ITUPublicaciones

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Informe de resultados de la Cuestión 3/2 del UIT-D

Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad

Periodo de estudios 2022-2025

Informe de resultados de la Cuestión 3/2 del UIT-D

Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad

Periodo de estudios 2022-2025

Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad: Informe de resultados de la Cuestión 3/2 del UIT-D para el periodo de estudios 2022-2025

ISBN 978-92-61-41103-9 (versión electrónica)
ISBN 978-92-61-41113-8 (versión EPUB)

Cita propuesta. Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad: Informe de resultados de la Cuestión 3/2 del UIT-D para el periodo de estudios 2022-2025. Ginebra: Unión Internacional de Telecomunicaciones, 2025. Licencia: CC BY-NC-SA 3.0 IGO.

Créditos de la foto de portada: Adobe Stock

Agradecimientos

Las Comisiones de Estudio del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) constituyen una plataforma neutral en la que expertos de gobiernos, del sector privado, de organizaciones de telecomunicaciones y de instituciones académicas de todo el mundo se reúnen para elaborar herramientas y recursos prácticos a fin de abordar problemas del desarrollo. En ese contexto, las dos Comisiones de Estudio del UIT-D se encargan de elaborar informes, directrices y recomendaciones basados en las aportaciones que reciben de los miembros. Las Cuestiones de estudio se deciden cada cuatro años en la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT). Los miembros de la UIT, reunidos en la CMDT-22 en Kigali en junio de 2022, acordaron que, de cara al periodo de estudios 2022-2025, la Comisión de Estudio 2 se ocuparía de siete cuestiones enmarcadas en el ámbito de la transformación digital.

El presente Informe se ha elaborado en respuesta a la Cuestión 3/2, **Seguridad en las redes de información y comunicación: prácticas idóneas para el desarrollo de una cultura de ciberseguridad**, bajo la dirección y coordinación generales del equipo directivo de la Comisión de Estudio 2 del UIT-D, presidida por el Sr. Fadel Digham (República Árabe de Egipto), con el apoyo de los siguientes Vicepresidentes: Sr. Abdelaziz Alzarooni (Emiratos Árabes Unidos), Sra. Zainab Ardo (República Federal de Nigeria), Sr. Javokhir Aripov (República de Uzbekistán), Sra. Carmen-Mădălina Clapon (Rumania), Sr. Mushfig Guluyev (República de Azerbaiyán), Sr. Hideo Imanaka (Japón), Sra. Mina Seonmin Jun (República de Corea), Sr. Mohamed Lamine Minthe (República de Guinea), Sr. Víctor Antonio Martínez Sánchez (República del Paraguay), Sra. Alina Modan (Rumania)[1], Sr. Diyor Rajabov (República de Uzbekistán)[1], Sr. Tongning Wu (República Popular de China) y Sr. Dominique Würges (Francia).

El Informe ha sido redactado por las Correlatoras para la Cuestión 3/2, Sra. Vanessa Copetti Cravo (República Federativa del Brasil), Sra. Nicole Darabian (Reino Unido de Gran Bretaña e Irlanda del Norte) y Sra. Jabin Vahora (Estados Unidos de América)[1], en colaboración con los siguientes Vicerrelatores: Sr. Damnam K. Bagolibe (República Togolesa), Sr. Daniel Batty (Access Partnership Limited)[1], Sra. Maria Bolshakova (Federación de Rusia)[1], Sr. Tommaso De Zan (Access Partnership Limited), Sr. Idrissa Diallo (República de Guinea), Sr. Sidy Mouhamed Fall (República de Senegal), Sr. Álvaro García (Axon Partners Group), Sr. Doğukan Ömer Gür (República de Türkiye), Sr. Prachish Khanna (República de la India), Sr. Teng Ma (China International Telecommunication Construction Corporation), Sr. Rodgers Mumelo (República de Kenya), Sra. Uliana Stoliarova (Federación de Rusia), Sr. Samuel Tew (Axon Partners Group)[1], Sra. Xinxin Wan (República Popular de China), Sra. Kacie Yearout (Estados Unidos de América) y Sr. Jaesuk Yun (República de Corea).

Merecen un agradecimiento especial los autores referentes de los capítulos por su dedicación, apoyo y conocimientos especializados.

El Informe se ha elaborado con el apoyo tanto de los coordinadores de la Cuestión 3/2 del UIT-D, los editores y el equipo de producción de publicaciones, como de la secretaría de la Comisión de Estudio 2 del UIT-D.

[1] Dimitieron durante el periodo de estudios.

Índice

Lista de figuras y recuadros

Figuras

Recuadros

Resumen ejecutivo

El Informe de resultados de la Cuestión 3/2 del UIT-D para el periodo de estudios 2022-2025 constituye un esfuerzo concertado para aprovechar las experiencias y prácticas nacionales en materia de ciberseguridad de todo el mundo. El informe es un recurso que puede ayudar a los países a formular sus estrategias encaminadas a desarrollar una sólida cultura de ciberseguridad. El informe tiene en cuenta y refleja las contribuciones de los Miembros de la UIT, así como los debates de los talleres celebrados durante el periodo de estudios, que reflejan diversas perspectivas y experiencias destinadas a asegurar las redes de información y comunicación.

En una era en la que las tecnologías digitales están íntimamente relacionadas con la estructura de la vida diaria y el pilar de las economías de todo el mundo, el informe reconoce la mayor vulnerabilidad a la que se exponen las personas, las organizaciones y las naciones en un contexto marcado por ciberamenazas cada vez más sofisticadas. La ciberseguridad ya no es una preocupación específica sino un elemento fundamental de la transformación y la evolución digitales, que requiere que todas las partes interesadas le atribuyan una gran prioridad, entre ellas los gobiernos, el sector privado, las personas y las instituciones académicas. A nivel mundial, la inseguridad cibernética está clasificada como el cuarto riesgo más grave a corto plazo según el *Informe sobre riesgos mundiales de 2024* (*The Global Risks Report 2024*) del Foro Económico Mundial[2].

Además de las iniciativas emprendidas por la UIT y sus miembros, y los recursos mencionados en este Informe, es importante reconocer que existen también varias iniciativas mundiales destinadas a compartir información y buenas prácticas en materia de ciberseguridad. Estas iniciativas tienen por objeto ayudar a los países y las diversas partes interesadas en su senda de la ciberseguridad, dado que los países en desarrollo, especialmente los países menos adelantados (PMA), pueden tener dificultades para encontrar información sobre ciberseguridad y acceder a ella. En este contexto, cabe observar dos recursos exhaustivos señalados durante el presente ciclo de estudios que pueden beneficiar a los Estados Miembros de la UIT, a saber: el Portal de Política Cibernética del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR)[3] y el Portal de Conocimientos para la Creación de Cibercapacidad del Foro Mundial de Competencia Cibernética (GFCE)[4].

Otro recurso pertinente al que se hace referencia varias veces en este Informe es el Índice de Ciberseguridad Global (ICG) de la UIT[5], que mide el compromiso de los países con la ciberseguridad respecto de cinco pilares fundamentales: medidas de índole jurídica, técnica, organizacional, de desarrollo de capacidades y de cooperación. El ICG fue puesto en marcha por la UIT en 2015 y ha sido objeto de mejoras continuas para servir de herramienta de evaluación, sensibilización y capacitación, que ayuda a los países en su senda hacia el desarrollo y la aplicación de capacidades en materia de ciberseguridad.

---

2 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
3 https://cyberpolicyportal.org/es
4 https://cybilportal.org/
5 https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Este Informe se posiciona como un recurso que proporciona ideas y prácticas actualizadas, informadas por el dinámico y evolutivo abanico de amenazas, y que ofrece una instantánea del estado actual de la ciberseguridad y establece un camino estratégico para los futuros avances.

A continuación se presenta la estructura del informe, compuesto por diferentes capítulos centrados en distintos aspectos de la ciberseguridad, a saber:

- El capítulo 1 aborda el aspecto humano fundamental de la ciberseguridad, haciendo énfasis en la creciente necesidad de realizar importantes inversiones en la concienciación de los usuarios, y la educación y formación del personal de ciberseguridad. En este capítulo se destaca la crítica demanda de profesionales de la ciberseguridad cualificados capaces de gestionar las complejidades de las amenazas digitales contemporáneas y se insta a los países a que den prioridad a los programas educativos y los planes de contratación destinados a cultivar una plantilla de trabajadores competentes y resilientes en materia de ciberseguridad, y a que prioricen también la concienciación como elemento clave para fomentar una cultura de ciberseguridad.
- El capítulo 2 desplaza el foco hacia las prácticas en materia de garantía de la ciberseguridad, que son indispensables para proteger las redes, los sistemas y los datos contra las actividades maliciosas. En este capítulo se evalúan diversas metodologías, controles, directrices y normas que se han adoptado en todo el mundo y que pueden ayudar a prevenir y mitigar el riesgo de ciberataques.
- En el capítulo 3 se resalta la función crucial que desempeñan los equipos de intervención en caso de incidente de ciberseguridad (EIIC) respecto de la salvaguardia de las infraestructuras vitales. En él se presentan modelos de éxito para la respuesta a los incidentes y se destaca la importancia de crear y desarrollar EIIC, así como de garantizar la coordinación entre ellos.
- El capítulo 4 evalúa la formulación y ejecución de estrategias nacionales de ciberseguridad. En este capítulo se detalla la importancia de adaptar las estrategias de ciberseguridad a la transformación digital general y los programas nacionales de seguridad y economía a fin de impulsar la resiliencia digital.
- En el capítulo 5 se examinan los esfuerzos para asegurar las redes 5G. Frente a los desafíos mundiales del despliegue de las redes 5G, en este capítulo se destacan las políticas, los marcos regulatorios y las acciones proactivas de la industria para ayudar a mitigar las amenazas a la ciberseguridad 5G.
- En el capítulo 6 se investiga el creciente uso de tácticas de suplantación por servicios de mensajes cortos (SMS) por parte de los ciberdelincuentes para engañar a los usuarios a través del SMS, lo que pone de manifiesto la necesidad de adoptar un enfoque colectivo que abarque normas del gobierno, iniciativas de la industria y una mayor concienciación pública para proteger a los consumidores y mantener la fiabilidad de las redes de comunicación.

Este Informe viene acompañado de anexos que proporcionan recursos adicionales, como contribuciones detalladas de Miembros de la UIT presentadas en este ciclo, y un resumen de los proyectos y programas en curso del UIT-D en materia de ciberseguridad. Estos anexos ofrecen información de gran utilidad y constituyen materiales básicos para las partes interesadas que deseen ampliar sus conocimientos sobre la ciberseguridad y su función crítica en la era digital.

En esencia, el Informe de resultados de la Cuestión 3/2 del UIT-D para el periodo de estudios 2022-2025 es un plan estratégico para conseguir un elevado nivel de ciberseguridad en todos los miembros de la UIT. Constituye un llamamiento a la acción para lograr un enfoque unificado destinado a asegurar nuestro futuro digital, en el que se destaca la importancia de la concienciación, la educación, la formulación de estrategias, las capacidades de los EIIC, las políticas y estrategias, y la cooperación internacional para hacer frente y mitigar las complejidades de los desafíos en materia de ciberseguridad de cara a la transformación digital.

Abreviaturas y acrónimos

Abreviatura	Término
2G	tecnología móvil de segunda generación
3G	tecnología móvil de tercera generación
3GPP	Proyecto de Asociación Tercera Generación (*3rd generation partnership project*)
4G	tecnología móvil de cuarta generación
5G	tecnología móvil de quinta generación[6]
CE 17	Comisión de Estudio 17 del UIT-T
CISA	Agencia de Ciberseguridad y Seguridad de las Infraestructuras (*Cybersecurity and Infrastructure Security Agency*)
EIIC	equipo de intervención en caso de incidente de ciberseguridad
ENISA	Agencia de la Unión Europea para la Ciberseguridad (*European Union Agency for Cybersecurity*)
ETSI	Instituto Europeo de Normas de Telecomunicaciones (*European Telecommunications Standards Institute*)
FIRST	Foro sobre los equipos de seguridad y respuesta ante incidentes (*Forum of Incident Response and Security Teams*)
GFCE	Foro Mundial de Competencia Cibernética (*Global Forum on Cyber Expertise*)
GSMA	Asociación GSM (*GSM Association*)
IC	infraestructuras críticas
ICG	Índice de Ciberseguridad Global
IoT	Internet de las cosas (*Internet of things*)
NESAS	sistema de garantía de seguridad de equipos de red (*network equipment security assurance scheme*)
NIST	Instituto Nacional de Normas y Tecnología (*National Institute of Standards and Technology*)
OCDE	Organización de Cooperación y Desarrollo Económicos

[6] Si bien en este documento se ha prestado atención a utilizar y reseñar adecuadamente la definición oficial de las generaciones de IMT (véase la Resolución 56 del UIT-R titulada "Denominación de las Telecomunicaciones Móviles Internacionales"), algunas partes de este documento contienen material proporcionado por los miembros que hace referencia a los nombres de mercado frecuentemente utilizados "xG". Puede que dicho material no se corresponda necesariamente con una generación específica de IMT, dado que los criterios subyacentes utilizados por los miembros no se conocen, pero, en general, las IMT-2000, las IMT-Avanzadas, las IMT-2020 y las IMT-2030 se conocen respectivamente como la 3G/4G/5G/6G.

(continuación)

Abreviatura	Término
PIeL	Protección de la Infancia en Línea
PMA	países menos adelantados
RAN	red de acceso radioeléctrico (*radio access network*)
SDN	redes definidas por *software* (*software defined networks*)
SDO	organismo de normalización (*standards development organization*)
SMS	servicio de mensajes breves (*short message service*)
TIC	tecnologías de la información y las comunicaciones
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
UIT-D	Sector de Desarrollo de las Telecomunicaciones de la UIT
UIT-R	Sector de Radiocomunicaciones de la UIT
UIT-T	Sector de Normalización de las Telecomunicaciones de la UIT
UNIDIR	Instituto de las Naciones Unidas de Investigación sobre el Desarme (*United Nations Institute for Disarmament Research*)

Capítulo 1 – Promoción de la sensibilización de los usuarios y la creación de capacidad en materia de ciberseguridad

La implementación de programas contundentes en materia de sensibilización y competencias de ciberseguridad es fundamental para garantizar que podamos seguir aprovechando de manera segura los beneficios de la digitalización. Estas iniciativas en materia de ciberseguridad no solo ayudan a mitigar los riesgos asociados a la suplantación de identidad y otras ciberamenazas, sino que también contribuyen a crear una fuerza de trabajo cualificada capaz de hacer frente a los complejos desafíos de la era digital. En este capítulo se analizan elementos fundamentales y ejemplos destacados, y se sugiere un camino a seguir para los países que deseen hacerlo.

1.1 Sensibilización en materia de ciberseguridad

El error humano sigue siendo un factor importante en las violaciones de la ciberseguridad, dado que, según los estudios, más del 88% de estos incidentes implican alguna forma de error humano[7]. Esto pone de manifiesto la importancia de contar con programas de sensibilización exhaustivos que vayan más allá de las soluciones técnicas y abarquen el elemento humano de la ciberseguridad.

La sensibilización en materia de ciberseguridad hace referencia al enfoque estratégico consistente en educar a las personas, las organizaciones y las comunidades acerca de los riesgos cibernéticos y las buenas prácticas para proteger los activos digitales y la información. El principal objetivo de las iniciativas de sensibilización en materia de ciberseguridad radica en cultivar una cultura de seguridad y empoderar a las personas para que reconozcan, prevengan y respondan de manera eficaz a los riesgos de ciberseguridad. Los programas de sensibilización pueden abarcar diversos métodos y herramientas, como los programas de formación, los simulacros de suplantación de identidad, la utilización de juegos como herramienta educativa y los microprogramas de aprendizaje. Los principales temas que suelen cubrirse en dichas iniciativas van desde la sensibilización en materia de ingeniería social y suplantación de identidad hasta la gestión de contraseñas, la protección de datos y el uso seguro de los dispositivos móviles y los medios sociales.

El impacto de los programas de sensibilización en materia de ciberseguridad bien implementados puede ser importante[8]. Con frecuencia, las organizaciones que dan prioridad a la sensibilización registran importantes disminuciones del número de ataques exitosos por suplantación y mejoras generales de su situación de seguridad (según los estudios, la disminución de los ataques exitosos es de hasta un 70%)[9]. La inversión en la sensibilización en materia de ciberseguridad

[7] https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error
[8] https://www.sciencedirect.com/science/article/pii/S0167404823004959
[9] https://keepnetlabs.com/blog/2024-security-awareness-training-statistics; https://www.knowbe4.com/press/knowbe4-analysis-finds-security-awareness-training-and-simulated-phishing-effective-in-reducing-cybersecurity-risk

también genera un alto rendimiento, dado que los estudios indican que hasta los programas de formación más modestos pueden multiplicar por siete el rendimiento[10]. Además, estos programas contribuyen a crear una cultura de ciberseguridad que va más allá del lugar de trabajo, y ayudan también a las personas a convertirse en "ciberciudadanos" responsables en sus vidas personales. Por otro lado, la sensibilización en materia de ciberseguridad es fundamental para cumplir las normas de la industria y las leyes de protección de datos, como la "Directiva de Seguridad de las Redes y los Sistemas de Información (NIS2)" de la Unión Europea. Muchos sectores obligan a las organizaciones a implementar programas de seguridad para cumplir las normas reglamentarias y evitar posibles multas o consecuencias legales[11].

Según los datos del ICG, 152 países llevaron a cabo campañas de sensibilización en materia de ciberseguridad destinadas a la población general entre 2021 y 2024[12]. Los Estados Miembros de la UIT han puesto en marcha varias iniciativas para aumentar la sensibilización sobre las amenazas a la ciberseguridad. Algunas de estas iniciativas son programas exhaustivos destinados a diversos segmentos de la población. Algunos proyectos se centran específicamente en la ciberdelincuencia y la prevención del fraude, mientras que otros utilizan diversos medios en línea para promover prácticas de higiene cibernética entre la población.

Por ejemplo, un programa exhaustivo adaptado a diversos segmentos de la población es el "Programa de higiene cibernética" de la **Federación de Rusia**. Puesto en marcha en agosto de 2022, constituye una iniciativa trienal exhaustiva cuyo objetivo es mejorar la sensibilización en materia de ciberseguridad entre los ciudadanos de la Federación de Rusia. A fin de propiciar una comunicación más específica y efectiva, el programa dividió a la población en tres grupos de edad: los niños y adolescentes (de 12 a 18 años), los adultos de 18 a 45 años y los adultos mayores de 45 años. Para el grupo de personas de entre 12 y 18 años, que recibe especial atención debido a su vulnerabilidad a las ciberamenazas, se implementaron dos proyectos clave:

- El proyecto titulado "Ciberacoso" presta asesoramiento a las víctimas, agresores y observadores y destaca la importancia de responder al ciberacoso con humor y con una indiferencia saludable.
- El proyecto titulado "Mejora tus competencias de protección" se centra en educar a los niños sobre las estafas en los entornos de juegos en línea.

Para los adultos de 18 a 45 años, algunos de los proyectos incluidos en el programa son:

- "Estilo de vida saludable en la esfera cibernética";
- "Contraseñas complejas y sencillas"; y
- "Aprenda su función".

Estas iniciativas abarcan temas como la protección de los dispositivos móviles, la prevención de la suplantación de identidad, la seguridad de las contraseñas y la sensibilización sobre el fraude telefónico. El programa abarca también las necesidades de los adultos mayores de 45 años, haciendo especial énfasis en su protección contra el fraude telefónico. Además, un curso especializado tiene por objeto mejorar la alfabetización sobre la seguridad de la información entre los funcionarios públicos. Un estudio realizado en toda la Federación de

[10] https://blog.usecure.io/es/cual-es-la-eficacia-de-la-formacion-en-materia-de-seguridad; https://ostermanresearch.com/wp-content/uploads/2021/01/ORWP_0313-The-ROI-of-Security-Awareness-Training-August-2019.pdf
[11] https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/
[12] https://www.itu.int/epublications/es/publication/global-cybersecurity-index-2024

Rusia en 2022 reveló que el índice global de alfabetización cibernética era del 48,2%, y abarcó temas como la protección antivirus, el uso seguro de Internet y la seguridad de los datos personales. El Programa de higiene cibernética está diseñado para ser actualizado cada año, lo que garantiza su continua pertinencia respecto de las nuevas amenazas digitales y la evolución de las necesidades de la población[13].

En la **República de Côte d'Ivoire** se implementó un programa de sensibilización en materia de ciberseguridad, centrado especialmente en la ciberdelincuencia, que formaba parte de un conjunto de iniciativas de sensibilización y formación en materia de ciberseguridad llevadas a cabo por conducto de las principales instituciones del país encargadas de esta esfera. La Plataforma de lucha contra la ciberdelincuencia (PLCC) lleva a cabo campañas de sensibilización en las instituciones educativas, incluidas las escuelas y las universidades, así como las instituciones financieras y religiosas, y publica contenido e información educativa sobre las detenciones de ciberdelincuentes en los medios sociales. El CI-CERT (Côte d'Ivoire – equipo de intervención en caso de emergencia informática), que es el coordinador nacional de la ciberseguridad, ofrece un programa de formación especializado denominado "DIGISEC", para que las empresas e instituciones mejoren sus actividades de sensibilización en materia de seguridad digital en el lugar de trabajo. Otra iniciativa importante reciente fue CyberCAN23, que se llevó a cabo durante la Copa Africana de Naciones de 2024. Este sistema de ciberseguridad, gestionado por el CI-CERT, se centró en crear conciencia sobre las estafas en las plataformas digitales, en especial el fraude por suplantación de identidad. La campaña utilizó las plataformas de los medios sociales, la televisión y la radio para difundir información en materia de ciberseguridad. El país también lleva a cabo una campaña de sensibilización nacional titulada "En ligne tous responsables" (En línea todos somos responsables) en diversas ciudades y municipios[14].

La **República de Rwanda** ha llevado a cabo varias iniciativas para mejorar la sensibilización, educación y formación en materia de ciberseguridad, en particular el Programa nacional de concienciación y formación en ciberseguridad, que promueve la sensibilización sobre la ciberseguridad para los usuarios de Internet y desarrolla al mismo tiempo las capacidades de los profesionales de la ciberseguridad para ayudar a las instituciones públicas y privadas a proteger los sistemas críticos frente a las ciberamenazas[15].

Centrada en la prevención del fraude cibernético, **China** ha trabajado para construir una "red contra el fraude" para toda la sociedad y multidimensional, alentando la instalación de la aplicación del Centro Nacional Contra el Fraude y sensibilizando en pro de la adopción de medidas de higiene cibernética en diversos grupos de la población específicos, como los estudiantes, las personas de edad, los agricultores, etc.[16]

Por último, una iniciativa de **Brasil** centrada en la mejora de las prácticas en materia de higiene cibernética de la población se basa en herramientas de comunicación en línea como YouTube. Brasil ha puesto en marcha iniciativas en materia de higiene cibernética por conducto del organismo nacional encargado de las telecomunicaciones, Anatel. En el marco de su planificación estratégica de 2023-2027, Anatel ha creado un portal específico para la prevención del fraude digital y la higiene cibernética, que ofrece información sobre las amenazas digitales comunes y las estrategias de prevención. Este organismo lleva a cabo periódicamente

[13] Documento 2/71 de la CE 2 del UIT-D, presentado por la Federación de Rusia
[14] Documento SG2RGQ/160 de la CE 2 del UIT-D, presentado por Réseau International Femmes Expertes du Numérique (RIFEN)
[15] Documento 2/35 de la CE 2 del UIT-D, presentado por Rwanda
[16] Documento 2/370 de la CE 2 del UIT-D, presentado por China

eventos de sensibilización con asociados y mantiene una lista de reproducción especializada en ciberseguridad en su canal de YouTube. Otras iniciativas importantes son las campañas #OctoberCyberSafe celebradas en octubre de 2023 y octubre de 2024, y las celebraciones del Día de la Seguridad en Internet en febrero de 2024 y febrero de 2025[17].

1.2 Creación de capacidad en materia de educación y formación sobre ciberseguridad

En un informe elaborado por el Foro Económico Mundial titulado *Global Cybersecurity Outlook 2025* (*Perspectivas mundiales sobre la ciberseguridad de 2025*), se destacó una creciente deficiencia de competencias en materia de ciberseguridad, ya que la brecha de estas competencias creció un 8% desde el anterior informe (publicado en 2024). Dos de cada tres organizaciones comunicaron tener deficiencias críticas de competencias en materia de ciberseguridad, que les impedían cumplir sus requisitos de seguridad. En el informe se destaca la urgente necesidad de llevar a cabo iniciativas para hacer frente a estas deficiencias de capacidades, en particular actividades de formación, reconversión y esfuerzos para contratar y retener a talentos especializados en ciberseguridad[18].

La educación y formación en materia de ciberseguridad puede considerarse un proceso integral diseñado para dotar a las personas de los conocimientos, competencias y capacidades necesarios para proteger los activos digitales, detectar y mitigar las ciberamenazas, y garantizar la seguridad de los sistemas de información. La educación y formación en ciberseguridad abarcan una amplia variedad de temas y enfoques destinados a crear una fuerza de trabajo capaz de hacer frente a la evolución de los desafíos que surgen en el ámbito de la ciberseguridad. La educación y formación en materia de ciberseguridad pueden adoptar diversas formas, como los programas académicos oficiales, las certificaciones profesionales, los talleres prácticos y las iniciativas de aprendizaje continuo.

Los programas de educación y formación en materia de ciberseguridad son fundamentales en el panorama digital actual, dado que ayudan a prevenir las violaciones de datos y a mitigar los riesgos cibernéticos dotando a las personas y los profesionales con los conocimientos y competencias que necesitan para detectar las posibles ciberamenazas y reaccionar ante ellas[19]. La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de Estados Unidos considera que la educación y formación en materia de ciberseguridad son "fundamentales para proteger las infraestructuras críticas de la nación"[20] y destaca el papel esencial que desempeñan los profesionales de la ciberseguridad correctamente formados para salvaguardar la seguridad y los intereses económicos nacionales.

La magnitud y el nivel de aplicación de las políticas de educación y formación en materia de ciberseguridad de los diferentes Estados Miembros de la UIT varía considerablemente, dado que algunos Estados Miembros implementan instrumentos de política exhaustivos para aumentar el número de profesionales de la ciberseguridad en todos los niveles, mientras que otros se centran en programas de formación en ciberseguridad específicos. Algunos Estados Miembros se han centrado en los estudiantes graduados estableciendo programas de

---

17 Documento SG2RGQ/165 de la CE 2 del UIT-D, presentado por Brasil; https://www.youtube.com/playlist?list=PLOmVJ5Ex3R10wEUM3edKTSErojXs_07xg (lista de reproducción sobre ciberseguridad)

18 https://es.weforum.org/publications/global-cybersecurity-outlook-2025/

19 https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students/

20 https://niccs.cisa.gov/education-training

enseñanza terciaria en las universidades, mientras que otros han hecho hincapié en la necesidad de formar a los empleados que forman parte del personal existente. Además, también se han creado varios programas internacionales ejecutados por organismos internacionales. Asimismo, se han observado disparidades en el plano regional, dado que se imparten cursos sobre ciberseguridad en universidades en el 91% de los países europeos, mientras que esa proporción es del 60% en el caso de los países de la región de las Américas y del 61% en el de la región de África[21].

El **Reino Unido** ofrece un ejemplo de enfoque avanzado sobre la educación y las competencias en materia de ciberseguridad, que le ha permitido implementar diversas políticas y programas en todos los niveles para reducir las deficiencias de competencias en materia de ciberseguridad. Su estrategia se centra en tres esferas principales, a saber: las competencias en ciberseguridad para adultos, las competencias en ciberseguridad para jóvenes y el desarrollo de las profesiones cibernéticas. Para los adultos, el Reino Unido ofrece cursos en campamentos intensivos de 12 a 16 semanas de duración, como la iniciativa centrada en la mejora de las competencias cibernéticas, a fin de volver a formar a las personas y mejorar sus competencias en materia de ciberseguridad. Asimismo, el Reino Unido promueve programas de aprendizaje como el Programa de aprendizaje de primer grado en ciberseguridad (CyberFirst), a fin de ofrecer una experiencia profesional práctica. Para los jóvenes, el Reino Unido ha creado un ecosistema de ofertas bajo el lema "CyberFirst". Esto incluye un concurso nacional para niñas interesadas en carreras profesionales en el ámbito de la ciberseguridad, cursos introductorios durante las vacaciones escolares y un programa de reconocimiento para las escuelas que ofrecen programas educativos excelentes en materia de ciberseguridad. La plataforma de aprendizaje faro para los jóvenes en el Reino Unido, Cyber Explorers, es gratuita para todas las personas de entre 11 y 14 años y ha alcanzado una participación casi igualitaria entre los géneros. El Reino Unido está también trabajando para desarrollar las profesiones de la ciberseguridad por conducto del Consejo de Ciberseguridad del Reino Unido (UKCSC). Este órgano profesional tiene por objeto crear trayectorias y normas definidas en la esfera de la ciberseguridad, haciendo que sea más accesible y estructurado para las personas en todas las etapas de su carrera[22].

