ITU Publicaciones

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Índice Mundial de Ciberseguridad
2020

Índice Mundial de Ciberseguridad 2020

Medir el compromiso con la ciberseguridad

Agradecimientos

El Índice de Ciberseguridad Global (ICG) es una iniciativa de la Unión Internacional de Telecomunicaciones (UIT), el organismo de las Naciones Unidas especializado en las TIC, que ha sido elaborado y mejorado gracias a la contribución de diversos expertos y colaboradores de los países y de otras organizaciones internacionales. La UIT desea manifestar su reconocimiento y dar las gracias a todos los asociados y colaboradores por su arduo trabajo y su compromiso en la prestación de apoyo al ICG y, lo que es más importante, por su ayuda para lograr un mayor entendimiento colectivo de los compromisos en materia de ciberseguridad.

La UIT desea destacar especialmente las contribuciones recibidas por conducto de la Comisión de Estudio 2 del UIT-D y del Grupo Consultivo de Gestión de la Oficina de Desarrollo de las Telecomunicaciones (BDT), y su labor para la modificación del cuestionario del ICG. El equipo de ciberseguridad de la BDT desea agradecer a los Miembros de la UIT el haber designado expertos para asesorar en el proceso de ponderación. Para más información sobre el proceso de ponderación y la participación de expertos, véase la metodología. Las contribuciones de los siguientes expertos de los Miembros de la UIT brindaron una ayuda inestimable en la asignación de los coeficientes de ponderación:

Sr. Abdelaziz Alzarooni (Autoridad de Reglamentación de las Telecomunicaciones y el Gobierno Digital (TDRA), Emiratos Árabes Unidos), Prof. Dr. Marco Gercke (Cybercrime Research Institute GmbH, Alemania), Sra. Melissa Hathaway (The Potomac Institute for Policy Studies, Estados Unidos de América), Vanessa Copetti Cravo (ANATEL, Brasil), Sr. Scott James Shackelford (Indiana University, Program on Cybersecurity and Internet Governance, Estados Unidos de América), Sr. Gueric Goncalves (ANNSI, Benin), Pr. Eng Emmanuel Thekiso (BOCRA, Botswana), Sr. Dlamini (Ministerio de TIC, Eswatini), Sr. Fillemon Johannes (Ministerio de Tecnologías de la Información y la Comunicación, Namibia), Sr. Palakiyem ASSIH (Cyber Defense Africa S.A.S., Togo), Sr. Nawa J. Samatebele (Zambia Information & Communication Technology Authority, Zambia), Sr. Gonzalo Díaz de Valdés Olavarrieta (Chile), Sra. Jessica Machado Álvarez (Administración de Cuba, Cuba), Ing. Raquel Piña (Venezuela), Mtro. Jacobo Bello Joya (Guardia Nacional de la Secretaría de Seguridad y Protección Ciudadana, México), Sr. Renzo Zegarra (Ministerio de Transportes y Comunicaciones, Perú), Sr. Junior McIntyre (The Caribbean Telecommunications Union (CTU), Trinidad y Tobago), Sr. Fernando Hernández (Unidad Reguladora de Servicios de Comunicaciones, Uruguay), Sra. Anne-Rachel Inné (American Registry for Internet Numbers (ARIN), Estados Unidos de América), el Sr. Mohammad Odeh Alsalamin (Jordania), Sra. Nada Khater (Ministerio de Economía Digital y Emprendimiento, Jordania), el Sr. Yusuf Ahmed Buhijji (Ministerio de Transporte y Comunicación, Reino de Bahrein), Sra. Aziza Al Rashdi (Ministerio de Transporte, Comunicación y Tecnología de la Información, Omán), Sr. Abdulrahman AlHassan (Autoridad Nacional de Ciberseguridad (ANC), Arabia Saudí), Inf. Mohammad Alawi (Ministry of Telecomm. & Information Technology, Estado de Palestina), Sr. Khalili Urahman Kabirzoy (Afghanistan Root Certification Authority(ARCA), Afganistán), Sr. Nasratullah Ghafoory (Afghanistan Root Certification Authority(ARCA), Afganistán), Sra. Xu Ming (Ministry of Information and Technology, National Computer Network Emergency Response Team, China), Sra. Wan Xinxin (Ministry of Information and Technology, National Computer Network Emergency Response Team, China), Sra. Catherine M. Subhyadas (Department of Communications, Fiji), Puan Lyana Shohaimay (Ministry of Communications and Multimedia, Malaysia), Puan Nurul Adiah Hani Husin (Ministry of Communications and Multimedia, Malaysia), Sr. Yan Naung Soe (National Cyber Security Center, Departamento de Tecnología de la Información y Ciberseguridad, Myanmar), Sr. Jakkrapong Chavong (Ministerio de Economía y Sociedad Digital, Tailandia), Sr. Alan Olegovich Khubaev (Departamento de Seguridad de la Información, Rusia), Sr. Andrey Sergeevich Zhivov (Departamento de Cooperación Internacional, Rusia), Sr. Ilgyz Turganbaev (Comité Estatal de

Tecnologías de la Información y Comunicaciones de la República Kirguisa, República Kirguisa), Sr. Muhamedjan Alymkulov (Comité Estatal de Tecnologías de la Información y Comunicaciones de la República Kirguisa, República Kirguisa), Sr. Vladimir Yuryevich Shurin (Departamento de Seguridad de la Información del Servicio de Seguridad de la Empresa Unitaria Republicana, Belarús), Sr. Nestoras Chouliaras (Secretaría General de Telecomunicaciones y Correos del Ministerio de Gobernanza Digital, Grecia), Sra. Eglė Vasiliauskaitė (Ministerio de Defensa Nacional de la República de Lituania, Lituania), Sr. Tadas Šakūnas (Ministerio de Defensa Nacional de la República de Lituania, Lituania), Sra. Radoja (Serbia), Sr. Matej Šalmík (Centro Nacional de Ciberseguridad SK-CERT, Eslovaquia), Sr. Rastislav Janota (National Cyber Security Centre SK-CERT, Eslovaquia), Sr. Aidan Murchland (Reino Unido), Sr. Miguel Pinto (BitSight, Estados Unidos de América), Sra. Nunil Pantjawati (Indonesia), Sra. Intan Rahayu (Indonesia), Sr. Makaireh JONGA (Gambia Computer Security & Incident Response Team (gmCSIRT), Gambia), Sra. Banchale Gufu (Kenya), Sra. Sonam Choki (Department of Information Technology and Telecom, Bhután), Aqeel Taha Saadoon (ICT Secretariat, Irak) y Thar Kadhim Ali (CERTIraq, Iraq).

El equipo de ciberseguridad de la UIT desea dar las gracias a los coordinadores del ICG, que recopilaron datos de sus respectivos países sobre los compromisos en materia de ciberseguridad. Este informe no hubiera podido elaborarse sin los coordinadores nacionales del ICG.

El equipo agradece a los numerosos colegas y pasantes de la UIT que han ayudado en la preparación del presente informe.

El equipo pide disculpas a cualquier persona u organización que se haya omitido por error en la lista anterior y extiende su agradecimiento a todos los que han contribuido al ICG.

Sírvase dirigirse al equipo de ciberseguridad de la UIT, gci@itu.int, si tiene cualquier comentario o pregunta con respecto a esta publicación.

Descargo de responsabilidad

Las denominaciones empleadas en la presente publicación y la forma en que aparecen presentados los datos que contiene no implican juicio alguno por parte de la UIT ni de la Secretaría de la UIT sobre la situación jurídica de ninguno de los países, territorios, ciudades o zonas o de sus autoridades, ni respecto de la delimitación de sus fronteras o La mención de determinadas empresas o productos no implica en modo alguno que la UIT los apoye o recomiende en lugar de otros de carácter similar que no se mencionen. Salvo error u omisión, las denominaciones de los productos patentados se distinguen mediante iniciales en mayúsculas.

La UIT ha tomado todas las precauciones razonables para comprobar la información contenida en la presente publicación. Sin embargo, el material publicado se distribuye sin garantía de ningún tipo, ni explícita ni implícita. El lector es el único responsable en cuanto a su interpretación y utilización del material presentado. Las opiniones, resultados y conclusiones expresadas en esta publicación no coinciden necesariamente con la opinión de la UIT o de sus Miembros.

ISBN:

978-92-61-33923-4 (versión electrónica)
978-92-61-33933-3 (versión EPUB)
978-92-61-33943-2 (versión Mobi)

Prólogo

Disponer de un ciberespacio seguro es ahora más necesario que nunca, sobre todo porque cada vez dependemos más del "soporte digital". Uno de los mayores retos derivados de la pandemia de COVID-19 ha sido encontrar formas de conectarnos adecuadamente con los demás, a pesar de la incertidumbre, la ansiedad y el cambio. La ciberseguridad ya era importante antes de la pandemia para mantenernos seguros en línea y poder desempeñar las funciones cotidianas esenciales.

La capacidad de las personas para adaptarse a esta situación incierta y utilizar la tecnología para encontrar soluciones creativas es una fuente de inspiración. Muchas organizaciones, entre ellas la Unión Internacional de Telecomunicaciones, han tenido que lidiar con los problemas derivados del trabajo a distancia. La ciberseguridad está inherentemente relacionada con el trabajo a distancia, tanto a la hora de gestionar la participación en videoconferencias como para garantizar la transferencia segura de documentos. Por consiguiente, la UIT ha seguido colaborando con los países para ser más eficiente y dinámica, y lograr una incidencia en las zonas donde más se nos necesita.

En 2015, cuando se publicó por vez primera el Índice de Ciberseguridad Global, pocos podían imaginar la situación en la que nos encontramos actualmente. Esta última edición del Índice de Ciberseguridad Global ayudará a promover nuevas acciones hacia ecosistemas digitales seguros necesarios para la recuperación y el crecimiento, mediante la medición de los tipos de compromisos de ciberseguridad que los países han asumido y su prevalencia.

Esta edición revela que muchos países están avanzando en sus compromisos para responder a los retos de la ciberseguridad, a pesar de los oportunistas que se han aprovechado de nuestro afán de información, nuestros temores sobre la pandemia, el teletrabajo desde el hogar y el aprendizaje a distancia, la dependencia de los sistemas sanitarios, etc.

El informe del Índice de Ciberseguridad Global muestra que muchos países han promulgado nuevas leyes y reglamentos de ciberseguridad para abordar aspectos como la privacidad, el acceso no autorizado y la seguridad en línea. También pone de relieve la necesidad de establecer estrategias y mecanismos en materia de capacitación y ayudas a gobiernos y empresas para que estén mejor preparados y reducir así los riesgos cibernéticos. Más de la mitad de los países del mundo cuentan ya con un equipo de intervención en caso de incidente de informático (EIII) y casi dos tercios han adoptado algún tipo de estrategia nacional de ciberseguridad que orienta su postura general en esta materia.

