COMISIÓN
EUROPEA

Estrasburgo, 18.4.2023
COM(2023) 207 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE

(«Academia de Cibercapacidades»)

Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE

(«Academia de Cibercapacidades»)

1. Necesidad urgente de reducir los riesgos abordando la escasez y las carencias de capacidades en materia de ciberseguridad

La ciberseguridad no solo forma parte de la seguridad de los ciudadanos, las empresas y los Estados miembros. También es necesaria para garantizar la estabilidad política de la UE, la estabilidad de sus democracias y la prosperidad de nuestra sociedad y nuestras empresas. El **panorama de las amenazas** a la ciberseguridad ha evolucionado considerablemente en los últimos años, con la preocupante tendencia a que un número creciente de ciberataques se dirijan a infraestructuras críticas militares y civiles en la UE. Los agentes de tales amenazas fortalecen sus capacidades, mientras surgen también otras amenazas nuevas, híbridas y emergentes, como el uso de bots y técnicas basadas en la inteligencia artificial[1]. En particular, los agentes que amenazan con programas de secuestro están causando de forma rutinaria daños considerables, tanto financieros como de reputación, a las entidades[2].

Un gran número de incidentes de ciberseguridad se han dirigido a la administración pública y a los Gobiernos de los Estados miembros, así como a las instituciones, órganos y organismos europeos[3]. Los sectores financiero[4] y sanitario[5], que son la columna vertebral de la sociedad y la economía, también han sido objetivos constantes[6]. Las tensiones geopolíticas vinculadas a la guerra de agresión de Rusia contra Ucrania han potenciado la amenaza a la ciberseguridad[7] y pueden desestabilizar nuestra sociedad. La **seguridad** de la UE no puede garantizarse sin el **activo más valioso de la UE: su gente.** La UE necesita urgentemente profesionales con las capacidades y competencias necesarias para prevenir, detectar y disuadir los ciberataques y defender a la UE, incluidas sus infraestructuras más críticas, de estos, así como para garantizar su **resiliencia**.

---

1 Panorama de las amenazas de la ENISA 2022 – ENISA (europa.eu) (en inglés).

2 Europol: Evaluación de la amenaza de la delincuencia organizada en internet (IOCTA) 2021 de Europol. Estos agentes se basan en el modelo de programas de secuestro como servicio. El coste anual para las empresas superó los 18 400 millones EUR en 2022 (Informe de Cybereason 2022 sobre el coste real de los programas de secuestro).

3 Véase, por ejemplo, la publicación conjunta de la ENISA y CERT-UE, JP-23-01 titulada «Sustained activity by specific threat actors» [«Actividad sostenida por agentes de amenaza específicos», documento en inglés], TLP: CLEAR, 15 de febrero de 2023.

4 Véase, por ejemplo, el hecho de que en Alemania, el 90 % del fraude por correo notificado entre el 1 de junio de 2021 y el 31 de mayo de 2022 fue de *phishing* financiero, o el ataque a una empresa del sector financiero, en el que participaron más de 20 000 dispositivos infectados procedentes de 125 países, *The State of IT Security in Germany in 2022* [«Estado de la seguridad informática en Alemania en 2022», documento en inglés], Bundesamt für Sicherheit in der Informationstechnik (BSI), 1 de enero de 2023.

5 Véanse, por ejemplo, en Francia, ataques con programas de secuestro contra instalaciones sanitarias públicas, como en el Centre Hospitalier Sud Francilien, durante el cual 11 GB de datos personales y médicos, así como datos relacionados con el personal, se vieron comprometidos y publicados por el agente de la amenaza, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023.

6 Panorama de las amenazas de la ENISA 2022.

7 Véase también: CERT-UE — La guerra de Rusia contra Ucrania: un año de operaciones cibernéticas (europa.eu); Operaciones cibernéticas de Rusia contra Ucrania:Declaración del Alto Representante en nombre de la Unión Europea, 10 de mayo de 2022; Declaración del Alto Representante, en nombre de la Unión Europea, sobre las actividades informáticas malintencionadas llevadas a cabo por piratas informáticos y grupos de piratas informáticos en el contexto de la agresión de Rusia contra Ucrania, 19 de julio de 2022.

La brecha de talento en materia de ciberseguridad obstaculiza aún más la **competitividad** y el **crecimiento** de Europa, que dependen en gran medida del desarrollo y la adopción de tecnologías digitales estratégicas (por ejemplo, inteligencia artificial, 5G y nube). Se necesita una mano de obra cualificada en el ámbito de la ciberseguridad para que la UE siga estando en condiciones de ofrecer tecnologías avanzadas clave en un entorno mundial.

Para prepararse y hacer frente a este panorama cambiante de amenazas y fomentar la competitividad de la UE, la política de ciberseguridad de la UE ha avanzado significativamente en los últimos años, lo que ha dado lugar a la adopción de una serie de iniciativas, como la Estrategia de Ciberseguridad para la Década Digital de la UE[8], la Directiva revisada sobre Ciberseguridad (Directiva SRI 2)[9], la legislación sectorial de la UE en materia de ciberseguridad[10], la política de ciberdefensa de la UE[11], la Ley de ciberresiliencia[12] y la Ley de cibersolidaridad, propuestas por la Comisión junto con la presente Comunicación. Pero sin las personas cualificadas necesarias para aplicarlas, estos actos legislativos no alcanzarán sus objetivos. Si bien el conocimiento básico de la ciberseguridad por parte de la población en general se aborda como parte de las iniciativas que apoyan el desarrollo de las capacidades generales necesarias para participar en la sociedad[13], es esencial contar con una mano de obra competente tanto en el sector público como en el privado, a escala nacional y de la UE, incluido en las organizaciones de normalización, **para cumplir esos requisitos jurídicos y políticos en materia de ciberseguridad**.

Por lo tanto, la seguridad y la competitividad de la UE dependen de contar con una mano de obra profesional cualificada en el ámbito de la ciberseguridad. Sin embargo, la UE se enfrenta a una escasez muy importante de profesionales cualificados de la ciberseguridad, lo que pone a la Unión, sus Estados miembros, sus empresas y sus ciudadanos en riesgo de incidentes de ciberseguridad. En 2022, la escasez de profesionales de la ciberseguridad en la Unión Europea osciló **entre 260 000**[14] **y 500 000**[15], mientras que las necesidades de mano de

---

[8] Comunicación conjunta al Parlamento Europeo y al Consejo: La Estrategia de Ciberseguridad de la UE para la Década Digital, JOIN(2020) 18 final.

[9] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

[10] Como, en el caso del sector financiero, el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del 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, (UE) n.º 909/2014 y (UE) 2016/1011 (Reglamento DORA).

[11] Comunicación conjunta al Parlamento Europeo y al Consejo: Política de ciberdefensa de la UE, JOIN(2022) 49 final.

[12] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de la ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020, COM(2022) 454 final.

[13] Entre las iniciativas pertinentes que abordan las capacidades digitales generales de la población: que el 80 % de la población alcance las capacidades digitales básicas de aquí a 2030 como objetivo del Plan de Acción del Pilar Europeo de Derechos Sociales y la Brújula Digital, el Plan de Acción de Educación Digital 2021-2027, la herramienta del Marco de Competencias Digitales o la propuesta de Recomendación del Consejo sobre la mejora de la provisión de capacidades digitales en la educación y la formación.

[14] (ISC)² en la evaluación de las cibercapacidades sobre la base del ECSF, seminario web de la ENISA, 16 de febrero de 2023.