Brasil ofrece un ejemplo de política de ciberseguridad bien diseñada con enfoque y resultados específicos. El país ha puesto en marcha el programa "Hackers do Bem" (hackers de sombrero blanco) a fin de hacer frente a la identificada carencia de profesionales de la ciberseguridad respecto de 230 000 puestos, mediante la formación de 30 000 personas como profesionales de la ciberseguridad para cubrirlos. El programa es ejecutado por la Red Nacional de Educación e Investigación de Brasil (RNP), SENAI-SP y Softex, con el apoyo del Ministerio de Ciencia, Tecnología e Innovación. El programa sigue un enfoque estructurado en cinco niveles sobre la educación en materia de ciberseguridad. El programa comienza con la fase de nivelación que abarca los conceptos básicos sobre las tecnologías de la información, sigue con los conceptos básicos y fundamentales sobre la ciberseguridad y termina con una formación especializada. El nivel especializado se centra en cinco perfiles profesionales clave, a saber: el Equipo Rojo (evaluación de la seguridad), el Equipo Azul (arquitectura de la seguridad), DevSecOps (seguridad de aplicaciones), CSIRT (respuesta a incidentes) y GRC (gobernanza, riesgo y conformidad). El último nivel incluye un programa semestral de residencia de la ciberseguridad, con una mentoría profesional en los estados de Brasil. A fin de garantizar la sostenibilidad, el programa ha creado un centro nacional de ciberseguridad que conecta a

[21] https://www.itu.int/epublications/es/publication/global-cybersecurity-index-2024
[22] Documento 2/77 de la CE 2 del UIT-D, presentado por el Reino Unido

diversas partes interesadas, en particular las instituciones educativas, los organismos públicos, las empresas y los estudiantes. Este centro nacional de ciberseguridad tiene por objeto adaptar las necesidades de la industria a los resultados educativos y ampliar las oportunidades de formación en materia de ciberseguridad en todo Brasil[23].

Algunos países han estado promoviendo la ciberseguridad en la educación terciaria en un esfuerzo por mejorar las competencias de su población. Por ejemplo, el Gobierno de **Rwanda** ha introducido módulos sobre la seguridad de la información en los programas de tecnologías de la información (TI) e ingeniería informática de los centros de educación terciaria. La Universidad Carnegie Mellon en África (CMU-África) de Kigali ofrece programas que abarcan la ciberseguridad, la ingeniería de *software* y otros temas de las tecnologías de la información y las comunicaciones (TIC). Estos programas de la CMU-África se centran en la enseñanza y la investigación en materia de ciberseguridad y privacidad, desde la seguridad de los sistemas de *software* y de red hasta la mejora de la usabilidad de la seguridad y la privacidad[24].

De manera alternativa, en lugar de centrarse en las instituciones educativas, otros países se han estado dirigiendo a los actores profesionales que ya forman parte del personal, especialmente en los sectores que son más susceptibles a las ciberamenazas. En la **República Argentina**, se han diseñado específicamente programas de formación para los empleados del sector público, que abarcan temas fundamentales sobre la seguridad de los datos y las buenas prácticas en materia de gestión de la información. Estos cursos tienen por objeto dotar a los participantes de conocimientos y competencias esenciales para salvaguardar la privacidad, la confidencialidad, la integridad y la disponibilidad de la información. También se imparte formación especializada a los funcionarios designados coordinadores en materia de ciberseguridad. Las sesiones de formación especializada abarcan temas como los nuevos desafíos de la ciberseguridad, las pruebas digitales, las pruebas de penetración y el refuerzo de los sistemas informáticos[25].

De manera análoga, la **República Árabe Siria** ha organizado actividades de formación destinadas a los empleados del sector público, las universidades y el personal del sector bancario. Un Centro de Excelencia del Organismo Nacional de Servicios de Red ofreció cursos de formación en materia de seguridad de la información, aunque sus actividades se interrumpieron durante la guerra antes de volver a reanudarse en 2021[26].

Egipto creó en 2021 el Centro Africano de Formación en Reglamentación de las Telecomunicaciones de Egipto (EG-ATRC), lo que ilustra el poder de la cooperación regional al ofrecer formación académica y profesional para mejorar las competencias humanas en los países africanos en la esfera de la seguridad de la información y las redes[27].

Otro ejemplo es el Centro de Cibercapacidades de Latinoamérica y el Caribe (LAC4), una iniciativa dirigida por la **Unión Europea**, CyberNet y el Gobierno de la República Dominicana. El LAC4 fomenta las cibercapacidades regionales mediante el intercambio exhaustivo de conocimientos, la formación y el desarrollo de buenas prácticas en materia de ciberseguridad y transformación digital. Situado en Santo Domingo (República Dominicana), el LAC4 sirve de punto central para intercambiar experiencias colectivas, y ayuda a más de 25 países de la región de América Latina y el Caribe a reforzar los marcos de ciberseguridad y a fomentar

---

23 Documento SG2RGQ/184 de la CE 2 del UIT-D, presentado por Brasil
24 Documento 2/35 de la CE 2 del UIT-D, presentado por Rwanda
25 Documento 2/150 de la CE 2 del UIT-D, presentado por Argentina
26 Documento SG2RGQ/163 de la CE 2 del UIT-D, presentado por la República Árabe Siria
27 Documento 2/329 de la CE 2 del UIT-D, presentado por Egipto

la cooperación regional. Algunas de las diversas actividades de formación y cibersimulacros del LAC4 versan sobre la concienciación, la gestión de los riesgos cibernéticos, la protección de las infraestructuras críticas y la conformación de políticas y leyes en materia de ciberseguridad. Asimismo, ofrece numerosas sesiones de formación técnica destinadas a mejorar las competencias y conocimientos de los profesionales de la ciberseguridad en toda la región. Cabe señalar que el LAC4 hace hincapié en la diversidad de género en el ámbito de la ciberseguridad, y organiza talleres de formación especializada destinados a empoderar a las mujeres en este ámbito. Estos esfuerzos son fundamentales para constituir una fuerza de trabajo diversa y resiliente en materia de ciberseguridad, capaz de hacer frente a la evolución de los desafíos que se presentan en el panorama digital[28].

Los cibersimulacros, que simulan ciberataques, incidentes de seguridad de la información y otro tipo de alteraciones, son un componente importante de las iniciativas de capacitación en materia de ciberseguridad, y han sido el centro de atención de los esfuerzos realizados por la Oficina de Desarrollo de las Telecomunicaciones de la **UIT** (BDT), como medio para mejorar las capacidades de los países respecto de la preparación, protección y respuesta a incidentes de ciberseguridad. La UIT organiza cibersimulacros regionales y mundiales, así como ejercicios nacionales, y elabora materiales para apoyar estas iniciativas[29].

Dado que la ciberseguridad va adquiriendo importancia en la agenda política mundial, las organizaciones internacionales también se han introducido en esta esfera con programas destinados a mejorar las competencias cibernéticas de las generaciones futuras. Algunos esfuerzos internacionales importantes son los programas llevados a cabo por la UIT. El programa Her CyberTracks de la BDT es un proyecto que consta de tres partes e incorpora actividades de formación técnica en línea y presenciales en materia de diplomacia y política de ciberseguridad, cursos de formación sobre aptitudes interpersonales, círculos de mentorías mensuales guiadas, ponencias inspiradoras y eventos regionales de constitución de redes de contactos. Todas estas actividades se ponen a disposición en forma de un programa holístico complementario y centralizado inscrito en el marco del proyecto "Política y diplomacia". El objetivo del proyecto es promover la representación y participación de las mujeres, así como intentar mejorar su contribución a los procesos nacionales e internacionales en materia de política de ciberseguridad[30].

1.3 Protección de la infancia en línea

Según el Global Child Safety Institute (Childlight), uno de cada ocho niños de todo el mundo (o aproximadamente 302 millones de jóvenes) han sido víctimas de tomas, compartición y exposición a imágenes y vídeos sexuales en 2024[31].

La protección y seguridad de la infancia en línea hacen referencia a las medidas, prácticas y estrategias implementadas para salvaguardar a los niños y jóvenes frente a los posibles riesgos y amenazas en el entorno digital. La protección de la infancia en línea abarca diversos esfuerzos destinados a crear una experiencia en línea segura para los menores, incluida la protección

[28] Documento SG2RGQ/117 de la CE 2 del UIT-D, presentado por la República Dominicana
[29] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx
[30] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx
[31] https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa

contra varias formas de abuso en línea como la explotación sexual y la seducción[32], la exposición a contenidos perniciosos e inapropiados para la edad, el ciberacoso, la pornografía y el uso de plataformas en línea para llevar a cabo actividades ilegales[33].

La protección y seguridad de la infancia en línea es fundamental en la era digital actual, en la que los niños están cada vez más expuestos a Internet y a sus posibles riesgos, por lo que la educación sobre la seguridad en línea es esencial para empoderar a los niños a navegar de manera responsable por el mundo digital. Si educamos a los niños sobre los riesgos en línea, el pensamiento crítico y el comportamiento responsable en línea, pueden desarrollar las competencias necesarias para protegerse y adoptar decisiones informadas en línea[34].

Las contribuciones de los Estados Miembros demuestran que los países se han tomado muy en serio la protección de la infancia en línea en los últimos años, y que han utilizado diversos instrumentos para garantizar la seguridad de los niños en línea. Según los datos del ICG, a nivel mundial, el 69% de los gobiernos han llevado a cabo campañas destinadas específicamente a los padres, educadores y niños como parte de sus esfuerzos en materia de protección de la infancia en línea[35]. Varios países han estado elaborando marcos legales y políticos exhaustivos, así como programas y herramientas de utilidad para salvaguardar el entorno en línea para los niños. Se han recabado pruebas empíricas sobre la conducta de los niños en línea a fin de entender y encarar mejor algunas de las cuestiones más desafiantes de la seguridad en línea. Los países han reconocido la importancia de la adopción de soluciones entre múltiples interesados, que reúnan a las partes interesadas adecuadas para hacer frente a este problema multifacético. Por último, los países han llevado a cabo programas que combinan la sensibilización en materia de ciberseguridad con la seguridad en línea, lo que demuestra la importancia de adoptar un enfoque integral.

Australia constituye un ejemplo de país que ha decidido aprobar un sólido marco jurídico para hacer frente a la cuestión de la protección de la infancia en línea. En 2021, el Gobierno estableció un marco contundente mediante la aprobación de la Ley de Seguridad en Línea, que aborda el ciberacoso, el ciberabuso adulto y el abuso por imágenes. En 2022, Australia creó también el Consejo de la Juventud para la Seguridad Electrónica, formado por 24 miembros de 13 a 24 años, que contribuye directamente a las políticas y programas y trabaja con las principales empresas tecnológicas para mejorar la responsabilidad de los usuarios[36].

China es otro país que dispone de una política exhaustiva en materia de protección de la infancia en línea, y que ha implementado programas educativos de gran alcance sobre la seguridad de Internet. Las escuelas constituyen el canal principal para impartir educación en materia de ciberseguridad, alcanzando al 90,3% de los menores, mientras que las familias son el segundo canal más importante al llegar al 61,7% de dicha población. En total, el 85,4% de los menores han recibido alguna forma de educación sobre la seguridad en Internet. El programa titulado "Protección de los menores en la banda ancha" se estableció por conducto de los operadores de telecomunicaciones nacionales, ha ayudado a proteger a 160 millones

---

[32] Según el artículo 23 del Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual, la seducción puede definirse como la propuesta deliberada de un adulto, a través de las tecnologías de la información y las comunicaciones, de reunirse con un niño menor de edad legal para actividades sexuales, con el fin de abusar sexualmente de él o producir material de abuso sexual infantil. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201

[33] https://www.nspcc.org.uk/keeping-children-safe/online-safety/

[34] https://www.cois.org/about-cis/child-protection/resources; https://learning.nspcc.org.uk/online-safety

[35] https://www.itu.int/epublications/es/publication/global-cybersecurity-index-2024

[36] Documento 2/167 de la CE 2 del UIT-D, presentado por Australia

de familias con niños en edad escolar y tiene la capacidad de gestionar más de 1 020 millones de llamadas. Asimismo, el Gobierno ha iniciado campañas específicas para abordar las preocupaciones relativas a la seguridad en línea. China ha aprobado varias políticas clave, en particular un reglamento sobre la protección de la información personal de los niños en la red y un reglamento sobre la protección de los menores en Internet. La eficacia de estos programas se reveló en las estadísticas: más del 70% de los menores pueden reconocer ahora el fraude en línea, y más de la mitad demuestran ser conscientes del uso saludable de Internet[37].

Otros países también han estado combinando la sensibilización en materia de ciberseguridad con la educación sobre la seguridad en línea. Por ejemplo, la **Federación de Rusia** ha puesto en marcha la "Campaña de alfabetización digital" como parte de su programa nacional más amplio sobre "economía digital", iniciado en 2018. El programa ofrece contenidos mediante vídeos interactivos animados que cubren temas esenciales de la ciberseguridad como la detección de la suplantación de identidad, la protección de la información personal, la respuesta al ciberacoso, las prácticas seguras en los medios sociales y la verificación de la información. También se cubren esferas específicas como la sensibilización sobre los derechos de autor, la prevención del fraude en línea, la protección contra los virus informáticos, la cortesía digital y la seguridad del dinero electrónico. A fin de garantizar una implementación eficaz, la campaña proporciona a los docentes materiales metodológicos para integrar estas lecciones de ciberseguridad en las clases de informática y en las reuniones entre padres y docentes[38].

Varias administraciones públicas han establecido herramientas tecnológicas específicas para proteger a los niños en línea. Como parte de una estrategia nacional más amplia de protección y empoderamiento de la infancia y la juventud en línea, **Côte d'Ivoire** puso en marcha el sitio web "jemeprotegeenligne.ci" (me protejo en línea)[39], que ofrece herramientas interactivas, motores de búsqueda y sitios de medios sociales específicamente diseñados para los niños. El sitio incluye también un mecanismo de denuncia que permite a los usuarios denunciar de manera anónima y discreta los abusos. La iniciativa implica la colaboración entre varias partes interesadas y recibió el apoyo de la Fundación Internet Watch[40].

Además, los países y las organizaciones también han reconocido la necesidad de incluir a varias partes interesadas en el proceso de protección de la infancia en línea. En **Nigeria**, la "Iniciativa de Protección de la Infancia en Línea" constituye el principal marco, que incorpora las políticas en los términos y condiciones de los proveedores de servicios de Internet. Como uno de los principales actores de la esfera política en el país, la Comisión de Comunicaciones de Nigeria (NCC) ha constituido mecanismos de denuncia de contenidos de maltrato infantil y ha implementado medidas para bloquear dicho material[41]. La **República de Zambia** puso en marcha la "Estrategia Nacional de Protección de la Infancia en Línea" en 2020 y su plan de implementación quinquenal (2020-2024) centrado en las estructuras organizativas, la creación de capacidad, las medidas jurídicas, la cooperación internacional y los procedimientos técnicos. Zambia identificó varias lecciones aprendidas como la ampliación de la colaboración entre las partes interesadas, la financiación sostenible y sostenida, y la creación de un sólido marco de seguimiento y evaluación[42]. Por último, la Iniciativa de Protección de la Infancia en Línea de la **UIT** constituye una plataforma de liderazgo mundial que abarca una comunidad de múltiples

[37] Documento SG2RGQ/212 de la CE 2 del UIT-D, presentado por China Mobile Communications Co. Ltd.
[38] Documento SG2RGQ/170 de la CE 2 del UIT-D, presentado por la Federación de Rusia
[39] https://www.jemeprotegeenligne.ci/
[40] Documentos 2/34 y 2/137 de la CE 2 del UIT-D, presentados por Côte d'Ivoire
[41] Documento SG2RGQ/20 de la CE 2 del UIT-D, presentado por Nigeria
[42] Documento SG2RGQ/114 de la CE 2 del UIT-D, presentado por Zambia

partes interesadas y goza de una experiencia probada y un exitoso historial de asistencia técnica de más de diez años en las actividades de protección de la infancia en línea en todo el mundo. Formada por más de 80 asociados para el conocimiento, algunas de las actividades de protección de la infancia en línea son la elaboración de materiales para niños[43], la creación de directrices para padres y educadores[44], la industria[45] y los encargados de formular políticas[46], la impartición de formación en línea por conducto de la Academia de la UIT, y la organización de actividades de formación presenciales para educadores y jóvenes[47]. Las directrices señaladas anteriormente representan un conjunto exhaustivo de recomendaciones para todas las partes interesadas sobre cómo contribuir al desarrollo de un entorno en línea seguro y habilitador para niños y jóvenes. Estas directrices se han elaborado y difundido por conducto de su traducción, adaptación al contexto y la realización de campañas de sensibilización.

Varios países también se han centrado en actividades de creación de capacidad y en la recopilación de datos empíricos para entender la manera en que los niños interactúan en línea. En **Kenya**, la Autoridad de Comunicaciones llevó a cabo las campañas tituladas "Be the COP" y "Huwezi Tucheza, Tuko Cyber Smart", destinadas a los padres, tutores, docentes y jóvenes. Kenya, en colaboración con el Instituto Africano de Telecomunicaciones Avanzadas, también ha creado recursos educativos e iniciativas de creación de capacidad, como un programa de formación sobre la protección de la infancia en línea y medidas de seguridad. Este programa ha impartido formación sobre la protección de la infancia en línea y la seguridad a 951 participantes de varios sectores. Asimismo, Kenya está llevando a cabo un estudio nacional sobre la protección y seguridad de la infancia en línea con el fin de recabar datos empíricos sobre el comportamiento de los niños en línea. Estaba previsto que concluyese este estudio nacional en 2024[48].

43 https://www.itu-cop-guidelines.com/children
44 https://www.itu-cop-guidelines.com/parentsandeducators
45 https://www.itu-cop-guidelines.com/industry
46 https://www.itu-cop-guidelines.com/policymakers
47 https://www.itu-cop-guidelines.com/
48 Documento 2/119 de la CE 2 del UIT-D, presentado por Kenya

Capítulo 2 – Experiencias sobre prácticas de garantía de la ciberseguridad

Las prácticas de garantía de la ciberseguridad se han convertido en un elemento esencial para la protección de redes, sistemas y datos contra actividades maliciosas[49]. En líneas generales, las prácticas de garantía de la ciberseguridad se refieren a los procedimientos utilizados para garantizar que se aplican controles pertinentes para proteger la confidencialidad, integridad y disponibilidad de los dispositivos, sistemas, redes y datos electrónicos. Si bien las prácticas de garantía de la ciberseguridad no previenen directamente los ataques cibernéticos, su objetivo, si se implementan correctamente, es minimizar el riesgo de estos ataques. Las prácticas de garantía de la ciberseguridad pueden contrastarse con los controles, directrices y normas de seguridad específicos y pueden ser impuestas por reglamentos o adoptadas voluntariamente por la industria. Sin embargo, no existe un enfoque único para todos, ya que las autoridades nacionales y los reguladores del sector a menudo emplean prácticas diferentes, desde autoevaluaciones y directrices voluntarias hasta sistemas de etiquetado y controles rígidos de cumplimiento.

Si bien no hay un único enfoque recomendado, es evidente que, en los últimos años, se ha producido un movimiento sostenido hacia la adopción de prácticas para garantizar la ciberseguridad en todo el mundo, con diferentes evoluciones en varios países y regiones. Como ejemplo de este impulso, la **Organización de Cooperación y Desarrollo Económicos (OCDE)** lanzó en diciembre de 2022 la Recomendación del Consejo sobre la "seguridad digital de los productos y servicios", que recomienda la adopción de políticas para mejorar la seguridad digital de los productos y servicios que sean proporcionales al riesgo, comenzando con un enfoque moderado basado en medidas políticas voluntarias, y estudiando después la necesidad de adoptar medidas obligatorias[50]. Este capítulo transmite los desafíos afrontados, evalúa los efectos y presenta las lecciones extraídas hasta la fecha, respecto de la definición y aplicación de prácticas de garantía de la ciberseguridad.

2.1 Enfoques para valorar la criticidad, los riesgos y los costes

Al considerar la aplicación de prácticas para garantizar la ciberseguridad, es crucial determinar en primer lugar lo que una entidad está tratando de proteger y los riesgos a los que se enfrentan los activos identificados. Los países y las empresas que desean protegerse contra los ciberataques deben, con carácter prioritario, identificar qué sistemas y activos necesitan protección y evaluar sus vulnerabilidades. En este sentido, disponer de un marco o un plan para realizar evaluaciones de riesgos es una herramienta útil. Uno de los marcos más conocidos es el Marco de ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST) de **Estados**

[49] La seguridad operacional está estrechamente ligada a las prácticas para garantizar la ciberseguridad, en el sentido de que la primera puede constituir una buena base para las segundas. Broadcom presentó el modelo de buenas condiciones destacando que está compuesto por cuatro elementos clave, a saber: las personas y los procesos, el conocimiento, los productos de seguridad (seguridad exógena) y la seguridad de los activos (seguridad endógena). Véase "Reduce Risk and Protect Reputation" (Reducir los riesgos y proteger la reputación), Documento SG17-C214 de la CE 17 del UIT-T, presentado por Broadcom Corporation.

[50] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

Unidos[51], que se ha actualizado recientemente[52] y que ofrece un enfoque ampliamente utilizado para ayudar a determinar y minimizar los riesgos organizacionales. Establece directrices no reglamentarias que permiten a las organizaciones de todo el mundo identificar su propio panorama de riesgos y aplicar los controles de ciberseguridad adecuados. El marco revisado, publicado a principios de 2024, se basa en un compromiso amplio y a largo plazo con la comunidad de partes interesadas que utilizan estas directrices, así como en la armonización continua con otras normas internacionales[53].

La posición del NIST como agencia no reguladora ha permitido lograr un compromiso más profundo con las partes interesadas de la industria de todo el mundo para comprender mejor los desafíos del mundo real y recibir comentarios, que se han incorporado a las nuevas directrices[54]. Estas directrices están destinadas a ser adaptables y flexibles, y aplicables a todas las organizaciones y sectores. **BitSight** integra el Marco de ciberseguridad del NIST en su plataforma que ha sido utilizada por diversas agencias gubernamentales responsables de la ciberseguridad (como los equipos de intervención en caso de emergencia informática, las agencias nacionales de ciberseguridad y los organismos reguladores de las telecomunicaciones)[55]. A través de la plataforma, los países pueden realizar evaluaciones de riesgos de sus infraestructuras y activos considerados esenciales y medir sus factores de riesgo.

Las evaluaciones de riesgos también pueden ayudar a determinar qué nivel de garantía es apropiado teniendo en cuenta la sensibilidad de los datos y activos protegidos, las consecuencias que tendría una violación y el entorno de las amenazas (es decir, si una entidad es susceptible de sufrir un ciberataque). En algunos casos, los niveles de garantía vendrán dictados por requisitos reglamentarios. Cuanto mayor sea el nivel de garantía, más estrictos serán los controles de seguridad. Por ejemplo, un nivel bajo de garantía requeriría una contraseña del sistema o un cortafuegos, mientras que un nivel de garantía más alto requeriría la adición de controles más avanzados, como el cifrado avanzado y la autenticación multifactor.

Si bien las prácticas para garantizar la ciberseguridad aumentan los presupuestos de la tecnología de la información, la no aplicación de controles de seguridad puede ser aún más costosa. Los costes inducidos por un ataque cibernético no solo se miden en términos financieros, ya que el coste adicional para la reputación puede ser mucho más perjudicial. La pérdida de confianza de los clientes y ciudadanos tiene un efecto a largo plazo que trasciende el ámbito económico, y las organizaciones deben ser capaces de entenderlo estratégicamente. Del mismo modo, para el sector público, los ataques fructuosos pueden afectar la prestación de servicios públicos y la realización de actividades críticas, y la interrupción de dichos servicios y actividades tampoco puede medirse únicamente en términos financieros, ya que afecta a la vida de los ciudadanos.

La planificación y elaboración de presupuestos de inversión en la esfera de la ciberseguridad para garantizar el cumplimiento de las normas nacionales pueden resultar difíciles para diferentes organizaciones. A fin de ayudar a las organizaciones a planificar sus costes para los controles de ciberseguridad exigidos por la ley, la Autoridad Nacional de Ciberseguridad (NCA) del **Reino de Arabia Saudita** ha desarrollado una herramienta de estimación de costes para aplicar

[51] https://www.nist.gov/cyberframework
[52] https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
[53] https://www.nist.gov/cyberframework
[54] Presentación del taller Q3/2_2023_07 de la CE 2 del UIT-D por Estados Unidos
[55] Presentación del taller Q3/2_2023_02 de la CE 2 del UIT-D por BitSight

los "controles fundamentales de ciberseguridad" del país[56]. Tras las primeras pruebas, la NCA concluyó que la herramienta de estimación de costes era eficaz y proporcionaba una buena estimación, especialmente para las organizaciones en las primeras etapas de aplicación de controles relacionados con la ciberseguridad y que, por consiguiente, carecían frecuentemente de un historial sobre la estimación del presupuesto, tiempo o recursos necesarios para aplicar dichos controles de ciberseguridad.

2.2 Enfoques de múltiples partes interesadas

Es importante comparar unas iniciativas con otras para comprender las buenas prácticas y aprender de los éxitos y errores de los demás durante la elaboración de una iniciativa. También es importante colaborar con múltiples partes interesadas, en particular de la industria, con miras a obtener información importante para el desarrollo de la iniciativa.

Aunque en los PMA las prácticas para garantizar la ciberseguridad sean cada vez más necesarias, estas pueden ser aún difíciles de implementar. El caso de Cyber Defense Africa (CDA) en **Togo** puede servir para explicar las dificultades que encaran algunos de los Operadores de Servicios Esenciales (OSE) en los mercados locales para garantizar la ciberseguridad[57]. Se citaron algunas de las dificultades encontradas como la falta de financiación, la falta de confianza en el Gobierno como proveedor de servicios y la falta de capacidad e instalaciones humanas locales. Para ayudar a los OSE a cumplir los controles de ciberseguridad recientemente publicados, el Gobierno de Togo creó una alianza público-privada con un gran proveedor de ciberseguridad de renombre con el fin de proporcionar servicios de ciberseguridad en los sectores público y privado. A través de este modelo de asociación, Togo creó la CDA como un proveedor local de ciberseguridad autosuficiente y de alta calidad para apoyar a los OSE sin carácter obligatorio. El modelo autosuficiente utilizado permitió a Togo reducir los numerosos problemas mencionados y comenzar a fomentar el talento local en el ámbito de la ciberseguridad, así como a impulsar el desarrollo del mercado local. Se señaló la importancia de la CDA como entidad privada en un mercado competitivo a fin de garantizar la adaptabilidad, la alta calidad de los servicios y la fijación de precios competitivos.

También es importante fomentar la cooperación entre los responsables de formular políticas que pueden determinar el entorno reglamentario y las organizaciones de la sociedad civil. Las organizaciones de la sociedad civil pueden aumentar la demanda de seguridad, así como fundamentar el desarrollo de políticas y normas sobre la base de prácticas regionales e internacionales existentes e identificadas. Por ejemplo, la **DiploFoundation** es una organización internacional que ofrece programas de formación y conocimientos especializados en materia de creación de capacidad a gobiernos, organismos reguladores, empresas y la sociedad civil sobre cuestiones de actualidad relacionadas con la ciberseguridad, y que también participa en el "Diálogo de Ginebra sobre el comportamiento responsable en el ciberespacio"[58]. En 2020, del Diálogo de Ginebra emanó una colección de buenas prácticas[59] que incluye sugerencias de definiciones sobre el diseño seguro y la gestión de vulnerabilidades, la elaboración de modelos sobre amenazas, la seguridad de terceros y de la cadena de suministro, el desarrollo seguro, la gestión y divulgación de vulnerabilidades, así como la cultura institucional.