El Índice de Ciberseguridad Global revela que la ciberseguridad es realmente una cuestión de desarrollo y que es preciso abordar urgentemente la creciente brecha de cibercapacidad entre los países desarrollados y en desarrollo mediante el fomento de conocimientos, aptitudes y competencias. Tenemos que erradicar esta brecha y crear capacidad en materia de infraestructura digital, aptitudes digitales y recursos en el mundo en desarrollo.

Espero que el Índice de Ciberseguridad Global siga siendo una herramienta de capacitación útil para los gobiernos, los responsables políticos, los expertos en ciberseguridad y las instituciones académicas a la hora de determinar los aspectos susceptibles de mejora y destacar las prácticas idóneas para reforzar la ciberseguridad nacional.

Me gustaría dar las gracias a los países por su inestimable implicación y su contribución a este esfuerzo, en particular por su contribución a la preparación, recopilación de datos y validación de esta edición del Índice. Asimismo, me gustaría agradecer a todos los participantes en los trabajos de las Comisiones de Estudio su apoyo y orientación. Invito a todos los Estados Miembros de la UIT a que sigan comunicándonos sus progresos en los compromisos relacionados con la ciberseguridad a fin de que podamos compartir eficazmente las experiencias, las investigaciones y las soluciones para crear un ciberespacio de confianza para todos.

Doreen Bogdan-Martin
Directora de la Oficina de Desarrollo de las Telecomunicaciones de la UIT

Resumen ejecutivo

El Índice de Ciberseguridad Global (ICG) fue publicado por primera vez en 2015 por la Unión Internacional de Telecomunicaciones (UIT) para medir el grado de compromiso de sus 193 Estados Miembros de la UIT y el Estado de Palestina[1] en lo que respecta a la ciberseguridad, con el fin de ayudarles a determinar los aspectos susceptibles de mejora e instar a los países a tomar medidas, recurriendo, a tal efecto, a la sensibilización sobre la situación de la ciberseguridad en el mundo. A medida que evolucionan los riesgos, las prioridades y los recursos en materia de ciberseguridad, el ICG también se ha ido adaptando para describir con mayor exactitud las medidas de ciberseguridad adoptadas por los países.

El presente informe tiene por objeto ayudar a comprender mejor el grado de compromiso de los países en materia de ciberseguridad, identificar las lagunas, fomentar la adopción de buenas prácticas y proporcionar información útil para que los países mejoren sus posturas en materia de ciberseguridad.

Los países han indicado que utilizan el ICG para facilitar:

- el debate en foros oficiales, que permiten la autoevaluación y una mejor coordinación;
- la recopilación de información sobre las iniciativas y recursos nacionales generales utilizados para gestionar la ciberseguridad a escala nacional;
- la evaluación comparativa en lo que respecta a las buenas prácticas, los asociados y los vecinos de la región;
- la sensibilización de las distintas partes interesadas sobre las necesidades de coordinación en el plano nacional.

Los resultados del ICG muestran una mejora y un fortalecimiento general de los cinco pilares de la Agenda de Ciberseguridad, pero que persisten las brechas regionales en materia de cibercapacidad. En el informe se destacan prácticas ilustrativas de los países.

Países medidos	Año de recopilación	Coordinadores de los países	Cuestionarios presentados	Crecimiento medio de la puntuación general respecto de 2018
194	**2020**	**169**	**150**	**9.5%**

El Índice consiste en 82 preguntas sobre los compromisos de ciberseguridad de los Estados Miembros divididas en cinco pilares:

- medidas jurídicas;
- medidas técnicas;
- medidas institucionales;
- medidas de capacitación;

[1] El Estado de Palestina participa en los trabajos de la UIT en virtud de la Resolución 99 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios.

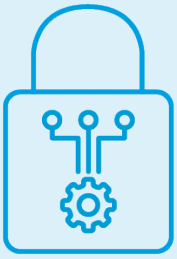
- medidas de cooperación.

El siguiente cuadro muestra el nivel de compromiso global con indicadores específicos desglosado por pilar.

Jurídico

Medición de las leyes y reglamentos sobre ciberdelincuencia y ciberseguridad

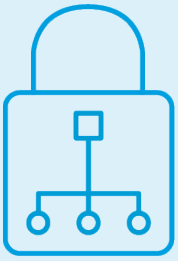
167	Países con algún tipo de legislación sobre ciberseguridad
133	Reglamentación sobre la protección de datos
97	Reglamentación sobre infraestructuras esenciales



Técnico

Medición de la aplicación de las capacidades técnicas a través de los organismos nacionales y sectoriales

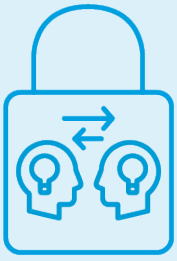
131	EIII activos
104	Participa en un EIII regional
101	Mecanismos de notificación de la protección de la infancia en línea



Organización

Medición de las estrategias nacionales y organizaciones que aplican la ciberseguridad

127	Estrategias nacionales de ciberseguridad
136	Agencias de ciberseguridad
86	Se informa de las estrategias e iniciativas de protección de la infancia en línea



Capacitación

Medición de las campañas de sensibilización, formación, educación e incentivos para la capacitación en materia de ciberseguridad

142	Países que llevan a cabo iniciativas de sensibilización
94	Países con programas de I+D en ciberseguridad
98	Los países que declaran tener industrias nacionales de ciberseguridad

Cooperación

Medición de asociaciones entre organismos, empresas y países

166	Países que participan en asociaciones público-privadas de ciberseguridad
90	Países con acuerdos bilaterales de ciberseguridad
112	Países con acuerdos multilaterales de ciberseguridad

Cambios en el Índice de Ciberseguridad Global que afectan a las puntuaciones

- Esta edición del Índice de Ciberseguridad Global se basa en los datos comunicados con una cifra récord de participación de los Estados Miembros, que ha pasado de 105 respuestas en 2013-2014 a 150 respuestas en 2020.
- Se ha actualizado el Cuestionario del ICG. Se han redefinido, añadido o eliminado preguntas en cada uno de los cinco pilares (medidas jurídicas, técnicas, organizativas, de capacitación y de cooperación) con arreglo a la evolución de las preocupaciones y los esfuerzos en materia de ciberseguridad. Los cambios en el cuestionario afectan los resultados y constituyen un factor en las puntuaciones y clasificaciones de los países.
- La ponderación difiere de las iteraciones anteriores, lo que responde, en parte, a los cambios en la estructura de las preguntas, así como la adición y eliminación de preguntas.
- La ponderación de los indicadores se basa en las recomendaciones de los expertos. Los Miembros de la UIT designaron a expertos para que asesoraran en el proceso de ponderación a fin de asignar pesos a los indicadores en función de su importancia relativa para la ciberseguridad. Las variaciones en la asignación de pesos pueden afectar a la puntuación y clasificación de los países.
- Se ha preparado una sección para dar más información sobre la construcción, la composición y los cambios recientes del Cuestionario del ICG (Anexo A).
- Muchos países, especialmente los de mayor puntuación, tienen cada vez más puntuaciones similares, por lo que las clasificaciones individuales deben interpretarse cuidadosamente.
- Algunos países se negaron a verificar los datos recopilados o a participar en esta edición del Índice de Ciberseguridad Global. Los datos relativos a estos países (marcados con un *) no han sido refrendados oficialmente por ningún representante de éstos. Como esos datos se recabaron mediante búsquedas en línea, cabe suponer que los datos que faltan no se han encontrado o no existen.

Por otra parte, en algunos casos la colaboración de los países puede haber influido positivamente en las puntuaciones, ya que cuanto más contribuya un país al cuestionario, más probable será que se encuentren respuestas afirmativas.

Hay ámbitos en los que muchos países destacan y otros ámbitos en los que hay margen para intensificar los esfuerzos, razón por la cual los países no deberían obcecarse en la clasificación.

Se realizó una investigación documental de los países que no respondieron al cuestionario, mediante la información disponible en los sitios web oficiales y otros recursos. Para esos países, los datos recopilados quizá no se correspondan con exactitud con la postura de ciberseguridad del país. El ICG no contiene datos estimados.

Índice

Lista de cuadros y figuras

Cuadros

Figuras

1 Índice de Ciberseguridad Global: Antecedentes y contexto

La cuarta edición del Índice de Ciberseguridad Global (IGC) aparece en un momento muy diferente al de sus predecesores. Cuando se publicó por vez primera la Agenda de Ciberseguridad Global en 2007, aún faltaba un mes para que saliera a la venta el primer iPhone y Facebook sólo llevaba un año abierto a los usuarios fuera de las universidades de Estados Unidos. Mil millones de personas estaban conectadas y se temía que la cantidad de datos creados, 255 exabytes, rebasaría el almacenamiento disponible.[1] Hoy en día, los teléfonos inteligentes han transformado la vida cotidiana y las redes sociales se han integrado en una esfera más amplia de la sociedad. En la actualidad, 3 500 millones de personas están conectadas y se calcula que el mundo digital alcanza los 44 zettabytes, sin riesgo alguno de que falte almacenamiento gracias a la computación en nube.[2] Además, la proliferación de las TIC ha afectado al ecosistema nacional general, generando nuevas posibilidades organizativas, como los servicios de gobierno electrónico, y nuevos paradigmas económicos y productivos, como la Industria 4.0 y la economía digital generalizada.

Todos los países se ven afectados en cierta medida por la brecha digital y se debería conferir alta prioridad a la ciberseguridad, por cuanto es un factor esencial para la economía, la sociedad y el gobierno, que dependen de sistemas digitales.

La pandemia de la COVID-19 ha repercutido drásticamente en el funcionamiento de las sociedades. Cuando la pandemia cobró fuerza en abril de 2020, Akamai observó un aumento del tráfico de Internet de un 30%.[3] La tecnología ha desempeñado un papel fundamental para mantener a las personas conectadas, ya sea para el teletrabajo o para la enseñanza a distancia. Para que la era digital desarrolle plenamente su potencial, es indispensable que el ciberespacio sea seguro y fiable. Un año después de que la Organización Mundial de la Salud declarara la pandemia de la COVID-19 y de la aparición de nuevos sistemas de gestión y de vacunas, nuestra dependencia de las tecnologías digitales sigue creciendo. A medida que se conecta a quienes carecen de conexión, se ha de velar por que el ciberespacio sea seguro y fiable.

Cada vez se tiene más conciencia sobre los riesgos para la ciberseguridad.[4] La actual pandemia ha creado desconfianza, especialmente en línea. Los datos recabados en el ICG pueden sentar las bases para debatir más detalladamente acerca de la ciberseguridad, pero resulta fundamental conocer el contexto y las observaciones en el plano local para determinar la forma de proceder.

El ICG puede contribuir a crear un ciberespacio seguro y de confianza tras la pandemia, por cuanto puede servir de punto de partida a comprender cómo la pandemia ha afectado a las iniciativas en materia de ciberseguridad y cómo los países se esfuerzan por abordar la ciberseguridad y la confianza. Por ejemplo, algunos países informaron de que se han producido

---

1 http://core.xsomo.com.jm/images/web/File/white%20papaers/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf.
2 https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.
3 https://blogs.akamai.com/2020/04/can-the-internet-keep-up-with-the-surge-in-demand.html.
4 http://reports.weforum.org/global-risks-report-2020/executive-summary/.

retrasos en la aprobación y entrada en vigor de leyes, en la creación o mejora de los EIII, en la elaboración o revisión de estrategias nacionales de ciberseguridad, y en la realización de actividades de capacitación. También ha afectado a los acuerdos de cooperación, por cuanto se interrumpió la interacción y la colaboración en persona.