[15] Según la Organización Europea de Ciberseguridad (ECSO), como se indica en la Comunicación conjunta al Parlamento Europeo y al Consejo: Política de ciberdefensa de la UE, JOIN(2022) 49 final.

obra de la UE en este sector se estimaron en 883 000 profesionales[16], lo que indica un desajuste entre las competencias disponibles y las requeridas por el mercado laboral. La mano de obra en el ámbito de la ciberseguridad sigue viéndose afectada por ideas equivocadas en relación con su imagen técnica y aún no atrae a las **mujeres**, que representan el 20 % de los titulados en ciberseguridad[17] y el 19 % de los especialistas en tecnologías de la información y de las comunicaciones[18] (TIC). Para abordar este problema, el **Programa Estratégico de la Década Digital**[19] de Europa ha fijado el objetivo de aumentar el número de profesionales de las TIC en 20 millones de aquí a 2030, al tiempo que se logra la convergencia de género. Además, la aplicación de las nuevas políticas de la UE requiere una mano de obra adecuadamente cualificada y suficiente. Por ejemplo, más del 42 % de los altos dirigentes informáticos del sector de los servicios financieros destacaron la falta de capacidades y conocimientos especializados en materia de ciberseguridad como obstáculo principal para sus negocios en lo que respecta a la defensa de la ciberseguridad y la gestión de incidentes[20], en un momento en que tendrán que aplicar la legislación sectorial en materia de ciberseguridad, como la Ley de resiliencia operativa digital (DORA).

La reticencia de los empleadores a invertir en capital humano, buscando mano de obra ya formada y experimentada, contribuye aún más a limitar el mercado laboral[21]. Esta escasez afecta a todo tipo de empresas, incluidas las pequeñas y medianas empresas (**pymes**), que representan el 99 % de todas las empresas de la UE[22]. También es un arduo desafío para las **administraciones públicas**, que son las más afectadas por los incidentes de ciberseguridad[23].

Por lo tanto, es urgente colmar la brecha de talento profesional en materia de ciberseguridad de la UE, ya que están en juego la seguridad y la competitividad de la UE.

2. Falta de sinergias y de acción coordinada para colmar la brecha de capacidades en materia de ciberseguridad

Están prosperando las iniciativas a escala europea y nacional llevadas a cabo por entidades públicas y privadas para abordar las deficiencias del mercado laboral en materia de ciberseguridad. Sin embargo, están dispersas y hasta ahora no han logrado alcanzar una masa crítica que marque una verdadera diferencia.

Para empezar, actualmente existe una comprensión común limitada de la composición de la mano de obra de la UE en el ámbito de la ciberseguridad y de las capacidades asociadas, mientras que unos perfiles laborales similares en materia de ciberseguridad deben conllevar el mismo conjunto de capacidades. La escasa adopción por parte de los agentes pertinentes de un **marco de referencia común europeo para los profesionales de la ciberseguridad** se

---

[16] (ISC)² en la evaluación de las cibercapacidades sobre la base del ECSF, seminario web de la ENISA, 16 de febrero de 2023.

[17] Base de datos de educación superior en ciberseguridad (CyberHEAD) (en inglés).

[18] Solo el 19 % de los especialistas en TIC de la UE son mujeres. Índice de la Economía y la Sociedad Digitales (DESI) 2022.Configurar el futuro digital de Europa (europa.eu). No se dispone de cifras en relación con la mano de obra femenina de la Unión en el ámbito de la ciberseguridad.

[19] Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030, que crea un mecanismo de seguimiento y cooperación para alcanzar los objetivos y metas comunes para la transformación digital de Europa establecidos en la Brújula Digital 2030, incluido el ámbito de las capacidades.

[20] Informe de 2022 sobre las perspectivas en materia de ciberseguridad de S-RM (en inglés).

[21] ENISA: *Cybersecurity Skills Development in the EU* [«Desarrollo de capacidades en materia de ciberseguridad en la UE», documento en inglés], diciembre de 2019.

[22] Definición de pyme (europa.eu) (en inglés).

[23] Panorama de las amenazas de la ENISA 2022 – ENISA (europa.eu) (en inglés).

traduce en la falta de una herramienta de comunicación entre empleadores, educadores y responsables políticos, y en la incapacidad para llevar a cabo mediciones y evaluar las deficiencias del mercado laboral en materia de ciberseguridad. Además, impide el diseño de planes de estudios de educación y formación y la creación de itinerarios profesionales que respondan a las necesidades políticas y del mercado para quienes deseen acceder a la profesión. **La mejora de las capacidades y el reciclaje profesional** de la mano de obra dependen en gran medida de la formación y los certificados en materia de ciberseguridad, que suelen ofrecer proveedores privados. Sin embargo, a los trabajadores les resulta difícil obtener una visión general de la calidad de las formaciones en materia de ciberseguridad ofrecidas y de los certificados correspondientes expedidos.

Si bien la educación y la formación, así como la creación de itinerarios profesionales, son necesarias para mejorar la oferta del mercado laboral, actualmente se subestima el papel de la **demanda** en la formación de su mano de obra y en la adaptación a su evolución. La industria y los empleadores públicos carecen de foros y lugares comunes para aunar ideas sobre la mejor manera de formar a la mano de obra y abordar la forma de **evaluar mejor las capacidades**, especialmente durante el proceso de contratación. Las **capacidades técnicas** más demandadas pueden estar relacionadas con la ciberseguridad[24], como el desarrollo de software o la computación en la nube[25], pero las **capacidades transversales** siguen sin tenerse en cuenta, sin motivo alguno. El pensamiento y el análisis críticos, la resolución de problemas y la autogestión son grupos de capacidades muy solicitados por los empleadores[26] y que ocuparán un lugar cada vez más destacado de aquí a 2025[27].

Ya existen muchas iniciativas de inversión pública y privada en capacidades en materia de ciberseguridad, con una amplia **financiación** por parte de la UE de proyectos en el marco de diferentes instrumentos[28]. Sin embargo, la continua escasez de capacidades en la UE plantea dudas en cuanto a su visibilidad e impacto e indica que no responden sistemáticamente a las necesidades del mercado, que deben cartografiarse con urgencia a escala de la UE. Además, varias fuentes de financiación dan lugar a duplicaciones, perdiendo la oportunidad de ampliarse y tener un impacto real. Por otra parte, quienes necesitan la inversión no siempre pueden identificar las fuentes más adecuadas a sus necesidades.

Las **partes interesadas** han intentado abordar la compleja y polifacética cuestión de la escasez de capacidades en materia de ciberseguridad. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha estado desarrollando instrumentos relacionados con los perfiles de funciones o la educación superior[29], el Centro Europeo de Competencia en Ciberseguridad (ECCC)[30] está abordando las capacidades en materia de ciberseguridad en un

---

[24] *LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most* [«Capacidades más demandadas de 2023 de LinkedIn. Conoce las capacidades más necesarias para las empresas», documento en inglés].

[25] Infografía de ISACA sobre el estado de la ciberseguridad de 2022.

[26] Como la herramienta CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu) (en inglés).

[27] *The Future of Jobs Report, October 2020, World Economic Forum* [«Informe sobre el futuro del empleo, octubre de 2020, Foro Económico Mundial», documento en inglés].

[28] Por ejemplo: Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project (financiado por el programa Erasmus+); proyectos de apoyo al Centro de Competencia en Ciberseguridad [ECHO, CONCORDIA, CyberSec4Europe, SPARTA (financiados por Horizonte 2020) y proyecto Cybersecpro (financiado por el programa Europa Digital)].