---

[56] Documento SG2RGQ/201 de la CE 2 del UIT-D, presentado por Arabia Saudita
[57] Presentación del taller Q3/2_2023_09 de la CE 2 del UIT-D por Cyber Defense Africa
[58] Presentación del taller Q3/2_2023_11 de la CE 2 del UIT-D por DiploFoundation
[59] https://genevadialogue.ch/goodpractices/

El **GFCE** es una plataforma internacional que apoya la coordinación de proyectos, promueve el intercambio de conocimientos y experiencias, hace coincidir las solicitudes con ofertas de apoyo a la creación de capacidad, y desarrolla proyectos de investigación[60]. El GFCE estableció cuatro centros regionales en las islas del Pacífico, en África, en América y el Caribe, y en el sudeste asiático. Dada su presencia mundial y su diverso apoyo prestado en los países en desarrollo, el GFCE está en condiciones de proporcionar opiniones regionales más diversas sobre las necesidades y demandas de la cibercapacitación. El GFCE incluye un portal en línea que sirve de repositorio de los proyectos implementados y en curso en materia de cibercapacitación, así como de recursos y herramientas. El portal en línea del GFCE contribuye a reducir la duplicación de esfuerzos y también ayuda a identificar deficiencias y patrones en la prestación de servicios de fomento de la capacidad[61].

2.3 Evolución de los enfoques reglamentarios

En muchos casos, las prácticas para garantizar la ciberseguridad se introducen como voluntarias antes de convertirse en obligatorias. El cambio a su obligatoriedad generalmente ocurre cuando los gobiernos consideran que la industria no está haciendo lo suficiente para asegurar los productos y que los consumidores no tienen necesariamente el conocimiento necesario para evaluar si los productos son seguros o no. Esto puede llevar a los gobiernos y las autoridades nacionales a actuar y estipular prácticas de garantía que esperan que cumpla la industria. Ya se trate o no de una obligación impuesta por la ley, es conveniente revisar y adaptar las prácticas de garantía de la ciberseguridad a lo largo del tiempo en vista del panorama dinámico de las amenazas y la evolución de los riesgos de ciberseguridad.

Por ejemplo, en **Brasil**, el organismo regulador de las telecomunicaciones, Anatel, ofrece un ejemplo de enfoque evolutivo al crear un sistema de organismos de certificación y laboratorios de pruebas en el país para la certificación de equipos en las instalaciones del cliente (CPE) o de pasarelas domésticas. El enfoque inicial de Anatel era proporcionar directrices sobre ciberseguridad no obligatorias para el sector de las telecomunicaciones. Sin embargo, tras realizar evaluaciones de riesgos se determinó que las recomendaciones no eran suficientes para asegurar los CPE, dadas las vulnerabilidades y amenazas asociadas a este tipo de equipos, y que era necesario establecer requisitos mínimos de seguridad obligatorios para estos productos. Los requisitos obligatorios para los proveedores de servicios de telecomunicaciones en Brasil se publicaron a principios de 2023 y se centran en vulnerabilidades como las contraseñas no seguras y las partes de servicio habilitadas innecesariamente[62]. Los requisitos entraron en vigor a principios de 2024 como parte de las pruebas de laboratorio obligatorias para la aprobación del producto[63]. Anatel explicó que solo era posible evolucionar desde un enfoque no obligatorio hasta un requisito de certificación obligatoria de la ciberseguridad para un conjunto específico de equipos si se mantenía un amplio debate con el sector.

Del mismo modo, en **Arabia Saudita**, la NCA destacó su iniciativa para construir un ecosistema de verificación y validación independiente (IV&V)[64] a fin de probar y certificar productos desde una perspectiva de la garantía de la ciberseguridad a nivel nacional. Además, la iniciativa tiene

---

60 Presentación del taller Q3/2_2023_12 de la CE 2 del UIT-D por el Foro Mundial de Competencia Cibernética
61 https://cybilportal.org/
62 Documento SG2RGQ/58 de la CE 2 del UIT-D, presentado por Brasil
63 Presentación del taller Q3/2_2023_12 de la CE 2 del UIT-D por Brasil; https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1505; y https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2023/1850-ato-2436
64 https://nca.gov.sa/en/news?item=535

por objeto identificar y clasificar los equipos y programas informáticos que sean altamente sensibles a los riesgos y amenazas cibernéticos. La iniciativa también busca contribuir al desarrollo de capacidades humanas en materia de IV&V. La hoja de ruta para la iniciativa considera comenzar con un programa voluntario antes de dar obligatoriedad a la garantía de la ciberseguridad. La agencia también indicó la importancia de que dicho ecosistema finalmente se convirtiese en "autosostenible", lo que ha alimentado el enfoque adoptado por la NCA para alentar a las partes interesadas del mercado a realizar dichas evaluaciones de IV&V.

En el ámbito de la seguridad de la Internet de las cosas (IoT), el Reino Unido y Australia también presentaron estudios de caso sobre la evolución de un enfoque de garantía de la ciberseguridad voluntario a un enfoque obligatorio. En los últimos años, ambos países han decidido exigir, mediante leyes, un requisito de seguridad básico para los productos de consumo IoT basado en la norma EN 303 645[65] del Instituto Europeo de Normas de Telecomunicaciones (ETSI), que es la primera norma de ciberseguridad aplicable a nivel mundial para dispositivos IoT de consumo.

En el **Reino Unido**, los fabricantes, importadores y distribuidores estarán obligados a cumplir tres de las 13 directrices de seguridad del ETSI, y la ley otorga poderes al Gobierno para adoptar requisitos adicionales si es necesario, dependiendo de las evaluaciones periódicas de amenazas. La decisión de imponer una base de requisitos de seguridad se tomó tras un periodo de adopción voluntaria. En 2018, el país formuló un código de prácticas voluntario[66] para la seguridad de la IoT del consumidor, pero el cumplimiento de la industria no fue el esperado. La evidencia recopilada a través de ejercicios de consulta mostró que los consumidores valoran la seguridad y están dispuestos a pagar un precio mayor por productos seguros. Sin embargo, las amenazas de ciberseguridad no están sujetas al mismo nivel de regulación robusta que la seguridad del producto, lo que lleva a una falta de transparencia por parte de los fabricantes y a una adopción más lenta de las políticas de seguridad. La evidencia también determinó que el mercado de productos de consumo conectables desincentiva la adopción de características básicas de seguridad, ya que la inmensa mayoría de los consumidores asumen que los productos ya son seguros. El régimen en materia de Seguridad de los Productos e Infraestructura de las Telecomunicaciones (PSTI) tiene por objeto subsanar esta deficiencia imponiendo elementos del código de prácticas para garantizar que los fabricantes sean conscientes de las vulnerabilidades y tomen medidas para mitigarlas. El régimen PSTI entró en vigor en abril de 2024 y se aplica a cualquier producto de consumo que pueda conectarse a Internet[67].

De manera análoga, en **Australia**, el Gobierno determinó que había una baja adopción de su código de prácticas voluntario titulado "Protección de la Internet de las cosas para los consumidores", publicado en 2020. En 2024, el Gobierno propuso una ley que impondría la obligatoriedad del código de prácticas, y la propuesta de ley fue objeto de consenso tras una consulta pública. La ley se ajusta en gran medida al enfoque del Reino Unido, que tiene por objeto otorgar facultades al Ministro para imponer la obligatoriedad de normas de seguridad específicas para los dispositivos de IoT por conducto de la legislación secundaria (reglamento). Al incorporar las normas en un reglamento en lugar de hacerlo en la legislación primaria, el Gobierno de Australia tiene la intención de actualizar estas normas rápidamente a fin de

[65] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
[66] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[67] Presentación del taller Q3/2_2023_03 de la CE 2 del por Estados Unidos

garantizar la protección de los consumidores en Australia sobre la base de las buenas prácticas internacionales y de la industria[68].

En el **Reino Unido**, uno de los desafíos identificados es el posible impacto en las pequeñas empresas y las microempresas que podrían enfrentar dificultades para cumplir con el nuevo régimen PSTI. La autoridad encargada del cumplimiento del PSTI en el Reino Unido está elaborando directrices para mitigar los posibles efectos desproporcionados. Además de trabajar con la industria, el Reino Unido observó que los tres requisitos principales que se exigirían en el sistema se habían identificado y comunicado de manera transparente durante varios años. Durante este periodo, el Reino Unido ha realizado una serie de ejercicios sobre el proceso de implementación del régimen, incluidos los requisitos de contraseña, la arquitectura fundamental del producto, la exposición a la vulnerabilidad y los requisitos de transparencia de seguridad. La evaluación del impacto ha demostrado que se espera que los beneficios globales de reducir el volumen de ciberataques a consumidores y empresas superen los costos asociados con la implementación del régimen PSTI. Dado que la Ley PSTI (2022) es el primer instrumento legislativo obligatorio sobre productos de ciberseguridad en el mundo, el costo de hacer cumplir el régimen es incierto, pero las estimaciones iniciales sugieren que los fondos asignados serán suficientes.

En algunos casos, la diferencia entre si una práctica de aseguramiento de la ciberseguridad es obligatoria o sigue siendo voluntaria viene dictada por el tipo de usuario o cliente. Por ejemplo, la **República de Corea** lanzó su Programa de garantía de seguridad en la nube (CSAP), una certificación de seguridad para los servicios de computación en la nube[69]. En general, esta certificación es voluntaria. No obstante, los clientes del sector público (las agencias públicas) deben utilizar un servicio en la nube que haya obtenido la certificación CSAP de conformidad con la reglamentación pertinente y, por tanto, los proveedores de servicios en la nube deben obtener la certificación CSAP cuando prestan servicios en la nube a organismos públicos.

La realización de auditorías internas periódicas que pueden ayudar a identificar deficiencias en los controles y el riesgo de exposición, así como las suscripciones a la inteligencia de amenazas, se consideran buenas prácticas. Incluso si un producto está certificado, podría, a lo largo de su ciclo de vida, sufrir fallas de seguridad. Los planes de certificación requieren la presentación de información en un momento específico, por lo que el proceso no tiene en cuenta los cambios dinámicos de las amenazas en el futuro. Un estudio reciente de BitSight mostró una fuerte correlación entre una mala "cadencia de parches" para las vulnerabilidades y la probabilidad de experimentar un incidente de ciberseguridad[70], señalando la importancia crítica de actualizar los sistemas tan pronto como estén disponibles los parches de seguridad, teniendo en cuenta la diversa distribución de parches en todo el mundo.

Las pruebas de penetración, o "pen-testing", son un ejercicio de garantía de seguridad que ayuda a evaluar la seguridad de un sistema de TI e identificar vulnerabilidades que de otro modo podrían utilizarse para explotar sistemas. OFCOM, organismo regulador de las comunicaciones del **Reino Unido**, ejecuta voluntariamente con los proveedores de telecomunicaciones el plan TBEST. Este sistema de prueba de penetración tiene por objeto simular un ciberataque a fin de identificar vulnerabilidades de seguridad que, a continuación, puedan ser resueltas mediante

---

68 Documento 2/320 de la CE 2 del UIT-D, presentado por Australia

69 https://isms.kisa.or.kr/main/csap/intro/index.jsp y Documento SG2RGQ/34 de la CE 2 del UIT-D, presentado por la República de Corea

70 https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

un proceso de reparación para mejorar el nivel de seguridad de la red de los operadores[71], [72]. De manera más general, este sistema es un ejemplo del enfoque de supervisión que está adoptando OFCOM, en el que se hace hincapié en la importancia de establecer relaciones de colaboración con la industria regulada por dicha autoridad. Hasta la fecha, todos los proveedores de comunicaciones del Reino Unido se han sometido o están aplicando el plan TBEST voluntariamente y han implementado cambios como resultado de ello. TBEST no constituye una "norma" ni un proceso de certificación. El objetivo consiste en permitir a los proveedores de servicios de comunicación tomar conciencia de las ciberamenazas e implementar los cambios apropiados de manera oportuna para mejorar sus capacidades de ciberdefensa. Al conocer y abordar dichas vulnerabilidades y debilidades, los operadores se encuentran en una posición mucho más fuerte para proteger sus redes.

2.4 Educar a los consumidores y los fabricantes

Se han hecho esfuerzos para educar a la población sobre la importancia de la ciberseguridad y las ventajas de elegir productos más seguros.

Uno de ellos es el desarrollo de un sistema de etiquetado de ciberseguridad en el que, como ejemplifica la **República de Singapur**, los productos certificados pueden ir acompañados de una etiqueta. Los sistemas de etiquetado sirven principalmente como una herramienta informativa para los consumidores. En Singapur, la Agencia de Ciberseguridad (CSA), responsable del sistema de etiquetado de ciberseguridad, tiene por objeto ayudar a los consumidores a distinguir entre los dispositivos IoT más seguros y los menos seguros[73]. El sistema es voluntario (con la excepción de los enrutadores Wi-Fi, para los que el etiquetado es obligatorio) y tiene cuatro niveles, siendo el nivel 1 la seguridad básica. Los niveles 1 y 2 se basan en la autoevaluación de los fabricantes y los niveles 3 y 4 implican la evaluación de terceros por parte de un laboratorio aprobado. El sistema es multinivel para incentivar a los fabricantes a incorporar medidas de seguridad adicionales a los requisitos básicos.

La CSA también examinó los pros y contras de la imposición de normas de ciberseguridad con carácter obligatorio, incluido el riesgo de que los fabricantes eviten el mercado debido al aumento de los costos de cumplimiento. Sin embargo, el objetivo es cambiar la mentalidad de los fabricantes para que consideren la ciberseguridad como un habilitador y diferenciador del mercado y no como un costo adicional. En lo que respecta a las repercusiones del sistema de etiquetado de la ciberseguridad en Singapur, este aún se encuentra en una fase temprana del proceso y se están realizando esfuerzos para alentar a los fabricantes a participar en el plan y a mejorar su ciberseguridad. En el futuro se llevará a cabo una encuesta pública para evaluar la sensibilización y el comportamiento de los consumidores. El costo del cumplimiento para los fabricantes es mínimo en los niveles 1 y 2, y no ha habido un aumento significativo del costo de los productos para los consumidores. Con el sistema voluntario, se espera que las fuerzas del mercado impulsen mejoras en la ciberseguridad entre los fabricantes.

En **Estados Unidos**, el nuevo programa de Marca de Confianza Cibernética constituye un ejemplo de programa voluntario de etiquetado de la ciberseguridad para los productos IoT[74].

---

[71] Trabaja en estrecha asociación con el Departamento de Ciencia, Innovación y Tecnología (DSIT) y el Centro Nacional de Ciberseguridad (NCSC) para su aplicación.
[72] Documento SG2RGQ/74 de la CE 2 del UIT-D, presentado por el Reino Unido
[73] Presentación del taller Q3/2_2023_05 de la CE 2 del UIT-D por Singapur
[74] Documento 2/196 de la CE 2 del UIT-D, presentado por Estados Unidos

En el marco del desarrollo del programa, la Comisión Federal de Comunicaciones (FCC) destacó que era fundamental solicitar las aportaciones públicas y las observaciones de todas las partes interesadas, en particular la industria, el Gobierno y la sociedad civil, para concebir y administrar un programa que atienda las necesidades identificadas. Si bien el programa de Marca de Confianza Cibernética está dirigido por la FCC, será puesto en marcha junto con diversos socios interinstitucionales que requerirán una estrecha cooperación con todas las ramas del Gobierno implicadas.

Más allá de las etiquetas, es igual de importante invertir en controles técnicos y crear conciencia y educar a la población sobre los riesgos de ciberseguridad a los que se enfrentan las organizaciones y los países. Actualmente, los ataques de *ransomware* son la tendencia más preocupante. Para este tipo de ataques, el principal vector de ataque, es decir, el medio por el que un delincuente se introduce en una red o sistema, es el correo electrónico de suplantación de identidad[75]. En este contexto, con frecuencia, los ciberdelincuentes pueden eludir los controles de seguridad haciendo clic simplemente en un correo electrónico de suplantación de identidad. Por lo tanto, para garantizar la ciberseguridad es fundamental que los ciudadanos y los empleados estén al corriente de estas cuestiones. El fomento de la concienciación de los usuarios sobre la ciberseguridad se examina en el capítulo 1 del presente Informe.

2.5 Enfoques sobre los acuerdos internacionales de sinergia/armonización y reciprocidad

La existencia de acuerdos de reciprocidad entre los modelos de garantía de la ciberseguridad, como los sistemas de certificación y etiquetado, puede ser determinante para la ampliación de estas prácticas. Como han destacado las partes interesadas, los acuerdos de reciprocidad pueden ayudar a facilitar el cumplimiento para los actores industriales que operan en múltiples mercados. Sin embargo, habida cuenta de que los acuerdos de reciprocidad son un mecanismo formal que podrían tener muchas condiciones nacionales y que lleva tiempo aprobar y firmar, es necesario que las prácticas de garantía de la ciberseguridad encuentren sinergias con enfoques internacionales existentes que estén en consonancia con las necesidades y prioridades nacionales. Esto reducirá la carga reglamentaria sobre los proveedores de productos y servicios para evitar requisitos contradictorios.

La CSA destacó la importancia de la colaboración internacional en el desarrollo y la aplicación de su sistema de etiquetado de ciberseguridad. **Singapur** ha firmado acuerdos de reconocimiento mutuo con Finlandia y la República Federal de Alemania, y está trabajando para ampliar sus asociaciones en esta esfera. Singapur reflexionó sobre su experiencia y observó que los gobiernos deben ser proactivos en el establecimiento del reconocimiento, aunque los fabricantes también tienen interés en apoyar el proceso de reconocimiento, ya que los acuerdos de reconocimiento mutuo reducen la carga que supone la repetición de pruebas y certificaciones, y ayudan a lograr el acceso al mercado, en diferentes jurisdicciones. El proceso implica reunir a las partes interesadas para armonizar los requisitos y establecer normas comunes que sean realistas y no excesivamente onerosas.

A nivel europeo, la **Agencia de la Unión Europea para la Ciberseguridad (ENISA)** tiene el mandato de desarrollar tres sistemas de certificación que tendrían reconocimiento en todo el mercado interior, por lo que garantizarían un "reconocimiento mutuo" automático en toda la

[75] Una táctica común utilizada por los ciberdelincuentes para engañar a las personas a fin de que revelen información confidencial o descarguen un programa malicioso que infecta el sistema o la red de destino.

Unión Europea. Esos sistemas son el *plan de criterios comunes de la Unión Europea para los productos de TIC*, cuyo reglamento de aplicación se aprobó a principios de 2024; y el *sistema de servicios en la nube*, que está siendo objeto de debate; y, por último, el *sistema 5G*, que se está desarrollando actualmente[76].

Además de la reciprocidad, y teniendo en cuenta los mercados internacionales en los que opera la industria, la armonización de los requisitos de seguridad básicos es también una consideración importante. Las normas del ETSI sobre los productos de consumo IoT son un ejemplo de un intento por armonizar los requisitos básicos de seguridad. La pregunta principal es hasta qué punto los diferentes marcos reglamentarios estarán armonizados y en qué medida estarán conectados a través de las mismas normas internacionales. A este respecto, se ha observado que fortalecer e incluso encontrar el lugar adecuado para el diálogo supone un desafío. En lo que respecta a la armonización, las actividades de la ENISA en materia de normalización de la ciberseguridad y 5G requieren la colaboración entre el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC), el ETSI, la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI), la Asociación GSM (GSMA), el Proyecto de Asociación Tercera Generación (3GPP) y GlobalPlatform. Uno de los principales resultados de la ENISA ha sido la consolidación de los controles de seguridad 5G de diferentes organismos de normalización en un solo repositorio[77].

[76] Presentación del taller Q3/2_2023_10 de la CE 2 del UIT-D por la Agencia de la Unión Europea para la Ciberseguridad

[77] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Capítulo 3 – Coordinación nacional de EIIC para la resiliencia de las infraestructuras críticas y la respuesta a los incidentes de ciberseguridad

En el actual panorama digital en rápida evolución, las organizaciones se enfrentan a una amenaza en constante crecimiento de que se produzcan incidentes de ciberseguridad que puedan comprometer los datos sensibles, alterar las operaciones y socavar la confianza de las partes interesadas. La coordinación nacional de las actividades de los EIIC refuerza la resiliencia de las infraestructuras críticas (IC). Al fomentar la colaboración, el intercambio de información y los protocolos normalizados, estas iniciativas tienen por objeto mejorar la capacidad colectiva de detectar y mitigar los incidentes cibernéticos de manera eficaz y de recuperarse tras ellos. A fin de alcanzar este objetivo, los Estados Miembros deben intensificar sus esfuerzos encaminados a establecer y desarrollar los EIIC, ya que esto suele ser la primera etapa importante hacia la creación de una cultura de la ciberseguridad. Cabe observar que los EIIC también se denominan equipos de intervención en caso de incidente de seguridad informática (EIISI) y equipos de intervención en caso de emergencia informática (EIEI) y, a los efectos de este Informe, se consideran sinónimos[78].

Una tarea de los EIIC nacionales es responder a las amenazas contra las IC. Las IC hacen referencia a un conjunto de sistemas, redes y activos que se consideran fundamentales para la seguridad pública. No existe una única definición de "infraestructuras críticas", dado que estas se definen a nivel nacional, sobre la base de las necesidades y prioridades nacionales de los países, aunque suele incluir sectores como el transporte, los sistemas de energía, comunicaciones, abastecimiento de agua y financieros, y la salud. La actividad cibernética maliciosa contra las IC nacionales sigue siendo un desafío importante para los gobiernos y puede plantear riesgos para los ciudadanos. En un informe de KnowBe4 publicado en 2024 se indica que la actividad cibernética maliciosa contra las IC ha aumentado un 30% desde 2022, lo que representa más de 420 millones de ataques producidos entre enero de 2023 y 2024. Esto equivale a 13 ataques por segundo[79].

Los ataques contra las IC constituyen la mayor amenaza para la vida de los ciudadanos. Con frecuencia, se producen contra los servicios de emergencia y salud, y afectan a la capacidad de recibir atención médica, como la realización de intervenciones quirúrgicas y la emisión de recetas. Otros ejemplos de blancos de estos ataques son las infraestructuras energéticas, como las redes eléctricas. Dada la probabilidad de que estos ataques afecten a las vidas, la coordinación de dichos incidentes y la respuesta a ellos son fundamentales y constituyen una función clave de los EIIC.

---

[78] Para más información sobre la terminología, véase la publicación de la ENISA titulada *How to Setup up CSIRT and SOC* en https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

[79] https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf?hsLang=en-us

En el marco del desarrollo y perfeccionamiento de los EIIC, los países elaboran con frecuencia planes contundentes de respuesta a los incidentes de seguridad a fin de detectar, contener y mitigar eficazmente las brechas de seguridad y recuperarse tras ellas. Es fundamental que las organizaciones dispongan de un plan de respuesta a incidentes de ciberseguridad proactivo y bien definido para mitigar eficazmente los efectos de los incidentes de seguridad. Existen varios modelos de planes de respuesta a incidentes de ciberseguridad que los países han adoptado para gestionar de la mejor manera posible los riesgos y mitigar la actividad cibernética maliciosa. Esos modelos suelen utilizar un enfoque holístico, que integra las buenas prácticas y fomenta una cultura de mejora continua a fin de reforzar la resiliencia contra las ciberamenazas y salvaguardar los activos digitales. En vista de la evolución del panorama de amenazas, las estrategias de respuesta a los incidentes deben permanecer por delante de los adversarios cibernéticos y proteger la integridad y confianza de la organización.

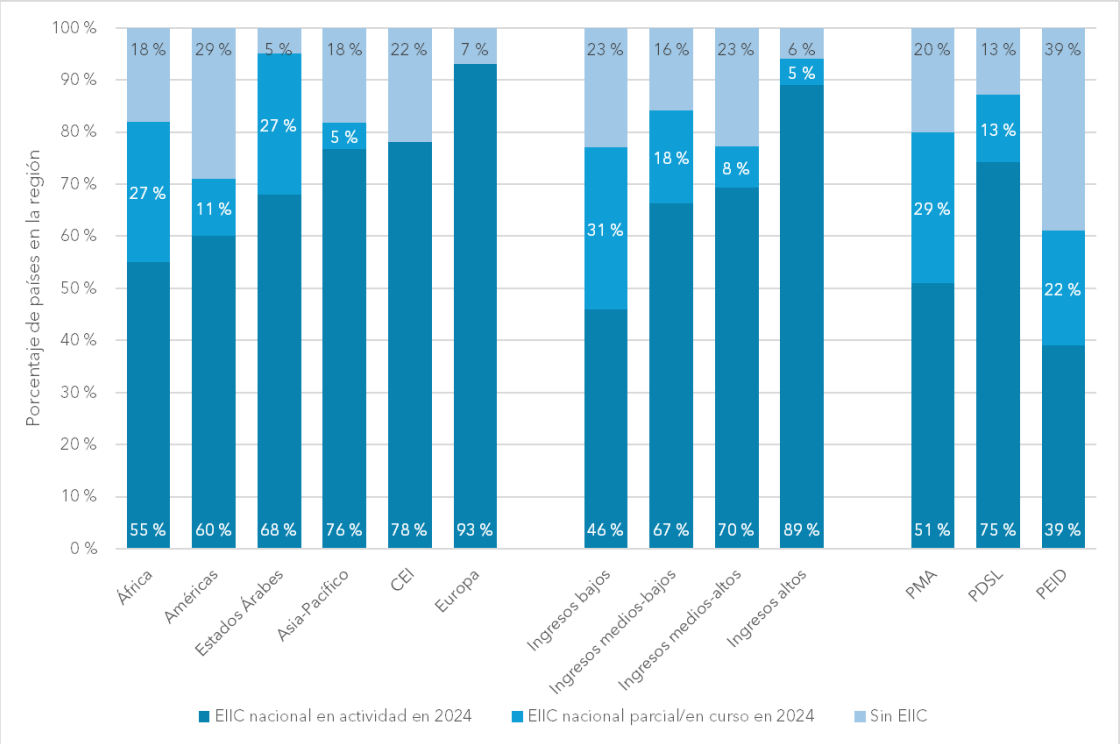
Una tendencia más reciente observada en la gestión de las respuestas a los incidentes es la creación de centros nacionales de coordinación cibernética a fin de mejorar la coordinación pangubernamental. Cuando se produce un incidente cibernético grave, este afecta con frecuencia a varios organismos gubernamentales; la coordinación de una respuesta rápida puede marcar la diferencia entre consecuencias menores y mayores. El disponer de un centro o unidad de coordinación centralizada puede permitir la respuesta rápida y una gestión y control generales. Cabe señalar que las IC no son necesariamente infraestructuras poseídas y gestionadas por el sector público, por lo que también es extremadamente importante garantizar la coordinación con el sector privado a la hora de hacer frente y responder a un incidente cibernético.

3.1 Creación de los EIIC

Según el ICG de 2024[80], "139 países tienen un EIIC nacional, mientras que 55 no disponen de ningún EIIC ni lo están creando".

[80] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Figura 1: Porcentaje de países con un EIIC, desglosado por región/grupo de ingresos/ situación de desarrollo



Fuente: UIT

Aunque las funciones de los EIIC varían, una de las principales consiste en detectar y analizar las posibles amenazas en las redes y sistemas, responder a ellas y mitigar el impacto de los incidentes. Con frecuencia, la creación de los EIIC es un paso importante hacia el fomento de la cultura de la concienciación y resiliencia en materia de ciberseguridad. Parte de la constitución de un EIIC radica en crear la capacidad y los mecanismos necesarios para la protección de las IC.

El Gobierno de **Kenya** creó el Equipo Nacional de Intervención en caso de Incidentes Informáticos – Centro de Coordinación de Kenya (KE-EIEI/CC), encargado de coordinar las actividades nacionales en materia de ciberseguridad y servir de punto de contacto nacional en asuntos de ciberseguridad. El KE-EIEI/CC nacional consta de un equipo multipartita dotado de diversas competencias para gestionar eficazmente los incidentes de seguridad informática y responder a ellos. Reconociendo la importancia de la ciberseguridad para fomentar una economía digital próspera, la Autoridad de Comunicaciones de Kenya (CA) puso en marcha una serie de sesiones de entrenamiento y hackatones de ciberseguridad a fin de crear capacidad local en materia de ciberseguridad[81].

Con la ayuda de la UIT, la **República Kirguisa** ha estado trabajando para crear un EIIC nacional. Algunas de las funciones del EIIC son la identificación, gestión y respuesta a las amenazas cibernéticas junto con las capacidades de vigilancia, alerta y respuesta a incidentes, la creación de capacidad nacional y la transmisión de conocimientos para seguir reforzando la protección de las infraestructuras críticas de información[82].

