información intercambiada y compartida a través de este mecanismo puede ayudar a los Estados miembros a evaluar mejor las posibles amenazas para la seguridad de las cadenas de suministro de las TIC y a adoptar las medidas necesarias en consecuencia. PIDE a los agentes nacionales pertinentes que también tengan en cuenta esta dimensión del mecanismo de control, cuando proceda.

11. Por lo que respecta a la defensa, REAFIRMA su invitación a la Comisión a que en 2023 evalué, junto con los Estados miembros, los riesgos para las cadenas de suministro de infraestructuras críticas en diversos ámbitos, incluido el digital, relacionados con los intereses de la UE en materia de seguridad y defensa, así como a que estudie opciones para aumentar la ciberseguridad en toda la cadena de suministro de la base tecnológica e industrial de la defensa de la UE. Además, INVITA a los Estados miembros y a la Comisión a reflexionar sobre la seguridad de la cadena de suministro de las TIC en la aplicación de los compromisos y acciones de la Brújula Estratégica.

12. Reconociendo la importancia de las materias primas fundamentales, así como la de todo tipo de semiconductores como componentes básicos de los productos de TIC, ANIMA a entablar negociaciones constructivas sobre la propuesta de Reglamento por el que se establece un marco de medidas para reforzar el ecosistema europeo de semiconductores y la propuesta de Reglamento del Consejo que modifica el Reglamento (UE) 2021/2085, por el que se establecen las empresas comunes en el marco de Horizonte Europa, en lo que respecta a la Empresa Común de Chips.

INSTRUMENTOS ESPECÍFICOS DEL CIBERESPACIO

13. Por lo que se refiere específicamente a las infraestructuras de telecomunicaciones, RECONOCE los logros a escala de la Unión para mejorar la seguridad de la cadena de suministro de las redes 5G, en particular gracias al conjunto de instrumentos de la UE para la seguridad de las redes 5G (conjunto de instrumentos de la UE para las redes 5G). INSTA a los Estados miembros a seguir intercambiando información sobre las mejores prácticas y metodologías en relación con la aplicación de las medidas recomendadas en el conjunto de instrumentos de la UE para las redes 5G y en particular a aplicar, cuando proceda, 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. PONE DE RELIEVE que el conjunto de instrumentos de la UE para las redes 5G constituye un ágil instrumento basado en el riesgo para hacer frente a los retos de seguridad identificados, que permite tratar aspectos de ciberseguridad de la 5G de manera oportuna y eficaz, respetando al mismo tiempo las competencias de los Estados miembros, y RECONOCE que es un instrumento valioso para seguir mejorando, con total transparencia, la seguridad de la cadena de suministro de las redes de telecomunicaciones de manera coordinada, que puede servir de inspiración para herramientas de evaluación y mitigación de riesgos relacionadas con otros sectores esenciales. RECUERDA la invitación a las autoridades pertinentes de formular recomendaciones dirigidas a los Estados miembros y a la Comisión, que se basen en evaluaciones de riesgos y entre las que se incluya la aplicación continuada del conjunto de instrumentos de la UE para las redes 5G, con el fin de reforzar la resiliencia de las redes e infraestructuras de comunicaciones dentro de la Unión Europea

14. SEÑALA la importancia de los enfoques interoperables que puedan abordar la dependencia de un solo proveedor y diluir el riesgo de concentración, mejorando al mismo tiempo la seguridad de la cadena de suministro en todo el espectro de infraestructuras y servicios de TIC. En lo que se refiere concretamente a las redes 5G, RECONOCE los beneficios potenciales del concepto de la red de acceso por radio abierta a este respecto, al tiempo que RECUERDA el informe sobre la ciberseguridad de la red de acceso por radio abierta publicado por el Grupo de Cooperación SRI, en el que se señala que este concepto sigue en fase de desarrollo y que su seguridad, transparencia y normalización se encuentran en una fase temprana de madurez, y DESTACA la importancia de evaluar los riesgos antes de cualquier transición hacia nuevas normas o arquitecturas.