[29] En particular: el Marco Europeo de Capacidades en Ciberseguridad (ECSF) (en inglés); la Base de datos de educación superior en ciberseguridad (CyberHEAD) (en inglés); la Plataforma de Ciberejercicios (CEP) (en inglés); el Reto Europeo de Ciberseguridad (en inglés); el Mes Europeo de la Ciberseguridad (en inglés).

[30] Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

grupo de trabajo específico, la Escuela Europea de Seguridad y Defensa (EESD) está trabajando en las capacidades en materia de ciberseguridad de la mano de obra civil y militar en el contexto de la política común de seguridad y defensa[31], las organizaciones privadas están intentando abordar el problema[32], y el sector de certificación de la ciberseguridad está elaborando una hoja de ruta y formaciones para abordar la brecha de capacidades[33]. Los Estados miembros también están intentando subsanar esta cuestión a través de diversas iniciativas, que van desde la regulación[34] hasta la creación de academias de capacidades en materia de ciberseguridad[35] o cibercampus[36], centros de excelencia en ciberdelincuencia[37] o asociaciones público-privadas[38]. Sin embargo, el trabajo de todas estas partes interesadas a menudo carece de coordinación y sinergias y no ha alcanzado su potencial de crear una verdadera diferencia en el mercado laboral, como demuestra la creciente escasez de mano de obra en el ámbito de la ciberseguridad en la UE. También es necesario potenciar las sinergias entre las cibercomunidades, ya que los conjuntos de capacidades necesarios para defender la ciberseguridad, luchar contra la **ciberdelincuencia** o desarrollar respuestas de **ciberdefensa** son a menudo similares.

Por último, en la actualidad, la UE dispone de medios limitados para evaluar **el estado y la evolución del mercado laboral en materia de ciberseguridad** y de las capacidades de su mano de obra. Los Estados miembros y las instituciones, órganos y organismos europeos se basan en datos recopilados por entidades privadas o en un conjunto más amplio de datos recopilados por la UE, en particular por Eurostat[39] y el Centro Europeo para el Desarrollo de la Formación Profesional (Cedefop)[40] sobre profesionales de las TIC. En otras palabras, la UE tiene una visión parcial y fragmentada de sus necesidades, lo que le impide consolidar una visión agregada del estado del mercado laboral en materia de ciberseguridad.

3. Respuesta coordinada a escala de la UE: la Academia de Cibercapacidades

3.1.Objetivo

Para superar el reto de fortalecer las capacidades en materia de ciberseguridad y colmar la brecha del mercado laboral, la Comisión presenta la **Academia de Cibercapacidades**, tal como anunció la presidenta de la Comisión Europea en su carta de intenciones sobre el estado de la Unión de 2022[41, 42], y en el contexto del Año Europeo de las Competencias.

La Academia de Cibercapacidades (en resumen, «la Academia») tiene por objeto crear una **ventanilla única y sinergias** para las ofertas de educación y formación en materia de

[31] En particular, la plataforma de cibereducación, formación, ejercicio y evaluación (ETEE) (en inglés).

[32] Por ejemplo, el grupo de trabajo 5 de la Organización Europea de Ciberseguridad (ECSO) sobre «Educación, formación, sensibilización, campos de maniobras virtuales, factores humanos»; la organización DIGITALEUROPE (en inglés).

[33] Por ejemplo, el Instituto SANS (en inglés), (ISC)², ISACA.

[34] Por ejemplo, en las estrategias nacionales de educación o ciberseguridad.

[35] Por ejemplo, la C-Academy de Portugal (en inglés).

[36] Por ejemplo, los Cyber Campuses de Francia (en francés).

[37] Por ejemplo, el Centro de Excelencia sobre Ciberdelincuencia de Lituania para la formación, la investigación y la educación en Lituania (L3CE) (en inglés).

[38] Por ejemplo, la Iniciativa «Cybersecurity Skilling» de Microsoft (en inglés).

[39] *ICT specialists in employment – Statistics Explained* [«Especialistas en TIC en el empleo: Estadísticas explicadas», documento en inglés] (europa.eu).

[40] Como la herramienta CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu) (en inglés).

[41] Carta de intenciones sobre el estado de la Unión de 2022 dirigida a la presidenta Roberta Metsola y al primer ministro Petr Fiala.

[42] Comunicación conjunta al Parlamento Europeo y al Consejo: Política de ciberdefensa de la UE, JOIN(2022) 49 final.

ciberseguridad, así como para las oportunidades de financiación y acciones específicas destinadas a apoyar el desarrollo de capacidades en materia de ciberseguridad. Ampliará las iniciativas de las partes interesadas a fin de alcanzar una masa crítica que marque la diferencia en el mercado laboral, también en materia de defensa. Estas actividades se adaptarán a objetivos comunes e indicadores clave de rendimiento para buscar un mayor impacto.

La Academia se centrará en la capacitación de los **profesionales de la ciberseguridad**. La actividad de la Academia contribuirá a las políticas de la UE en materia de ciberseguridad, pero también a la educación y el aprendizaje permanente. Complementa las dos recomendaciones del Consejo relativas a la educación y las capacidades digitales propuestas por la Comisión al mismo tiempo que la presente Comunicación[43].

La Academia se basará en cuatro pilares: 1) fomentar la **generación de conocimientos a través de la educación y la formación** trabajando en un marco común para los perfiles de funciones de la ciberseguridad y las capacidades asociadas, mejorar la oferta europea de educación y formación para satisfacer las necesidades, crear itinerarios profesionales y proporcionar visibilidad y claridad sobre las formaciones y certificaciones en materia de ciberseguridad para mejorar la oferta de mano de obra; 2) garantizar una mejor canalización y visibilidad de las **oportunidades de financiación** disponibles para actividades relacionadas con las capacidades, a fin de maximizar su impacto; 3) pedir a las partes interesadas **que tomen medidas**; y 4) definir indicadores para **supervisar la evolución del mercado** y poder evaluar la eficacia de sus acciones.

La ejecución de la Academia contará con el apoyo de una financiación de 10 millones EUR del programa Europa Digital[44].

3.2.Gobernanza de la Academia

En última instancia, para proporcionar una infraestructura que sirva de **ventanilla única** para fomentar la cooperación entre el mundo académico, los proveedores de formación y la industria, en la que la oferta y la demanda del ecosistema de ciberseguridad de la UE puedan encontrarse y recibir formación, la Academia podría adoptar la forma de un **Consorcio de Infraestructuras Digitales Europeas (EDIC)**[45]. Este instrumento permitiría a los Estados miembros trabajar conjuntamente para colmar la brecha de capacidades en materia de ciberseguridad, así como cooperar estrechamente con la Comisión, la ENISA y el Centro Europeo de Competencia en Ciberseguridad (ECCC), en consonancia con sus mandatos y competencias, e integrar a todas las partes interesadas pertinentes, pero también dirigir la inversión europea, nacional y privada a un objetivo común. A tal fin, se anima a los Estados miembros interesados a presentar a la Comisión, a más tardar el 30 de mayo de 2023, una notificación previa de su futura solicitud para dicho EDIC. Esta notificación previa voluntaria permitiría a la Comisión formular observaciones tempranas sobre el proyecto de solicitud del EDIC, lo que permitiría su ulterior desarrollo y presentación formal de manera más rápida. Durante todo el proceso y en la medida en que lo soliciten los Estados miembros, la Comisión, actuando como acelerador de proyectos plurinacionales, facilitará la preparación de la solicitud del EDIC. A continuación, tras una evaluación positiva de la solicitud por

[43] Propuestas de recomendaciones del Consejo sobre los factores facilitadores clave para el éxito de la educación y la formación digitales, y sobre la mejora de la provisión de capacidades digitales en la educación y la formación.