[81] Documento 2/112 de la CE 2 del UIT-D, presentado por Kenya
[82] Documento 2/170 de la CE 2 del UIT-D presentado por la BDT de la UIT y presentación de la sesión de información SG2_2023_05 de la CE 2 del UIT-D por la BDT de la UIT

La **UIT** colabora con los Estados Miembros y las organizaciones de todo el mundo para reforzar la ciberseguridad mediante la creación y la mejora de los EIIC nacionales. Por conducto de la BDT, la UIT lleva a cabo evaluaciones de la madurez de los EIIC, y hasta ahora ha ayudado a 84 países a evaluar su grado de preparación en materia de ciberseguridad y a establecer o mejorar los EIIC nacionales. La UIT ha llevado a cabo 21 proyectos relacionados con los EIIC y está actualmente implicada en tres más. Se han realizado evaluaciones de la madurez de los EIIC para Azerbaiyán, Sierra Leona y la República Unida de Tanzanía, y se están llevando a cabo actualmente otras para la República de Zimbabwe, el Reino de Bhután y el Reino de Lesotho[83]. Las evaluaciones se utilizan para la preparación por los EIIC nacionales de los planes operativos de mejora. La UIT colabora asimismo con la comunidad FIRST en la mejora del marco de servicio de los EIIC y en la revisión de los materiales de capacitación en gestión de las operaciones de los EIIC nacionales[84].

3.2 Función y responsabilidades de los EIIC e infraestructuras críticas

Los EIIC desempeñan un papel fundamental en la protección de las IC de diversos sectores, al encargarse de la supervisión en tiempo real, la gestión de incidentes, el análisis de las amenazas y las evaluaciones de la vulnerabilidad. Los EIIC suelen ser responsables de garantizar la resiliencia de los sistemas de TIC, permitir la rápida detección y resolución de las amenazas a la ciberseguridad, y coordinar los esfuerzos para reducir al mínimo los efectos de los incidentes en la seguridad nacional, la seguridad pública y la economía. Sobre la base de las necesidades del país, su desarrollo y los sectores de las IC, los EIIC asumen diferentes funciones y establecen distintas relaciones para garantizar la ciberseguridad.

En la **República de Lituania**, el EIIC nacional trabaja bajo la responsabilidad del Centro Nacional de Ciberseguridad (NCSC) y se centra específicamente en la respuesta a los incidentes cibernéticos y la coordinación de la resiliencia entre los sectores de las IC. El Gobierno ha trabajado para garantizar que este equipo tenga las responsabilidades y las capacidades técnicas necesarias para proteger activamente las IC, y este trabajo sirve de modelo para otros países que desean crear capacidades en materia de estos equipos. El EIIC es fundamental para prestar servicios de gestión de incidentes a las partes interesadas de los sectores público y privado, que garantizan la implementación de respuestas adecuadas durante los ciberataques y tras ellos. Uno de los principales aspectos de la función de un EIIC respecto de la gestión de incidentes es su capacidad de coordinarse con el administrador de la red o el sistema afectado, lo que facilita una rápida recuperación de las operaciones.

Durante los incidentes graves en Lituania, los especialistas del EIIC se despliegan in situ para ayudar a los operadores de IC a restaurar las operaciones ordinarias. Por ejemplo, durante un ataque de denegación de servicio distribuido (DDoS) al sector de telecomunicaciones de Lituania, el EIIC nacional desempeñó un papel fundamental al coordinar la comunicación entre los operadores afectados y proporcionar recomendaciones técnicas que ayudaron a restaurar rápidamente los servicios.

Una parte esencial de la protección de las IC es no solo responder a los incidentes cibernéticos maliciosos, sino también prevenirlos mediante una función más avanzada de los EIIC. Asimismo, Lituania ha otorgado a sus EIIC la responsabilidad de gestionar las vulnerabilidades mediante la

[83] Documento 2/201 de la CE 2 del UIT-D, presentado por la BDT de la UIT
[84] Puede consultarse más información acerca del Programa de la UIT sobre los EIIC en https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

recopilación de información de fuentes públicas, foros privados y mecanismos de notificación de vulnerabilidades. El equipo analiza activamente los activos digitales de Lituania para identificar las vulnerabilidades que podrían ser explotadas por actores maliciosos. Al difundir información sobre vulnerabilidades y amenazas, el EIIC nacional ayuda a fortalecer los sistemas de las IC contra los posibles ciberataques, lo que garantiza la protección proactiva en todos los sectores clave[85].

Brasil ha creado varias organizaciones generales para garantizar que las IC sigan siendo reactivas, estén protegidas y empleen los procedimientos necesarios en materia de ciberseguridad. En Brasil, hay dos EIIC que asumen responsabilidades nacionales, a saber, el equipo nacional de intervención en caso de emergencia informática de Brasil (EIEI.br) y el Centro de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos Gubernamentales (CTIR Gov). También hay varios EIIC sectoriales, así como la Red Federal de Gestión de Incidentes Cibernéticos (ReGIC), establecida en 2021, que están coordinados por el centro CTIR Gov[86].

Un ejemplo de EIIC sectorial es el Centro de Respuesta a Incidentes de Seguridad (CAIS) de la RNP. Desde su creación en 1997, el CAIS ha sido el principal EIIC de la red académica de Brasil. Con arreglo a las pautas de la Petición de Comentarios (RFC) 2350, el CAIS se encarga de la detección, la resolución y la prevención de incidentes de seguridad en la red académica de Brasil. Si bien el CAIS no tiene autoridad directa sobre las instituciones del sector académico, desempeña un papel de coordinación clave en la gestión de incidentes. Las actividades del CAIS reflejan la creciente necesidad de colaboración en sectores específicos para gestionar eficazmente los riesgos de ciberseguridad. El caso del CAIS ofrece un ejemplo de EIIC para un sector específico que garantiza la protección de las IC[87].

Como parte de otro esfuerzo reciente realizado por Brasil para aumentar la ciberseguridad nacional, la ReGIC, que constituye el marco federal de respuesta a los incidentes cibernéticos de Brasil, mejora la coordinación entre las entidades gubernamentales federales para la protección de las IC.

La ReGIC establece mandatos y expectativas para las agencias federales. En el marco de la ReGIC, las agencias federales deben participar en la red, lo que incluye medidas para compartir información sobre las amenazas, alertar sobre ciberataques y coordinarse durante los incidentes activos. Otra función específica de la ReGIC es su mandato de coordinación sectorial, en virtud del cual las agencias reguladoras, como la Agencia Nacional de Telecomunicaciones (Anatel), deben establecer EIISI sectoriales e informar sobre sus respectivos sectores.

El establecimiento de EIEI específicos para sectores, además de la creación de un EIEI nacional, también ha sido el enfoque adoptado por **Tanzanía**[88], que ha creado EIEIfin-TZ para las instituciones financieras y bancarias, el EIEI académico para las instituciones académicas y el eGSoC para los ministerios, departamentos, organismos y autoridades públicas. Estos avances han permitido aumentar la eficacia en la respuesta a las amenazas, lo que se ha traducido en una mejora del nivel de protección, la respuesta a incidentes en términos generales y la coordinación en relación con las cuestiones sectoriales.

---

85 Documento 2/322 de la CE 2 del UIT-D, presentado por NRD Cyber Security
86 Documento SG2RGQ/182 de la CE 2 del UIT-D, presentado por Brasil
87 Documento SG2RGQ/183 de la CE 2 del UIT-D, presentado por Brasil
88 Documento 2/346 de la CE 2 del UIT-D, presentado por Tanzanía

Los EIIC desempeñan una función indispensable en la salvaguardia de sus propias infraestructuras críticas contra las ciberamenazas. Al coordinar la gestión de los incidentes, compartir la información sobre las amenazas, realizar evaluaciones de la vulnerabilidad y ofrecer orientaciones específicas, los EIIC refuerzan la resiliencia cibernética de los sistemas críticos, garantizando la rápida recuperación y reduciendo el impacto de los ciberataques. Los ejemplos señalados en este capítulo destacan la importancia de las respuestas específicas de cada sector, la colaboración entre las entidades públicas y privadas, y la necesidad de adoptar medidas continuas en pro de la resiliencia para proteger las infraestructuras nacionales frente a las ciberamenazas sofisticadas. A fin de garantizar que los EIII nacionales apliquen buenas prácticas de respuesta a los incidentes de ciberseguridad y fomentar la cooperación técnica entre los EIII nacionales, la **UIT** organiza cibersimulacros[89] a nivel regional e intrarregional. Mediante ejercicios de ciberseguridad, los Estados Miembros de la UIT crean capacidades que promueven la preparación, la protección y la mejora de la respuesta a los incidentes.

3.3 Más allá de lo básico: la coordinación para el éxito transfronterizo

A medida que los países desarrollan sus EIIC y fortalecen su cultura de ciberseguridad, existen medidas y modelos que permiten la coordinación para la protección de las IC más allá de la básica. Una vez que un país crea un EIIC sólido y programas y políticas nacionales para la gestión de los incidentes, es fundamental mirar más allá de las fronteras nacionales e iniciar la coordinación internacional para prevenir y mitigar los incidentes cibernéticos y responder a ellos. En el mundo actual interconectado, las ciberamenazas transcienden a menudo las fronteras, por lo que se necesitan estrategias cooperativas para fortalecer la resiliencia mundial en materia de ciberseguridad. Tanto Estados Unidos como la Unión Europea han desarrollado modelos exitosos de colaboración internacional que demuestran la importancia de dichos esfuerzos, en particular el establecimiento de relaciones en los planos nacional e internacional.

En **Estados Unidos**, la CISA ha implementado un programa de notificaciones contra los ataques por *ransomware*, que constituye una iniciativa progresista diseñada para identificar y responder a las amenazas de *ransomware* antes de que causen daños. Este programa es un ejemplo de aplicación de la ciberseguridad proactiva por conducto de alertas tempranas, cuyo objetivo es ayudar a las organizaciones a evitar pérdidas de datos críticos, interrupciones de las operaciones y consecuencias financieras por causa de los ataques por *ransomware*. El programa se basa en dos pilares fundamentales, a saber, el establecimiento de fuertes relaciones y la recopilación sistemática de información de utilidad[90].

La iniciativa Joint Cyber Defense Collaborative (JCDC) de la CISA desempeña un papel central al filtrar las sugerencias de la comunidad de investigadores en materia de ciberseguridad, los proveedores de infraestructuras y las organizaciones encargadas de la información sobre las amenazas. Además, el establecimiento de relaciones sólidas con las entidades del sector privado y los investigadores garantiza la presentación oportuna de información de gran calidad. Una vez que se recibe una sugerencia fiable, la JCDC recurre a su personal nacional y de campo para notificar a las organizaciones de víctimas y brindar orientaciones para la mitigación.

Una parte importante del programa es su alcance internacional gracias a su estrecha coordinación con los EIIC extranjeros. Cuando una sugerencia de amenaza se refiere a una organización situada fuera de Estados Unidos, la JCDC trabaja con sus homólogos internacionales para

[89] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx
[90] Documento SG2RGQ/164 de la CE 2 del UIT-D, presentado por Estados Unidos

garantizar que la entidad afectada sea avisada sin demora. Estas relaciones entre EIIC son indispensables, en particular cuando se necesitan tomar rápidamente medidas para evitar el despliegue de *ransomware*. En los casos en que ya se ha desplegado el *ransomware*, la JCDC ayuda a las organizaciones afectadas proporcionándoles información sobre las tácticas, las técnicas y los procedimientos utilizados por los actores de las amenazas, y brindando su ayuda en las actividades de investigación y reparación. Con frecuencia, esta ayuda incluye la identificación de datos extraídos y la orientación para mitigar los efectos de un ataque a largo plazo.

De manera análoga, la **Unión Europea** también ha dado prioridad a la coordinación internacional para mejorar su resiliencia cibernética. Un buen ejemplo de ello es el proyecto de los equipos de respuesta telemática rápida y la asistencia mutua en el ámbito de la ciberseguridad de la Cooperación Estructurada Permanente (CEP)[91]. Este programa permite desplegar rápidamente a expertos en materia de ciberseguridad en los Estados Miembros de la Unión Europea a fin de responder a incidentes de gran escala, en particular los que atacan las infraestructuras críticas. Al reunir a expertos y recursos, la Unión Europea refuerza su capacidad colectiva de hacer frente a las crisis cibernéticas en los planos nacional y regional. La iniciativa también testimonia el compromiso de la Unión Europea con la ciberseguridad colaborativa, dado que garantiza que los Estados Miembros de la Unión Europea puedan brindarse asistencia mutua durante las situaciones de emergencia.

Además de estas iniciativas, tanto Estados Unidos como la Unión Europea destacan la importancia de compartir información sobre amenazas, fomentar la confianza y establecer protocolos normalizados para la coordinación transfronteriza.

Dado que las ciberamenazas siguen evolucionando a nivel de su sofisticación y magnitud, la coordinación transfronteriza se ha convertido en un elemento fundamental para el éxito. Los modelos señalados anteriormente demuestran la manera en que la colaboración internacional puede mejorar las capacidades de respuesta a los incidentes y reforzar la protección cibernética a nivel mundial. Al dar prioridad a la cooperación y al aprovechamiento de los conocimientos especializados de los asociados en todo el mundo, los países pueden encarar mejor los desafíos del panorama digital cada vez más interconectado.

3.4 Establecimiento de centros de coordinación

Tanto Australia como la Federación de Rusia han creado centros de coordinación nacional y han experimentado los beneficios de sus respectivos modelos. Para ambos Gobiernos, los centros de coordinación nacional forman parte de una respuesta pangubernamental más amplia a los incidentes cibernéticos. Los centros de coordinación no son EIIC pero trabajan con ellos.

El Gobierno de **Australia** creó la Unidad de Coordinación de Respuestas a los Incidentes de Seguridad Cibernética (CSRCU) como dependencia del Departamento de Interior tras las violaciones de datos de Optus y Medibank en 2022. El objetivo era crear una unidad de coordinación central para los incidentes cibernéticos de importancia nacional[92]. La **Federación de Rusia** creó su Centro Nacional de Respuesta y Coordinación de Incidentes Informáticos (NCIRCC) tras la aprobación de una ley nacional para mejorar las infraestructuras críticas de

[91] Documento 2/322 de la CE 2 del UIT-D, presentado por NRD Cyber Security; https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
[92] Documento SG2RGQ/218 de la CE 2 del UIT-D, presentado por Australia

información. Estos centros llevan a cabo tareas similares: coordinar la respuesta a los incidentes y comunicar la información crítica. El NCIRCC se centra en la coordinación de medidas para responder a los incidentes cibernéticos y en la comunicación con las IC sobre los medios y métodos para recopilar, almacenar y analizar datos sobre dichos incidentes[93]. Tanto la CSRCU de Australia como el NCIRCC están facultados para crear grupos de trabajo, implicar a organizaciones y expertos pertinentes, y difundir información y materiales de referencia.

[93] Documento SG2RGQ/79 de la CE 2 del UIT-D, presentado por la Federación de Rusia

Capítulo 4 – Enfoques y buenas prácticas, y experiencias recopiladas sobre la aplicación de estrategias y políticas nacionales de ciberseguridad

En vista del aumento de la dependencia mundial de las tecnologías digitales, no puede sobreestimarse la importancia de contar con políticas y estrategias nacionales contundentes en materia de ciberseguridad. Las ciberamenazas están evolucionando rápidamente, y se dirigen tanto a las naciones desarrolladas como a las que están en desarrollo. A fin de proteger las infraestructuras críticas, la economía digital y la privacidad de los ciudadanos, los países deben adoptar estrategias de ciberseguridad exhaustivas y adaptables. En este capítulo se analizan los diversos enfoques y buenas prácticas que diversos países están utilizando para construir marcos de ciberseguridad resilientes. Al analizar las experiencias de diferentes países, este capítulo tiene por objeto ofrecer una hoja de ruta para el diseño y la aplicación de políticas y estrategias nacionales en materia de ciberseguridad.

Las políticas y estrategias nacionales de ciberseguridad abarcan un amplio espectro de prácticas, cada una de ellas adaptadas a los distintos contextos políticos, sociales, económicos, jurídicos y tecnológicos de diferentes países. La aplicación de estas políticas y estrategias está marcada por un conjunto único de desafíos y oportunidades, profundamente influido por las condiciones específicas de cada país. Esta sección profundiza en las experiencias prácticas de diversos países, destacando tanto los desafíos como los éxitos registrados en sus esfuerzos por fortalecer su protección y resiliencia digital en un contexto de amenazas en constante evolución.

El debate abarca esferas críticas como la alineación estratégica, la participación de las partes interesadas, la creación de capacidad y la adaptación continua al panorama dinámico de ciberamenazas. Este análisis exhaustivo procura no solo aclarar las complejidades que implica la salvaguardia eficaz de los intereses nacionales en la esfera cibernética cada vez más criticada, sino también ofrecer información estratégica que pueda orientar a los responsables de formular políticas y a los profesionales de la ciberseguridad para mejorar sus propias estrategias.

4.1 Armonización estratégica y del liderazgo y marco de políticas

La aplicación exitosa de las estrategias nacionales de ciberseguridad depende considerablemente de la armonización de dichas estrategias con políticas más amplias en materia de transformación digital, seguridad nacional y economía. Esta armonización garantiza que las iniciativas en materia de ciberseguridad no solo apoyen, sino que también integren los objetivos generales y los marcos de gobernanza del país. Por ejemplo, la **República de Estonia**, ampliamente reconocida por su avanzada sociedad digital, ha armonizado eficazmente su estrategia de ciberseguridad con sus objetivos en materia de cibergobernanza y economía digital, creando con ello una infraestructura digital resiliente que apoya las iniciativas tanto públicas como privadas[94]. La armonización estratégica en Estonia está facilitada por actualizaciones periódicas

[94] https://www.weforum.org/stories/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/

de su estrategia de ciberseguridad, que están sincronizadas con los cambios ocurridos en el entorno tecnológico y geopolítico más amplio.

Además de esto, las políticas y estrategias de ciberseguridad deben adaptarse a políticas y objetivos económicos más amplios a nivel nacional. Esta adaptación garantiza que las medidas de ciberseguridad no solo aborden las amenazas inmediatas, sino que también apoyen los intereses nacionales a largo plazo, fomentando un entorno digital seguro y resiliente que conduzca al crecimiento y la innovación. Esta adaptación estratégica es necesaria para la eficacia de las medidas de ciberseguridad y apoya objetivos nacionales más amplios, lo que mejora la capacidad del país para prevenir, tratar y responder a los incidentes cibernéticos, y favorece a su vez el crecimiento de la industria nacional de la ciberseguridad.

La **República Democrática de Timor-Leste**[95] ofrece un ejemplo convincente de la importancia de hacer hincapié en la ciberseguridad en el contexto de las políticas, estrategias, planes y hojas de ruta de transformación digital. Timor-Leste reconoció que, en vista de la transformación digital, se deben gestionar los riesgos de ciberseguridad para prevenir ciberataques y violaciones de datos. En este sentido, los PMA deben dar prioridad a la ciberseguridad como un pilar fundamental, en reflejo del entendimiento del papel crítico que desempeña la ciberseguridad en la transformación digital y esta última en el desarrollo nacional.

Otro elemento importante para fomentar la ciberseguridad radica en garantizar un liderazgo fuerte y armonizado en las organizaciones encargadas de la coordinación cibernética nacional, como parte integrante de la comunidad gubernamental más amplia en materia de ciberseguridad. La designación de un coordinador puede facilitar e impulsar una respuesta pangubernamental. A este respecto, el modelo de **Australia** incluye un Coordinador Nacional de la Ciberseguridad, cuya función principal consiste en dirigir la gestión de los eventos cibernéticos nacionales. Este puesto de coordinador se creó en febrero de 2023, y el titular designado rinde cuentas al Ministro de la Ciberseguridad[96]. En mayo de 2022, el Presidente de la **Federación de Rusia** emitió un decreto en el que se expusieron criterios estrictos para nombrar a los encargados de la seguridad de la información, haciendo énfasis en requisitos de elegibilidad como los relativos a la educación y la experiencia en el terreno y requisitos organizacionales. Asimismo, en dicho instrumento se alienta al reciclaje profesional de las personas que carezcan de experiencia especializada en la seguridad de la información[97].

4.2 Marcos jurídicos y gobernanza

La **República Centroafricana**[98] y la **República Democrática del Congo**[99] ilustran la manera en que la adopción de medidas legislativas y marcos de gobernanza específicos puede mejorar considerablemente las capacidades de ciberseguridad. En la República Centroafricana, el Gobierno ha emprendido reformas legales y ha creado agencias dedicadas a la ciberseguridad para hacer cumplir sus políticas, lo que demuestra un enfoque proactivo sobre el refuerzo de las defensas digitales. De manera análoga, la República Democrática del Congo ha adoptado una carta exhaustiva sobre la base de las buenas prácticas, que abarca la legislación en materia normativa, la cooperación multinivel y amplias campañas de sensibilización pública. Estas

[95] Documento 2/120 de la CE 2 del UIT-D, presentado por Timor-Leste
[96] Documento SG2RGQ/218 de la CE 2 del UIT-D, presentado por Australia
[97] Documento SG2RGQ/79 de la CE 2 del UIT-D, presentado por la Federación de Rusia
[98] Documento 2/141 de la CE 2 del UIT-D, presentado por la República Centroafricana
[99] Documento 2/115 de la CE 2 del UIT-D, presentado por la República Democrática del Congo

medidas son fundamentales para que los países, en particular los situados en regiones en desarrollo aseguren sus ciberespacios contra las crecientes amenazas.

La **República de Albania**[100] añade otra dimensión a esta narrativa con sus recientes y exhaustivas reformas en materia de ciberseguridad. La creación de un EIISI nacional y la restructuración de su organismo de ciberseguridad reflejan el compromiso de Albania de ajustar su marco de ciberseguridad a las normas y buenas prácticas internacionales. Estas acciones estratégicas están diseñadas para fortalecer la infraestructura nacional de ciberseguridad de Albania garantizando una respuesta coordinada a los incidentes cibernéticos y mejorando la gobernanza de los esfuerzos en materia de ciberseguridad. Además, las reformas jurídicas emprendidas por Albania tienen por objeto actualizar y fortalecer el marco legislativo en vigor, garantizando que el país atienda los desafíos y amenazas actuales en materia de ciberseguridad. Esta armonización de elementos jurídicos, institucionales y operativos en la estrategia de ciberseguridad de Albania sirve de modelo para otras naciones que buscan impulsar sus defensas en materia de ciberseguridad mediante reformas holísticas de la gobernanza.

Côte d'Ivoire está también realizando diversas actualizaciones legislativas como parte de su objetivo político de establecer la confianza digital para 2025[101]. Una de las acciones destacadas es la mejora de las estructuras legales para dar soporte a una sociedad de la información de confianza, en consonancia con normas regionales como las de la Comunidad Económica de los Estados de África Occidental y la Convención de la Unión Africana sobre la Ciberseguridad y la Protección de los Datos Personales. La Autoridad de Reglamentación de las Telecomunicaciones/TIC de Côte d'Ivoire (ARTCI) desempeña una función central, y se enfoca específicamente en la confianza digital y la seguridad de la red, la protección de los datos personales y la gestión de las operaciones electrónicas. La creación de comités consultivos como el Comité Consultivo para la Confianza Digital y el Comité Consultivo para la Protección de los Datos Personales pone de manifiesto la profundidad del compromiso con el fomento de un ciberentorno seguro. Estos esfuerzos estructurados tienen por objeto crear un espacio digital de confianza, mejorando la seguridad de la infraestructura digital de Côte d'Ivoire y fomentando la confianza de la población en la economía digital.

Estos ejemplos demuestran la importancia de adaptar las estrategias de ciberseguridad a los marcos nacionales de gobernanza, lo que no solo mejora la eficacia de estas estrategias sino también garantiza su sostenibilidad y adaptabilidad frente a la evolución de las ciberamenazas.

4.3 Colaboración y apoyo en el plano internacional

La función de las organizaciones internacionales respecto del apoyo de los esfuerzos nacionales en materia de ciberseguridad es fundamental, como lo ilustran diversas iniciativas llevadas a cabo por el **Banco Mundial**[102]. El Banco Mundial ayuda a sus países clientes, en especial los clasificados como PMA, proporcionando apoyo financiero y técnico a fin de construir bases digitales sólidas y acelerar la utilización digital en diversos sectores. Este apoyo es vital para que dichos países adapten sus políticas y estrategias de ciberseguridad a los avances mundiales, lo que garantiza que sigan siendo resilientes frente a las ciberamenazas actuales y emergentes.

[100] Documento 2/309 de la CE 2 del UIT-D, presentado por Albania
[101] Documento SG2RGQ/29 de la CE 2 del UIT-D, presentado por Côte d'Ivoire
[102] Documento 2/74 de la CE 2 del UIT-D, presentado por el Banco Mundial

Los esfuerzos llevados a cabo por el Banco Mundial destacan el importante efecto que tienen las asociaciones mundiales y la compartición de experiencias en la mejora de los marcos nacionales de ciberseguridad. Al facilitar la integración de tecnologías innovadoras y buenas prácticas, el Banco Mundial ayuda a los países no solo a defenderse contra las ciberamenazas, sino también a aprovechar la transformación digital para el crecimiento económico y social.

En la **República de Haití**[103], las asociaciones internacionales, en particular con el Banco Mundial y el Banco Interamericano de Desarrollo, proporcionan apoyo financiero y técnico fundamental. Este apoyo es esencial para desarrollar infraestructuras digitales robustas y mejorar las medidas de ciberseguridad en todo el país.

Una iniciativa clave es el grupo de trabajo conjunto formado por el Consejo Nacional de Telecomunicaciones de Haití (CONATEL) y el Instituto Haitiano de Estadística e Informática (IHSI). Este grupo de trabajo conjunto se encarga de elaborar una estrategia nacional armonizada en materia de ciberseguridad, centrada en la protección de las infraestructuras críticas y la lucha contra la ciberdelincuencia. La función reglamentaria de CONATEL garantiza el cumplimiento de los protocolos de seguridad, mientras que el IHSI gestiona las amenazas y riesgos de ciberseguridad, lo que mejora la seguridad general de los sistemas digitales en Haití.

Estos esfuerzos están respaldados por proyectos internacionales como el Proyecto de Aceleración Digital de Haití, que tiene por objeto mejorar la conectividad de banda ancha y crear resiliencia digital. Este enfoque integral no solo protege a Haití contra las nuevas ciberamenazas sino que también apoya su crecimiento socioeconómico en la era digital. A fin de seguir reforzando estos esfuerzos, Haití llevó a cabo una evaluación exhaustiva de su nivel de desarrollo en materia de ciberseguridad en colaboración con el Centro Mundial de Capacidad en Ciberseguridad y el Banco Mundial. En esta evaluación participaron diversas partes interesadas y se utilizó el Modelo de Madurez de las Capacidades de Ciberseguridad para Naciones a fin de identificar las esferas críticas que necesitaban inversión estratégica. Las conclusiones de dicho ejercicio han orientado una serie de mejoras específicas para fortalecer la infraestructura de ciberseguridad de Haití.

4.4 Marcos colaborativos y participación de las partes interesadas

Brasil[104] ha implementado una serie de medidas estratégicas destinadas a reforzar su infraestructura nacional de ciberseguridad mediante la participación activa e inclusiva de las partes interesadas. El enfoque adoptado por el país destaca la importancia de la colaboración entre los órganos gubernamentales, las entidades del sector privado y las instituciones académicas. Esta colaboración multipartita se facilita mediante diversas iniciativas y asociaciones que aprovechan las fortalezas y perspectivas únicas de cada sector para mejorar el panorama general de la ciberseguridad. Uno de los recientes avances es la creación del Comité Nacional de Ciberseguridad con el fin de supervisar la implementación y evolución de la Política Nacional de Ciberseguridad. El comité consta de 25 miembros, 15 miembros representan a entidades y organismos representantes de la Administración Federal Pública, incluida Anatel, y 10 representan a otras organizaciones como el Comité de Dirección de Internet de Brasil (CGI.br), mientras que 3 puestos representan a la sociedad civil, 3 puestos a las instituciones académicas y 3 puestos al sector privado relacionado con la ciberseguridad.

[103] Documento SG2RGQ/121 de la CE 2 del UIT-D, presentado por Haití
[104] Documentos SG2RGQ/57 y SG2RGQ/181 de la CE 2 del UIT-D, presentados por Brasil

Australia ha adoptado medidas más allá de sus EIIC para garantizar la protección y resiliencia de las IC, lo que constituye un paso más hacia el desarrollo de la ciberseguridad. En lugar de centrarse simplemente en la respuesta y la protección, el Programa de Mejora de las Infraestructuras Críticas (CI-UP) está diseñado para ayudar a las organizaciones de IC de Australia a mejorar su resiliencia contra los ciberataques sofisticados. El programa, ejecutado por el Gobierno de Australia, trabaja conjuntamente con el sector privado, a fin de fortalecer las IC contra las vías de ataques a los activos de las IC y los entornos tecnológicos operacionales. El CI-UP opera como programa voluntario nacional impulsado por las amenazas[105].