Es importante que los gobiernos hagan un balance de las políticas y prácticas vigentes en materia de ciberseguridad, ya que el mundo sigue cambiando. La forma de medir la ciberseguridad ha evolucionado y se ha adaptado a los cambios en este ámbito. Se han modificado las preguntas del ICG relativas al papel de los EIII, los acuerdos de cooperación, los marcos institucionales y la sensibilización pública. Aunque estos cambios hacen que el ICG sea menos comparable a lo largo del tiempo, esta edición responde con mayor precisión a los compromisos actuales de los países.

2 Temas fundamentales

2.1 Medidas jurídicas: Planificación de futuras intervenciones

Las numerosas dificultades que existen hoy en día menoscaban la confianza en línea e impiden que la sociedad digital alcance su pleno potencial. Por ejemplo, se estima que las pérdidas a escala mundial debidas a la ciberdelincuencia oscilan entre 1 billón de dólares en 2020[5] y 6 billones en 2021.[6] En este sentido, la creación de un marco jurídico y reglamentario para proteger a la sociedad y promover un entorno digital seguro resulta indispensable y debe ser el primer paso de cualquier iniciativa nacional en materia de ciberseguridad.

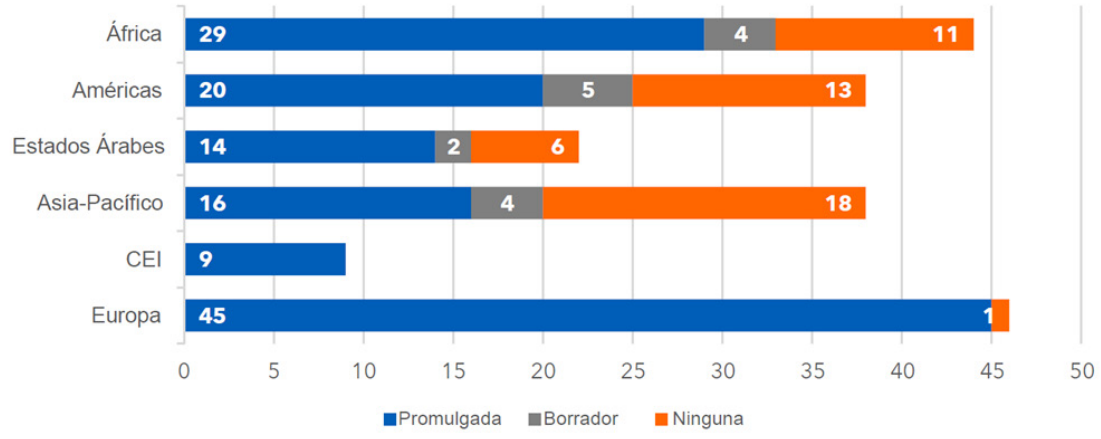
Los marcos jurídicos y reglamentarios comprenden la promulgación de una legislación que defina lo que constituye actividades ilícitas en el ciberespacio y los instrumentos necesarios para investigar, perseguir y hacer cumplir dicha legislación; el establecimiento de parámetros de referencia sobre ciberseguridad y mecanismos de observancia para un conjunto de actores nacionales; y procedimientos para garantizar la coherencia con las obligaciones internacionales.

En esta cuarta edición del Índice de Ciberseguridad Global se hace un balance de las intervenciones en materia de ciberseguridad en el marco jurídico del país, midiendo la presencia de:

- requisitos básicos que deben cumplir los agentes públicos y privados;
- instrumentos jurídicos que prohíben acciones nocivas.

Protección de datos

Figura 1: Países con legislación en materia de protección de datos



Fuente: UIT

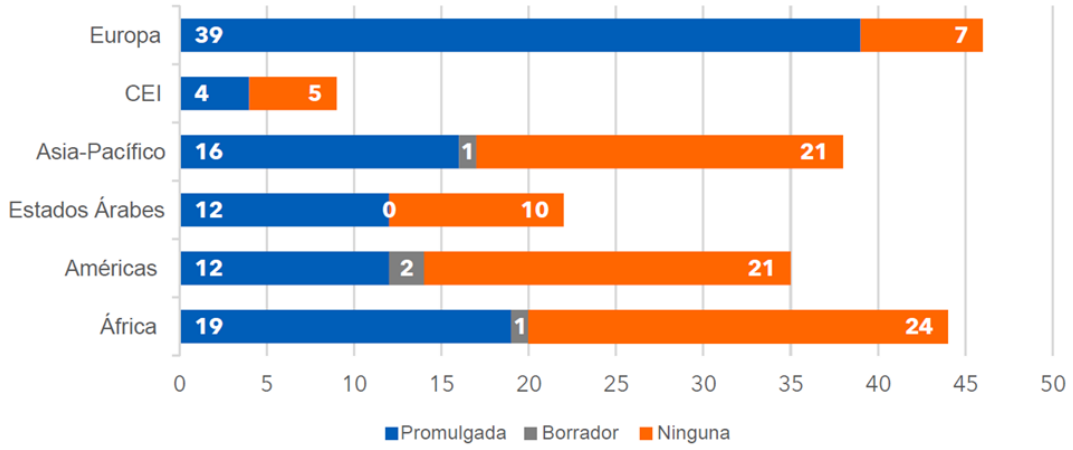
La legislación en materia de protección de datos puede adoptar la forma de una reglamentación que, por ejemplo, obligue a las organizaciones a notificar los incidentes ciberseguridad o establezca requisitos de auditoría anuales.

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
[6] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

A primera vista, los defensores de la privacidad pueden observar que ya son numerosos los países que han actualizado su reglamentación en materia de protección de datos y privacidad. Además, 133 países han promulgado normas de protección y privacidad, 15 están en proceso de redacción y 46 no tienen ninguna regulación en vigor. Muchos países que ya cuentan con reglamentación han actualizado su legislación para incorporar en ella los nuevos acuerdos y normas.

Desde la última edición se ha incrementado el número de países que exigen la notificación de incidentes. En esta edición, son 102 países los países que exigen en su legislación y políticas la notificación de incidentes y de filtración de datos.

Figura 2: Países que exigen la notificación de incidentes

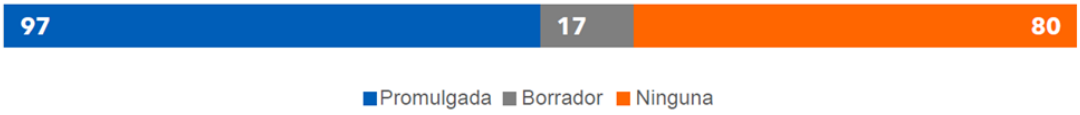


Fuente: UIT

Usurpación de identidad y robo de datos en línea

Aunque algunos países han tomado medidas contra el acceso ilícito, todavía no se presta suficiente atención a la legislación en materia de usurpación de identidad y robo de datos en línea, pese a que la protección de la identidad en línea es muchísimo más importante a tenor de la transformación en curso hacia el entorno digital. La población mundial ha entrado en el mundo de Internet a través de las redes sociales y las prácticas laborales, que requieren un nivel de seguridad considerable, por cuanto toda usurpación de identidad puede poner en peligro la vida cotidiana tanto en el ámbito privado como en el profesional.

Figura 3: Países con legislación sobre el robo de datos personales

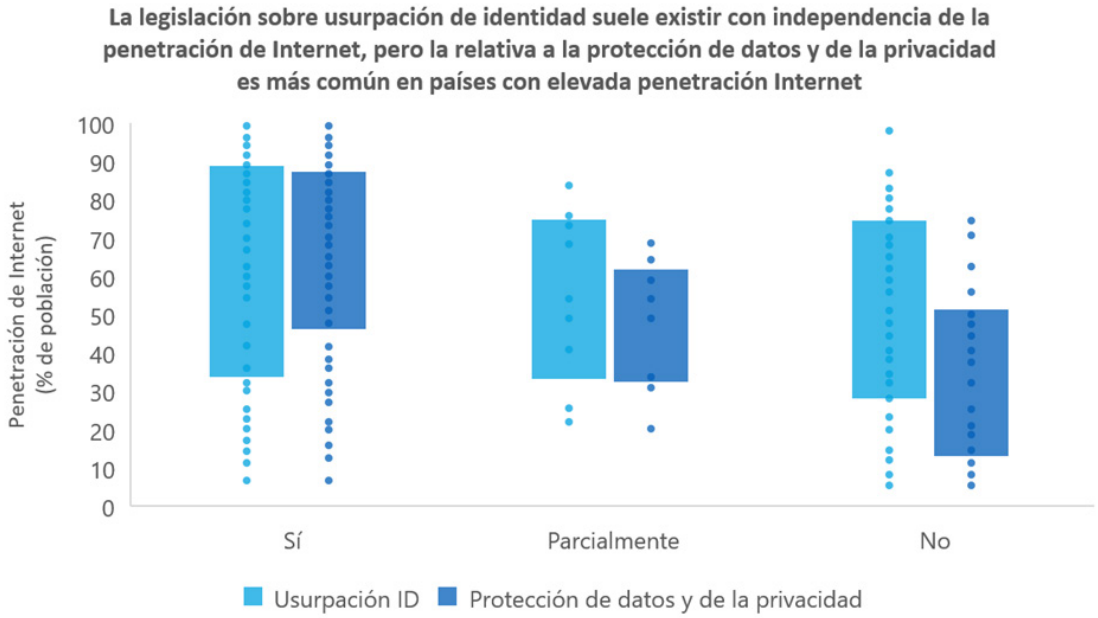


Fuente: UIT

Como se desprende de la Figura 4, cuando se observa los valores medios del índice de penetración de Internet, los países con mayor penetración de Internet son algo más propensos a tener una ley o reglamento sobre protección de datos en línea que los países con un bajo índice de penetración de Internet. Por el contrario, es más probable que los países con elevada penetración de Internet cuenten con reglamentación en materia de protección de datos y de la

privacidad. Estas tendencias responden, en parte, a las circunstancias económicas, el desarrollo general y las estrategias de digitalización gubernamentales. Cabe destacar que algunos países han promulgado legislación en materia de usurpación de identidad y protección de datos y de la privacidad con el fin de estar preparados para para una mayor penetración de Internet.