[44] Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240.

[45] Los EDIC se establecieron en la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030, artículo 13 y siguientes.

parte de la Comisión y la aprobación del Comité del Programa para la Década Digital, la Comisión emitiría una decisión por la que se crearía el EDIC y, posteriormente, ayudaría a coordinar su aplicación[46].

Entretanto, y mientras se está creando formalmente el EDIC, la Comisión creará una ventanilla única virtual mejorando la **Plataforma de Capacidades y Empleos Digitales**[47] de la Comisión con la ayuda del proyecto europeo de apoyo a la comunidad de la ciberseguridad (ECCO)[48].

La **ENISA** contribuirá a la aplicación de la Academia en consonancia con los objetivos de la Agencia[49], en particular en lo que se refiere a la asistencia en la educación y la formación en materia de ciberseguridad, y teniendo en cuenta sus obligaciones de información en virtud de la Directiva SRI 2[50]. El **ECCC** trabajará en consonancia con su Agenda Estratégica para apoyar la aplicación de la Academia de Cibercapacidades. En particular, el ECCC aplicará el objetivo estratégico 3 (ciberseguridad) del programa Europa Digital. Se beneficiará del apoyo de la Comisión y de los Estados miembros a través de los **centros nacionales de coordinación (CNC)**. Cuando proceda, se solicitará al **Grupo de Cooperación** establecido en virtud de la Directiva SRI 2[51]. Por último, será necesario aunar fuerzas con la **industria** y el **mundo académico** para alcanzar el objetivo de la Academia de colmar la brecha de capacidades en materia de ciberseguridad.

4. Formación y generación de conocimientos: establecer un enfoque común de la UE para la formación en materia de ciberseguridad

En el marco del pilar sobre formación y generación de conocimientos de la Academia de Cibercapacidades, se desarrollará un enfoque estructurado con el objetivo claro de aumentar el **número** de personas con capacidades en ciberseguridad en la UE, orientar mejor la formación hacia las **necesidades del mercado** y dar visibilidad a los **itinerarios profesionales**.

4.1. Hablando la misma lengua: un enfoque común sobre los perfiles de funciones de la ciberseguridad y las capacidades asociadas

La ENISA ya ha trabajado en la definición de perfiles de funciones de los profesionales de la ciberseguridad en el Marco Europeo de Competencias en Cibercapacidades (**ECSF**)[52]. Esto

---

[46] *Ibidem*, artículo 12.

[47] Página de inicio | Plataforma de Capacidades y Empleos Digitales (europa.eu) (en inglés).

[48] Véanse la Red y el Centro Europeos de Competencia en Ciberseguridad:nuevo proyecto financiado por la UE para apoyar a la cibercomunidad (europa.eu) (en inglés). En diciembre de 2022, la Comisión Europea firmó un contrato de 3 millones EUR para apoyar a la cibercomunidad de la UE en el marco del Centro Europeo de Competencia en Ciberseguridad. Este proyecto contribuirá a los objetivos de la UE en materia de desarrollo comunitario y de capacidades en relación con la investigación, la innovación, la adopción y la base industrial en materia de ciberseguridad.

[49] «ENISA prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros y las partes interesadas públicas y privadas [...] a fin de desarrollar las capacidades y competencias en el ámbito de la ciberseguridad». Artículo 4, apartado 3, del Reglamento sobre la Ciberseguridad.

[50] Artículo 18 de la Directiva SRI 2.

[51] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

[52] Marco Europeo de Capacidades en Ciberseguridad (ECSF) – ENISA (europa.eu) (en inglés). El ECSF apoya la identificación y articulación de tareas, competencias, capacidades y conocimientos asociados a las funciones de los profesionales europeos de la ciberseguridad. Resume todas las funciones relacionadas con la ciberseguridad en perfiles,

debería convertirse en la base para que la Academia defina y evalúe las capacidades pertinentes, supervise la evolución de la brecha de capacidades y proporcione indicaciones sobre las nuevas necesidades. Para cada función de ciberseguridad del ECSF, se incorpora un conjunto de competencias aplicables del Marco Europeo de Competencia Electrónica[53] como elemento de la descripción del perfil[54].

Por lo tanto, la ENISA revisará el ECSF e **identificará la evolución de las necesidades y las carencias en materia de capacidades** de la mano de obra en el ámbito de la ciberseguridad, en particular a través de herramientas avanzadas (por ejemplo, inteligencia artificial, macrodatos[55], prospección de datos). A tal fin, la ENISA trabajará bajo la dirección del EDIC, una vez establecido, el ECCC, junto con los CNC, la Comisión, el proyecto ECCO y los agentes del mercado[56]. Para la mano de obra en el ámbito de la ciberdefensa, la ENISA tendrá debidamente en cuenta el trabajo realizado por la EESD. Del mismo modo, en el ámbito de la lucha contra la ciberdelincuencia, la ENISA tendrá en cuenta las actividades llevadas a cabo por la Agencia de la Unión Europea para la Formación Policial (CEPOL) y Europol para preparar un análisis de las necesidades de formación operativa[57] sobre ciberataques.

El ECSF se complementará y revisará periódicamente en el marco de la Academia a lo largo de un ciclo bienal. Además, la Comisión y el Servicio Europeo de Acción Exterior contribuirán a definir perfiles específicos y capacidades asociadas para los sectores en caso necesario, con el apoyo de las agencias y organismos de la UE, como la EESD[58], Europol y la CEPOL[59].

También se establecerán vínculos entre el ECSF y los instrumentos pertinentes de la política de empleo de la UE[60]. En particular, los perfiles laborales del ECSF, así como las capacidades relacionadas, se integrarán en la **clasificación ESCO**. Esto mejorará la clasificación de las ocupaciones y las capacidades en el ámbito de la ciberseguridad, así como los vínculos entre ellas, facilitando a las personas la mejora de las capacidades y el reciclaje profesional y apoyando la adecuación entre la demanda y la oferta de empleo basada en las capacidades y la movilidad transfronteriza.

---

que se analizan individualmente en los detalles de sus responsabilidades, capacidades, sinergias e interdependencias correspondientes.

53 Marco Europeo de Competencia Electrónica | ESCO (europa.eu) (en inglés). El Marco Europeo de Competencia Electrónica ofrece vínculos coherentes en el contexto de las cualificaciones de las TIC y otros marcos pertinentes para el sector, entre ellos DigComp (en inglés).

54 Véase a este respecto el Manual del usuario – Marco Europeo de Capacidades en Ciberseguridad (ECSF), septiembre de 2022 (en inglés).

55 Véase, por ejemplo, Skills-OVATE, desarrollado por el Cedefop.

56 La Agencia seguirá aprovechando los resultados de otros proyectos financiados por la UE [por ejemplo, REWIRE, Data Space for Skills (DS4), CyberSecPro, Concordia] y metodologías derivadas de iniciativas similares (por ejemplo, *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States* [«Crear una mano de obra en el ámbito de la ciberseguridad en cinco países: Perspectivas de Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos», documento en inglés], informe de la OCDE, publicado el 21 de marzo de 2023) para garantizar en el futuro una visión actualizada de las necesidades en un entorno en el que la demanda está en constante evolución.