El CI-UP se centra principalmente en ayudar a las organizaciones de IC a mejorar su situación en materia de ciberseguridad en varias esferas clave:

- Mejora de la visibilidad y la sensibilización: el CI-UP ayuda a las entidades a adquirir mayor visibilidad sobre los incidentes cibernéticos y a crear conciencia sobre las posibles vulnerabilidades a que se enfrentan sus sistemas.
- Contención de incidentes y respuesta a ellos: el programa refuerza la capacidad de las organizaciones de IC de contener eficazmente los incidentes cibernéticos y responder a ellos.
- Promoción de la cultura de ciberseguridad: el CI-UP alienta también el desarrollo de una cultura consciente de la ciberseguridad en todos los sectores de las infraestructuras críticas de Australia.

Este programa refleja la importancia de la seguridad de las colaboraciones multipartitas entre el Gobierno y el sector privado. El CI-UP presta estos servicios mediante diversas actividades de implicación, como las presentaciones, los talleres, los intercambios de información y la prestación de asesoramiento detallado en materia de mitigación. El programa también trabaja in situ con el personal de las entidades de las IC más vitales, ofreciendo asesoramiento exhaustivo y a medida adaptado a las necesidades específicas de cada organización.

La implicación de diversas partes interesadas es fundamental para la implementación eficaz de políticas y estrategias nacionales en materia de ciberseguridad. Esta implicación abarca los organismos públicos, las entidades del sector privado, las instituciones académicas y la sociedad civil, y cada una de estas partes realiza aportaciones únicas en materia de perspectivas, necesidades, prioridades y experiencia. Estas colaboraciones ayudan a construir, revisar, mejorar y perfeccionar las políticas nacionales y garantizan que las estrategias implementadas sean prácticas y reflejen las necesidades y realidades de todos los sectores.

4.5 Desarrollo de infraestructuras para la ciberseguridad

La **República Democrática del Congo**[106] ha iniciado un plan ambicioso para reformar y modernizar su infraestructura digital. Esta iniciativa está impulsada por el reconocimiento de que los sistemas digitales contundentes y seguros son la base de la ciberseguridad eficaz y son fundamentales para el desarrollo nacional. El Gobierno ha dado prioridad a la actualización de las infraestructuras de redes críticas para no solo resistir al creciente espectro de ciberamenazas sino también atender las demandas digitales de su economía cada vez mayor. La estrategia de la República Democrática del Congo abarca el despliegue de tecnologías de ciberseguridad avanzadas como cortafuegos de vanguardia, sistemas de detección de intrusiones y métodos exhaustivos de cifrado de datos. Estas tecnologías son fundamentales para garantizar la

[105] Documento SG2RGQ/214 de la CE 2 del UIT-D, presentado por Australia
[106] Documento SG2RGQ/104 de la CE 2 del UIT-D, presentado por la República Democrática del Congo

protección contra el acceso no autorizado y salvaguardar la información sensible. Además, la República Democrática del Congo está trabajando en la ampliación de su acceso de banda ancha, que es vital para garantizar que las medidas de ciberseguridad lleguen a todas las partes del país, incluidas las zonas remotas e insuficientemente atendidas.

La **República de Burundi**[107] está modernizando su infraestructura de ciberseguridad como componente central de su futura estrategia nacional de ciberseguridad. El Gobierno está comprometido con la transformación digital y la digitalización de los servicios, en reconocimiento de la importancia vital que tienen las TIC para el desarrollo. En respuesta al aumento de las ciberamenazas, Burundi, por conducto del Ministerio de Tecnologías de la Información y la Comunicación, ha creado un comité para el desarrollo de un plan nacional exhaustivo en materia de ciberseguridad que incluye la mejora de los marcos jurídicos para regular la ciberseguridad, la promoción de la cultura de ciberseguridad, la creación de conocimientos técnicos y la participación en los esfuerzos regionales e internacionales, así como la creación de conciencia sobre las amenazas a la ciberseguridad en todos los sectores. Este desarrollo de las infraestructuras se implementa con mecanismos de seguridad y protección de datos para mantener la integridad y la confianza entre los usuarios y los proveedores de servicios.

4.6 Creación de capacidad

La creación de la capacidad necesaria para implementar las estrategias nacionales de ciberseguridad implica la mejora de las competencias de los profesionales de la ciberseguridad, la creación de infraestructuras tecnológicas y la instauración de marcos jurídicos y reglamentarios. Es fundamental seguir invirtiendo en la formación y la creación de capacidad para mantener la ciberseguridad nacional. Como se analizó en el capítulo 1, mediante el continuo desarrollo de las competencias de los profesionales de la ciberseguridad y la educación de la población, las naciones pueden gestionar y responder mejor a los incidentes cibernéticos y apoyar a la vez los objetivos más amplios del desarrollo económico y social por conducto de la mejora de las competencias en materia de TIC.

4.7 Adaptación continua al panorama de ciberamenazas

La naturaleza dinámica del panorama de ciberamenazas requiere que las políticas y estrategias nacionales en materia de ciberseguridad sean inherentemente adaptables, así como cualquier otra ley o reglamento en materia de ciberseguridad. La supervisión continua de la evolución de dicho panorama, en particular los desafíos que plantean las tecnologías nuevas y emergentes, así como la evaluación de la eficacia de las políticas y estrategias, y la actualización periódica de las prácticas de ciberseguridad son componentes esenciales de esta adaptabilidad de la ciberseguridad. La necesidad de contar con una ciberseguridad adaptable se examinó en el capítulo 2, al abordar las prácticas de garantía de la ciberseguridad.

[107] Documento SG2RGQ/134 de la CE 2 del UIT-D, presentado por Burundi

Capítulo 5 – Desafíos y enfoques en materia de ciberseguridad de la 5G

La introducción de la tecnología 5G representa un avance significativo en las telecomunicaciones, ya que ofrece velocidades más rápidas y una mejor conectividad con el potencial de mejorar la economía, ampliar las aplicaciones de IoT y aportar nuevas soluciones a la comunicación digital. Con todo, la sofisticada arquitectura que permite estos avances también plantea complejos desafíos de ciberseguridad que requieren una comprensión exhaustiva y medidas de protección sólidas.

A medida que las redes 5G se despliegan en todo el mundo, es necesario establecer un ecosistema seguro para garantizar la integridad, disponibilidad y confidencialidad de la información, así como para proteger la infraestructura que se ha convertido en la columna vertebral de la economía digital.

Este capítulo presenta los debates sobre las complejidades de la ciberseguridad 5G y tiene por objeto compartir información sobre las prácticas existentes y explorar soluciones innovadoras para las nuevas amenazas, compartiendo ideas y buenas prácticas para la ciberseguridad 5G de las redes públicas electrónicas que los Estados Miembros de la UIT puedan considerar e implementar en sus contextos nacionales.

5.1 Aspectos generales de la ciberseguridad 5G

La 5G se caracteriza por sus avanzados sistemas de *software* que permiten una configuración más flexible y una conectividad masiva de suscriptores y dispositivos. La tecnología 5G soporta aplicaciones de baja latencia, como la realidad aumentada, la telecirugía y los servicios integrados de Internet, que dependen de la robustez y fiabilidad de la red. Uno de los principales casos de uso de la 5G es la IoT, que aprovecha la capacidad de la 5G para conectar un gran número de puntos extremos. La tecnología 5G está llamada a revolucionar la conectividad, lo que también plantea nuevos y dinámicos riesgos y desafíos en materia de ciberseguridad.

A diferencia de las generaciones anteriores de tecnologías inalámbricas, la 5G introduce un cambio significativo hacia la arquitectura basada en la nube, las redes definidas por *software* (SDN) y la virtualización de la función de red (NFV). Este cambio crea un panorama de ciberseguridad más complejo y dinámico.

A medida que la 5G se generalice, también se espera que la infraestructura de telecomunicaciones se convierta en un objetivo aún más atractivo para las actividades cibernéticas maliciosas que requieren medidas de seguridad avanzadas que se adaptan a las amenazas en evolución. La ciberseguridad para la 5G debería centrarse en aumentar la resiliencia de todo el ecosistema, incluidas las infraestructuras y aplicaciones. Esto incluye proteger dispositivos, datos, y redes conectadas contra las ciberamenazas.

Reconociendo que las distintas organizaciones emplean diferentes definiciones de ciberseguridad[108], cabe recordar que en este Informe por "ciberseguridad 5G" debe entenderse la ciberseguridad en el contexto de la 5G con sus nuevos parámetros, normas y particularidades

[108] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

tecnológicas, que deben gestionarse adecuadamente para poner a salvo el ecosistema digital en su integridad y garantizar la ciberresiliencia.

Recuadro 1: Definición de ciberseguridad

En la UIT, la ciberseguridad se define en la Recomendación X.1205 del UIT-T como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, el personal, la infraestructura, los servicios y aplicaciones, los sistemas de telecomunicaciones, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Los objetivos generales de seguridad comprenden los siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad".

5.2 Despliegue de redes tradicionales

Los proveedores de servicios de telecomunicaciones tienden en un primer momento a desplegar las redes 5G de forma no autónoma, aprovechando la infraestructura 4G existente antes de desplegar una red de extremo a extremo autónoma[109]. Las redes 5G no autónomas heredan las vulnerabilidades de las redes 4G e incluso de las redes 2G y la 3G, que deberán gestionarse debidamente. Para algunos operadores, esto equivale a una "deuda técnica", en cuyo marco la gestión de sistemas más antiguos implica que se ha de establecer un conjunto de controles de seguridad normalizados para medir el estado de seguridad de los componentes de la infraestructura en las distintas etapas de su madurez generacional[110].

Es importante destacar que la 5G autónoma presenta oportunidades para mejorar la ciberseguridad en comparación con las generaciones pasadas de tecnología móvil, ya que está diseñada para ser más segura que la 4G. Se han observado mejoras en ámbitos tales como la seguridad y privacidad de los abonados, la red de acceso radioeléctrico (RAN), el núcleo de red y la seguridad de la itinerancia[111, 112].

---

[109] Los dispositivos se conectarán a las frecuencias 5G para la transmisión de datos cuando necesiten mayor ancho de banda y menor latencia (como para la comunicación entre automóviles inteligentes), o para reducir el consumo de energía de los dispositivos habilitados para IoT, pero seguirán dependiendo de las redes 4G e incluso 2G/3G para las llamadas de voz y los mensajes SMS. Fuente: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[110] https://www.itu.int/md/D22-SG02.RGQ-ADM-0019/es y https://www.itu.int/md/D22-SG02.RGQ-ADM-0043/es

[111] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

[112] https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

5.3 Actividades de normalización relativas a la seguridad de la 5G

5.3.1 Organismos de normalización activos en la ciberseguridad 5G

Debido a la complejidad de la tecnología 5G y a los problemas que conlleva, ningún organismo de normalización tiene mandato exclusivo en materia de ciberseguridad de la 5G. A fin de evitar la duplicación se han desarrollado mecanismos para el intercambio de información entre organismos de normalización y para la coordinación de sus propuestas y temas de trabajo.

Con el fin de ayudar a conocer estas diferentes actividades y orientar la labor de normalización de la seguridad relacionada con la 5G en el Sector de Normalización de las Telecomunicaciones de la **UIT** (UIT-T), la Comisión de Estudio 17 (CE 17) preparó un informe técnico en el que establecía la correspondencia entre las normas presentes y las que están en desarrollo y sus correspondientes organismos y aplicación en las redes 5G[113]. En el informe se identifican las normas del UIT-T, el 3GPP, el ETSI y el Instituto de Ingenieros Electrotécnicos y de Electrónica – Asociación de Normas (IEEE-SA), además de otros recursos no normalizados pertinentes para la ciberseguridad 5G.

La Comisión de Estudio ha publicado 11 Recomendaciones sobre seguridad de la 5G sobre la base de las contribuciones presentadas por operadores, proveedores, fabricantes de teléfonos inteligentes y proveedores de contenido, entre otros. Esas recomendaciones se centran en cinco esferas: las redes definidas por *software* y la virtualización de la función de red (SDN-NFV), la segmentación de red, la computación periférica móvil, la gestión de redes 5G y los servicios 5G. La CE 17 ha establecido vínculos con otros organismos de normalización (como el 3GPP y el Grupo de Tareas sobre Ingeniería de Internet (IETF)) y con grupos del sector que trabajan en especificaciones importantes para la normalización de la ciberseguridad 5G.

Uno de esos grupos del sector es la **GSMA**. Aunque no es un organismo de normalización, la GSMA redacta especificaciones convocando a sus miembros y colabora con los organismos de normalización para mejorar y/o adoptar dichas especificaciones como normas. La GSMA ha publicado una lista de controles de seguridad básicos que los operadores móviles pueden voluntariamente tener en cuenta al desplegar redes 5G[114].

Dadas las numerosas fuentes de información relevantes para la seguridad de la 5G, la **ENISA** ha publicado un repositorio unificado de controles técnicos de seguridad para redes 5G denominado "5G Security Controls Matrix"[115]. Este repositorio se publica actualmente como una hoja de cálculo, pero la agencia también está desarrollando una herramienta web para mejorar su facilidad de uso.

A medida que las redes se vuelven cada vez más complejas y que las telecomunicaciones convergen con las redes IP, es cada vez más difícil atribuir áreas específicas de trabajo de normalización a cada uno de los organismos de normalización. Esto aumenta el riesgo de solapamiento y duplicación del trabajo, lo que hace que la comunicación y el intercambio de información entre los organismos de normalización sean aún más importantes.

---

113 https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf
114 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
115 https://www.enisa.europa.eu/publications/5g-security-controls-matrix

5.3.2 Integración de las normas en los requisitos reglamentarios

Las normas ayudan a garantizar la interoperabilidad entre tecnologías y a reducir el tiempo necesario para que una innovación llegue a los mercados mundiales. Las normas de ciberseguridad pueden definir una base de referencia común en materia de seguridad que refleje las buenas prácticas universales. Las normas son el resultado de procesos basados en el consenso. Pueden ser de obligado cumplimiento, pero en la mayoría de los casos son opcionales, lo que da a los proveedores y operadores una mayor flexibilidad a la hora de tomar decisiones de despliegue. En algunos casos, las normas pueden convertirse en obligatorias si la reglamentación técnica nacional integra una norma específica entre sus requisitos de seguridad.

Las estrategias de ciberseguridad 5G nacionales deben equilibrar las buenas prácticas mundiales con la realidad operativa local. Por lo general, los requisitos reglamentarios nacionales deben basarse en normas internacionales acordadas, adaptándolas al contexto y las necesidades locales para garantizar el éxito del despliegue de la 5G y la ciberseguridad de las redes.

5.4 Complementar las normas y especificaciones con medidas de ciberseguridad proactivas

5.4.1 Consideraciones de seguridad a nivel de los proveedores

Las normas y especificaciones son solo uno de los componentes de la ciberseguridad de la 5G. La forma en la que los proveedores y operadores implementan esas normas y las configuran define la situación de seguridad de las redes 5G. Ericsson ha adoptado un enfoque integral de la seguridad de la 5G que atañe a cuatro niveles: normas, desarrollo de productos de proveedores, despliegue de redes y operaciones de red[116]. La empresa considera que este enfoque integral puede garantizar que las medidas de mitigación se implementen de tal manera que las interdependencias entre los niveles, así como las necesidades específicas de cada uno de ellos, se aborden de manera efectiva.

Como ejemplo concreto de medida de seguridad de la 5G, el sistema de garantía de seguridad de equipos de red (NESAS)[117], desarrollado por la **GSMA** y el **3GPP**, busca mejorar los niveles de seguridad de los equipos de redes móviles proporcionando un sistema de garantía que pueda aplicarse a nivel mundial. El sistema de garantía se basa en auditorías internas y de expertos independientes (es una combinación de evaluación entre procesos de proveedores y evaluación de productos) para ofrecer acreditación. El objetivo de este sistema es reducir la carga de las pruebas de seguridad para los proveedores de equipos de red, que suelen operar a escala mundial. Los principales proveedores ya han obtenido la acreditación NESAS. El NESAS también es un candidato para el sistema de certificación de ciberseguridad 5G de la Unión Europea[118], una certificación a nivel de la Unión Europea que daría conformidad en todos sus Estados Miembros. Esta certificación no sustituiría al actual sistema NESAS, sino que ambos existirían en paralelo al mismo. Es esencial desarrollar sistemas/iniciativas de certificación de manera que sigan siendo flexibles y puedan actualizarse rápidamente, ya que el panorama de amenazas está en constante evolución.

---

116 https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security
117 https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/
118 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

En el **Reino Unido**, el NCSC recomienda utilizar el marco de evaluación de proveedores[119], una guía que ayuda a los operadores a evaluar el riesgo cibernético asociado a la utilización del equipo del proveedor.

5.4.2 Consideraciones de seguridad a nivel de los operadores

El NESAS puede garantizar la seguridad de un equipo de red antes de su despliegue. A medida que los operadores despliegan y explotan sus redes, se han de integrar otras consideraciones de seguridad, por ejemplo, la detección de ataques y la respuesta automatizada. Aquí es donde los operadores deberían plantearse la posibilidad de aprovechar la inteligencia artificial (IA), la información sobre amenazas y el análisis para ayudar a respaldar su ciberseguridad. La ciberseguridad de la 5G ofrece beneficios, como la seguridad en tiempo real y las estrategias como la confianza cero, que mejoran la visibilidad del sistema. Sin embargo, la ciberseguridad de la 5G también presenta sus propios desafíos, como el mantenimiento de la conectividad entre diferentes redes con distintos niveles de seguridad; el trabajo con componentes heredados y diversos tipos de redes; y las complejidades de integrar la IA en las medidas de seguridad. Al aplicar controles de acceso estrictos conformes con el principio del "menor privilegio", se reducen al mínimo diversos derechos en la red, como los derechos de acceso entre funciones de red, los derechos de administrador de red y la configuración de la virtualización. Existe una gran cantidad de documentos sobre las estrategias de ciberseguridad específicas de la 5G que los operadores pueden tener en cuenta[120].

Las pruebas reales de redes de telecomunicaciones también son fundamentales para determinar el verdadero riesgo cibernético para estas redes. Los operadores pueden llevar a cabo algún tipo de prueba de seguridad en sus propias redes y sistemas, ya sea utilizando recursos internos o recurriendo a contratistas externos independientes. Por ejemplo, en el **Reino Unido**, TBEST es un programa de pruebas de penetración basado en resultados que simula las técnicas y tácticas que pueden utilizar ciberatacantes con muchos recursos. Mediante TBEST se evalúa la capacidad de un proveedor de comunicaciones de detectar, contener y responder a un ataque de este tipo. El objetivo general es encontrar y eliminar vulnerabilidades de la seguridad u otras debilidades de las funciones, procesos, políticas, sistemas o redes de un proveedor que podrían utilizarse en conjunto para poner en peligro los sistemas fundamentales de una empresa antes de su detección. Al someterse al programa TBEST voluntario, los proveedores de comunicaciones pueden conocer en qué áreas concretas se podría mejorar su seguridad. A continuación, el organismo regulador OFCOM trabaja con el proveedor para ayudarle a implementar los cambios apropiados de manera oportuna[121].

Es fundamental que haya razones comerciales contundentes que justifiquen la ciberseguridad de la 5G. Si bien los operadores deben rentabilizar sus inversiones en servicios 5G, el cumplimiento de medidas de seguridad básicas debe considerarse indispensable y presupuestarse adecuadamente.

---

119 https://www.ncsc.gov.uk/report/vendor-security-assessment

120 Véanse por ejemplo: https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf y https://www.5gamericas.org/security-for-5g/

121 Documento SG2RGQ/74 de la CE 2 del UIT-D, presentado por el Reino Unido

Recuadro 2: Open RAN

Open RAN es la desagregación de la RAN y la normalización de las interfaces que conectan los elementos desagregados, lo que permite construir redes con equipos de diferentes proveedores.

Por un lado, Open RAN puede añadir complejidad a la cadena de suministro de las redes de telecomunicaciones. Esta arquitectura, que fomenta la diversidad de proveedores en la RAN, requiere mayores esfuerzos de integración en toda la cadena de suministro de la red, lo que puede aumentar los vectores de ataque. Por otro lado, Open RAN añade transparencia a las cadenas de suministro, da a los operadores mayor visibilidad y les permite supervisar y detectar los riesgos de seguridad. En pocas palabras, Open RAN les permite entender mejor la arquitectura y los equipos de red, y facilita una detección y gestión de vulnerabilidades más completas. La O-RAN Alliance, principal fuente de especificaciones de Open RAN, está trabajando en especificaciones de seguridad para la arquitectura de estas redes con el objetivo de normalizar estas especificaciones en el ETSI.

En Japón, NTT Docomo es uno de los operadores que ha adoptado la arquitectura Open RAN por su flexibilidad en la elección de equipos. La decisión planteó interrogantes desde el punto de vista de la seguridad, ya que en general se considera que la apertura significa un aumento en el número de oportunidades de ataques. Ahora bien, el operador comparó la RAN tradicional y la Open RAN, y llegó a la conclusión de que hay poca diferencia entre ambas a nivel de la seguridad[1].

[1] Para más información sobre la seguridad de Open RAN, véase por ejemplo https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

5.5 Ejemplos de políticas y reglamentos nacionales para asegurar la red 5G

Además de las normas y prácticas de los proveedores y operadores, a nivel nacional se pueden proponer políticas y reglamentos para asegurar las redes 5G. Estas pueden adoptar diversas formas, desde evaluaciones de proveedores, hasta pruebas, certificaciones y definición de directrices o requisitos. Aunque los enfoques difieren en función de los contextos nacionales, todas estas iniciativas tienen por objeto reducir los riesgos de seguridad que presenta la 5G, incluidos los riesgos cibernéticos específicos. Los regímenes de aplicación y cumplimiento también deberían tenerse en cuenta como parte del marco general.

Los ejemplos siguientes ofrecen una instantánea de las diferentes medidas adoptadas por varios países y regiones para conseguir la ciberseguridad en las redes 5G y su estado actual:

- El enfoque integral de **Brasil** para la ciberseguridad de la 5G se centra en la gestión de riesgos con los operadores. De acuerdo con los términos de la subasta de espectro 5G y el Reglamento de Ciberseguridad del Sector de las Telecomunicaciones[122], los operadores 5G están obligados a cumplir el marco reglamentario que incluye principios, directrices y controles *ex ante* para velar por la ciberseguridad en todo el sector. Estos controles combinan la gobernanza en materia de ciberseguridad, la notificación obligatoria de incidentes, el intercambio de información, los ciclos de evaluación de vulnerabilidades y la presentación de informes sobre las infraestructuras críticas, entre

[122] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740; https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (ambos documentos están en portugués)

otras disposiciones. La Agencia Nacional de Telecomunicaciones de Brasil (Anatel) también se ha asociado con instituciones académicas para realizar estudios al respecto[123].

- El Gobierno del **Reino Unido** desarrolló un marco de seguridad para los proveedores de redes o servicios públicos de comunicaciones electrónicas mediante la Ley de Comunicaciones de 2003, modificada por la Ley de Telecomunicaciones (Seguridad) de 2021 (la TSA). Este marco se aplica a la 5G y a todas las demás redes: aunque el Reino Unido está haciendo la transición a una futura 5G y a todas las redes de fibra óptica completa, muchos proveedores de red incorporan tecnologías más antiguas en su infraestructura. En la TSA se establecen nuevas obligaciones de seguridad para todos los proveedores de telecomunicaciones públicas[124] y se otorgan nuevas facultades al Secretario de Estado para aprobar reglamentos y publicar códigos de práctica, que desde entonces han sido elaborados y justificados mediante consulta pública[125]. En la TSA también se incluyen disposiciones que refuerzan las facultades reglamentarias de OFCOM para supervisar la manera en que los proveedores cumplen con sus nuevas obligaciones y para hacer que estos las cumplan.
- Se sabe que los reglamentos y las políticas de ciberseguridad de la 5G de la **República de Corea** son de los más estrictos del mundo, lo que refleja la posición de liderazgo del país en la adopción de la tecnología 5G. El Gobierno coreano, a través del Ministerio de Ciencia y TIC (MSIT) y la Agencia de Internet y Seguridad de Corea (KISA), ha implementado un marco integral para salvaguardar las redes 5G. El marco incluye requisitos estrictos de ciberseguridad para que los operadores de telecomunicaciones aseguren la infraestructura de red, protejan los datos de los usuarios y reduzcan los riesgos de ciberseguridad. Los reglamentos se centran en la necesidad de contar con cadenas de suministro seguras, normas de cifrado avanzadas y el despliegue de principios de seguridad por diseño en la arquitectura de red. Además, la República de Corea colabora con asociados internacionales y organismos de normalización para que sus medidas de seguridad 5G se ajusten a las buenas prácticas mundiales.
- El marco jurídico y técnico establecido para fortalecer la ciberseguridad de la 5G en la **India** incluye:
  - directivas de seguridad nacionales en el sector de las telecomunicaciones, que garantizan que se atiendan las preocupaciones y vulnerabilidades de las cadenas de suministro y sus fuentes;
  - pruebas y certificaciones obligatorias de equipos de telecomunicaciones, que garantizan el cumplimiento de los requisitos de seguridad esenciales de cada función de la red 5G; y
  - condiciones de concesión de licencias a los proveedores de servicios de telecomunicaciones, en las que se prevé la realización de auditorías públicas periódicas de seguridad de la infraestructura de telecomunicaciones.

  Para apoyar lo anteriormente expuesto, se han puesto en marcha diversos mecanismos institucionales, por ejemplo: el Centro Nacional para la Seguridad de las Comunicaciones (NCCS), encargado de preparar requisitos y normas de seguridad de las telecomunicaciones (denominados también requisitos para velar por la seguridad de las telecomunicaciones de la India o ITSAR, por sus siglas en inglés), y sus laboratorios de prueba y certificación de seguridad asociados; la creación de Telecom-CSIRT, un EIISI dedicado al sector nacional de las telecomunicaciones; y varias medidas de gestión del fraude y de protección del consumidor centradas en el ciudadano. En lo que respecta a los protocolos y normas de seguridad como 3GPP, la India tuvo en cuenta las especificaciones propuestas en las normas del sector para la supervisión de la

[123] Algunos de los resultados pueden consultarse en https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (en portugués)
[124] Excepto microentidades
[125] https://www.legislation.gov.uk/uksi/2022/933/contents/made; https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

conformidad y otras condiciones de las licencias de telecomunicaciones donde se incluían auditorías de seguridad periódicas en las redes de los proveedores de servicios.

- En los **Emiratos Árabes Unidos**, la seguridad de las redes 5G se trabaja mediante una estrategia múltiple que incluye rigurosos cibersimulacros y cursos de formación nacionales, la creación del Centro Nacional de Operaciones de seguridad (SOC) para la visibilidad y respuesta a las amenazas en tiempo real, y la iniciativa Cyber Pulse, que sensibiliza y forma al personal en estrategias de defensa clave. Se hace hincapié en la colaboración y el intercambio de información con asociados internacionales, proveedores, instituciones académicas y otras partes interesadas para reforzar las medidas de ciberseguridad. Además, se ha establecido un marco de ciberseguridad resiliente en consonancia con normas internacionales como las de la ISO y el NIST para garantizar el cumplimiento en todo el sector de las telecomunicaciones. A fin de fomentar la confianza de los consumidores y las empresas en la seguridad de la 5G, el país cuenta con políticas, procedimientos y leyes de gobernanza que promueven los principios de seguridad por diseño y las prácticas de seguridad responsables entre los proveedores. Por último, el país ha adoptado un enfoque de ciberseguridad centrado en las personas, la formación, la sensibilización y el apoyo para empoderar a los individuos y las organizaciones en la lucha contra las ciberamenazas, a fin de cimentar así una sólida defensa contra las posibles amenazas en la red 5G.
- **Zimbabwe** está trabajando en la ciberseguridad 5G, centrándose en la reciente importancia que tiene la computación periférica y explorando la adopción de la tecnología Open RAN para ofrecer flexibilidad a los proveedores. Aunque no existe una ley de seguridad 5G como tal en Zimbabwe, la legislación vigente sobre protección de datos y un documento de gobernanza de la IA en curso sustentan el enfoque del país. Zimbabwe armonizará sus prácticas de seguridad con normas internacionales como la ISO/CEI 27001 y las normas de NIST, para que las nuevas interfaces radioeléctricas 5G cumplan con los protocolos de seguridad establecidos. El Organismo Regulador de Correos y Telecomunicaciones de Zimbabwe vela por el cumplimiento de las directrices de seguridad y sensibiliza al sector sobre el mantenimiento de la integridad de la infraestructura nacional de telecomunicaciones.
- **Kenya** adoptó su hoja de ruta y estrategia para la 5G de comunicaciones móviles en abril de 2022. En la estrategia se reconoce que la seguridad es un aspecto importante de la arquitectura de red 5G. La naturaleza cambiante de los servicios conectados y el aumento significativo previsto en el número y los tipos de dispositivos conectados aumentan la importancia de la privacidad de los datos, la protección de estos y la ciberseguridad en Kenya; esto incluye la detección de amenazas, la autenticación de los usuarios y las buenas prácticas operativas. La 5G proporciona una mayor seguridad por diseño, integrando requisitos de seguridad mejorados sobre la base de la evolución de la red y adaptando las enseñanzas extraídas de tecnologías anteriores. La Autoridad de Comunicaciones de Kenya ha adoptado una norma internacional aprobada y elaborada por la UIT y 3GPP para velar por la interoperabilidad y seguridad de los sistemas móviles. El organismo tiene previsto aprovechar los conocimientos especializados de diversas partes interesadas y las buenas prácticas internacionales en materia de ciberseguridad para elaborar códigos técnicos y aplicar una lista de comprobación mínima normalizada para la evaluación de la seguridad a fin de garantizar que las redes 5G cumplan las normas técnicas más modernas y estén en consonancia con las normas mundiales en relación con la seguridad 5G.
- Tras un amplio examen de los riesgos de ciberseguridad de las redes 5G, la **Unión Europea** elaboró un conjunto de herramientas para reducir los riesgos[126] con el objetivo de definir un conjunto común de medidas destinadas a atenuar los principales riesgos de ciberseguridad 5G y facilitar la selección de medidas prioritarias de mitigación a escala nacional y europea. En la Estrategia de Ciberseguridad para la Década Digital se destaca la importancia de salvaguardar la próxima generación de redes móviles de banda ancha y figura un apéndice específico sobre los próximos pasos para la ciberseguridad de

[126] https://digital-strategy.ec.europa.eu/es/node/1215

las redes 5G[127]. El marco de certificación de la Unión Europea comprende la constante evolución de un sistema de certificación de ciberseguridad 5G[128].