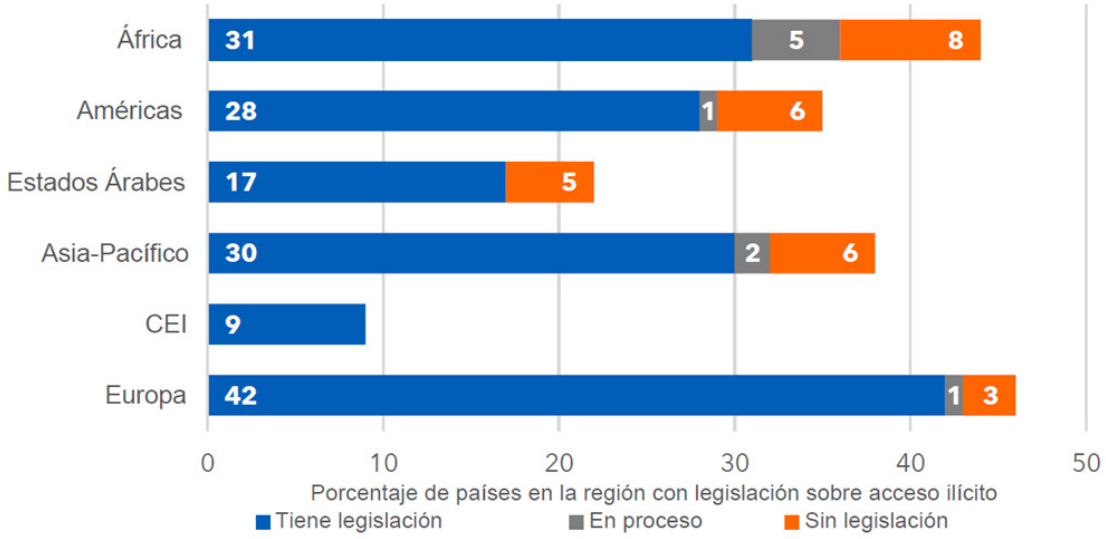
Figura 4: Legislación sobre usurpación de identidad y protección de datos y de la privacidad, respecto del acceso a Internet (% de la población)



Fuente: Base de datos de la UIT sobre indicadores de telecomunicaciones/TIC mundiales

Como se observa en la Figura 5, la mayoría de los países disponen de legislación sobre acceso ilícito, con escasas diferencias significativas entre las regiones.

Figura 5: Legislación sobre acceso ilícito



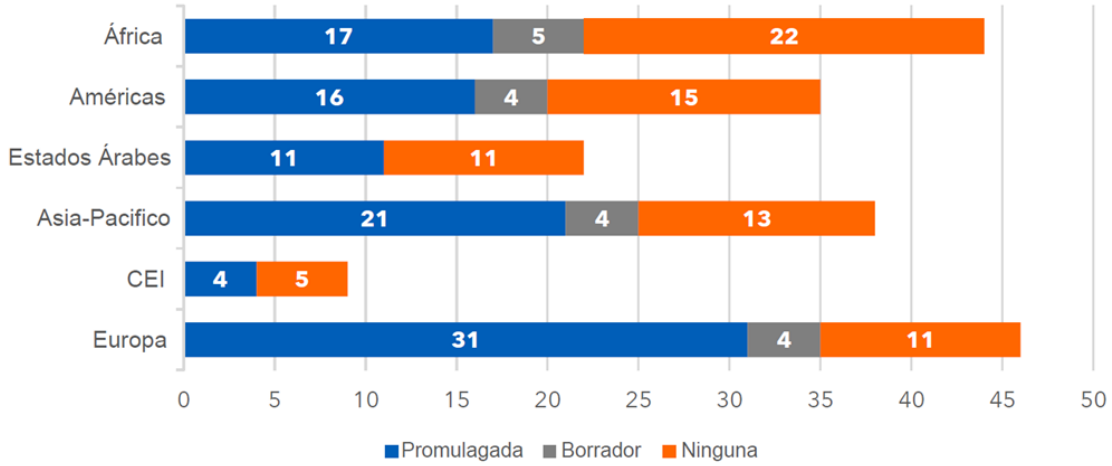
Fuente: Base de datos de la UIT sobre indicadores de telecomunicaciones/TIC mundiales

Conducta antisocial en línea

La conducta antisocial en línea supone un problema constante al que los países conceden cada vez más importancia en su legislación. El ICG mide dos aspectos: el acoso en línea y el racismo y la xenofobia en línea.

El acoso en línea sigue siendo un problema recurrente: en Estados Unidos de América en 2020, "el 41% de los estadounidenses experimentaron alguna forma de acoso en línea"[7] y en la Unión Europea al menos 1 de cada 10 mujeres ha sufrido acoso en línea.[8] En una encuesta realizada en 32 países, uno de cada cinco adultos declaró haber sido víctima de discursos de odio en línea.[9]

Figura 6: Países con legislación sobre acoso en línea



Fuente: Base de datos de la UIT sobre indicadores de telecomunicaciones/TIC mundiales

A escala mundial, 100 países han adoptado una legislación que penaliza los casos de acoso y abuso en línea, 17 están en proceso de elaboración y aplicación de estas medidas y 77 no disponen de legislación alguna al respecto. Sin embargo, la definición de lo que constituye abuso es a menudo incorrecta.

Uno de los principales obstáculos a lo hora de abordar el problema del racismo y la xenofobia es la falta de claridad, si bien son numerosos los países que están redactando algún tipo de legislación en ese sentido. Varios países están ampliando o adaptando las leyes generales relativas al racismo y la xenofobia al contexto en línea. El umbral de lo que constituye un delito varía mucho, de modo que lo que en un país es legal puede ser delito en otro. No obstante, algunos países han optado por redactar disposiciones específicas para la conducta racista en línea.

---

7 https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

8 https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf.

9 https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1.

2.2 Medidas técnicas: Mayor despliegue de EIII/EIEI

Para hacer frente a los riesgos e incidentes cibernéticos de forma fiable es preciso disponer de mecanismos y estructuras institucionales eficaces en el plano nacional. Los equipos de intervención en caso de incidente informático (CIRT) o los equipos intervención en caso de emergencia informática (EIEI), permiten a los países reaccionar a escala nacional de manera centralizada, rápida y sistemática ante cualquier incidente de este tipo, además de recabar experiencia y aumentar la resiliencia en el ámbito de la ciberseguridad.

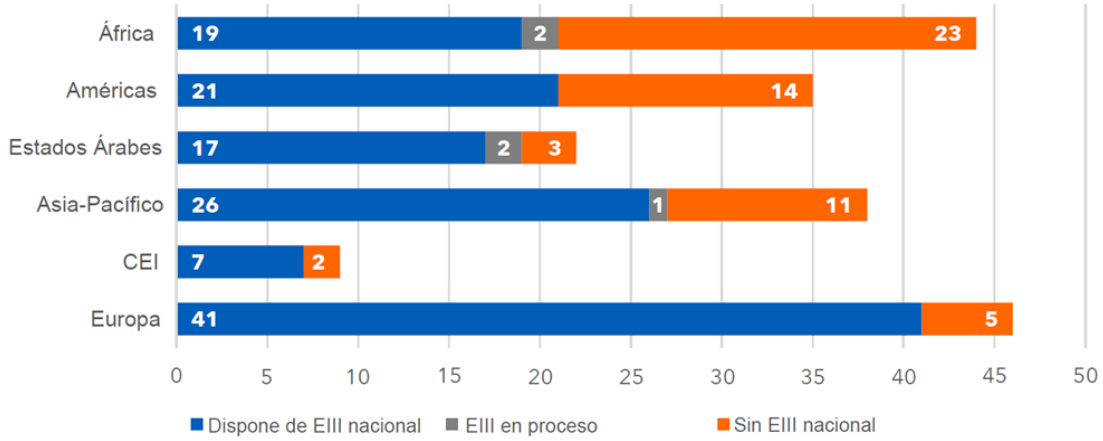
Los EIII nacionales se suelen constituir y realizar con arreglo a la legislación o política nacional. Los EIII pueden formar parte de una institución gubernamental o depender de un ministerio específico u otra entidad. Cuando los países carecen de tiempo, conocimientos o recursos para crear un EIII nacional, suelen subcontratar a un tercer las responsabilidades del EIII.

Se están creando nuevos EIII

A finales de 2020, el número de países que disponían de EIII nacionales se elevaba a 131, de los cuales 10 se crearon después de la publicación del Índice de Ciberseguridad Global de 2018. Otros cuatro EIII nacionales se encuentran en fase de desarrollo.

Aunque muchos países han avanzado en la creación de EIII, muchos otros tienen grandes dificultades para crearlos, especialmente los países menos adelantados (PMA). La falta de recursos, de conocimientos tecnológicos, de ecosistema de ciberseguridad, de investigación y el desarrollo, de prioridades y de voluntad política pueden menoscabar las medidas técnicas para hacer frente a los desafíos de la ciberseguridad.

Figura 7: Número de países con EIII nacional



Fuente: UIT

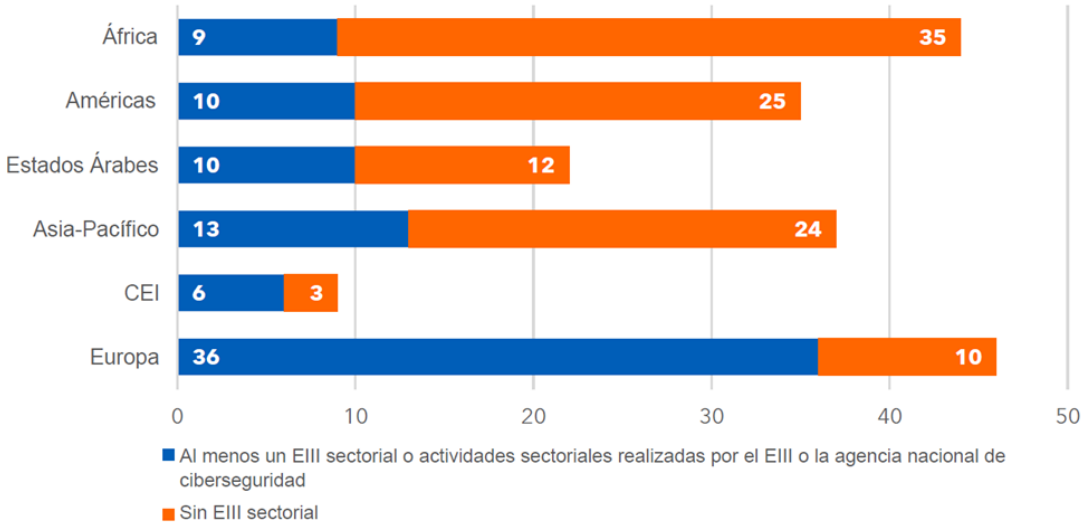
A pesar de que no está a la vanguardia en el campo de la técnica, en la región de África se han establecido seis EIII adicionales desde la publicación del Índice de Ciberseguridad Global de 2018, y el número de países que disponen de un EIII nacional en la región ha pasado de 13 a 19. En la región de las Américas el número de EIII asciende en total a 21 y en la región de los Estados Árabes son 17 países los países que cuentan con un EIII. Asimismo, sólo dos países de la región de la CEI y seis de Europa carecen de EIII nacionales.

El ICG también hace un seguimiento de las actividades de los EIII. De los 131 EIII existentes, 11 participaron en todas las actividades siguientes:

- sensibilización en materia de ciberseguridad y de protección de la infancia en línea, mediante consejos, guías, manuales, formación y vídeos;
- asesoramiento en materia de ciberseguridad a los profesionales de TI;
- realización de cibersimulacros en los dos últimos años;
- colaboración con los EIII regionales y con FIRST[10];
- certificación de Trusted Introducer[11] u otra certificación reconocida.