57 Evaluación de las necesidades de formación operativa de la CEPOL (en inglés).

58 Véase a este respecto la Comunicación conjunta al Parlamento Europeo y al Consejo: Política de ciberdefensa de la UE, JOIN(2022) 49 final.

59 A este respecto, se prestará atención a los trabajos sobre el Marco de Competencias de Formación en Ciberdelincuencia actualmente en fase de desarrollo.

60 Como la Clasificación Europea de Capacidades, Competencias, Cualificaciones y Ocupaciones (ESCO), Europass, la red europea de cooperación de servicios de empleo (EURES).

4.2.Fomentar la cooperación para diseñar planes de estudios de educación y formación en materia de ciberseguridad

Una vez creado el EDIC, la Academia debe recibir el apoyo de los Estados miembros para convertirse en el **lugar de referencia en Europa para diseñar e impartir formación en materia de ciberseguridad** que aborde las capacidades más demandadas y ofrezca formación en el lugar de trabajo y oportunidades de prácticas para las empresas emergentes y las pymes, así como para las administraciones públicas en empresas innovadoras en ciberseguridad y en centros de competencia en ciberseguridad. El EDIC debe trabajar con todas las partes interesadas pertinentes, incluida la industria, para diseñar dichas formaciones y basarse en proyectos como **CyberSecPro**[61] financiado por el programa Europa Digital, que reúne a diecisiete instituciones de educación superior y trece empresas de seguridad de dieciséis Estados miembros, con el fin de convertirse en la mejor práctica para todos los programas de formación en ciberseguridad.

La Academia trabajará con todas las partes interesadas pertinentes para **atraer a las jóvenes generaciones** a emprender carreras en el ámbito de la ciberseguridad. En consonancia con la propuesta de Recomendación del Consejo sobre la mejora de la provisión de capacidades digitales en la educación y la formación, los Estados miembros deben establecer y reforzar medidas para contratar y formar a profesores y formadores especializados y facilitar la adquisición de capacidades en materia de ciberseguridad, en particular mediante prácticas de aprendizaje. Debe fomentarse la integración de la ciberseguridad en los programas de educación y formación, garantizando al mismo tiempo su accesibilidad, desarrollando la oferta de **formación de aprendices** y de prácticas, fomentando enfoques innovadores que incluyan, por ejemplo, juegos serios y plataformas de simulación compartidas, organizando semanas de inmersión en puestos de ciberseguridad y explicando los perfiles de funciones no técnicos. También debe apoyarse la participación en estas oportunidades de aprendizaje en materia de ciberseguridad de grupos de difícil acceso, como los jóvenes con discapacidad, las personas que viven en zonas remotas o rurales y otros grupos minoritarios.

La Comisión seguirá prestando apoyo al desarrollo de microcredenciales y programas de educación y formación profesionales. En particular, seguirán financiándose en el marco de Erasmus+ **programas conjuntos de grado y máster, cursos o módulos conjuntos que puedan dar lugar a microcredenciales** y **programas intensivos combinados**[62] sobre todos los temas, incluida la **ciberseguridad**. También se apoyará un mayor despliegue de la **Iniciativa «Universidades Europeas»**[63] y de **centros de excelencia profesional**[64] para fomentar una mayor cooperación entre la educación superior y las instituciones pertinentes de educación y formación profesionales de toda Europa. Los programas de financiación de la UE, incluidos Erasmus+ y el programa Europa Digital, apoyarán este objetivo de una

[61] CyberSecPro, por ejemplo, llevará a cabo un análisis de los programas, cursos y escuelas de verano en materia de ciberseguridad ofrecidos en las universidades y de los cuadros de clasificación del Sistema Europeo de Transferencia y Acumulación de Créditos (ECTS) utilizados, garantizará la participación del número objetivo de más de 530 becarios durante el período de tres años y formará a personas externas de diversas industrias y sectores.

[62] Los programas intensivos combinados compaginan la enseñanza en línea con un breve período de movilidad física.

[63] Iniciativa «Universidades Europeas» | Espacio Europeo de Educación (europa.eu).

[64] Centros de excelencia profesional |. Erasmus+ (europa.eu).

cooperación más estrecha, al igual que los fondos de la UE para el desarrollo de **cuentas de aprendizaje individuales**[65].

Para facilitar la cooperación a nivel nacional entre el mundo académico y los proveedores de formación en capacidades en materia de ciberseguridad con empleadores de los sectores público y privado y fomentar las sinergias entre dichos sectores, se invita a los CNC a estudiar la creación de **cibercampus** en los Estados miembros. El objetivo de los cibercampus sería proporcionar polos de excelencia a nivel nacional para la comunidad de la ciberseguridad, y la Academia ayudaría a su creación de redes y a una mayor coordinación de sus actividades.

La ENISA también mejorará su oferta de formación en ciberseguridad, adaptando **su catálogo de cursos**[66] a los perfiles del ECSF y elaborando módulos de formación por perfil, lo que puede mejorar las ofertas de formación de los Estados miembros. La ENISA también ampliará su **programa de «formación de formadores»**[67], centrándose en las necesidades profesionales de las instituciones, órganos y organismos europeos, las autoridades públicas de los Estados miembros y los **operadores críticos públicos y privados** en el ámbito de aplicación de la Directiva SRI 2.

Además, otras agencias y organismos de la UE reforzarán su oferta de formación en ciberseguridad. Por ejemplo, al aplicar la política de ciberdefensa de la UE, la **EESD** desarrollará un nuevo conjunto de cursos sobre ciberseguridad y adaptará algunos de sus cursos actuales al ECSF. Estos cursos darán lugar a la certificación de los resultados del aprendizaje[68]. La EESD, en colaboración con la Comisión, estudiará la posibilidad de integrar los certificados en la cartera de la EUeID. La EESD seguirá explorando posibles mecanismos de evaluación de las capacidades, con los que se emitirán los certificados. Del mismo modo, en el ámbito de la lucha contra la ciberdelincuencia, se buscarán estrechas conexiones con la **Academia de Ciberdelincuencia de la CEPOL**[69] para fomentar sinergias y complementariedades en el diseño y la aplicación de los planes de estudios de formación.

4.3. Crear sinergias y dar visibilidad a la formación y la certificación en materia de ciberseguridad en todos los Estados miembros

La Academia debe abordar la cuestión de la visibilidad y las sinergias de la formación y la certificación. Esto beneficiaría a las cibercomunidades civil, de defensa, policial y diplomática, ya que todos los sectores requieren en muchos casos los mismos conocimientos especializados, basados en planes de estudios y resultados de aprendizaje similares.

La Academia proporcionaría una **ventanilla única** para las personas interesadas en una carrera en ciberseguridad. A corto plazo, esto se hará mejorando la **Plataforma de Capacidades y Empleos Digitales** de la Comisión con el apoyo del proyecto ECCO. Una sección específica de las carreras en ciberseguridad se vinculará a las herramientas existentes,

---

[65] En consonancia con la Recomendación del Consejo, de 16 de junio de 2022, relativa a las cuentas de aprendizaje individuales.

[66] Cursos de formación – ENISA (europa.eu) (en inglés).

[67] Programa de formación de formadores – ENISA (europa.eu) (en inglés).

[68] De conformidad con el artículo 20, apartado 4, de la Decisión (PESC) 2020/1515 del Consejo de 19 de octubre de 2020 por la que se crea la Escuela Europea de Seguridad y Defensa y se deroga la Decisión (PESC) 2016/2382.