15. DESTACA la relevancia de los instrumentos legislativos horizontales vigentes y futuros en materia de ciberseguridad para aumentar la seguridad de la cadena de suministro de las TIC, en particular el Reglamento 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 (Reglamento sobre la Ciberseguridad), la futura Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (SRI 2), la propuesta de Reglamento por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión, así como la propuesta de Reglamento sobre los requisitos horizontales de ciberseguridad de los productos con elementos digitales (Reglamento sobre Ciberresiliencia). Además, SEÑALA los importantes avances en la normativa específica del sector de la ciberseguridad, en particular el futuro Reglamento sobre la resiliencia operativa digital del sector financiero, que incluye un marco de supervisión para proveedores terceros de servicios de TIC que son esenciales para las entidades financieras. Esos Reglamentos establecen obligaciones generales relacionadas con la seguridad de la cadena de suministro, así como requisitos detallados y específicos pertinentes para el sector en cuestión. Al mismo tiempo, DESTACA que los proveedores suelen suministrar sus productos y servicios en distintos sectores en lugar de a una sola industria. Por lo tanto, es muy importante garantizar que los requisitos de seguridad de la cadena de suministro estén, en la medida de lo posible, armonizados en todos los sectores pertinentes, especialmente los cubiertos por la futura Directiva SRI 2, con el fin de evitar discrepancias entre las obligaciones impuestas a los proveedores y aliviar la carga para los operadores de sectores críticos de evaluar el cumplimiento de dichas obligaciones por los proveedores, teniendo en cuenta al mismo tiempo las especificidades del sector.

16. ACOGE CON SATISFACCIÓN la propuesta del Reglamento sobre Ciberresiliencia como instrumento legislativo importante para impulsar el desarrollo seguro de productos con elementos digitales y para garantizar que la ciberseguridad se tenga en cuenta en todo el ciclo de vida de los productos con elementos digitales. SEÑALA que la propuesta de Reglamento sobre Ciberresiliencia puede contribuir significativamente a reforzar la seguridad de la cadena de suministro de las TIC. ANIMA a entablar unas negociaciones constructivas y a la adopción oportuna del Reglamento.

17. A este respecto, RECONOCE el trabajo en curso dirigido por ENISA, junto con los Estados miembros y otras partes interesadas, para proporcionar a la UE esquemas de certificación de productos, servicios y procesos de TIC, de conformidad con el Reglamento sobre la Ciberseguridad, que contribuyan a elevar el nivel general de ciberseguridad en el mercado único digital. ANIMA a todas las partes interesadas a que participen en los trabajos preparatorios sobre los distintos esquemas europeos de certificación, con el fin de generar confianza en la seguridad de los productos, procesos y servicios de TIC y de reforzar su resiliencia, y PIDE a la Comisión a que elabore rápidamente actos de ejecución sobre esquemas europeos de certificación una vez finalizados los trabajos preparatorios, en particular el esquema europeo de certificación de la ciberseguridad basado en criterios comunes (EUCC, por sus siglas en inglés). SEÑALA que los esquemas europeos de certificación deben incluir, cuando sea necesario, requisitos relativos a la seguridad de la cadena de suministro, también en lo que se refiere a las relaciones con los proveedores.

18. DESTACA la necesidad de una aplicación exhaustiva de todas las disposiciones de la futura Directiva SRI 2 relacionadas con la seguridad de la cadena de suministro de las TIC. A este respecto, SUBRAYA la relevancia de las evaluaciones coordinadas de riesgos de la UE de las cadenas de suministro críticas (evaluaciones coordinadas de los riesgos de la cadena de suministro), las políticas nacionales en materia de seguridad de la cadena de suministro y las medidas de seguridad relacionadas con la cadena de suministro. SEÑALA que debe prestarse atención no solo a los proveedores primarios, sino también a los subcontratistas pertinentes, en lo que respecta a los riesgos para la seguridad del proveedor primario o del cliente final. Con el fin de facilitar la aplicación de las medidas de gestión de los riesgos de la cadena de suministro, ANIMA a ENISA a realizar, con la ayuda del Grupo de Cooperación SRI, un balance de las mejores prácticas disponibles para la gestión de los riesgos de la cadena de suministro y a recopilarlas en directrices metodológicas. Además, ANIMA a ENISA a supervisar las inversiones realizadas en el ámbito de la seguridad de la cadena de suministro de las TIC por las entidades reguladas en virtud de la futura Directiva SRI 2.

19. DESTACA asimismo los beneficios y los riesgos de usar proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados en el contexto de la seguridad de la cadena de suministro. Si bien usar esos proveedores puede mejorar significativamente la seguridad dentro de las organizaciones y lograr niveles más elevados de ciberseguridad, la gestión a distancia de los sistemas y servicios de TIC combinada con un acceso privilegiado al entorno TIC de los clientes —que podría ser necesario para los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados— puede, en caso de que los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados se vean comprometidos, producir efectos en cascada significativos para un gran número de clientes. Por lo tanto, es de suma importancia que los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados mantengan un alto nivel de seguridad, tanto en lo que se refiere a su propia seguridad interna como a la seguridad de los servicios que prestan, y adopten un enfoque transparente con sus clientes en lo que respecta a la seguridad de los servicios que prestan. A este respecto, ACOGE CON SATISFACCIÓN su futura inclusión en el ámbito de aplicación de la futura Directiva SRI 2.