Mientras que los EIII nacionales se ocupan de los problemas a nivel nacional, los EIII sectoriales se ocupan de las necesidades de ciberseguridad específicas de un determinado sector, como la sanidad, el transporte, las telecomunicaciones o los servicios públicos. Existen otros tipos de EIII que prestan servicio a empresas multinacionales o a grandes empresas y a universidades privadas, por ejemplo, así como otros tipos de EIII de los que no se ocupa este informe del ICG.

Figura 8: Número de EIII sectoriales



Fuente: UIT

Como se muestra en la Figura 8, dos tercios de los países no cuentan con EIII específicos del sector. De los 76 países que disponen de un EIII sectorial, 37 realizan campañas de sensibilización, cibersimulacros e intercambian de forma pública o confidencial con su comunidad información relativa a incidentes y amenazas.

2.3 Medidas institucionales: Estrategia de armonización

Las medidas institucionales se refieren a los mecanismos de gobernanza y coordinación dentro de los países en lo que respecta a la ciberseguridad. Consisten en garantizar que la ciberseguridad se toma en consideración al más alto nivel del ejecutivo y en asignar las funciones y responsabilidades pertinentes a las distintas entidades nacionales, que se responsabilizarán de la postura nacional en materia de ciberseguridad.

[10] www.first.org.
[11] www.trusted-introducer.org/.

Los países con una sólida infraestructura de telecomunicaciones no siempre cuentan con medidas institucionales. Si se compara el índice de infraestructura de telecomunicaciones, de la Encuesta sobre el e-gobierno de 2020: Gobierno digital en la década de acción para el desarrollo sostenible, de las Naciones Unidas, que forma parte del Índice de preparación para el gobierno electrónico,[12] con las puntuaciones generales en las medidas institucionales, se observa que, si bien existe una leve tendencia, son muchos los países cuyos resultados en las medidas relativas a la infraestructura de telecomunicaciones son buenos, pero no cuentan con las medidas institucionales necesarias para resolver los problemas de ciberseguridad.

La falta de medidas institucionales adecuadas puede dar lugar a una falta de claridad en las responsabilidades y de responsabilización en la gobernanza nacional de la ciberseguridad, y puede impedir una coordinación eficaz intragubernamental e intersectorial.

Importancia de mantener actualizadas las estrategias nacionales de ciberseguridad

La estrategia nacional de ciberseguridad (ENC) suele ser la piedra angular de las medidas instituciones a nivel de ciberseguridad nacional. Según la Guía de la UIT para la elaboración de una estrategia nacional de ciberseguridad, la ENC es un marco o estrategia integral que se debe elaborar, implementar y ejecutar en colaboración multipartita y que implica la acción coordinada para la prevención, preparación, respuesta y recuperación en caso de incidentes por las autoridades gubernamentales, el sector privado y la sociedad civil.[13]

Cada vez son más los países que elaboran estrategias nacionales de ciberseguridad (ENC) para gestionar la ciberseguridad de una manera más estructurada. La ENC presenta varias ventajas para los países, entre la que cabe destacar, que permite congregar a las distintas partes interesadas pertinentes, aclarar las prioridades nacionales y planificar la capacitación en materia de ciberseguridad.

A medida que el Índice de Ciberseguridad Global se ha ido afianzando, se presta más atención a los países que actualizan periódicamente su ENC con el fin de adaptarlo al contexto real. De hecho, disponer de una ENC constituye el primer paso a la hora de definir la postura del país en materia de ciberseguridad, pero es necesario revisarla periódicamente con arreglo a la evolución de los peligros y prioridades en el ámbito de la ciberseguridad. Los países suelen actualizar la ENC cada 4 a 5 años. Algunos países han optado por plazos más largos, llegando hasta un decenio o más.

De los 127 países que cuentan con una estrategia nacional de ciberseguridad, ya sea reciente, con más de cinco años de antigüedad o en proceso de elaboración, 60 países han logrado establecer objetivos más claros gracias a la revisión y elaboración de nuevas estrategias de ciberseguridad o a la actualización de su plan de acción.

Protección de la infraestructura esencial/resiliencia nacional

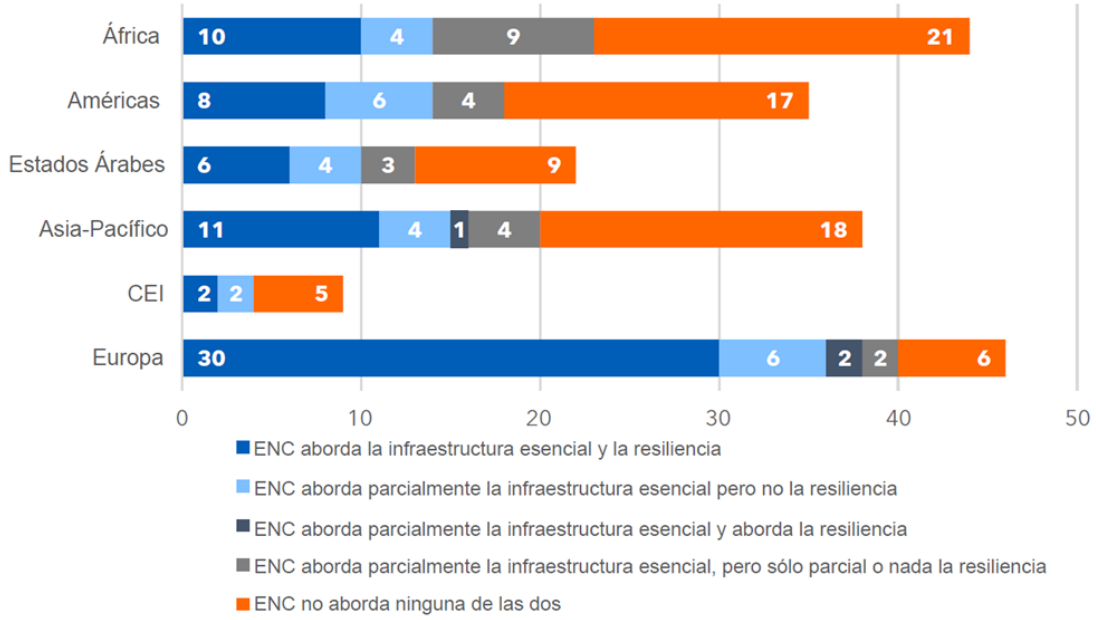
Un aspecto importante al elaborar una estrategia nacional de ciberseguridad es disponer de un conjunto claro de objetivos sobre la protección de la infraestructura esencial. Garantizar la continuidad de las operaciones a escala nacional es un reto permanente para los países. Las infraestructuras esenciales, como las redes eléctricas, las plantas de purificación de agua y los sistemas de transporte, siguen corriendo riesgos de ciberseguridad. Todo incidente que afecte

[12] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.
[13] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

a las infraestructuras esenciales suele tener consecuencias graves y, por ende, la estrategia debe prestar mayor atención a los mecanismos de gestión de riesgos destinados a reducir la probabilidad y gravedad de dichos incidentes.

Se espera que el gasto en ciberseguridad para las infraestructuras críticas aumente a 9 000 millones USD durante el próximo año para alcanzar los 105 990 millones USD en 2021.[14] Como los empleados en infraestructuras esenciales, al igual que el resto de la población activa, han pasado a trabajar en condiciones socialmente distantes, han tenido vigilar una mayor superficie de ataque. Según ABI Research, la inversión en ciberseguridad varía sobremanera en función de la región, el sector y la conectividad, siendo el gasto más elevado en defensa, servicios financieros y TIC, y los sectores industriales situándose a la zaga.[15]

Figura 9: Países que abordan la infraestructura esencial y la resiliencia



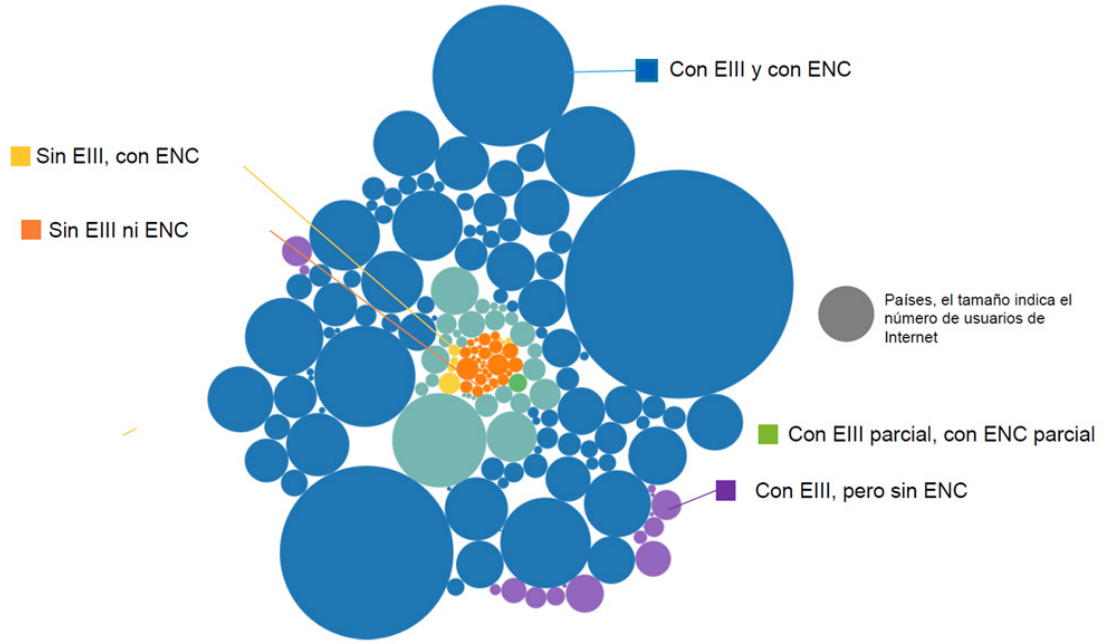
Fuente: UIT

Conceder prioridad a la ciberseguridad en cuanto infraestructura esencial y resiliencia no consiste exclusivamente en consignarlo en el presupuesto, sino también en las estrategias nacionales de ciberseguridad. Éstas suelen abordar más a menudo las infraestructuras esenciales y/o la resiliencia de la ciberseguridad. Sin embargo, muchos países no abordan ninguna de las dos cosas.

[14] https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/.

[15] https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/.