5.6 Dificultades relativas a la aplicación y el cumplimiento

Aunque la formulación de políticas es esencial, la atención debería centrarse en su aplicación efectiva. Para garantizar la solidez de la ciberseguridad de las redes 5G, es necesario contar con mecanismos de información, cumplir las normas pertinentes y disponer de medidas de política y aplicación prácticas. Los nuevos marcos por los que se introducirán cambios significativos en la seguridad de las redes de telecomunicaciones exigirán un proceso continuo de cumplimiento para los proveedores de servicios de telecomunicaciones y, por lo tanto, un estrecho compromiso con el sector. En el **Reino Unido**, OFCOM utiliza un modelo de supervisión en el marco de su política de seguridad de las telecomunicaciones y colabora con los equipos técnicos y reglamentarios de los proveedores de telecomunicaciones. El organismo regulador considera que la aplicación no se limita a las medidas técnicas, sino que requiere también un cambio cultural en la forma en que los proveedores de telecomunicaciones conciben la ciberseguridad, exigiéndoles que identifiquen y rindan cuentas por las partes que conforman sus redes y los servicios que han subcontratado. Comprometerse al nivel superior y obtener el compromiso y el patrocinio de los gobiernos, organismos reguladores y el sector es un requisito previo para cualquier éxito[129].

En **Malasia**, el Gobierno ha aprobado un nuevo proyecto de ley de ciberseguridad por el que se establece un único organismo para gestionar todas las infraestructuras críticas. Las redes de telecomunicaciones, incluidas las redes 5G, entran en el ámbito de aplicación de este nuevo proyecto de ley de ciberseguridad. El organismo regulador[130] está elaborando un conjunto de requisitos para que los operadores informen sobre la conformidad relativa a la seguridad. Como parte del producto intermedio de la Cuestión 3/2 sobre la ciberseguridad de la 5G[131], uno de los operadores del país destacó que la aplicación de la nueva política podía suponer dificultades, ya que implicaba comunicar el riesgo y elaborar requisitos mínimos de seguridad que requerían tiempo, costo y una concertación intensiva que con frecuencia incidía en los intereses de los accionistas. Para los operadores con accionistas, las estructuras, políticas y reglamentos en materia de seguridad a veces no son congruentes, lo que puede suponer dificultades para los equipos de seguridad. Por tanto, es necesario que todos los equipos colaboren, incluidos los altos directivos, a la hora de considerar nuevos marcos de seguridad.

5.7 Necesidad de priorizar la inversión en la educación y formación de la fuerza de trabajo

Según Allied Market Research[132], está previsto que el mercado mundial de la seguridad 5G alcance los 37 800 millones USD en 2031. Junto a ello se producirá una creciente demanda de profesionales de la ciberseguridad, en particular aquellos con habilidades especializadas para proteger las redes 5G. Los países, las organizaciones y las instituciones deben priorizar la formación y contratación de personal para velar por el avance de la ciberseguridad 5G. Las

127 https://digital-strategy.ec.europa.eu/es/node/435
128 https://certification.enisa.europa.eu/index_en?prefLang=es&etrans=es
129 Documento SG2RGQ/191 de la CE 2 del UIT-D, presentado por el Reino Unido
130 https://www.nacsa.gov.my/act854.php
131 https://www.itu.int/hub/publication/d-stg-sg02.03.2-2024/#/es
132 https://www.alliedmarketresearch.com/5g-security-market-A12820

competencias especializadas necesarias son actualmente difíciles de encontrar en la fuerza de trabajo; además, es difícil lograr el equilibrio de género en la contratación. Si la fuerza de trabajo no está preparada, esto ralentizará y complicará la transición a la 5G. Aunque los países deben dar prioridad a la formación y la educación a través de programas nacionales, el sector privado también puede explorar programas de formación y mejora de las competencias, ya que para satisfacer las necesidades se requiere la participación del sector en general.

Un ejemplo de país que está encontrando soluciones a los problemas ligados a la fuerza de trabajo es **Türkiye**, que ha aumentado la inversión en educación y capacitación de personal capaz de gestionar las complejidades de la seguridad 5G. En el marco de este compromiso, se creó el sitio de pruebas abierto 5G Valley por iniciativa de instituciones clave como la Autoridad de Tecnologías de la Información y la Comunicación, la Universidad Técnica de Oriente Medio, la Universidad İhsan Doğramacı Bilkent, la Universidad Hacettepe, y de los operadores de telecomunicaciones Türk Telekomünikasyon A.Ş., Turkcell İletişim Hizmetleri A.Ş. y Vodafone Telekomünikasyon A.Ş. Este sitio sirve de plataforma fundamental para la investigación, el desarrollo y las pruebas de tecnologías 5G y posteriores, lo que brinda oportunidades para la colaboración académica y del sector. El consejo ejecutivo de 5G Valley, integrado por representantes de las instituciones mencionadas, garantiza la implementación efectiva de esta iniciativa. Al proporcionar una plataforma en la que académicos, investigadores, estudiantes de doctorado y empresas emergentes pueden participar en trabajos relacionados con la 5G y tecnologías posteriores, el sitio de pruebas abierto 5G Valley no solo fomenta la innovación, sino que también contribuye al desarrollo de una fuerza de trabajo altamente calificada. Esta iniciativa forma parte integrante de la estrategia de Türkiye de priorizar y mejorar la seguridad de las redes 5G mediante inversiones continuas en educación, formación e investigación[133].

5.8 Más allá de la 5G: marcando el rumbo hacia la ciberseguridad 6G

Aunque la 5G aún se está planificando y desplegando en muchos países y regiones, el campo de la investigación y el desarrollo, así como de los procesos de normalización, ya ha comenzado a mirar más allá de estas redes. Así, a finales de 2023, el Sector de Radiocomunicaciones de la **UIT** (UIT-R) aprobó el marco y los objetivos generales del desarrollo futuro de las IMT para 2030 y las tecnologías posteriores[134], lo que comercialmente se conoce como 6G.

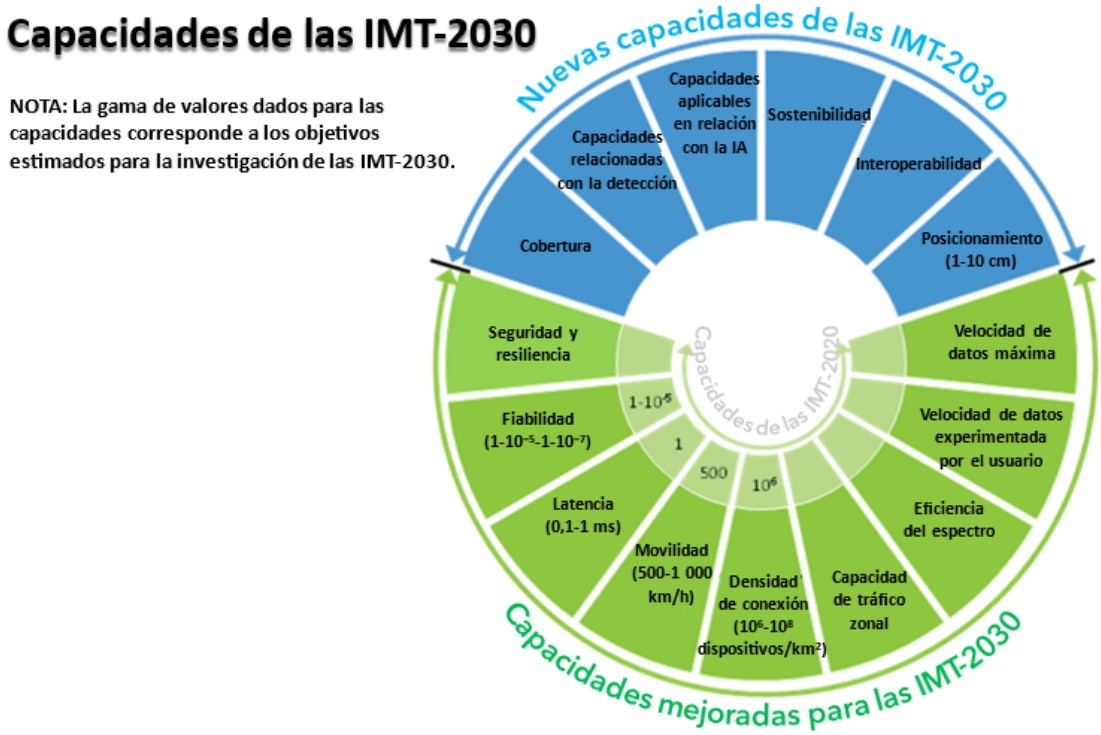
[133] https://5gtrforum.org.tr/en
[134] Recomendación UIT-R M.2160, disponible en https://www.itu.int/rec/R-REC-M.2160-0-202311-I/es

Recuadro 3: IMT-2030

En el marco se destaca la esperanza de que las IMT-2030 sean un factor de facilitación importante para lograr una mayor seguridad y resiliencia. Se cuenta con que la tecnología sea segura por diseño y tenga la capacidad de seguir funcionando durante un evento perturbador, ya sea natural o provocado por el hombre, y recuperarse rápidamente de él. En el documento también se reafirma que la seguridad y la resiliencia de los sistemas IMT-2030 son fundamentales para alcanzar objetivos sociales y económicos más amplios.

En el contexto de las IMT-2030, la seguridad está definida por el marco como la "preservación de la confidencialidad, integridad y disponibilidad de la información, como los datos de usuario y la señalización, y la protección de redes, dispositivos y sistemas contra ciberataques como el pirateo, la denegación de servicio distribuida, los ataques de intermediarios, etc.". La resiliencia se define como la "capacidad de las redes y sistemas para seguir funcionando correctamente durante y después de una perturbación natural o provocada por el hombre, como la pérdida de una fuente primaria de energía, etc.".

Figura 2: Capacidades de las IMT-2030



Fuente: UIT

Ha quedado claro que ya existe una visión de la 6G y que se ha planteado el inicio de sus procesos de normalización con una firme preocupación por la seguridad y la resiliencia, a diferencia de las primeras fases de diseño de la tecnología 5G, incluso desde el punto de vista de la normalización. La comparación con la perspectiva para las IMT-2020 (conocida comercialmente como 5G), que se aprobó en 2015[135], pone de manifiesto el cambio de planteamiento al reconocerse la necesidad de abordar adecuadamente la ciberseguridad y la ciberresiliencia, como pilar facilitador de la transformación digital y la economía digital.

[135] Recomendación UIT-R M.2083 disponible en https://www.itu.int/rec/R-REC-M.2083-0-201509-I/es

Capítulo 6 – Desafíos y enfoques para abordar la suplantación por SMS

Los SMS son utilizados por actores maliciosos como vector de ataques. En todo el mundo, se ha producido un importante aumento del uso del SMS para el envío de correo basura[136] y timos por mensaje de texto. Para estos últimos, se utilizan tácticas con el fin de engañar a los usuarios para que proporcionen sus datos personales, como los datos financieros, y descarguen programas maliciosos en sus dispositivos. Los timos por SMS no solo reducen la confianza del usuario en los servicios de telecomunicaciones y mensajería, así como su satisfacción, sino que además son una pérdida de recursos de red.

Según los datos de la Comisión Federal de Comercio de Estados Unidos, en 2022 se comunicaron pérdidas de 330 millones USD debidas a timos por mensajes de texto, lo que supera el doble de la cifra comunicada en 2021[137]. Durante el mismo periodo, en Australia, el programa Scamwatch del Centro Nacional Anti-Scam recibió casi 80 000 denuncias de timos por mensaje de texto de un valor total superior a 28 millones de dólares australianos (AUD)[138].

Aunque el uso de los servicios SMS varía en función de los países, y la innovación en el sector de las telecomunicaciones/TIC ha ofrecido nuevas maneras de comunicarse, en particular mediante las aplicaciones de mensajería móvil de difusión mundial, el servicio de SMS sigue siendo útil para los usuarios debido a su sencillez y disponibilidad en todos los teléfonos móviles.

En este contexto, este capítulo examina la "suplantación por SMS", que es uno de los tipos de incidentes por SMS más prevalentes, establece recomendaciones para combatir este fenómeno y ofrece algunas experiencias y enfoques nacionales para hacer frente a estos desafíos[139].

6.1 Suplantación por SMS

El término "suplantación de identidad" o "phishing" se aplica al uso de correos electrónicos, mensajes, llamadas de voz o mensajes por medios sociales que parecen legítimos pero que el autor realiza con el objetivo de engañar al destinatario, normalmente haciéndose pasar por una persona o entidad fiable como un banco, un organismo público, un empleador o un familiar. Con frecuencia, el usuario es dirigido hacia un sitio web en el que introducirá datos personales, lo que dará lugar a un robo de identidad, o bien podrá ser inducido a proporcionar información personal como su información bancaria o los datos de su tarjeta de crédito, o a realizar un pago a una cuenta falsa.

---

136 El correo basura se define como "la información electrónica que circula desde el remitente hasta el destinatario mediante terminales tales como computadores, teléfonos móviles, teléfonos, etc. que, por regla general, es información no solicitada ni deseada y perjudica a los destinatarios" en la Recomendación UIT-T X.1242 – https://www.itu.int/rec/T-REC-X.1242-200902-I/es.

137 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

138 https://www.scamwatch.gov.au/research-and-resources/scam-statistics

139 Este tema está muy interrelacionado con los servicios de telecomunicaciones generales y las actividades en línea contra el fraude. El Informe Final sobre la Cuestión 6/1 (Información, protección y derechos del consumidor) tiene un apartado especialmente dedicado al fraude en línea.

En el ámbito de la ciberseguridad, uno de los tipos de timos cada vez más frecuentes es el "smishing" o suplantación por SMS, que es un término que combina las palabras "phishing" y "SMS" y se refiere al envío de mensajes de suplantación de identidad a teléfonos móviles mediante SMS. Según el Suplemento 29 de la Recomendación UIT-T X.1242[140], el "smishing" o "suplantación por SMS" es "un ataque por el cual se induce al usuario a descargar un troyano, un virus u otro programa malicioso en su teléfono celular u otro dispositivo móvil" y el "phishing" o "suplantación de identidad" se define como "un ataque para adquirir información sensible como nombres de usuario, contraseñas y detalles de las tarjetas de crédito por motivos maliciosos, que el autor realiza haciéndose pasar por una entidad digna de confianza en una comunicación electrónica".

Los ataques por *smishing* se han convertido en una creciente amenaza en los últimos años, y el uso de las herramientas de IA ha intensificado su prevalencia, lo que pone de manifiesto la magnitud y la naturaleza cada vez más sofisticada de este nuevo tipo de ciberataques. En 2022, más de la mitad de los dispositivos móviles personales y la cuarta parte de los dispositivos móviles de empresa habían registrado al menos un ataque de suplantación de identidad por trimestre, y el uso del *smishing*, que era uno de los tipos de ataques de suplantación de identidad no basados en el correo electrónico, aumentó en más de siete veces en el segundo trimestre de 2022[141].

A veces, los usuarios de los servicios de comunicaciones tienen dificultades para identificar este tipo de ataques. Al utilizar técnicas de ingeniería social, los actores maliciosos envían mensajes falsos a dispositivos móviles, incitando a los destinatarios a pulsar los enlaces URL que figuran en dichos mensajes. Los ciberdelincuentes podrían utilizar servicios de acortamiento de URL para ocultar enlaces de conexión falsos, dificultando así la determinación de si el mensaje procede de un estafador. Hay unos pocos indicios del carácter fraudulento de un mensaje como, por ejemplo, la falta de relación del mensaje con el destinatario; el carácter a menudo urgente del mensaje; el envío del mensaje desde un número de teléfono desconocido; la inclusión en el mensaje de errores de ortografía o gramática; y la inclusión en el mensaje de un enlace sospechoso.

Los usuarios deben ser conscientes del riesgo y las medidas que pueden adoptar para no convertirse en víctimas de un ataque por *smishing*. Asimismo, hay funciones importantes que deben desempeñar los proveedores de servicios, así como el sector público, y no solo en el sector de las telecomunicaciones, a fin de garantizar el cumplimiento de las normas y las buenas prácticas y promover también la concienciación sobre la suplantación por SMS entre la población.

6.2 Enfoques adoptados para luchar contra la suplantación por SMS

6.2.1 Enfoques de los países para luchar contra la suplantación por SMS

Durante el ciclo de estudios, los Estados Miembros de la UIT se centraron en la elaboración de normas, la concienciación, la colaboración con el sector privado y la cooperación internacional a fin de luchar contra la suplantación por SMS. Si bien se realizan actualmente muchos esfuerzos para hacer frente los desafíos que plantea la suplantación por SMS, es evidente que no existe

[140] https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13409
[141] https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf

una única solución válida para resolver este problema, y que es necesario adoptar un enfoque multifacético, en particular teniendo en cuenta el carácter delictivo de estos ataques.

Este último enfoque ha sido adoptado por la **Federación de Rusia**[142], que en el artículo 159 de su Código Penal tipifica como delito las acciones cometidas por los autores de estafas por teléfono, entre ellas la suplantación por SMS. Además, la administración de la Federación de Rusia ha adoptado medidas para prohibir el arrendamiento de números móviles virtuales, que entraron en vigor en septiembre de 2024. El arrendamiento de números móviles virtuales se consideró una amenaza para la seguridad, dado que los actores maliciosos utilizan números provisionales para crear cuentas en redes sociales y aplicaciones de mensajería con el fin de difundir amenazas. Otra medida adoptada por la administración de la Federación de Rusia fue el lanzamiento de una plataforma antifraude para proporcionar servicios de verificación de las llamadas telefónicas. Con la ayuda de la plataforma, los proveedores de servicios de telecomunicaciones conectados comprueban los números y su autenticidad, y bloquean las llamadas y SMS antes de que puedan llegar a su destinatario. La conexión al sistema, que es obligatoria para todos los proveedores de servicios de telecomunicaciones aprobados para prestar servicios de comunicación por voz, es gratuita, y la no conexión conduce a una multa de entre 600 000 y 1 millón de rublos rusos (RUB). Estas iniciativas también han sido complementadas por campañas de sensibilización para empoderar a los usuarios.

El Gobierno de **Australia** también ha adoptado un enfoque integral que abarca iniciativas de la industria y el Gobierno junto con esfuerzos de sensibilización. La lucha contra las estafas por SMS se ha convertido en una prioridad en materia de conformidad en los últimos años para la Autoridad Australiana de Comunicaciones y Medios de Comunicación (ACMA), que ha emitido una serie de normas nuevas. Algunas de ellas son: la obligación de identificar, rastrear y bloquear las llamadas y mensajes de textos falsos, impuesta a los proveedores de telecomunicaciones; la imposición de procesos de verificación de identidad más estrictos antes de que los proveedores puedan transferirse números móviles; y la imposición de procesos de verificación de identidad más estrictos para las operaciones de alto riesgo, como el intercambio de SIM y las solicitudes de cambio de cuenta. La ACMA audita a los proveedores de servicios de telecomunicaciones que envían mensajes de texto masivos y estas medidas de observancia han revelado que los actores maliciosos han explotado las vulnerabilidades creadas por la falta de conformidad para enviar estafas por SMS de alto perfil a los australianos[143].

Otras actividades de observancia llevadas a cabo por la ACMA para luchar contra las estafas en las telecomunicaciones son: la emisión de alertas a los consumidores acerca de la suplantación de organismos públicos y las estafas relativas al acceso remoto; la colaboración en la sombra con los proveedores de servicios de telecomunicaciones, los organismos públicos y las marcas conocidas para poner fin a las estafas por teléfono; y el inicio de la cooperación internacional con otras naciones y organismos reguladores a fin de fortalecer la colaboración estratégica en la lucha mundial contra las estafas, el telemárketing no solicitado y el correo basura.

Además, el Gobierno de Australia empezó la puesta en marcha progresiva de medidas antifraude específicas en 2023, como el establecimiento de un Centro Nacional Anti-Scam (NASC), la creación de una página web con una función de retirada para suprimir las páginas destinadas a las estafas relativas a la inversión y la introducción de un registro de identificadores de emisores de SMS.

[142] Documento 2/158 de la CE 2 del UIT-D, presentado por la Federación de Rusia
[143] Documento 2/154 de la CE 2 del UIT-D, presentado por Australia

La cooperación y asociación entre los actores implicados han conformado un enfoque coherente que han adoptado numerosos países y constituye la piedra angular de las iniciativas emprendidas por la **República de Corea**. El país ha facilitado la compartición de datos sobre las amenazas relativas a las tácticas de suplantación por SMS a fin de identificar y mitigar con mayor rapidez los nuevos vectores de ataques, así como sistemas de denuncia automatizados que pueden utilizar los usuarios y compartir con los proveedores de servicios de telecomunicaciones con fines de bloqueo.

Las herramientas de IA también pueden ayudar a combatir la suplantación por SMS como lo ilustra el ejemplo de la República de Corea, donde el MSIT y la KISA implementaron una serie de medidas específicamente diseñadas para hacer frente a la suplantación por SMS, a saber:

- la supervisión y el bloqueo en tiempo real de mensajes de suplantación por SMS por conducto de un sistemas de detección y filtrado basado en la IA que analiza patrones de SMS;
- la identificación de mensajes sospechosos para su bloqueo, y la detección de URL maliciosas integradas en los SMS;
- la creación de una base de datos de números maliciosos mantenida y compartida por los proveedores de servicios de telecomunicaciones;
- la implementación de sistemas de filtrado por IA; y
- y la creación de una línea telefónica nacional de denuncias (118) y portales en línea operados por la KISA[144].

Estas actividades ilustran la importancia de abordar las diversas dimensiones del fenómeno y la necesidad de colaborar con los proveedores de servicios de telecomunicaciones; de adoptar tecnologías nuevas y emergentes que faciliten el análisis, filtrado y bloqueo de mensajes; de implementar los procedimientos y procesos necesarios; de desarrollar y mantener un sistema de denuncias; de hacer uso de los datos comunicados; y también de trabajar intensamente en la concienciación de la población. No puede subestimarse la importancia de concienciar a los usuarios. Con frecuencia, los actores maliciosos cambian, perfeccionan y reinventan frecuentemente sus métodos y un usuario bien informado, empoderado y consciente tiene muchas más probabilidades de no convertirse en víctima de sus ataques.

6.2.2 Enfoques de la industria para luchar contra la suplantación por SMS

El sector de las telecomunicaciones ha tomado medidas positivas para combatir y mitigar los efectos de la suplantación por SMS y de las estafas en general. En cuanto a los métodos técnicos, los proveedores han introducido medidas como los mecanismos de denuncia, los cortafuegos de SMS, el bloqueo de URL de sitios de suplantación de identidad conocidos y los registros de protección de los identificadores de emisores de SMS. Los cortafuegos de SMS pueden impedir que grandes cantidades de mensajes no deseados lleguen a los usuarios, y los registros de identificadores de emisores de SMS permiten a las organizaciones registrar y proteger los encabezamientos de mensajes utilizados al enviar SMS a los clientes, lo que limita el impacto de la suplantación por SMS y la usurpación de dirección IP. Las denuncias de estafas, cuando se realizan de manera coordinada entre múltiples operadores móviles, constituye un método eficaz para identificar y suprimir estafas. El servicio de señalamiento del 7726 implementado en el **Reino Unido** y **Canadá** permite denunciar mensajes sospechosos

[144] Documento 2/312 de la CE 2 del UIT-D, presentado por la República de Corea

a efectos de investigación[145]. En 2014, los cuatro operadores móviles principales del Reino Unido, en colaboración con la Oficina del Comisionado de Información del Reino Unido, implementaron voluntariamente el servicio de señalamiento del 7726 para que las personas reenviasen de manera gratuita los mensajes de texto sospechosos, así como el correo basura. En marzo de 2025, se habían suprimido 26 000 números de estafadores[146].

El fraude por pago autorizado es otro problema que conlleva una importante pérdida financiera para los consumidores debido a que los delincuentes entran en contacto con las víctimas por SMS o por una llamada telefónica haciéndose pasar por una organización legítima, como un banco, y a continuación logran recibir un pago por transferencia. La **GSMA** y **UK Finance** reunieron a los operadores móviles y bancos del Reino Unido para ofrecer "Scam Signal", una solución que utiliza una interfaz de programación de aplicaciones para que los bancos puedan identificar y detener mejor las transferencias fraudulentas[147].

En muchos países del África subsahariana, donde los servicios de dinero móvil son muy populares, la mejora de la seguridad en estas plataformas constituye un aspecto capital. "M-Pesa" en **Kenya**, y otros servicios similares en otros países, han integrado la autenticación biométrica y han mejorado el cifrado y los sistemas de detección de fraudes para proteger a los usuarios contra la suplantación de la identidad y los ataques por *phishing*[148]. En general, los operadores de todas las regiones están implementando diversas API como la de "verificación de números" que eliminan la necesidad de utilizar otro método de autenticación como el de la contraseña y pin de un solo uso y que, en su lugar, comprueban que el usuario está interactuando con un servicio desde un dispositivo dotado de un número de teléfono móvil previamente registrado/asociado. Los procesos de "conocimiento del cliente" se utilizan cada vez más para proporcionar un proceso de familiarización más seguro, incluso para los servicios de dinero móvil, validando la información de contacto del usuario y mitigando el riesgo de robo de identidad.

Telstra, el mayor operador de telecomunicaciones de Australia, opera un filtro de estafas por SMS que analiza el contenido de los mensajes a fin de detectar patrones y características dudosos, y a continuación identifica y bloquea los mensajes maliciosos que contengan enlaces o números de teléfono sospechosos[149]. Los proveedores de telecomunicaciones también se asocian con el sector privado para luchar contra los timos telefónicos. Por ejemplo, el segundo proveedor de telecomunicaciones más importante de Australia, **Optus**, puso en marcha una iniciativa de interrupción de llamadas junto con Australian Financial Crimes Exchange y miembros del sector bancario, incluidos los principales bancos[150]. Al centrarse en los timos por devolución de llamada, el programa impide que los clientes de Optus marquen números de estafadores identificados y, en su lugar, reenvía la llamada hacia un mensaje automático que los advierte del riesgo de estafa. Los bancos y operadores de telecomunicaciones también informan a los usuarios de métodos preventivos a fin de consolidar los esfuerzos encaminados a luchar contra la suplantación por SMS y el fraude en las telecomunicaciones.

---

145 https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/7726-reporting-scam-texts-and-calls/; https://www.getcybersafe.gc.ca/en/blogs/reporting-spam-text-messages-7726

146 Documento 2/393 de la CE 2 del UIT-D, presentado por el Reino Unido

147 https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/

148 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/social-engineering-and-impersonation-fraud/; https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf

149 Documento 2/154 de la CE 2 del UIT-D, presentado por Australia

150 *Ibid.*

La **GSMA** facilita la colaboración y la compartición de información por conducto del Grupo de Trabajo sobre el Fraude y la Seguridad (FASG)[151] y el Centro de Análisis e Intercambio de Información en el ámbito de las Telecomunicaciones (T-ISAC)[152]. Ambos son plataformas seguras que ayudan a facilitar el intercambio de información en tiempo real a escala mundial.