20. En cuanto a la aplicación del mecanismo de evaluación coordinada de los riesgos de la cadena de suministro en virtud de la futura Directiva SRI 2, TOMA NOTA de la relevancia de los factores de riesgo no técnicos en este contexto, como la influencia indebida de un tercer Estado sobre los proveedores y proveedores de servicios y, en este contexto, RECONOCE los factores que pueden utilizarse para evaluar el perfil de riesgo que se mencionan en la evaluación coordinada de riesgos realizada por la UE acerca de la ciberseguridad de las redes 5G. INVITA a la Comisión a que identifique, a más tardar en el segundo trimestre de 2023, previa consulta con el Grupo de Cooperación SRI y ENISA, los servicios, sistemas o productos de TIC específicos que, de forma prioritaria, podrían ser objeto de evaluaciones coordinadas de riesgos de la cadena de suministro.

21. SEÑALA que la dependencia de proveedores considerados de alto riesgo de productos y servicios de TIC utilizados para el funcionamiento de redes y sistemas críticos supone una amenaza estratégica que debe mitigarse mediante políticas adecuadas tanto a escala nacional como de la Unión y mediante la cooperación entre los Estados miembros y con socios internacionales afines. Con el fin de facilitar la mitigación de este riesgo estratégico y dar apoyo a las evaluaciones coordinadas de los riesgos de la cadena de suministro, INVITA al Grupo de Cooperación SRI, en cooperación con la Comisión y ENISA, a que desarrolle un conjunto de medidas para reducir los riesgos de las cadenas de suministro de las TIC críticas (conjunto de instrumentos para la cadena de suministro de las TIC). El conjunto de instrumentos para la cadena de suministro de las TIC debe basarse en escenarios de amenazas estratégicas identificados para las cadenas de suministro de TIC y establecer medidas para responder a esos escenarios aprovechando la experiencia adquirida a través del conjunto de instrumentos de la UE para las redes 5G y a nivel nacional. Debe complementar, de manera transparente, las evaluaciones coordinadas de los riesgos de la cadena de suministro para determinados servicios, sistemas o productos de TIC en el marco de la futura Directiva SRI 2, ofreciendo medidas genéricas para reducir los riesgos que puedan ajustarse para determinados servicios, sistemas o productos de TIC de manera modulable, sobre la base de los riesgos detectados en cada una de las evaluaciones de riesgos coordinadas de la cadena de suministro.

22. DESTACA el importante papel de las actividades en investigación, innovación, inversión y empresariales en el ámbito digital y de la ciberseguridad, así como el de la financiación de dichas actividades en lo que respecta a evitar posibles futuras dependencias estratégicas no deseadas y a reforzar la resiliencia general de las cadenas de suministro de las TIC. En este contexto, HACE HINCAPIÉ en el papel y la relevancia de las tareas estratégicas y de ejecución del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación para contribuir a maximizar los efectos de las inversiones destinadas a reforzar el liderazgo y la autonomía estratégica abierta de la Unión en el ámbito de la ciberseguridad, respaldar las capacidades y competencias tecnológicas de la Unión y aumentar la competitividad global de la Unión. A este respecto, PIDE que se ponga en funcionamiento rápidamente la Red de Centros Nacionales de Coordinación. INVITA a la Red de Centros Nacionales de Coordinación a que tenga en cuenta en su agenda estratégica los aspectos relacionados con la seguridad de la cadena de suministro de las TIC, incluido, por ejemplo, el desarrollo seguro de software, garantizando al mismo tiempo la coherencia y la complementariedad y evitando cualquier duplicación de esfuerzos. APOYA la mejora de la competitividad europea en el ámbito de la ciberseguridad a través de programas de financiación, como el programa Horizonte Europa para la investigación y la innovación, así como el programa Europa Digital para reforzar, desarrollar y adquirir capacidades esenciales para la economía digital, la sociedad y la democracia de la UE.

MECANISMOS DE APOYO

23. PROPUGNA que se impulsen los incentivos de apoyo financiero relacionados con las medidas destinadas a reforzar la seguridad de las cadenas de suministro de las TIC. INSTA, con carácter prioritario, también con vistas a la próxima aplicación de la Directiva SRI 2, al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, a la Comisión y a las partes interesadas pertinentes a que estudien opciones para incluir los aspectos relacionados con la seguridad de las cadenas de suministro de las TIC en las próximas convocatorias de los programas de trabajo en materia de ciberseguridad en el marco de los programas Europa Digital y Horizonte Europa, o cualquier otra posibilidad de financiación pertinente. Estas posibilidades de financiación deben tener por objeto, entre otras cosas, permitir a las organizaciones apoyar el mantenimiento de un alto nivel de ciberseguridad en lo que respecta a la adquisición de productos y servicios de TIC a lo largo de toda la cadena de suministro, en particular en relación con la sustitución de servicios, sistemas o productos de TIC críticos específicos considerados de alto riesgo de conformidad con las futuras evaluaciones coordinadas de riesgos de las cadenas de suministro.