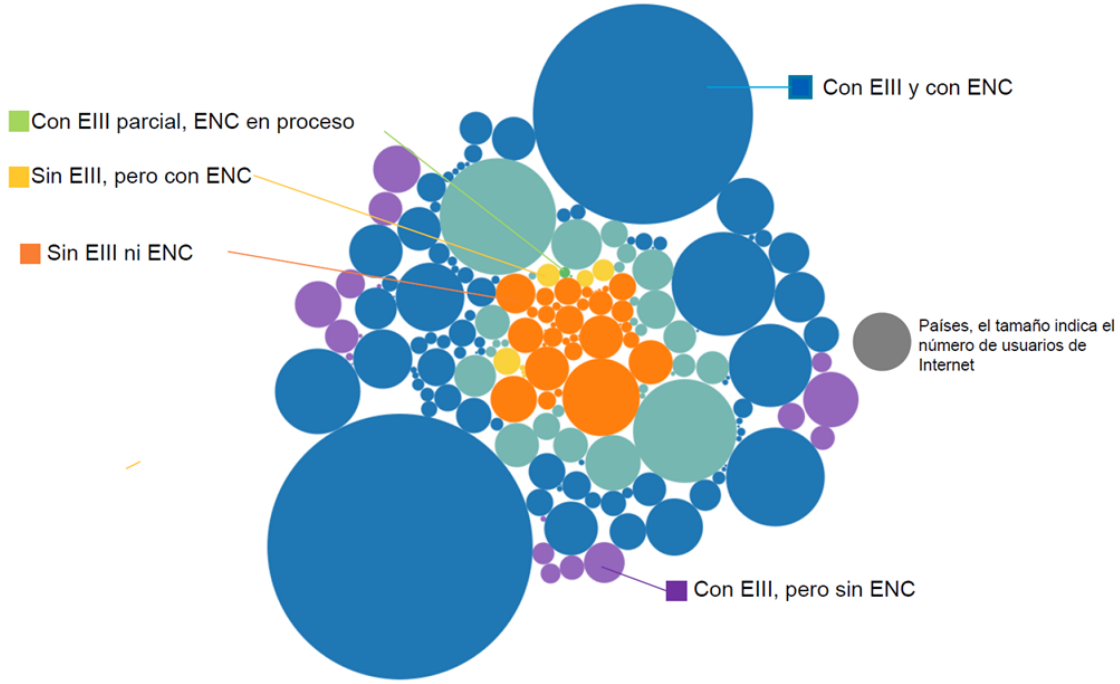
Figura 10: Usuarios de Internet (por cobertura de EIII y de estrategia nacional de ciberseguridad)



Fuente: Índice de Ciberseguridad Global, Indicadores Mundiales de Telecomunicaciones/TIC de la UIT

Si observamos los países del mundo por el número de usuarios de Internet, más del 95% de los usuarios de Internet se encuentran en países que cuentan con una estrategia nacional de ciberseguridad y un CIRT nacional.

Figura 11: Tamaño de la población no conectada (por cobertura de la CIRT y de la estrategia nacional de ciberseguridad)



Fuente: Índice de Ciberseguridad Global, Indicadores Mundiales de Telecomunicaciones/TIC de la UIT

Sin embargo, los países menos conectados son a menudo los carecen de un ENC y/o de un EIII nacional. El 9% de la población no conectada vive en países que carecen de un EIII nacional o de una ENC, mientras que otro 15% se encuentra en países sin ENC, pero con un EIII nacional. Más de la mitad de los países menos adelantados carecen de un EIII y el 60% carece de una estrategia nacional de ciberseguridad o aún no la ha elaborado.

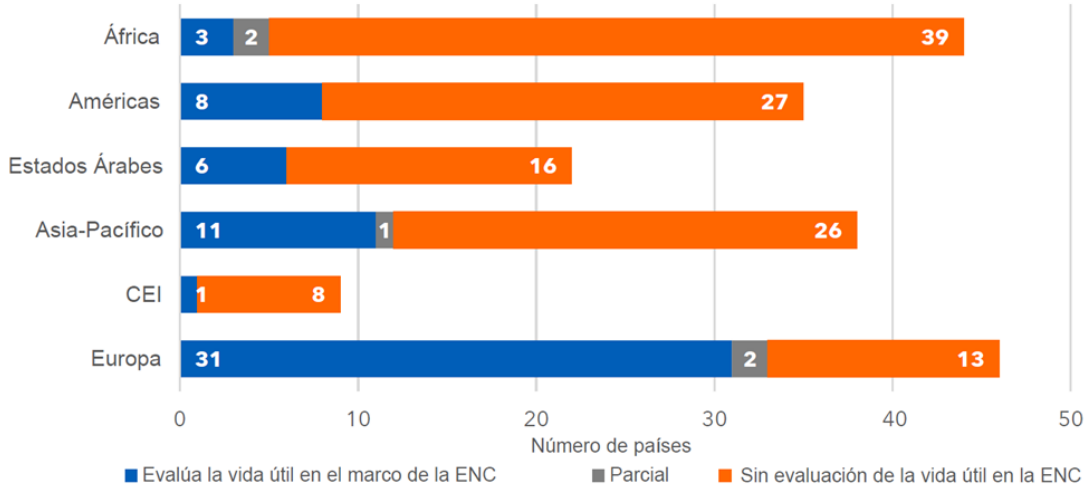
Cuadro 1: Número de países con una ENC y un EIII

	Con ENC	ENC en curso o con más de 5 años de antigüedad	Sin ENC
EIII nacional	90 países	29	18
Sin EIII nacional	7	1	49

Fuente: UIT

Los países sin estrategia nacional tienen menos probabilidades de disponer de un EIII. No es de extrañar que entre los 63 países sin EIII y los 67 países sin estrategia nacional, 49 países no tengan ni una cosa ni la otra.

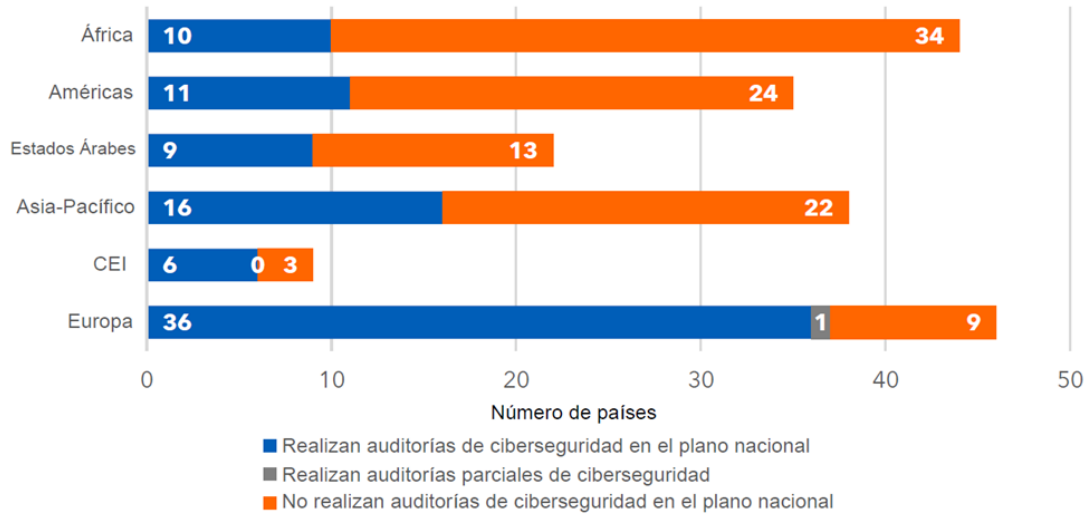
Figura 12: Evaluación de la vida útil en el marco de la ENC



Fuente: UIT

Disponer de una estrategia nacional de ciberseguridad es un primer paso para crear una postura de ciberseguridad, pero es preciso actualizarla y revisarla periódicamente. Muchos países que cuentan con una ECN no la revisan ni la reajustan periódicamente con arreglo a la evolución de las amenazas y prioridades de ciberseguridad. De los 98 países que cuentan con una NCS actualizada, sólo 60 actualizan la vida útil de su estrategia.

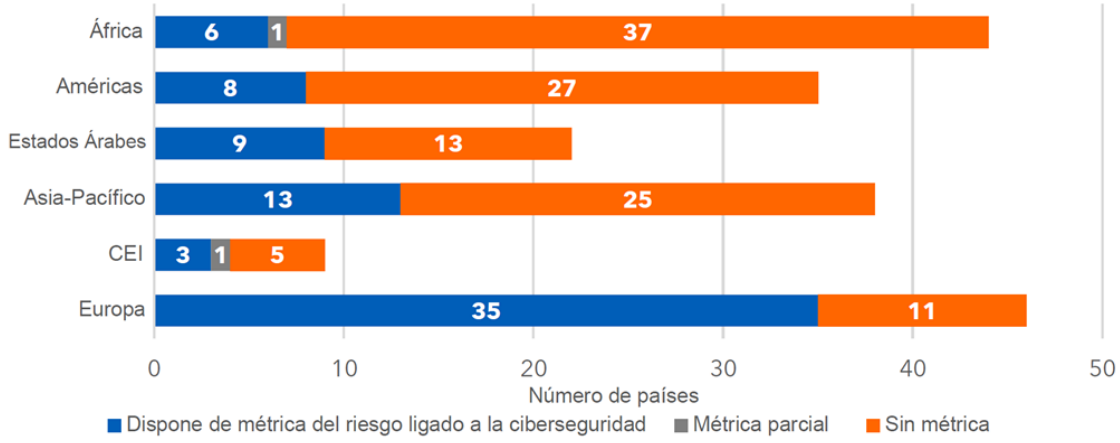
Figura 13: Auditorías de ciberseguridad a escala nacional



Fuente: UIT

Las auditorías nacionales de ciberseguridad (Figura 13) son más comunes que las evaluaciones de la vida útil. La frecuencia de estas auditorías no se evaluó en esta edición del ICG.

Figura 14: Métrica para evaluar el riesgo del ciberespacio en el plano nacional



Fuente: UIT

Del mismo modo, la mayoría de los países no disponen de métricas para evaluar el riesgo asociado al ciberespacio en el plano nacional. La falta de estas métricas dificulta la evaluación de los riesgos actuales, el establecimiento de prioridades en las intervenciones de ciberseguridad y el seguimiento del progreso.