Los esfuerzos para combatir la suplantación por SMS y los timos en las telecomunicaciones requieren asociaciones sólidas entre todas las partes interesadas. El Gobierno no puede por sí solo detener las actividades de los estafadores. Tras el registro y la aplicación de normas por la ACMA para identificar y bloquear las llamadas falsas en diciembre de 2020, y los mensajes de texto falsos en julio de 2022, los proveedores de telecomunicaciones han comunicado que se bloquearon más de 1 400 millones de llamadas falsas y más de 257 millones de mensajes falsos hasta finales de junio de 2023[153].

Además, se debe considerar la posibilidad de llevar a cabo campañas de información pública sobre las denuncias de estafas a fin de aumentar el número de denuncias. En el **Reino Unido**, algunas organizaciones como el Centro Nacional de Ciberseguridad y algunas fuerzas de la policía local han dado publicidad al servicio de denuncias del 7726, y OFCOM, el organismo regular de las telecomunicaciones, ha establecido instrucciones sencillas en un formato de vídeo por etapas, en el que se explica la manera de denunciar tanto los mensajes de texto como las llamadas al 7726 en la mayoría de los principales modelos de teléfonos inteligentes. Recientemente, la incorporación de un botón de denuncia de correo basura en la gran mayoría de los teléfonos inteligentes del mercado del Reino Unido ha disparado considerablemente la tasa de denuncias de mensajes falsos. Esta nueva funcionalidad actúa de la misma manera que el servicio del 7726, dado que la información se comunica a los operadores móviles por conducto de una base de datos común de terceros. Este cambio ha dado lugar a un aumento del número de denuncias en un 800% en un año[154].

Dado que las medidas adoptadas hasta la fecha han dado resultados positivos, debe considerarse la posibilidad de adoptar un enfoque holístico que incluya a las diferentes partes interesadas, como las autoridades públicas, los bancos y los operadores de telecomunicaciones, además de los usuarios.

151 https://www.gsma.com/get-involved/working-groups/fraud-security-group/
152 https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/
153 Documento 2/154 de la CE 2 del UIT-D, presentado por Australia
154 Documento 2/393 de la CE 2 del UIT-D, presentado por el Reino Unido

Conclusiones

El uso de las telecomunicaciones/TIC ha sido extremadamente importante para fomentar el desarrollo y crecimiento social y económico en todo el mundo. La seguridad en las redes de información y comunicación y el fomento de una cultura de la ciberseguridad son hoy en día fundamentales, especialmente en vista del continuo aumento de la adopción y el uso de las telecomunicaciones/TIC. Durante este periodo de estudios, la Cuestión 3/2 analizó numerosos aspectos de la ciberseguridad, examinó contribuciones de los miembros de la UIT y celebró dos talleres en cuyos debates se basan este Informe y sus conclusiones.

En el capítulo 1 se reveló que las iniciativas de sensibilización en materia de ciberseguridad han abarcado tanto programas amplios destinados a diversas partes de la población como intervenciones específicas centradas en temas como la higiene de la ciberseguridad y la sensibilización sobre los timos. De manera análoga, las políticas de educación y formación en materia de ciberseguridad han revelado diferentes grados de madurez. Algunos países han implementado estrategias completas destinadas a mitigar la falta de profesionales de la ciberseguridad, mientras que otros han optado por soluciones de formación más específicas destinadas a componentes de la fuerza de trabajo. Los Estados Miembros han hecho acertadamente hincapié en las iniciativas de protección de la infancia en línea, implementando marcos jurídicos contundentes y elaborando herramientas y programas pragmáticos para que Internet sea más segura para los niños.

En el capítulo 2 se analizaron diversas prácticas de garantía de la ciberseguridad que se han convertido en un elemento esencial para la protección de redes, sistemas y datos contra actividades maliciosas. Si bien no previenen directamente los ataques cibernéticos, su objetivo, si se implementan correctamente, es minimizar el riesgo de estos ataques. Si bien no hay un único enfoque recomendado, las distintas iniciativas han demostrado un movimiento sostenible hacia la adopción de estas prácticas en todo el mundo con autoridades nacionales que, con frecuencia, utilizan enfoques diferentes y combinados, que van desde las autoevaluaciones y directrices voluntarias hasta los sistemas de etiquetado y los controles estrictos del cumplimiento.

En el capítulo 3 se expuso la manera en que los EIIC desempeñan una función esencial para mejorar la resiliencia cibernética de cada país. Su creación y funcionamiento debe seguir priorizándose en los países en desarrollo. La UIT puede ofrecer facilidades de evaluación y creación de EIIC a los países que quieran aumentar su capacidad en materia de EIIC a fin de aumentar la resiliencia de sus IC.

En el capítulo 4 se examinaron enfoques y experiencias en relación con las hojas de ruta nacionales que pueden orientar la mejora de los marcos nacionales de ciberseguridad. En él se destaca que, si bien el panorama de ciberamenazas evoluciona continuamente, los principios fundamentales de la planificación integral, la participación inclusiva de las partes interesadas y la adaptabilidad proactiva siguen siendo esenciales para lograr una implementación exitosa de las estrategias de ciberseguridad. De cara al futuro, estos principios son los que seguirán conformando las defensas de la ciberseguridad resiliente necesarias para salvaguardar los intereses nacionales en un mundo interconectado.

El capítulo 5 se centró en las medidas de ciberseguridad para asegurar las redes 5G. Se han elaborado normas y especificaciones en todos los organismos de normalización y grupos de la industria, y su aplicación debe completarse con medidas proactivas de ciberseguridad

adoptadas por los proveedores y operadores, así como con políticas y reglamentos nacionales. Estos instrumentos pueden adoptar diversas formas en función de los contextos nacionales, como las evaluaciones de proveedores, las pruebas, las certificaciones y la definición de directrices o requisitos.

Por último, en el capítulo 6 se examinaron los esfuerzos para combatir los timos de las telecomunicaciones, en especial la suplantación por SMS, y se destacó la necesidad de contar con fuertes asociaciones entre los sectores público y privado. En el capítulo se destacaron ejemplos de iniciativas gubernamentales y de la industria exitosas para hacer frente al aumento de la suplantación por SMS. Asimismo, la concienciación y educación de los usuarios es fundamental, en particular en vista del mayor grado de sofisticación y de dificultad de detección que presentan estos ataques.

En cuanto al futuro de la Cuestión 3/2, dada la continua evolución del panorama mundial de la ciberseguridad, seguirá siendo fundamental compartir información y enfoques en materia de ciberseguridad. Conviene mantener este tema en el siguiente ciclo de estudios, aunque con una revisión del mandato que preste mayor atención a cuestiones específicas de la ciberseguridad en reflejo del mandato y los destinatarios de la Comisión de Estudio del UIT-D.

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions for Question 3/2

Web	Received	Source	Title
2/408	2025-04-29	RIFEN	Securing contractualization and deed production during the real estate sales process via blockchain technology and machine learning: practices and use cases
Describes the integration of blockchain technology and machine learning solutions for securing real estate transactions. Together, these technologies strengthen stakeholder confidence, while improving the efficiency of real estate transactions. This contribution takes into account existing work and provides an overview of the system we have implemented in Cameroon for the sale of real estate.			
2/405	2025-04-28	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
This contribution provides an update on the activities currently being undertaken by BDT to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated.			
2/393	2025-04-23	United Kingdom	Scam reporting within the UK
Summarises how the largest mobile operators in the United Kingdom voluntarily provide the 7726 reporting service, as a way of identifying, removing, and preventing scams calls and messages.			
2/392	2025-04-2025	RIFEN	Developing countries: strengthening cyber-security
Describes how developing countries face multiple and complex cybersecurity challenges, but with limited means to address the question of how they can ensure that disparities in technical capabilities and funding do not hamper their efforts to enhance cybersecurity.			
2/370	2025-04-14	China	Jointly building cybersecurity: typical practices of safeguarding cyberspace security
Provides an overview of the laws and regulations enacted by China to safeguard cyberspace security, the national campaigns launched to raise people's awareness of cybersecurity, as well as the international initiatives proposed by China on cybersecurity, with the aim of providing reference practices and paths for the world to build secure cyberspaces together.			
2/350	2025-02-27	RIFEN	Artificial intelligence for the detection and reporting of online cyberbullying
Presents the challenge to combat online harassment and the opportunity to integrating artificial intelligence, particularly deep learning techniques, as a promising avenue for improving the protection of sensitive data. The contribution highlights the advantages of designing an intelligent system capable of proactively and automatically identifying threats by combining advanced analysis techniques with proactive cybersecurity strategies.			

(continuación)

Web	Received	Source	Title
2/346	2025-02-04	Tanzania	Best practices for coordinating efforts and developing cybersecurity culture
Highlights good practices for coordinating efforts to promote a culture of cybersecurity in Tanzania. It outlines how various legal, technical, organizational, and capacity development measures, along with cooperation, have been vital in enabling Tanzania to achieve a "Tier 1" ranking and be recognized as a "role model" in the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). It also identifies areas for continuous improvement, especially in technical and capacity development measures.			
2/TD/10 +Ann.1	2024-11-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Reports on the recently conducted CIRT Maturity Assessments in Azerbaijan, Bhutan, Sierra Leone, and Tanzania, the cyberdrills carried out in 2024 to enhance incident response readiness across different regions, the launch of the 5th edition of the Global Cybersecurity Index, BDT assistance in countries and territories in the assessment of their cybersecurity strategies, the Women in Cyber Mentorship Programme and the Her CyberTracks programme, the launch of new online safety tools for children and ongoing capacity building efforts, and other initiatives.			
2/339	2024-11-07	Republic of the Congo	Online communication and transactions via new and emerging telecommunications/ICTs, such as the Internet of Things (IoT)
Outlines challenges in consumer protection with the rise of IoT technology. It highlights issues with data protection, privacy, fair business practices, and device security. Various international responses include legislation, certification, monitoring, and technical standards to safeguard consumer rights and ensure device security.			
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
Details Egypt's dedication to enhancing African nations' communication and information technology skills via the Egyptian African Telecom Regulatory Training Centre (EG-ATRC), providing ITU-accredited training and hosting 381 participants from 30+ countries.			
2/322	2024-10-29	NRD Cyber Security	Strengthening cyber resilience: the role of Lithuania's national CIRT in critical infrastructure protection
Presents a case study on Lithuania's National Computer Incident Response Team within the National Cyber Security Centre, highlighting its functions in critical infrastructure protection through monitoring, incident handling, threat analysis, and collaboration efforts, including European Union initiatives.			
2/320	2024-10-29	Australia	Mandating a minimum standard for consumer-grade smart devices
Describes Australia's transition to mandatory smart device security standards from voluntary security standards, prompted by poor guideline adoption. A Bill proposes enforceable Internet of Things standards, requiring compliance statements from manufacturers and suppliers, and introduces a regulatory model with update flexibility.			
2/312	2024-10-28	Republic of Korea	Challenges and approaches to addressing smishing and SMS incidents in South Korea

(continuación)

Web	Received	Source	Title
Examines smishing threats in the Republic of Korea, detailing the Ministry of Science and ICT and Korea Internet & Security Agency countermeasures, challenges, and government strategies such as AI detection, awareness campaigns, and international cooperation, with recommendations for improvement.			
2/309	2024-10-25	Albania	Creation of a safer cyber ecosystem in a country: the case of Albania
Summarizes Albania's post-cyberattack cybersecurity reforms, including legal and strategic updates, new operations centres, human capital investment, and enhanced international cooperation with entities like the UN and NATO, leading to stronger legal frameworks and preparedness.			
2/301	2024-10-22	China	Mobile anonymous subscription service based on data security protection
Proposes a service for user privacy protection by using temporary numbers and anonymous IDs, with a focus on balancing privacy and digital economy growth, detailing a system architecture that ensures availability, scalability, reliability, usability, observability, and audit logs.			
2/300	2024-10-22	China	Based on anonymous data exchange network, release the value of telecommunications data
Examines the importance of telecommunications data in the digital economy and the challenges of using it, such as privacy issues and integration with Internet data. It details the China Academy of Information and Communications Technology creation of an anonymous data network, enhancing financial risk management and advertising, and supporting sustainable growth and employment in line with the United Nations Sustainable Development Goals.			
2/299	2024-10-22	China Telecommunications Corporation	Building security capabilities to alert phishing websites
Outlines the difficulties the elderly encounter with digital threats such as phishing, and details the China Telecom security tool, which shields them through gateway plug-ins, cloud engines, and a security database, serving over 10 million users in 31 provinces.			
2/276	2024-09-30	Côte d'Ivoire	Cybersecurity in action: strategies and challenges in a connected world - experience of Cote d'Ivoire
Presents the "O'KOHI" web series by a Platform for the Fight against Cybersecurity (PLCC), designed to educate on cybersecurity via videos. Funded by ARTCI and the *Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation*, it addresses hacking, data protection, and cyberattacks, ensuring content accuracy through expert collaboration.			
2/273	2024-09-29	RIFEN	Machine learning-based CVE and CWE analysis
Highlights the need for machine learning to automate Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) analysis, improve identification and prioritization of software vulnerabilities, and overcome challenges such as data quality and model complexity through solutions including data validation and continuous learning. It advocates for collaboration to enhance cybersecurity.			
2/271	2024-09-29	RIFEN	Cybersecurity and cyberspace protection in developing countries

(continuación)

Web	Received	Source	Title
Examines the Internet and information and communication technology impact on Africa's socio-economic progress, addressing cyberattack risks and the necessity for collaborative security efforts. It discusses Africa-specific challenges, infrastructure vulnerabilities, and advocates for a multi-stakeholder strategy to safeguard essential Internet resources.			
2/268	2024-09-24	RIFEN	Cybersecurity awareness for rural youth through online training organized by RIFEN-SADA
Outlines the RIFEN-SADA (Smart Africa Digital Academy) cybersecurity training, which enhanced awareness and skills in cybersecurity among young Africans through fourteen modules. It fostered a security-conscious culture, practical protection knowledge, and guided talent development, leading to certifications and improved job prospects.			
2/254	2024-09-19	Co-Rapporteur for Question 6/1; Co-Rapporteur for Question 3/2	Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024
Presents the workshop on consumer protection in the digital age, discussing infrastructure in underserved regions, security, digital literacy, and data privacy. It stressed digital inclusion, consumer behaviour, and skill gaps, concluding with good practices for ITU deliverables.			
2/246	2024-09-16	RIFEN	Securing the contracting procedure and the production of deeds of purchase in the real estate sale process using blockchain technology and machine learning
Discusses how blockchain technology and machine learning are revolutionizing the real estate industry by enhancing security, efficiency, and decision-making in the sales process. It highlights the benefits of smart contracts and improved market analysis, while acknowledging the challenges of adoption and regulation.			
2/242	2024-09-12	Central African Republic	Operationalization of CSIRT/SOC/PKI platforms and training
Outlines the Central African Republic's cybersecurity measures post-broadband expansion, including the deployment of a Security Operations Centre - Computer Security Incident Response Team (SOC-CSIRT) and public key infrastructure (PKI) systems, and requests Union support for network security.			
RGQ2/218	2024-04-29	Australia	National Office of Cyber Security and the Cyber Security Response Coordination Unit
Presents the Cyber Security Response Coordination Unit, the National Office of Cyber Security and the National Cyber Security Coordinator, entities established by the Government of Australia within the Department of Home Affairs for central coordination, following the Optus and Medibank data breaches of 2022.			
RGQ2/214	2024-04-19	Australia	Critical Infrastructure Uplift Program (CI-UP)
Outlines the Critical Infrastructure Uplift Programme (CI-UP) in Australia, designed to enhance cyber security and resilience of critical infrastructure against cyber-attacks. It details CI-UP activities and emphasizes the voluntary and collaborative nature with industry partners.			

(continuación)

Web	Received	Source	Title
RGQ2/212	2024-04-18	China Mobile Communications Co. Ltd.	China's initiatives to protect the cyber-security rights and interests of minors
Presents the critical nature of cybersecurity for Chinese minors, addressing their high online presence, urban-rural digital divide, and exposure to risks such as addiction and privacy violations. It underscores China's advancements in safeguarding minors' Internet use and the collective role of government, industry, and society in bolstering cyber-security education and safety.			
RGQ2/201	2024-04-16	Saudi Arabia	Cost estimation tool for cybersecurity controls
Outlines the National Cybersecurity Authority (NCA) development of the "ECC Cost Estimation Tool" to aid Saudi organizations in budgeting for cybersecurity compliance. It details the creation process, including research, implementation and testing phases.			
RGQ2/191	2024-04-16	United Kingdom	Considerations in implementing a new and significant regulatory security framework for the telecoms sector: an example from the UK's Telecoms Security Act (TSA)
Outlines the United Kingdom new telecoms security framework under the Telecommunications Security Act 2021, detailing enhanced security duties for providers, a tiered approach based on turnover, and the Ofcom role in ensuring compliance and fostering a collaborative security culture.			
RGQ2/184	2024-04-15	Brazil	Creating cybersecurity capabilities: Hackers do Bem
Describes Brazil's "Hackers do Bem" ("White Hat Hackers") initiative, aiming to train 30 000 students in cybersecurity through a five-level curriculum, with government support, to build a national hub, boost employability, and strengthen the cybersecurity ecosystem.			
RGQ2/183	2024-04-15	Brazil	Cybersecurity in Brazilian National Research and Education Network: CAIS
Outlines the work of the Brazilian National Research and Education Network (RNP), which created the first network security centre in Brazil in 1995 (CAIS). CAIS serves as CSIRT for the Brazilian academic network, being the focal point for security incident notifications and providing coordination and support for the incident handling.			
RGQ2/182	2024-04-15	Brazil	Brazilian Federal Cyber Incident Management Network
Presents the Brazilian Federal Cyber Incident Management Network (ReGIC), presenting the two CSIRTs with national responsibilities, such as the Brazilian National Computer Emergency Response Team (CERT.br) and the Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR Gov), as well the CSIRT ecosystem in Brazil.			
RGQ2/181	2024-04-15	Brazil	Brazilian National Cybersecurity Policy
Summarizes Brazil's National Cybersecurity Policy and the formation of the National Cybersecurity Committee, detailing its principles, goals, and tasks like promoting cybersecurity, resilience, education, and global collaboration, with diverse members overseeing policy execution.			
RGQ2/170	2024-04-04	Russian Federation	Implementation of the educational project "Digital Literacy Campaign" in the Russian Federation

(continuación)

Web	Received	Source	Title
Outlines the Russian Federation's "Digital Economy" programme for human capital and economic growth by 2024, including "Digital Literacy Campaign" with partners like Kaspersky Lab to educate children on digital safety through animated videos.			
RGQ2/165	2024-04-02	Brazil	Meaningful connectivity
Summarizes the Anatel 2023 Strategic Planning, highlighting digital transformation and meaningful connectivity, which encompasses a cyber safety perspective. It details cyber hygiene initiatives, including the launch of a dedicated page to combat digital scams and frauds.			
RGQ2/164	2024-03-29	United States	U.S. Pre-Ransomware Notification capability
Details the CISA Pre-Ransomware Notification programme to pre-empt ransomware attacks. It emphasizes early warnings, international cooperation, and the success of the #StopRansomware campaign in averting threats in 2023.			
RGQ2/163	2024-03-26	Syrian Arab Republic	A paper on digital development in Syria and the current reality
Summarizes the Syrian Arab Republic digital transformation strategy for government services, detailing a phased approach from 2021 to 2030, encompassing e-government services, citizen centres, and cybersecurity. It includes strategic axes, programmes, and annexes on Internet capacity and security.			
RGQ2/160	2024-03-26	RIFEN	Initiatives to strengthen digital trust in Côte d'Ivoire
Highlights Côte d'Ivoire's National Digital Development Strategy 2021-2025, aiming to transform the nation into West Africa's digital hub by improving digital skills, cybersecurity, and women's tech inclusion, and by creating a national data centre.			
RGQ2/155	2024-03-26	RIFEN	Building a resilient security culture: a comprehensive approach to cybersecurity enhancement
Highlights the need for a robust cybersecurity culture in organizations, advocating for comprehensive strategies such as employee training, simulations, incident response teams, access control, encryption, and continuous monitoring to combat cyber threats.			
RGQ2/149	2024-03-15	Democratic Republic of the Congo	Development of cybersecurity in the Democratic Republic of Congo: issues and strategies for the protection of ICT infrastructures and digital actors
Outlines the Democratic Republic of the Congo's cybersecurity challenges, including its vulnerability to cyberattacks and the lack of a national strategy, legal framework, and incident reporting. It mentions a workshop for creating a national CIRT and ITU strategy support.			
RGQ2/140	2024-03-11	RIFEN	Internet and ICT: development levers and cybersecurity challenges in developing countries
Highlights the importance of Internet and ICTs for development, stressing security against cyberthreats. It combines research with expert opinions, identifies vulnerabilities, and addresses Africa's connectivity issues, advocating for information sharing, legislation, and collaboration to protect digital infrastructure.			

(continuación)

Web	Received	Source	Title
RGQ2/134	2024-03-05	Burundi	Implementation of a national cybersecurity strategy
Outlines the significance of information management and ICTs for a country's progress, emphasizing the necessity of cybersecurity measures in light of rising cybercrime. It details Burundi's efforts, supported by ITU, to create a national cybersecurity strategy by 2040, concentrating on legal structures, infrastructure security, and skill development.			
RGQ2/130	2024-02-29	RIFEN	Côte d'Ivoire's cybersecurity initiatives
Outlines Côte d'Ivoire's cybersecurity strategies, including the Platform for Combating Cybercrime and CI-CERT, stressing public awareness and education to foster a cybersecurity culture and safeguard the online space, particularly during events like the African Cup of Nations.			
RGQ2/128 +Ann.1	2024-02-29	Syrian Arab Republic	Cybersecurity strategy in Syria
Summarizes the Syrian Arab Republic cybersecurity strategy, focusing on creating a strong infrastructure, handling threats, legal development, capability enhancement, research, governance, and international collaboration via six programs, while stressing the importance of multi-layered protection.			
RGQ2/121	2024-02-29	Haiti	Taking control of cybersecurity in Haiti
Outlines Haiti's Haitian Institute for Statistics and Information and the CONATEL partnership to create a national cybersecurity strategy, aided by the World Bank and Inter-American Development Bank, including forming a working group, evaluating cybersecurity maturity, and establishing a CERT to enhance digital security.			
RGQ2/117 +Ann.1	2024-02-28	Dominican Republic	Cyberskills Center for Latin America and the Caribbean LAC4: Knowledge exchange, training and training in best practices at LAC4
Describes how the Latin America and Caribbean Cyber Competence Centre has enhanced cybersecurity in over 25 Latin American and Caribbean countries through workshops, legal framework support, and promoting regional cooperation, including empowering women and raising cyber awareness.			
RGQ2/114 +Ann.1	2024-02-27	Zambia	The role of the Authority in Child Online Protection in Zambia: A Zambia case study on the implementation of the National COP Strategy - Lessons learnt
Summarizes Zambia's dedication to child online safety by adopting ITU Resolution 179 and executing a national child online protection strategy, focusing on legal frameworks, education, combating exploitation, stakeholder cooperation, and ensuring effective oversight.			
RGQ2/104	2024-01-24	Democratic Republic of the Congo	Making Congolese cybersecurity a lever for integration and socio-economic growth
Describes the Democratic Republic of the Congo's strategy for using cybersecurity to enhance integration, governance, and growth, focusing on infrastructure, cybercrime, and digital services. It advocates for expert capacity building and ITU partnership for a secure digital transformation.			
2/212	2023-10-31	Republic of Korea	Misuse of Personally Identifiable Information

(continuación)

Web	Received	Source	Title
Presents the Republic of Korea's data protection mechanism that has been updated to address concerns related to the misuse and abuse of personal identifiable information (PII). The Personal Information Protection Act (PIPA) amended the existing PII Anonymization Guidelines on 28 April 2022, which aim to offer six step-by-step guidelines for the treatment (de-identification) of personal information. The Republic of Korea highlighted the challenge of crafting guidelines that guard against the abuse and misuse of PII without jeopardizing the benefits of new technologies.			
2/201	2023-10-17	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Discusses ongoing efforts to improve cybersecurity in ITU Member States, including future plans and new initiatives as well as how the Global Cybersecurity Agenda, launched in 2007, promotes international cooperation, and how BDT works with Member States and global organizations to establish national and regional CIRTs, measures cybersecurity commitments, supports strategy development, encourages diversity, and works to protect children online through the child online protection initiative.			
2/199	2023-10-17	United Kingdom	Building local capacity to adopt secure connected place technology: the UK's Secure Connected Places Playbook
Recognizes the benefits that connected places ("smart cities") technology can bring societies and local areas. However, it also recognizes that this interconnectivity creates cyber vulnerabilities and the potential for cyberattacks. Through its National Cyber Strategy 2022, the United Kingdom has been developing a 'Secure Connected Places Playbook'. This product, currently in alpha phase, has been developed in partnership with a diverse set of local government authorities and an industry consortium. The Playbook provides guidance on: i) governance; ii) procurement and supply chain management; and iii) risk and threat analysis. The United Kingdom has identified several good practices, including: i) working hand-in-hand with intended beneficiaries; ii) using a "test and iterate" approach; and iii) co-developing and testing with local government authorities. The United Kingdom has now begun beta testing, working with 13 local authorities.			
2/196	2023-10-17	United States	U.S. proposed Cyber Trust Mark Program: certifying that IoT products meet U.S. cyber standards
Presents the proposed Cyber Trust Mark program, by the United States Federal Communications Commission (FCC), a voluntary cybersecurity labelling initiative for IoT products. The programme aims to help consumers make informed decisions, differentiate trustworthy products, and encourage manufacturers to meet higher cybersecurity standards. The FCC seeks input on various aspects of the programme, including eligible devices, oversight, security standards, and consumer education. Certified products could be available for purchase by the end of 2024.			
2/187	2023-10-16	Republic of Korea	Privacy by Design certification in South Korea
Shares its contribution on Privacy by Design (PbD), a proactive approach to embedding privacy into the design and operation of information technologies and systems. The Personal Information Protection Committee (PIPC) of the Republic of Korea is piloting a PbD certification system to strengthen the safety of personal information collection devices. The certification helps organizations demonstrate their commitment to user privacy, increasing consumer trust and reducing the risk of privacy breaches.			
2/167	2023-10-11	Australia	eSafety Youth Council

(continuación)

Web	Received	Source	Title
Presents the eSafety Youth Council, established in April 2022, that consists of 24 members aged 13-24 from diverse backgrounds in Australia. It aims to involve young people in decision-making processes for policies and programmes impacting them. The Council is informed by the Western Sydney University Youth Engagement Report and follows six good practice principles. Members engage in various activities, including conferences, resource launches, and discussions with technology companies. The Council priorities include collaboration, improved reporting processes, age-appropriate content access, and increased engagement on online safety.			
2/158	2023-10-09	Russian Federation	Challenges and approaches to addressing smishing and SMS incidents. Combating illegal use of virtual mobile numbers
Contextualize smishing as a type of phishing attack that uses SMS messages to trick users into downloading malware or revealing personal information. The rise of mobile services and the pandemic have increased its popularity. To combat smishing, users should be cautious of unexpected messages, use anti-spam settings, and report suspicious messages. Governments, banks, and telecommunication operators are also working together to fight smishing through regulations, public awareness campaigns, and technological solutions.			
2/154	2023-10-05	Australia	Combating telecommunications scams
Presents the Australian Communications and Media Authority (ACMA) work to combats scams through regulatory powers, new rules, and international cooperation. Initiatives include varying the telecommunications numbering plan, registering the Reducing Scam Calls and Scam SMS Code, and mandating stronger identity verification processes. ACMA also collaborates with other nations and industries to fight scams. Despite progress, SMS scams remain a significant issue. A holistic approach involving industry, government, and consumer awareness is needed.			
2/150 +Ann.1	2023-09-29	Argentina	Promoting cybersecurity in Argentina: challenges, strategies and advances in the digital era
Presents the growing reliance on ICT for essential services highlighting the need for governments to prioritize cybersecurity. Challenges include fostering a cybersecurity culture and promoting safe cyberspace usage. Efforts include a National Cybersecurity Awareness Campaign, a joint publication on cybersecurity issues, training programmes for civil servants, strengthening legal frameworks, and addressing the gender gap in ICT access and use through national and international initiatives.			
2/141	2023-09-28	Central African Republic	Criminal aspects of physical protection of information and communication network infrastructures
Central African Republic shares the implementation of legislative reforms and creation of agencies to control and secure information systems. However, the country faces vandalism and theft on its new fibre optic network. Proposed solutions include adopting laws against theft, fraud, and vandalism in public information networks and establishing a national CIRT team to coordinate incident management.			
2/137	2023-09-14	Côte d'Ivoire	Cybercrime: Continuing campaign on child online protection