24. RECONOCE que la globalización y la especialización de los servicios de TIC y el aumento de la dependencia de productos y servicios de terceros hacen necesaria una estrecha cooperación dentro de la UE y a escala internacional a la hora de compartir conocimientos y experiencia técnica entre las partes interesadas pertinentes, y los ANIMA a encontrar una posición firme y coordinada que garantice la seguridad de las cadenas de suministro de las TIC de manera general. TOMA CONSTANCIA, asimismo, de la necesidad de seguir explorando los enfoques y técnicas pertinentes más avanzados, tanto en lo relativo a una ciberhigiene básica adecuada y soluciones a largo plazo para lograr cadenas de suministro de TIC seguras y resilientes, como para hallar las formas más adecuadas para su promoción y su posible incorporación a iniciativas de actuación o de otro tipo. RECONOCE, a este respecto, que debe prestarse especial atención al estudio de las ventajas y los inconvenientes de aplicar soluciones sistemáticas, como los principios de confianza cero, la lista de materiales de *software* y soluciones similares a largo plazo. RECOMIENDA recurrir a tal fin al Grupo de Cooperación SRI.

25. SEÑALA las ventajas del seguimiento y el intercambio efectivo de información sobre incidentes de ciberseguridad y amenazas para prevenir, detectar y mitigar los efectos de los ataques en las cadenas de suministro. HACE HINCAPIÉ en la necesidad de seguir fomentando la confianza entre los Estados miembros para que se intercambie dicha información de forma efectiva. RECUERDA, a este respecto, la propuesta de la Comisión de asistir a los Estados miembros en el establecimiento y el refuerzo de los centros de operaciones de seguridad (COS), con el fin de crear una red de COS en toda la UE para vigilar y anticipar mejor los indicios de ataque a las redes. RECUERDA la necesidad de complementariedad y coordinación dentro de las redes y mecanismos existentes; muy en particular PONE DE RELIEVE a este respecto el papel de la red de equipos de respuesta a incidentes de seguridad informática (CSIRT) y la necesidad de seguir explorando el potencial de esta red para promover una cultura de intercambio de información eficiente, segura y fiable. RECUERDA los esfuerzos dedicados por los Estados miembros, con el apoyo de la UE, a establecer CSIRT sectoriales, nacionales y regionales y centros de puesta en común y análisis de la información nacionales o europeos como parte de una red eficaz de asociaciones en materia de ciberseguridad en la Unión.

26. Dada la naturaleza interconectada y mundial de las amenazas a las cadenas de suministro de las TIC, DESTACA la importancia de abordar y mejorar la seguridad de las cadenas de suministro de las TIC a escala mundial. En vista de ello, RECOMIENDA hacer uso de asociaciones digitales, ciberdiálogos y otras iniciativas pertinentes de la UE, en particular de los acuerdos de libre comercio, si ha lugar, para promover evaluaciones basadas en riesgos de los proveedores de productos y servicios de TIC, el uso de proveedores fiables y para emplear un entorno digital seguro e innovador basado en normas abiertas, interoperables y transparentes. Asimismo, REITERA el concepto de las asociaciones de la Global Gateway, así como del Consejo UE-EE. UU. de Comercio y Tecnología, y de las actividades realizadas en el marco de sus grupos de trabajo, para promover el uso de proveedores fiables o que no planten un alto riesgo y desarrollar un mecanismo de financiación a fin de facilitar proyectos que permitan que la infraestructura y los servicios de TIC en terceros Estados sean más seguros, resilientes y fiables, en particular absteniéndose de financiar compras a proveedores no fiables o de alto riesgo de manera neutra desde el punto de vista tecnológico.

27. REAFIRMA su compromiso de contribuir a un ciberespacio abierto, libre, mundial, estable y seguro, y de promoverlo, así como de adherirse a las normas, reglas y principios de comportamiento responsable de los Estados en el ciberespacio establecidos en el marco de las Naciones Unidas. En relación con la seguridad de las cadenas de suministro de las TIC en particular, RECUERDA la norma aprobada por el grupo de expertos gubernamentales de las Naciones Unidas y el grupo de trabajo de composición abierta que anima a los Estados a adoptar disposiciones razonables para garantizar la integridad de las cadenas de suministro, especialmente mediante el desarrollo de medidas de cooperación objetivas, de modo que los usuarios finales puedan confiar en la seguridad de los productos de TIC, e intenten evitar la proliferación de herramientas y técnicas de TIC malintencionadas y el uso de funciones ocultas perjudiciales, y ABOGA por su amplia aplicación.