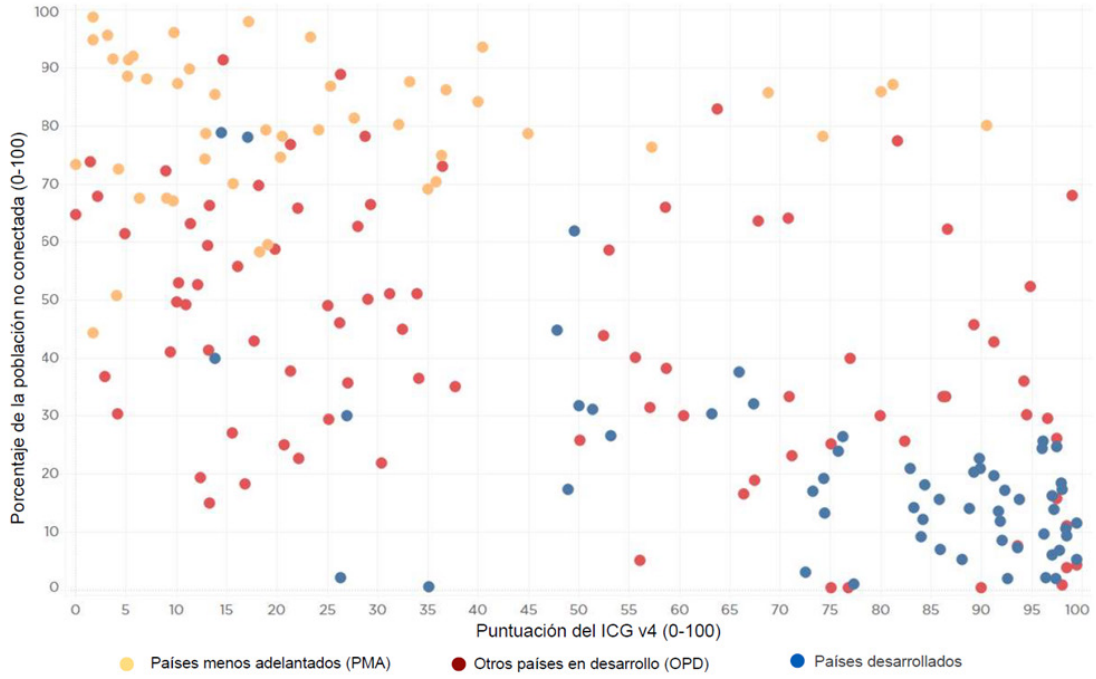
2.4 Medidas de capacitación: Capacitación en materia de ciberseguridad

El Foro Económico Mundial estima que "cada día, aproximadamente un millón de personas se conectan por primera vez a Internet, y dos tercios de la población mundial ya posee un dispositivo móvil".[16] Si bien la tecnología digital aporta enormes beneficios socioeconómicos,

[16] https://reports.weforum.org/global-risks-report-2020/executive-summary/.

los riesgos cibernéticos pueden neutralizar los beneficios de la digitalización. La protección del dominio cibernético a través de actividades de capacitación en materia de ciberseguridad resulta fundamental, por cuanto contribuye a reducir problemas como la brecha digital y los riesgos cibernéticos.

Figura 15: El Índice de Ciberseguridad Global y los desconectados



Fuente: Índice de Ciberseguridad Global, Indicadores Mundiales de Telecomunicaciones/TIC de la UIT

Como se observa en la Figura 15, países que suelen tener menos puntuación en el Índice de Ciberseguridad Global son con mucha probabilidad países menos adelantados y con un elevado porcentaje de su población sin conexión. A medida que estas personas comienzan a estar más conectadas, necesitan asistencia para desarrollar conocimientos en materia de ciberseguridad y poder responder mejor a las amenazas. Sin embargo, es más probable que muchos países, en particular los PMA, tengan dificultades en cuanto a disponibilidad de recursos para superar su brecha de cibercapacidad, como la falta de conocimientos institucionales, las restricciones políticas y la escasez de competencias, entre otros, para proteger sus sistemas de TIC, tanto física como virtualmente.

Varios países menos adelantados resultan atípicos, como Bangladesh, Benin, Rwanda y Tanzanía, que han demostrado un fuerte compromiso en lo que respecta a la ciberseguridad. En particular, todos estos países declararon tener industrias nacionales de ciberseguridad, una característica indispensable para las medidas de capacitación.

Figura 16: Objetivos de Desarrollo Sostenible (8, 9, 10)

Fuente: ONU (https://sdgs.un.org/goals)

Para promover el trabajo decente y el crecimiento económico, construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación, así como para reducir las desigualdades internas dentro de los países y en países, resulta indispensable la capacitación en materia de ciberseguridad a fin de poder reforzar los procesos, las competencias, los recursos y la investigación y desarrollo destinados a reforzar las capacidades nacionales. La capacitación en materia de ciberseguridad también contribuye a desarrollar las capacidades colectivas y a facilitar la cooperación y las asociaciones internacionales destinadas a reaccionar eficazmente a los problemas relacionados con la ciberseguridad digital.

Las herramientas y medidas de capacitación pueden, por añadidura, contribuir a la gestión de los riesgos en materia de ciberseguridad, a la protección de los ciudadanos, las infraestructuras y las empresas, y a la construcción de comunidades cibernéticas más sólidas.

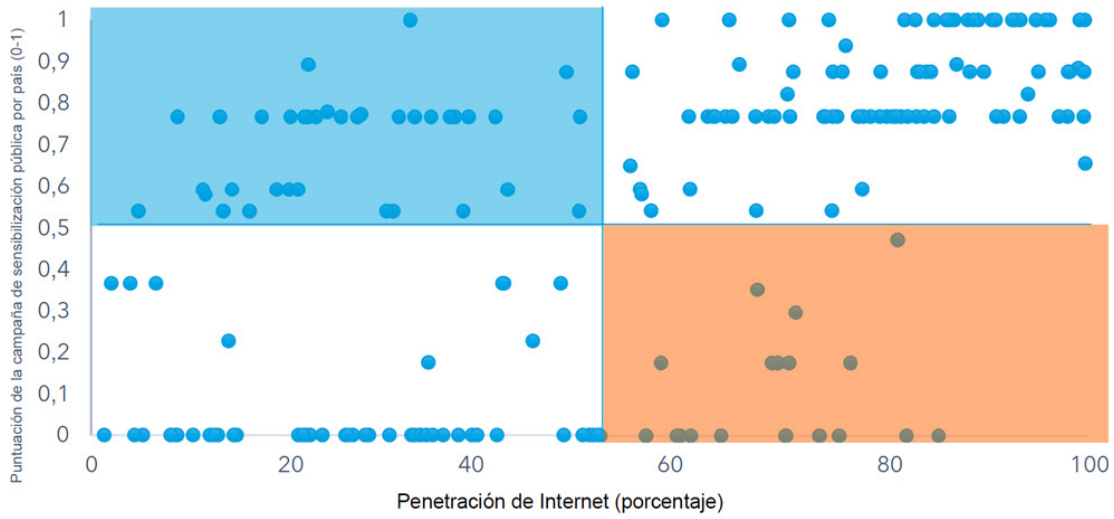
Sensibilización pública en materia de ciberseguridad

Las campañas eficaces de sensibilización en materia de ciberseguridad son esenciales para mantener alerta a los ciudadanos, las empresas, los gobiernos, los jóvenes y las organizaciones. Dada la actual transición hacia los servicios digitales, los gobiernos deben asegurarse de que todos los usuarios sean conscientes de los riesgos que corren en sus actividades digitales.

Contrastando las campañas de sensibilización sobre la ciberseguridad con el índice de penetración de Internet, se obtienen cuatro grupos principales de países:

1) Baja penetración de Internet y campañas de sensibilización sobre ciberseguridad (recuadro azul de la Figura 17): estos países están mejor preparados para conectar a quienes carecen de conexión y sensibilizar debidamente a las personas.
2) Baja penetración de Internet y sin campañas de sensibilización sobre ciberseguridad: estos países aún no han logrado conectar a quienes carecen de conexión y no sensibilizan a su población acerca de la ciberseguridad.
3) Alta penetración de Internet y campañas de sensibilización sobre ciberseguridad: estos países están conectados digitalmente y participan en actividades de sensibilización en materia de ciberseguridad para fomentar una conducta segura en línea.
4) Alta penetración de Internet y sin campañas de sensibilización en materia de ciberseguridad (recuadro naranja de la Figura 17): estos países están conectados digitalmente, pero su población no es consciente de los riesgos cibernéticos.

Figura 17: Puntuación de las campañas de sensibilización pública sobre ciberseguridad (por país, comparado con la penetración de Internet)



Fuente: UIT

Campaña de sensibilización para personas con discapacidad y personas mayores

Por mucho que Internet y el mundo digital ofrezcan oportunidades sin precedentes, la mayoría de las veces no se tiene en cuenta a las personas con discapacidad ni a los ancianos a la hora de tomar decisiones prácticas y opciones tecnológicas. Se calcula que en 2021 habrá 752 millones de personas de 65 años o más.[17] Al comparar esta cifra con el número de países que cuentan con campañas de sensibilización para personas con discapacidad y personas mayores, el resultado es significativamente reducido. De los 194 países, sólo el 18% realizan campañas de sensibilización para personas con discapacidad y el 25% para personas mayores. Resulta alarmante el escaso número de países que realizan campañas de sensibilización para estos dos grupos de población, ya que crea diferencias y una brecha digital importante, puesto que se insta a las personas con discapacidad y a las personas mayores a utilizar los servicios digitales, como las aplicaciones de localización de contactos COVID-19.

Mayor conciencia sobre ciberseguridad en las pequeñas y medianas empresas (PYME), el sector privado y el gobierno

Las operaciones comerciales se han intensificado en línea durante la pandemia de COVID-19, incrementando así las exigencias en las prácticas de ciberseguridad del sector privado. Las PYME suelen ser las empresas más comunes en los países en cuanto a su tamaño, puesto que el 90% de las empresas son PYMES, el 50% del empleo proviene de las PYMES y las PYMES formales representan el 40% del PIB en las economías incipientes.[18] Sin embargo, las PYME suelen ser las menos capacitadas para hacer frente a la ciberseguridad. Por ese motivo, las PYME necesitan actividades de sensibilización en materia de ciberseguridad.

[17] https://population.un.org/wpp/DataQuery/.
[18] https://www.worldbank.org/en/topic/smefinance.

Figura 18: Número de países con campañas de sensibilización sobre ciberseguridad dirigidas a las PYME, al sector privado y a los organismos gubernamentales

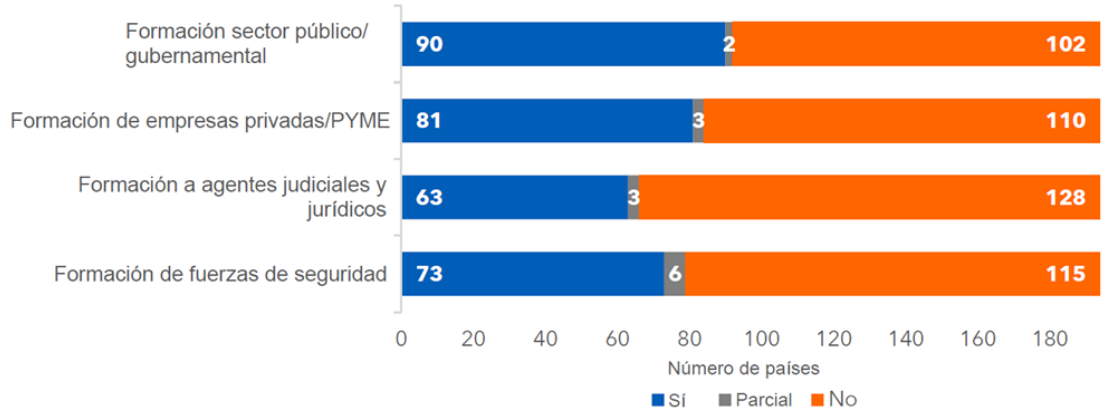
Fuente: UIT

Los resultados del ICG muestran que alrededor del 60% de los países realizan o han realizado durante los dos últimos años campañas para mejorar la sensibilización sobre ciberseguridad de las PYME, las empresas del sector privado o los organismos gubernamentales, mientras que el 38% no informó haber realizado campaña alguna sobre ciberseguridad. La actividad consistió en informar al grupo destinatario acerca de la seguridad en línea y los fundamentos de la ciberseguridad, proporcionándoles recursos a través del EIII nacional o herramientas para proteger las redes. El 2% de los países se encuentra en la fase inicial de preparación de campañas dirigidas a PYME, al sector privado y a organismos gubernamentales.