[69] La Academia de Ciberdelincuencia de la CEPOL se creó en 2019 para proporcionar una plataforma de vanguardia para mejorar los conocimientos sobre ciberdelincuencia y las cibercapacidades en Europa.

desde los programas de educación superior hasta las oportunidades de formación, incluidos los cursos que conduzcan a microcredenciales y los programas de educación y formación profesionales, pasando por las ofertas de empleo. Esto se logrará haciendo referencia a los trabajos e iniciativas en curso, o integrándolos en la plataforma, como los de la ENISA, que, en colaboración con el mundo académico, ha elaborado un **mapa de las instituciones educativas** que ofrecen programas de ciberseguridad. Esto se verá reforzado con el apoyo de los CNC. Además, la ENISA desarrollará y consolidará dos **repositorios de formaciones existentes de los sectores público y privado y de certificaciones de ciberseguridad**, con el apoyo de los CNC, la Comisión y el proyecto ECCO, y en colaboración con entidades que expiden certificaciones y que también aprovechan otras iniciativas pertinentes[70]. También se integrarán en la ventanilla única de la Plataforma de Capacidades y Empleos Digitales. Este trabajo beneficiará, asimismo, a los CNC, cuya tarea consiste, en particular, en promover y difundir programas educativos en materia de ciberseguridad[71].

También es necesario ofrecer garantías a los profesionales de que las formaciones que cursan son de la calidad requerida. A este respecto, la ENISA desarrollará un **proyecto piloto** que estudiará la creación de un sistema europeo de acreditación de las capacidades en materia de ciberseguridad.

Además, es esencial identificar las capacidades y formaciones y asociarlas a un perfil profesional, pero también es importante garantizar que los servicios de ciberseguridad cuenten con la competencia, los conocimientos y la experiencia necesarios, en particular en el caso de los proveedores de servicios de seguridad administrada en ámbitos como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría. La Directiva SRI 2 y la propuesta de Ley de cibersolidaridad establecen tareas específicas para dichos proveedores de servicios de seguridad administrada. Por lo tanto, la Comisión también propone una **modificación específica del Reglamento sobre la Ciberseguridad**[72] para habilitar los sistemas de certificación de los servicios de seguridad administrada a escala de la UE. Dichos sistemas de certificación deben tener por objeto, entre otras cosas, garantizar que estos servicios sean prestados por personal con un nivel muy elevado de conocimientos técnicos y de competencia en los ámbitos pertinentes.

Los mecanismos de garantía de la calidad y de reconocimiento de las microcredenciales[73] facilitan la transparencia, la comparabilidad y la portabilidad de los resultados del aprendizaje. En consonancia con la Recomendación del Consejo relativa a un enfoque europeo de las microcredenciales[74], se anima a los Estados miembros a incluir las microcredenciales de ciberseguridad en sus marcos nacionales de cualificaciones. Esto les

[70] Por ejemplo, la W4C Academy - Women4Cyber o el proyecto Global Cybercrime Certification para las autoridades policiales y judiciales.

[71] «1. Los centros nacionales de coordinación tendrán las siguientes funciones: [...] g) sin perjuicio de las competencias de los Estados miembros en materia de educación y teniendo en cuenta las funciones pertinentes de ENISA, colaborar con las autoridades nacionales a propósito de posibles contribuciones a la promoción y difusión de programas educativos de ciberseguridad», artículo 7, apartado 1, letra g), del Reglamento del CECC. Véase también el considerando 28 asociado.

[72] 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»).

[73] Por ejemplo, registro o certificados de resultados de aprendizaje que las personas adquieren tras pequeñas formaciones.

[74] Recomendación del Consejo, de 16 de junio de 2022, relativa a un enfoque europeo de las microcredenciales para el aprendizaje permanente y la empleabilidad.

permitiría relacionar tales microcredenciales con el Marco Europeo de Cualificaciones[75]. Las credenciales digitales europeas para la infraestructura de aprendizaje están disponibles para expedir cualificaciones y microcredenciales de ciberseguridad individuales firmadas por medios digitales. Estas contienen abundantes datos, en particular sobre los resultados del aprendizaje en materia de ciberseguridad, y pueden almacenarse en la futura **cartera digital de la EUeID**[76].

Acciones en el marco de la Academia

Estados miembros e industria

- Garantizar el apoyo al desarrollo y el reconocimiento de las **microcredenciales** del aprendizaje en materia de ciberseguridad, en consonancia con la Recomendación del Consejo relativa a un enfoque europeo de las microcredenciales.
- Incluir las cualificaciones en materia de ciberseguridad, incluidas las microcredenciales en los **marcos nacionales de cualificaciones**.
- Ofrecer **oportunidades de aprendizaje en el lugar de trabajo** a través de la formación de aprendices para las personas que participen en iniciativas de desarrollo de capacidades en materia de ciberseguridad.

Comisión

- A corto plazo, crear **una ventanilla única** para los programas de ciberseguridad, las formaciones existentes y las certificaciones de ciberseguridad a través de la **Plataforma de Capacidades y Empleos Digitales** antes de finales 2023.
- Proponer una modificación del **Reglamento sobre la Ciberseguridad** para permitir la certificación de los proveedores de seguridad administrada el 18 de abril de 2023.

Organismos y agencias de la UE

- Establecer el **ECSF** como un enfoque común sobre los perfiles de funciones de ciberseguridad y las capacidades asociadas antes de finales de 2023.
- La ENISA debe iniciar el desarrollo de un proyecto piloto por el que se establezca un **sistema europeo de acreditación** de las competencias en ciberseguridad en el segundo trimestre de 2023.
- La ENISA debe revisar su **catálogo de cursos** y abrir su **programa de «formación de formadores»** a los operadores críticos públicos y privados antes de finales de 2023.
- Finalizar la **armonización de los planes de estudios de la EESD con el ECSF** antes de mediados de 2023.

5. Participación de las partes interesadas: compromiso de colmar la brecha de capacidades en materia de ciberseguridad

En el marco de la Academia, se desarrollará un enfoque coordinado de la participación de las partes interesadas para abordar la brecha de capacidades en materia de ciberseguridad. El

[75] Recomendación del Consejo, de 22 de mayo de 2017, relativa al Marco Europeo de Cualificaciones para el aprendizaje permanente y por la que se deroga la Recomendación del Parlamento Europeo y del Consejo de 23 de abril de 2008 relativa a la creación del Marco Europeo de Cualificaciones para el aprendizaje permanente.

[76] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.

objetivo será maximizar la visibilidad y el impacto de los compromisos de las distintas partes interesadas destinados a reducir la brecha de capacidades en materia de ciberseguridad.

La Comisión pide a las partes interesadas que asuman compromisos concretos mediante promesas de mejora de las capacidades y reciclaje profesional de los trabajadores a través de acciones específicas, basándose en la medida de lo posible en la brecha de capacidades en materia de ciberseguridad detectada. Estos **compromisos en materia de ciberseguridad** de las partes interesadas deben comunicarse en la **Plataforma de Capacidades y Empleos Digitales**, al igual que otros compromisos digitales ya visibles en la plataforma. La Comisión anima además a las partes interesadas que se comprometan en materia de ciberseguridad en la Plataforma a participar en la **asociación digital a gran escala en el marco del Pacto por las Capacidades**[77]. Se anima a que los compromisos en materia de ciberseguridad contraídos en el marco de la asociación digital a gran escala se presenten en la Plataforma de Capacidades y Empleos Digitales. Del mismo modo, se anima a que los compromisos contraídos en el marco de la Plataforma de Capacidades y Empleos Digitales se notifiquen en el marco de la asociación digital a gran escala del Pacto por las Capacidades.