(continuación)

Web	Received	Source	Title
Discusses the digital knowledge challenge facing Côte d'Ivoire, that is hindering its development in the digital world. To address this, public and private sectors, along with international organizations, have launched an awareness campaign for middle and high school students. The campaign aims to educate and raise awareness about online risks, promote responsible digital behaviour, and provide support for reporting abuse. Over 1 000 students participated in the campaign, which emphasizes the importance of a safer digital environment for all citizens.			
2/120	2023-09-07	Timor-Leste	Advancing cybersecurity for Timor-Leste's digital transformation
Presents Timor-Leste digital transformation journey, focusing on improving government services, inclusivity, and crucial sectors such as healthcare, education, and agriculture. However, as a least developed country (LDC), it faces significant cybersecurity challenges, including weak frameworks, limited awareness, and inadequate resources. To enhance digital resilience, Timor-Leste must invest in infrastructure, capacity building, legal frameworks, public-private partnerships, awareness, incident response, and international cooperation. Addressing these challenges is crucial for sustainable development and economic growth in the digital era.			
2/119	2023-09-06	Kenya	The Authority's Child Online Protection and Safety Programme in Kenya: A case study on the implementation of the ITU's Guidelines on Child Online Protection
Shares the implementation of child online protection initiatives since 2011, by the Communications Authority of Kenya (CA), focusing on raising awareness and promoting responsible Internet usage. The CA has launched two campaigns, "Be The COP" and "*Huwezi Tucheza, Tuko Cyber Smart*," targeting parents, guardians, teachers, and children. The authority collaborates with various stakeholders, including government agencies, industry players, and NGOs, to implement the ITU Guidelines on Child Online Protection. Initiatives include legal and regulatory frameworks, reporting mechanisms, research and surveys, national strategies, industry initiatives, educational resources, capacity building, and national awareness campaigns.			
2/115	2023-09-04	Democratic Republic of the Congo	Digitalization of public services in the Democratic Republic of the Congo: key challenges and requirements for information security and cyberdefence
Presents the implementation of cybersecurity measures, including the enactment of Law No. 20/017 in 2020, and the adoption of a digital code in 2023. The country is working on creating a computer incident response team (CIRT) and improving its broadband infrastructure with a planned 50 000 km of optical fibre network. Cooperation and public awareness-raising are also essential components of their cybersecurity strategy.			
2/112	2023-08-21	Kenya	CSIRT/CIRT approaches and experiences towards the resilience of critical infrastructure in Kenya
Introduces the establishment of the National Computer Incidents Response Team (KE-CIRT) by the Communications Authority of Kenya to mitigate cyber threats and ensure a safer cyberspace. The country has a legal framework defining critical infrastructure and has adopted a cybersecurity framework supported by policy and operational frameworks. Challenges faced include a rapidly evolving threat landscape, lack of international cooperation, insufficient expertise, limited resources, balancing privacy and security, coordination and information sharing, technological advancements, insider threats, public-private collaboration, and public awareness and education.			
2/98	2023-07-25	Australia	Australia's national online safety awareness campaign

(continuación)

Web	Received	Source	Title
Introduces the Online Safety Act 2021, to keep pace with new technology and emerging online threats. The Online Safety campaign aimed to raise public awareness of the Online Safety Act and the strengthened laws for online safety. The campaign targeted various audience groups and successfully drove traffic to the eSafety Commissioner website.			
RGQ2/85	2023-05-18	Beihang University	Development of policies and legislation to protect consumer rights and interests in China in the digital era
China attaches great importance to the protection of consumer rights and interests. Firstly, in terms of policy guidance, the goal is to improve the consumer environment, strengthen consumer rights protection, and achieve social fairness and justice, adhering to the equal emphasis on development and regulation; Secondly, in terms of the legal system, China has steadily promoted the formulation and implementation of laws, regulations, and standards related to consumer rights protection. It has continuously strengthened the protection of consumers' digital rights and focused on the special protection of vulnerable consumers, gradually forming a comprehensive and three-dimensional legal system for consumer rights protection to adapt to the new development and needs of consumer rights protection. The content of this paper is based on the policy and legislative protection of consumer rights in China's new development pattern, so as to provide assistance for the international consumer rights protection cause.			
RGQ2/80	2023-05-10	Russian Federation	Information sharing practices to protect children from disruptive online content - Award "For a Safe Digital Childhood"
Presents its contribution which contained information on some practices on the exchange of information between two Russian Federation federal executive bodies to protect children from destructive online content, as well as information about the award "For a Safe Digital Childhood" by Alliance for the Protection of Children in the Digital Environment, aimed at supporting projects to develop a safe digital environment throughout the Russian Federation.			
RGQ2/79	2023-05-10	Russian Federation	National computer incident response and coordination centre - information security leaders
Presents a contribution on the operation of its National Computer Incident Response & Coordination Centre (NCIRCC) to ensure a stable critical infrastructure, as well as approaches regarding the appointment of leaders in the field of information security. In response to questions received during the meeting, the Russian Federation clarified that NCIRCC is not the only such centre, and the main criteria for leaders in the field of information security is not only their professional degree, but also wide-ranging experience and relevant professional skills.			
RGQ2/74	2023-05-09	United Kingdom	TBEST: an example of outcome-based pen-testing for communications providers to help improve their network security posture

(continuación)

Web	Received	Source	Title
Contribution on the TBEST scheme, an example of cybersecurity assurance practice that Ofcom, the United Kingdom regulator, runs voluntarily with communications providers. TBEST is a penetration testing that aims to stimulate a cyber-attack in telecommunications networks in order to identify security vulnerabilities which can then be, through a process of remediation, addressed to improve the operators' network security posture. The contribution provides an overview of the process, and the various stakeholders involved. More broadly, this scheme is an example of supervisory policy approach that Ofcom is taking, which stresses the importance of building collaborative relationships with the industry that Ofcom regulates. To date, all communications providers in the United Kingdom have already or are undergoing the TBEST scheme voluntarily and have implemented changes as a result. TBEST is not a "standard" nor a certification process. The goal is to enable communications providers to gain awareness of cyber threats and implement appropriate changes in a timely manner to improve their cyber defence capabilities. By being aware of, and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect their networks.			
RGQ2/66	2023-05-10	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated. The presentation addressed the ITU cybersecurity mandate, and through BDT, work on the national CIRT programme, regional and national cyberDrills, the Global Cybersecurity Index (GCI), national cybersecurity strategy (NCS) assistance, Women in Cyber, Her CyberTracks, child online protection, partnerships and collaboration, and Cyber for Good. The document emphasizes the importance of collaboration, partnerships, and resource mobilization to allow ITU to fulfil its mandate, considering the extensive list of tasks that membership have requested BDT to undertake. BDT also presented information about the 5th edition of the Global Cybersecurity Index.			
RGQ2/58	2023-04-27	Brazil	Cybersecurity assurance practices - Brazil experience
Introduces the contribution referring to the efforts of the Brazilian National Telecommunications Agency (ANATEL) regarding the establishment of cybersecurity minimum requirements for telecommunication equipment. ANATEL initially adopted a non-mandatory approach (Act 77/2021), which evolved into a cybersecurity compulsory certification requirement for a specific set of equipment (Act 2436/2023). This evolution was only possible with a comprehensive debate within the sector.			
RGQ2/57	2023-07-27	Brazil	Brazilian cybersecurity-related policies and regulations
Presents an overview on the cybersecurity-related policies and regulations that have been developed in Brazil in recent years, including the National Information Security Policy, the National Cybersecurity Strategy, the Cybersecurity Regulation for the Telecommunication Sector, the Federal Cyber Incident Management Network, and the 5G Spectrum Auction Notice. There were questions about the modular approach adopted by the National Information Security Policy, and the Brazilian delegation explained that in Brazil cybersecurity is one of the elements of Information Security.			
RGQ2/53	2023-04-25	Mexico	Privacy reports on user information in the use of digital platforms

(continuación)

Web	Received	Source	Title
Presents the Privacy Reports, which purpose is to make available in a clear, simple and transparent manner the privacy policies of operating systems, terminal equipment, social networks, and digital platforms that enable the provision of services such as: online commerce, transport and entertainment. These reports published by the Federal Telecommunications Institute help users to learn about the information that is collected by the platforms, and how this information is treated, and helps users make responsible use of such platforms. The Reports also empower users by providing transparent information about privacy policies.			
RGQ2/51	2023-04-25	Mexico	Internet of Things Devices Catalog
The *Internet of Things Devices Catalogue* is an electronic tool that allows users of telecommunication services to know the main characteristics of IoT devices, as well as the privacy policies defined by the manufacturers. The IoT devices published are those that are marketed in Mexico and have been certified by the Federal Telecommunications Institute. The tool allows users to be empowered with transparent information about privacy policies and the characteristics of terminal equipment that comply with technical regulations, for informed decision-making and for the proper use of IoT equipment.			
RGQ2/48	2023-04-25	Access Partnership Limited	Cybersecurity assurance practices - international standards and satellite communications
Contains information related to developing cybersecurity assurance practices for commercial satellite operators, as well as highlighting some of the existing general cybersecurity assurance practices which may be adopted by any commercial satellite operator, including ISO 27001. The contribution noted some of the unique cybersecurity threats which need to be overcome in satellite operations, including the cross-jurisdictional nature of satellite operations, and the vulnerabilities of ground stations. The contribution explained specific technical standards including the ETSI technical standard 103 732 and its measures to protect consumer mobile devices, as an example of standards towards specific technology which could inform the further development of standards for commercial satellite operators.			
RGQ2/44	2023-04-24	South Africa	The domain name cybersecurity culture
Provides a contribution concerning the security of the country code top-level domain name (.za). The South African Domain Name Authority (ZADNA) manages the .za domain namespace under the mandate of the Electronic Communications and Transactions Act (ECTA). Its policy framework was designed to ensure a secure, resilient, and efficiently managed domain namespace, promoting stakeholder engagement, growth of the namespace, policy compliance, and entrance of new Internet service providers. ZADNA also addresses cybersecurity threats through education and awareness programmes, alternative dispute resolution (ADR) workshops and regulations, and DNS training courses. Additionally, it adheres to international standards for dispute resolution, working in line with the World Intellectual Property Organization (WIPO) and organizations such as the South African Institute of Intellectual Property Law (SAIIPL) and the Arbitration Foundation of Southern Africa.			
RGQ2/38	2023-04-13	Australia	Sharing advice from Australia on securing smart places

(continuación)

Web	Received	Source	Title
Shares information on the lessons learned by the Australian Cyber Security Centre in response to risks identified for smart places. The contribution defined smart places as those designed to provide enhanced services through the use of smart information and ICT enabled systems and devices. The contribution noted that the highly connected nature of smart places makes them vulnerable to intrusions. This is exacerbated when the system scales. The contribution gave examples of Australian policies used to protect the various aspects of smart cities including IoT, supply chains, operational technology and cloud computing. The contribution also raised several examples of strategies which may be employed to mitigate security risks as well as ensuring operational redundancy.			
RGQ2/34	2023-04-06	Republic of Korea	Cloud Security Assurance Program (CSAP) in South Korea
Introduces the Cloud Security Assurance Programme (CSAP), a security certification for cloud computing services that meet security certification standards to improve and guarantee information protection levels. The purpose of the CSAP is to provide private cloud services with proven safety and reliability to national and public institutions. Also, it aims to implement an objective and fair security certification system for cloud services to address user security concerns and secure competitiveness of cloud services. The CSAP provides a number of benefits. By certifying the security level of a cloud system, CSAP helps to improve the cyber resilience of national and public institutions. This can also help to ensure that sensitive information is protected and that cloud services are reliable.			
RGQ2/29	2023-03-30	Côte d'Ivoire	Policy and strategy of Côte d'Ivoire for building a trusted digital space
Shares the initiatives taken by Côte d'Ivoire in its efforts to build digital trust, which concerns all economic sectors that use ICTs, such as media and communication, transport, health, industry, telecommunications and computing, distribution of goods and consumption, construction, finance and insurance, tourism, agriculture and e-commerce. To consolidate the freedom of online public communication and ensure interactions are secure, Côte d'Ivoire has enhanced the means for combating cybercrime and protecting personal data in order to build trust in cyberspace. Cybersecurity has become an issue of privacy, competitiveness and national sovereignty. A capacity to anticipate, build trust and protect personal data is essential. In this sense, the country has updated its legal and institutional framework, setting a visionary policy to enhance digital trust by 2025. The country has established a Consultative Committee for Digital Trust (CCCN) and a Consultative Committee for the Protection of Personal Data (CCDCP).			
RGQ2/20	2023-03-22	Nigeria	Child Online Protection practices in Nigeria
Presents its efforts in regard to child online protection through the Nigerian Communications Commission (NCC), the independent national regulatory authority for the telecommunication industry, in collaboration with the Office of the National Security Adviser in Nigeria who works with other stakeholders to ensure child protection in Nigeria's cyber space. It was decided by the meeting to liaise with the Council Working Group on Child Online Protection (CWG-COP) to share the relevant experiences shared by Nigeria.			
2/80	2022-11-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken by BDT and new initiatives to enhance cybersecurity in ITU Member States: CIRT programme, regional and national cyberdrills, national cybersecurity strategy (NCS), work related to Bridge the Cybersecurity Divide: Cyber for Good project, work on promoting a diverse and inclusive cybersecurity community through the Women in Cyber Mentorship Programme and Youth4Cyber initiative, child online protection, and partnerships and collaboration initiatives.			

(continuación)

Web	Received	Source	Title
2/77	2022-11-22	United Kingdom	Sharing experience from the UK on promoting and developing cybersecurity skills
Outlines the country's policy approach to address the cyber skills gap which, in addition to the final report of the study cycle, can also be included in a future repository of good practices as agreed through Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference. The United Kingdom's initiatives are focused in three areas: (1) cyber skills for young people, (2) cyber skills for adults, and (3) developing the cyber profession.			
2/74	2022-11-18	World Bank	World Bank Study Group 2 Submission: Digital transformation
Highlights their readiness to support the least developed client countries with a special emphasis on fragility, conflict and violence (FCV) and small island developing states (SIDS). Through the analytical work programme and strategic partnerships, the World Bank is working closely with client countries on issues related to the SG2 Questions' scopes. Relevant examples from the World Bank around using ICT services and applications for the promotion of transformative and sustainable development are provided in the contribution. For instance, one relating to cybersecurity is the Cybersecurity Multi-Donor Trust Fund, being a part of the broader Digital Development Partnership umbrella programme, aims at systematically incorporating cybersecurity in the development agenda as well as in World Bank operational programmes. Work includes building global knowledge to better define the cybersecurity development agenda, and country-specific technical assistance.			
2/71 (Rev.1)	2022-11-18	Russian Federation	New practices of the Russian Federation in the field of creating a culture of cybersecurity
Presents the Russian Federation Cyber Hygiene Program, launched in August 2022. The programme is planned for a three year period and includes various activities aimed at attracting the attention of citizens of the Russian Federation to the issues of cybersecurity and the training in skills on safe behaviour on the Internet. Large-scale information campaigns are one part of the programme. Citizens were segmented into age groups, and their online behaviour and the type of digital content consumed were taken into account. Based on this segmenting approach, more specifically targeted means of information dissemination could be applied for the 3 segmented groups of population (12-18 / 18-45 / 45+ years old). The contribution also covers the means of improving the information security literacy of civil servants, as well as the results of an all-Russian Federation study of the citizens' information security literacy.			
2/35	2022-10-12	Rwanda	National cybersecurity initiatives: current status
Highlights the programmes and initiatives put in place to guarantee the security and resilience of Rwanda's cyberspace. To support national economic growth and social mobility, the Government of Rwanda (GoR) is actively deploying various information technologies and has made major investments in ICT infrastructure and applications. GoR established the National Cybersecurity Authority (NCSA) as the authority to spearhead the implementation of National Cyber Security policies and strategies. Additionally, GoR established a law relating to protecting personal data and privacy and passed the prevention and punishment of cybercrimes law. NCSA roles include: coordinating national cybersecurity functions across the private and public sectors; promoting national education programmes and fostering awareness of cybersecurity good practices amongst the Rwandan population; operating the Rwanda Computer Security Incident Response Team (Rw-CSIRT); and overseeing the implementation of the Protection of Personal Data and Privacy Law. Furthermore, the Rwanda Utilities Regulatory Authority (RURA), Regulation No. 010/R/CR-CSI/RURA/020 OF 29/05/2020), Rwanda Information Society Authority (RISA), and capacity building collaborations and initiatives have been put in place to ensure preparation in preventing and responding to evolving cyber threats.			

(continuación)

Web	Received	Source	Title
2/34	2022-10-12	Côte d'Ivoire	Initiatives to support children and young people, national strategy for the protection and empowerment of children and young people online: the experience of Côte d'Ivoire
Presents an initiative undertaken by Côte d'Ivoire to protect children against the dangers and threats of using ICTs. The initiative, www.jemeprotegeenligne.ci is a website targeted at children between 5 and 19 years old as well as teachers and parents with the goal of educating children and young people and raising awareness.			
2/30	2022-10-11	Côte d'Ivoire	Proposal for State actions and initiatives to foster a culture of cybersecurity and ensure that information and communication networks are secure: the case of Côte d'Ivoire
Contextualizes cyberattacks and threats as a major concern for governments in this increasingly connected world, particularly in developing countries. Cybersecurity is now the priority issue for many States. This contribution gives an overview of the cybersecurity situation in developing countries, notably Côte d'Ivoire, and highlights strategies for raising user awareness and experience-sharing among Member States.			

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
2/410 +Ann.1	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 LS on update on the work of the Correspondence Group on Child online protection (CG-COP)
2/409	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development
2/241	2024-09-11	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Groups 1 and 2 on SG17 update on the work of the Correspondence Group on Child online protection (CG-COP)
RGQ2/151	2024-03-18	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 1 Question 6/1 and ITU-D Study Group 2 Question 3/2 on Establishment of the Correspondence Group on Child online protection (CG-COP)
RGQ2/107	2024-02-12	Chairman, ITU Council Working Group on COP	Liaison statement from ITU Council Working Group on COP to ITU-D Study Group 2 Question 3/2 on child online protection
RGQ2/83	2023-03-08	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on status of security studies in ITU-T SG17
2/20	2022-06-16	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development

Annex 2: List and summary of BDT on-going cybersecurity activities

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Data	Global Cybersecurity Index v5	ITU Member States	GCI Expert Group	Global Cybersecurity Index report and country reports. Link
Governance	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau	Guinea-Bissau	Government of Guinea-Bissau	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau with the aim to empower Guinea-Bissau's cybersecurity ecosystem by guiding key national stakeholders in developing strategic approaches to CIRT implementation and enhancing cybersecurity in Guinea-Bissau
Governance	Mauritania's Cybersecurity Governance Development	Mauritania	Government of Mauritania	Sessions to enhance of a national cybersecurity governance framework to enable Mauritania to strengthen the protection of the critical information systems of official institutions and vital operators, the fight against cybercrime, awareness raising, training, confidence-building in digital, more effective regional and international integration through cooperation.
Governance	National cyber risk assessment	Lesotho	Ministry of Communications Science and Technology	Workshop to enhance strategic thinking on cybersecurity governance among key national stakeholders, thereby advancing the objectives of Lesotho's National Cybersecurity Strategy.
Governance	Strengthening Critical Information Infrastructure Resilience	Cambodia	Ministry of Post and Telecommunications Cambodia (MPTC, Japan International Cooperation Agency (JICA)	Workshops on technical incident response, national cybersecurity strategy, and crisis management for critical information infrastructure stakeholders
Governance	Tabletop Exercise and a Cybersecurity Incident Simulation Exercise	ITU Arab States region Member States	CSC UAE	Tabletop exercise centred around cyber-attack directed at a financial institution.
Incident Response	13th Event of Cyber Capacity Building in America - Andino	ITU Americas region Member States	Ministry of Popular Power for Science and Technology of Venezuela, National Commission of Information Technologies (CONATI), Superintendency of Electronic Certification Services (SUSCERTE)	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Americas Regional CyberDrill	ITU Americas region Member States	INICTEL-UNI, Peruvian Ministry of Transportation and Communications, General Secretariat of the Andean Community	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CIRT Establishment in Bahamas	Bahamas	Government of Bahamas	Building and deploying the technical capabilities and related training necessary to develop Bahamas national cybersecurity strategy and to establish its National Cybersecurity Incident Response Team (CIRT). Link

(continuación)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	CIRT Maturity Assessment	Timor-Leste	ANC	Conducted Maturity Assessment of country CIRT through series of workshops, discussions, and inventories, providing recommendations for the Timor-Leste computer security incident response team (TLCSIRT) in collaboration with the Autoridade Nacional de Comunicações (ANC) to ensure TLCSIRT can enhance its cybersecurity maturity level. Link
Incident Response	Cyber 100x Global Cyber-Drill 2024	ITU Member States	Cyber Security Council United Arab Emirates	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CyberQ	ITU Member States	United Arab Emirates Cybersecurity Council	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Included specific trainings for women. Link
Incident Response	Cybersecurity Forum and CyberDrill for Europe and the Mediterranean	ITU Europe region and Arab States region Member States	Ministry of Transport and Communications of Bulgaria, Ministry of Electronic Governance of Bulgaria	Cybersecurity forum featuring trends and challenges, CSIRTs capacity-building training, and two days of cyberdrill exercises with emerging attack scenarios and collaborative learning sessions. Link
Incident Response	ITU National CyberDrill for Armenia	Armenia	Ministry of High-Tech Industry of Armenia	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Asia-Pacific CyberDrill	ITU Asia and the Pacific region Members States	Cyber Security Brunei (CSB)	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Cybersecurity Readiness Exercise	ITU Arab States region Member States	Directorate General for Information Systems Security (DGSSI) Morocco	Incident response trainings, discussions, and information sharing. Link
Incident Response	National CIRT Establishment in Gambia	Gambia	Ministry of Information and Communication Infrastructure (MOICI)	Assist MOICI in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Link
Incident Response	National Computer Incident Response Team (CIRT) Implementation – Suriname	Suriname	e-Government Directorate, Cabinet of the President of Suriname	Support for operationalization of Computer Incident Response Team. Link
Incident Response	Regional Cybersecurity Week	ITU Arab States region Member States	ARCC Oman	Regional Cybersecurity Conference focusing on "Cybersecurity as an enabler for the Digital Economy", the FIRST Organization Seminar, and the Regional and OIC-CERT Cyber Drill. Link
Incident Response	Rwanda National CyberDrill	Rwanda	Rwanda National Cyber Security Authority, Ministry of Foreign Affairs of the Czech Republic	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link

(continuación)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	Twelfth Edition of the Regional Cyberdrill for Africa Region (ITU-INTERPOL CyberDrill)	ITU Africa region Member States	Ghana's Cyber Security Authority (CSA), INTERPOL	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Partnerships	Cyber for Good	Least developed countries (LDCs)	Axon Consulting, BitSight Technologies, CTM360, DreamLab Technologies, ImmuniWeb, WelchmanKeen	Tools, trainings, and services offered for free to Least Developed Countries. Link
Skills Development	Child Online Protection National Assessment - Andorra	Andorra	SWGfL/UK Safer Internet Centre	Child Online Protection National Assessment with the national stakeholder consultation event
Skills Development	Child Online Protection Train the Trainers and Cybersecurity briefings - Maldives	Maldives	National Centre for Information Technology (NCIT)	Trainings on Child Online Protection as well as briefings on key topics. Link
Skills Development	Creating a Safe and Prosperous Cyberspace for Children	ITU Member States	CTO, CNIL, Council of Europe, European Commission, EC-Council, EBU, Europol, ILO, Interpol, MICITT, NCA KSA, OECD, United Nations Human Rights Special Procedures, UNICRI, UNESCO, UNICEF, UNODC, WIPO, World Bank, UC Berkley, LSE, Middlesex University London, Western Sydney University, Youth and Media, BBC, Disney, Ericsson, worldwide Group, Facebook, IBM, IEEE, Microsoft, Sony, TIM, Privately, Tencent, TrendMicro, Twitter, ASCSA, ACOPEA, 5Rights Foundation, ASDRA, Child Helpline International, Child Rights Connect, Family Online Safety Institute, Childhood, ChildOnline Africa, DeafKidz International, DISC Foundation, Families Europe, Halley Movement, End Violence Against Children, DOInstitute, ecpat, Fard Digital, HABLATAM, Cuber Coluntarios.org, Global Kids Online, GSMA, iKeepSafe, Inclusion international, InHope, Ins@fe, International Centre for Missing & Exploited Children, International Disability Alliance, Internet Matters, Internet Watch Foundation (IWF), Human Trafficking Front, ParentZone, Plan International, RNW media, Save the Children, Paniamor, Stiftung digitale chancen, SWGfL, Tech Coalition, terre des hommes suisse, United Kingdom Safer Internet Centre, WeProtect Global Alliance, Wise Kids, World Economic Forum, YouthIGF, Together Against Cybercrime	Advocacy, research, and in-country programmes related to Child Online Protection. Link

(continuación)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Skills Development	Her CyberTracks 2024	Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Comoros, Chad, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Iraq, Jordan, Kenya, Kuwait, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Qatar, Republic of the Congo, Rwanda, São Tomé and Príncipe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, State of Palestine*, Sudan, Syrian Arab Republic, Tanzania, Togo, Tunisia, Uganda, United Arab Emirates, Yemen, Zambia, Zimbabwe	GIZ, Microsoft	Her CyberTracks provides specialized, targeted training, maintaining the essential mentorship and role modelling aspects. The programme is poised to propel the next generation of women in cybersecurity into roles of leadership, ensuring that their voices and expertise shape the future of this critical field through training, mentorship, and inspiration across three tracks: Policy & Diplomacy, Incident Response, and Criminal Justice (implemented by UNODC). Link
Skills Development	Translation of Child online protection guidelines and capacity building activities - Albania	Albania	National Authority on Electronic Certification and Cyber Security	Child online protection guidelines translated into Albanian and the roll out of capacity-building activities
Skills Development	Translation of Child online protection guidelines and capacity building activities - Malta	Malta	SWGfL/UK Safer Internet Centre	Child online protection guidelines translated into Maltese and the roll out of capacity-building activities

Unión Internacional de las Telecomunicaciones (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20
Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y Jefe del Departamento de Administración y Coordinación de las Operaciones (DDR)
Place des Nations
CH-1211 Ginebra 20
Suiza

Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Departamento de Redes y Sociedad Digitales (DNS)
Correo-e: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento del Centro de Conocimientos Digitales (DKH)
Correo-e: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Asociaciones para el Desarrollo Digital (PDD)
Correo-e: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía
International Telecommunication Union (ITU)
Oficina Regional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Adis Abeba
Etiopía

Correo-e: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún
Union internationale des télécommunications (UIT)
Oficina de Zona
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Oficina de Zona
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar – Yoff
Senegal

Correo-e: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU)
Oficina de Zona
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Correo-e: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Américas

Brasil
União Internacional de Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 6
Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia – DF
Brasil
Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados
Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Correo-e: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras
Correo-e: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Estados Árabes

Egipto
International Telecommunication Union (ITU)
Oficina Regional
Smart Village,
Building B 147, 3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
El Cairo
Egipto

Correo-e: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia
International Telecommunication Union (ITU)
Oficina Regional
4th Floor NBTC Region 1 Building
101 Chaengwattana Road, Laksi
Bangkok 10210
Tailandia

Correo-e: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

Indonesia
International Telecommunication Union (ITU)
Oficina de Zona
Gedung Sapta Pesona, 13th Floor
Jl. Merdeka Barat no 17
Jakarta 10110
Indonesia

Correo-e: bd-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India
International Telecommunication Union (ITU) Area Office and Innovation Center
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Correo-e:
Oficina regional: itu-ao-southasia@itu.int
Innovation Center: itu-ic-southasia@itu.int
Sitio web: ITU Innovation Centre in New Delhi, India

Países de la CEI

Federación de Rusia
International Telecommunication Union (ITU) Oficina Regional
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120
Federación de Rusia
Correo-e: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europa

Suiza
Unión Internacional de las Telecomunicaciones (UIT)
Oficina Regional
Place des Nations
CH-1211 Ginebra 20
Suiza

Correo-e: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza

ISBN 978-92-61-41103-9

Publicado en Suiza
Ginebra, 2025

Créditos de las fotos: Adobe Stock