La Comisión pide además a los Estados miembros que **prosigan sus esfuerzos en la aplicación de la Declaración sobre las mujeres en el ámbito digital**[78] para animar a las mujeres a desempeñar un papel activo y destacado en el sector de la tecnología digital y lograr la convergencia de género en los puestos de ciberseguridad. La Comisión también anima a los Estados miembros a desarrollar sinergias con sus programas del **Fondo Social Europeo+** (FSE+) para seguir apoyando el objetivo de la igualdad de género en la participación laboral[79], por ejemplo, mediante el establecimiento de **programas de tutoría para niñas y mujeres**. Estos pueden facilitar la creación de modelos de referencia para atraer a las niñas a las profesiones relacionadas con la ciberseguridad, luchando al mismo tiempo contra los estereotipos de género. También fomenta la mejora de las capacidades y el reciclaje profesional de las mujeres y fomenta el desarrollo de una comunidad que puede apoyar a las mujeres en su entrada o promoción en el mercado laboral de la ciberseguridad.

Los Estados miembros deben adoptar, como parte de **sus estrategias nacionales de ciberseguridad, medidas específicas con vistas a mitigar la escasez de capacidades en materia de ciberseguridad**[80], determinar y canalizar mejor los esfuerzos para colmar la brecha de capacidades y, en última instancia, garantizar la correcta aplicación de sus obligaciones en virtud de la Directiva SRI 2.

Algunos Estados miembros hacen uso de las **sinergias entre las iniciativas civiles, de defensa y policiales**. Por ejemplo, el aumento de la mano de obra utilizando su servicio militar nacional obligatorio o los ciberreservistas, que son ciudadanos con formación militar que ocupan puestos de ciberseguridad en las fuerzas armadas[81], permiten a la población y,

---

[77] Puesta en marcha de nuevas asociaciones europeas para cumplir las ambiciones de la UE para la Década Digital | Configurar el futuro digital de Europa (europa.eu) (en inglés), constituidas en el marco del Pacto por las Capacidades para hacer frente a la escasez de tecnologías de la información y la comunicación (TIC).

[78] Los países de la UE se comprometen a impulsar la participación de las mujeres en el sector digital | Configurar el futuro digital de Europa (europa.eu) (en inglés).

[79] Reglamento (UE) 2021/1057 del Parlamento Europeo y del Consejo, de 24 de junio de 2021, por el que se establece el Fondo Social Europeo Plus (FSE+) y por el que se deroga el Reglamento (UE) n.º 1296/2013, artículo 4, apartado 1, letra c).

[80] Artículo 7, apartado 2, letra f), de la Directiva SRI 2.

[81] Martin Hurt y Tiia Sõmer: *Report - Cyber Conscription: Experience and Best Practice from Selected Countries* [«Informe – Ciberreclutamiento: experiencias y mejores prácticas de determinados países», documento en inglés], International Centre for Defence and Security, febrero de 2021.

especialmente, a los jóvenes adultos aumentar sus capacidades en materia de ciberseguridad y ciberdefensa. Lo mismo se aplica en el ámbito de la **lucha contra la ciberdelincuencia**, ya que existen muchas similitudes entre los esfuerzos generales de ciberseguridad y las actividades policiales en respuesta a los incidentes de ciberseguridad. La Comisión fomenta los debates entre los Estados miembros sobre estas iniciativas y les invita a evaluar la mejor manera en que una mano de obra cualificada puede servir tanto a las comunidades de defensa como a las de ciberseguridad civil.

La Comisión reflexionará sobre las propuestas relativas a cómo colmar la brecha actual y prevista identificada en su revisión de las necesidades de las instituciones, órganos y organismos europeos. En particular, animará al personal a beneficiarse de la próxima **beca de ciberseguridad entre la UE y los Estados Unidos**, creada en el marco del diálogo UE-EE. UU.

Acciones en el marco de la Academia

Industria

- Proponer **compromisos específicos en materia de ciberseguridad** en la Plataforma de Capacidades y Empleos Digitales a partir del 18 de abril de 2023.

Estados miembros

- Incluir en las **estrategias nacionales de ciberseguridad** medidas específicas para abordar la brecha de capacidades en materia de ciberseguridad.

Estados miembros e industria

- Aplicar la Declaración sobre las mujeres en el ámbito digital y lograr la **convergencia de género en los puestos de ciberseguridad** de aquí a 2030.

6. Financiación: crear sinergias para maximizar el impacto del gasto en el desarrollo de capacidades en materia de ciberseguridad

En el marco de la Academia, se maximizará el impacto de las inversiones en capacidades en materia de ciberseguridad proporcionando una ventanilla única, facilitando una mejor canalización de los fondos hacia las necesidades del mercado e integrando el uso de la financiación, promoviendo las sinergias entre los diferentes instrumentos y evitando al mismo tiempo la duplicación de esfuerzos[82].

6.1. Adecuación de los fondos a las necesidades

En el marco de la Academia, el ECCC, con el apoyo de la Comisión, el proyecto ECCO y los CNC, recopilará **información sobre cómo se utilizan los fondos de la UE para financiar las capacidades en materia de ciberseguridad** y evaluará cómo están contribuyendo los fondos de la UE a reducir la brecha de capacidades en materia de ciberseguridad. Teniendo en cuenta esta información agregada, el ECCC intentará garantizar una mejor canalización de los fondos de la UE hacia las necesidades detectadas. Financiará acciones que aborden las

[82] Oportunidades de financiación (europa.eu) (en inglés). Los servicios de apoyo del Pacto por las Capacidades ofrecen una ventanilla única para la información sobre financiación de las capacidades, incluido el ecosistema digital. Los servicios de apoyo del Pacto proporcionan información genérica sobre los instrumentos de financiación que no se centran específicamente en las capacidades en materia de ciberseguridad, a pesar de que la Academia debe tener en cuenta su trabajo para evitar duplicaciones.

brechas más acuciantes de la mano de obra en el ámbito de la ciberseguridad, incluidas las relacionadas con la aplicación de las necesidades de la política de ciberseguridad.

6.2. Dar visibilidad a los fondos disponibles y a las iniciativas de asociación para las capacidades en materia de ciberseguridad

A corto plazo, la **Plataforma de Capacidades y Empleos Digitales** se convertirá en la ventanilla única para las partes interesadas, donde estará disponible toda la información sobre las oportunidades de financiación de las capacidades en materia de ciberseguridad.

La UE está invirtiendo en las personas y en sus capacidades y utilizando asociaciones, en particular con la industria, para movilizar acciones de mejora de las capacidades y reciclaje profesional a través de varios instrumentos identificados en el marco de la **Agenda de Capacidades Europea**[83], en particular el **Pacto por las Capacidades**[84] y el **Plan de Acción de Educación Digital**[85]. El **programa Europa Digital** financia oportunidades de capacidades en materia de ciberseguridad, en particular a través de iniciativas de proyectos plurinacionales, en clara complementariedad con el apoyo que ofrece Horizonte Europa a la investigación y las soluciones tecnológicas innovadoras en materia de ciberseguridad. El **Fondo Europeo de Defensa**[86] financia la investigación y el desarrollo tecnológico para llevar a cabo operaciones cibernéticas eficientes, incluidas formaciones y ejercicios[87]. **Erasmus+** seguirá apoyando estas iniciativas, en particular a través de programas intensivos combinados y proyectos de cooperación.

Se anima a los Estados miembros a movilizar los fondos de la UE que gestionan directamente para apoyar las capacidades y los puestos de trabajo en materia de ciberseguridad. Los fondos de la política de cohesión, como el **Fondo Europeo de Desarrollo Regional (FEDER)** y el **FSE+**, tienen un importante potencial para las sinergias en este ámbito[88]. El alcance de las acciones en el marco del **Mecanismo de Recuperación y Resiliencia** (MRR)[89] e **InvestEU**[90] incluye otras complementariedades clave en la consecución de los objetivos de la Academia.

Acciones en el marco de la Academia

[83] Agenda de Capacidades Europea – Empleo, Asuntos Sociales e Inclusión – Comisión Europea (europa.eu).

[84] Instrumentos de financiación de la UE para la mejora de las capacidades y el reciclaje profesional – Empleo, Asuntos Sociales e Inclusión – Comisión Europea (europa.eu).

[85] Plan de Acción de Educación Digital 2021-2027.

[86] Reglamento (UE) 2021/697 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Fondo Europeo de Defensa y por el que se deroga el Reglamento (UE) 2018/1092.

[87] Los Estados miembros se han comprometido a realizar formaciones y ejercicios conjuntos, por ejemplo, mediante el establecimiento y la participación en ciberproyectos de formación y ejercicios de la Cooperación Estructurada Permanente (CEP), como el Centro de la Unión Europea para el Mundo Académico y la Innovación en el Ámbito del Ciberespacio (UE CAIH) y los campos de maniobras virtuales federados.

[88] Artículo 3, apartado 1, del Reglamento (UE) 2021/1058 y artículo 4, apartado 1, letra g), del Reglamento (UE) 2021/1057.

[89] Por ejemplo, el plan de recuperación y resiliencia de Estonia prevé inversiones (10 millones EUR) en capacidades digitales que incluirán la revisión de la formación a disposición de los expertos en TIC, financiarán la mejora de las capacidades y el reciclaje profesional de los especialistas en TIC en materia de ciberseguridad y contribuirán al desarrollo de un programa piloto para rediseñar el marco de cualificación de los especialistas en TIC.

[90] Las partes interesadas (por ejemplo, los proveedores de formación y las empresas que deseen diseñar o mejorar sus actividades de formación en materia de ciberseguridad) pueden dirigirse al Centro de Asesoramiento InvestEU, que presta apoyo técnico y asistencia, incluido el desarrollo de capacidades, a los desarrolladores de proyectos y las entidades, y consultar el Portal InvestEU.

Centro Europeo de Competencia en Ciberseguridad y ENISA

- **Localizar** la financiación existente de la UE para capacidades en materia de ciberseguridad en función de las necesidades del mercado, evaluar la **eficacia** e identificar las **prioridades** de financiación antes de finales de 2024.

Comisión

- Crear una **ventanilla única** para las oportunidades de financiación de las capacidades en materia de ciberseguridad en la Plataforma de Capacidades y Empleos Digitales antes de finales de 2023.

7. Medición de los avances: rendición de cuentas integrada

En el marco de la Academia se desarrollará una **metodología** que permitirá **medir los avances para colmar la brecha de capacidades en materia de ciberseguridad**.

7.1. Definición de indicadores de ciberseguridad para supervisar la evolución del mercado laboral de la ciberseguridad

El **Índice de la Economía y la Sociedad Digitales (DESI)** resume los indicadores pertinentes sobre el rendimiento digital de Europa y hace un seguimiento de los avances de los Estados miembros de la UE. En el marco de la Academia de Cibercapacidades, la ENISA, en cooperación con la Comisión y el Grupo de Cooperación SRI[91], desarrollará **indicadores**, también relacionados con el género, para hacer un seguimiento de los avances realizados en los Estados miembros de la UE para aumentar el número de profesionales de la ciberseguridad, consultando asimismo a los agentes del mercado pertinentes y a los CNC. La ENISA se basará en la metodología del DESI[92] y garantizará que los indicadores estén en consonancia con los objetivos digitales de Europa sobre los profesionales de las TIC y sobre la consecución de la convergencia de género en estas. A continuación, la Comisión trabajará para integrar dichos indicadores en el DESI, permitiendo así el seguimiento anual del estado de las capacidades en materia de ciberseguridad y del mercado laboral.

7.2. Recopilación de datos y presentación de informes

La ENISA recopilará los datos sobre los indicadores con el apoyo del proyecto ECCO y de los CNC. Sobre la base de los datos recopilados, la ENISA elaborará un **informe anual** que contribuirá al informe sobre el estado de la Década Digital[93], que, junto con el DESI, se incorporará a los análisis y recomendaciones específicos por país[94] del **Semestre Europeo**. Además, los indicadores sobre capacidades en materia de ciberseguridad contribuirán al **informe bienal** de la ENISA sobre el estado de la ciberseguridad en la UE previsto en la Directiva SRI 2, que abarca las capacidades, la sensibilización y la higiene en materia de ciberseguridad en toda la UE.

7.3. Preparación de indicadores clave de rendimiento para la ciberseguridad

---

[91] Aprovechando y complementando la metodología que desarrollará la ENISA a efectos del informe bienal de la Agencia sobre el estado de la ciberseguridad en la Unión de conformidad con el artículo 18, apartado 3, de la Directiva SRI 2.

[92] Véase la nota metodológica del Índice de la Economía y la Sociedad Digitales (DESI) 2022 disponible en El Índice de la Economía y la Sociedad Digitales (DESI) | Configurar el futuro digital de Europa (europa.eu) (en inglés).

[93] Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030.

[94] *Ibidem*, considerando 25.

Con vistas a colmar la brecha europea de talento en materia de ciberseguridad, la ENISA, en estrecha cooperación con la Comisión y los CNC, propondrá indicadores clave de rendimiento a la Comisión, basándose en la metodología del Programa Estratégico de la Década Digital 2030, así como en la experiencia de la industria. La ENISA tendrá debidamente en cuenta los indicadores clave de rendimiento utilizados por los Estados miembros para evaluar sus estrategias nacionales de ciberseguridad[95].

Acciones en el marco de la Academia

ENISA

- Preparar **indicadores e indicadores clave de rendimiento** sobre capacidades en materia de ciberseguridad antes de finales de 2023.
- **Recopilar datos** sobre los indicadores e informar al respecto, con una primera recopilación antes de finales de 2025.

Comisión

- Trabajar en pro de la integración de **indicadores sobre ciberseguridad en el DESI** y en el **informe sobre el estado de la Década Digital**.

8. Conclusión

La presente Comunicación sienta las bases de una renovación del enfoque de la UE para impulsar las capacidades en materia de ciberseguridad de los profesionales de la Unión. El objetivo es reducir la brecha de competencias en materia de ciberseguridad y dotar a la UE de la mano de obra necesaria para poder responder al panorama de amenazas en constante evolución y aplicar políticas propias destinadas a ofrecer protección frente a los ciberataques, pero también a impulsar las oportunidades de negocio y la competitividad. Una mano de obra cualificada en materia de ciberseguridad puede beneficiar a las comunidades **civil, de defensa, diplomática y policial**, facilitando las sinergias entre ellas.

La Comisión pide a los Estados miembros y a todas las partes interesadas que cumplan la ambición de la Academia de Cibercapacidades.

[95] Artículo 7, apartado 4, de la Directiva SRI 2.