Los gobiernos reconocen la necesidad de programas educativos específicos del sector y de formación para profesionales de la ciberseguridad

Cada vez es más importante ofrecer programas de formación que respondan a las distintas necesidades del sector. Los analistas de ciberseguridad prevén que en 2021 habrá entre 3,5 millones[19] y 4 millones[20] de puestos de trabajo de ciberseguridad vacantes en todo el mundo. A pesar de estas previsiones, son numerosos los países que todavía no ha desarrollado una formación específica para el sector y más del 50% de los países carecen de programas adaptados a sectores o profesiones específicas, como fuerzas del orden, agentes jurídicos, PYME, empresas privadas y funcionarios públicos.

Figura 19: Número de países con programas educativos/formación en materia de ciberseguridad para profesionales



Fuente: UIT

[19] https://cybersecurityventures.com/jobs/.
[20] ESG Research Report: 2019 Digital Work Survey (esg-global.com).

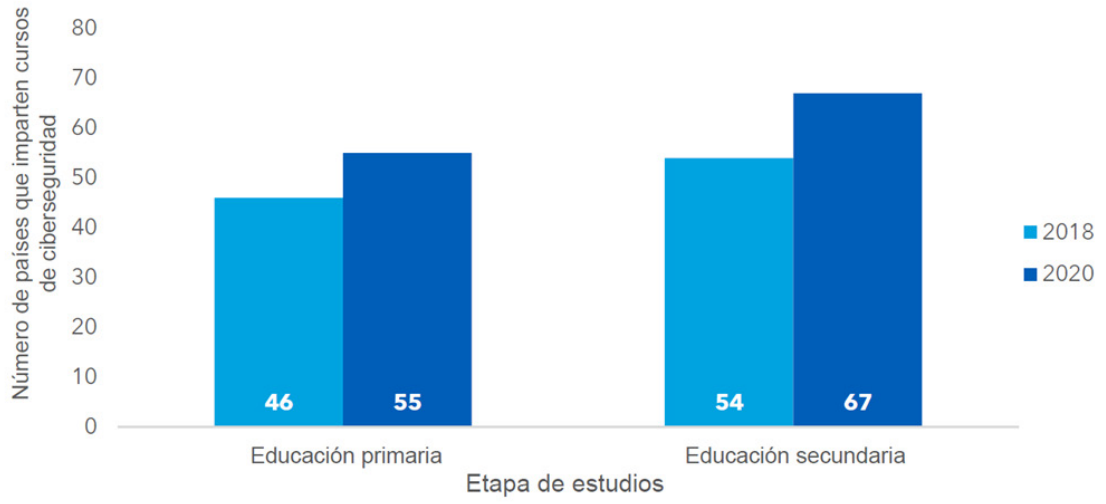
Como se muestra en la Figura 19, el 46% (90) de los países afirman impartir formación sobre ciberseguridad específica para el sector público y los funcionarios del gobierno, el 41% (81) de los países ofrecen ejercicios de capacitación sobre cuestiones de ciberseguridad para los profesionales de TI, incluidas las PYME y el sector privado, el 37% (73) para las fuerzas del orden y el 32% (63) se aseguran de que los actores judiciales y otros actores jurídicos no se queden a la zaga a la hora de garantizar la resiliencia y la seguridad.

Según los países, esta formación en ciberseguridad se imparte a través de sus EIII nacionales, centros nacionales de ciberseguridad y cursos de formación aprobados o respaldados por el gobierno e impartidas por otras instituciones regionales e internacionales. Algunos países que desean aumentar el número de profesionales de la ciberseguridad, pero que no podían impartir formación a escala nacional, recomiendan la formación internacional que brindan organismos de certificación de ciberseguridad como SANS[21], ISC2, ICSPA[22], ISACA[23] y otros.

Los cursos de ciberseguridad en la educación primaria y secundaria están cada vez más extendidos

A raíz de la transición en los países hacia la educación en línea, los cursos de seguridad y ciberseguridad en línea no sólo se imparten en la enseñanza superior, sino también en la primaria y la secundaria.

Figura 20: Número de países que incluyen cursos de ciberseguridad en los planes de estudio nacionales (por etapa educativa)



Fuente: UIT

Como se muestra en la Figura 20, los países están integrando más cursos de ciberseguridad en los planes de estudio nacionales desde el Índice de Ciberseguridad Global de 2018. Un 5% más de países, de 46 a 55, imparten cursos introductorios sobre cómo mantener a los niños a salvo de Internet en la educación primaria y un 7% más de países, de 54 a 67, ofrecen recursos en los planes de estudios académicos de secundaria para que los estudiantes interesados en seguir la ciberseguridad como carrera empiecen a aprender sobre ella a una edad temprana.

[21] https://www.sans.org/.
[22] https://icspa.org/about-us/.
[23] https://www.isaca.org/.

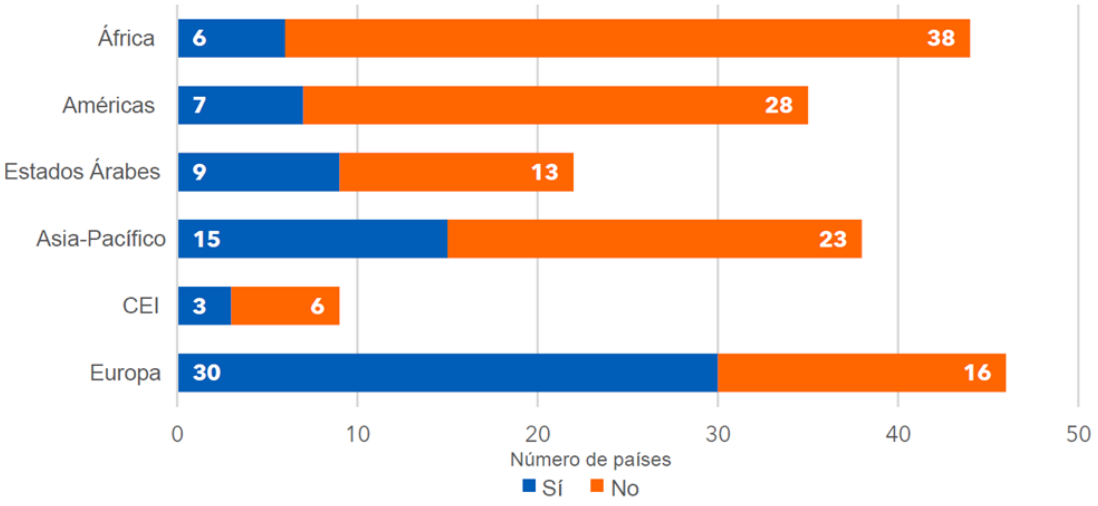
Los incentivos gubernamentales para el desarrollo de la ciberseguridad se quedan atrás

A fin de fomentar la ciberseguridad a nivel nacional es indispensable promover una cultura de la ciberseguridad que inste de los dirigentes empresariales a cambiar su actitud al respecto, para que, en lugar de considerar la ciberseguridad como un problema relacionado con la tecnología de la información, adopten una perspectiva más general que valore el papel que puede desempeñar la ciberseguridad a la hora de mejorar la eficiencia y el rendimiento general de la empresa. Conseguir que las organizaciones otorguen prioridad a la ciberseguridad es un proceso que depende de la disponibilidad de infraestructuras y mecanismos que fomenten la adopción de la ciberseguridad. Los países que fomentan la ciberseguridad en el sector privado y estimulan la creación de empresas relacionadas con la ciberseguridad incorporan incentivos en su marco de ciberseguridad.

Los mecanismos a los que pueden recurrir los países a fin de promover la adopción de la ciberseguridad en el sector privado son diversos, por ejemplo, incentivos fiscales basados en parámetros de ciberseguridad, exenciones fiscales o la incorporación de normas de ciberseguridad en los contratos. De esta forma, se insta a los actores del sector privado a conceder prioridad a la ciberseguridad en sus estructuras y procesos operativos, mejorando a su vez la postura de ciberseguridad del país a corto, medio y largo plazo.

Sin embargo, en esta edición del ICG se observa que 124 países no ofrecieron incentivo alguno en el ámbito de la ciberseguridad, por lo que se hace indispensable que los Estados Miembros adopten dichos incentivos para acelerar la adopción de medidas de ciberseguridad.

Figura 21: Número de países con mecanismos para incentivar la capacitación en materia de ciberseguridad



Fuente: UIT

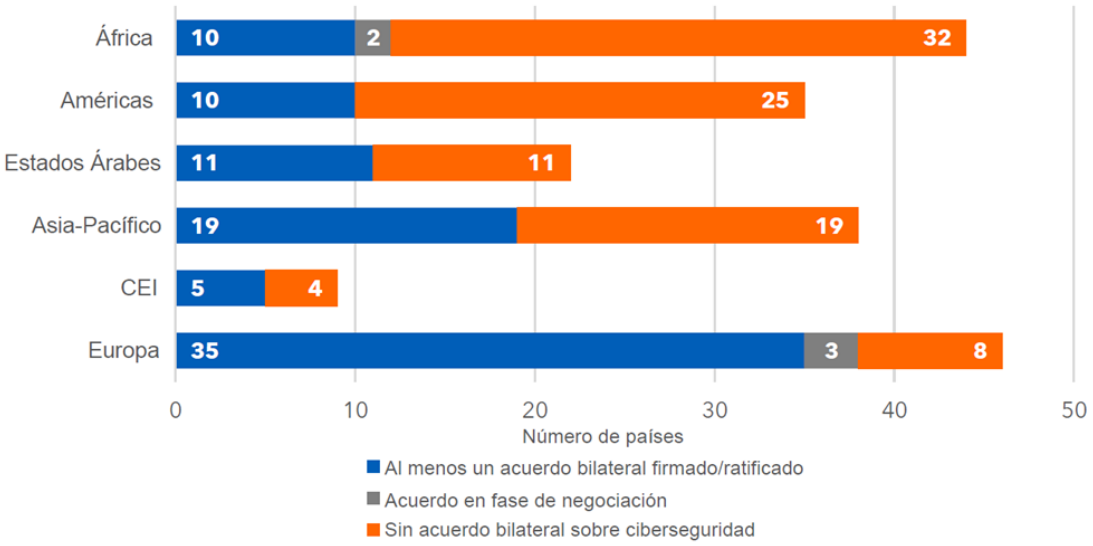
2.5 Medidas de cooperación: acción colectiva en materia de ciberseguridad

Los riesgos de ciberseguridad son cada vez más transfronterizos[24], por lo que la colaboración sigue siendo una herramienta esencial para afrontar los retos de la ciberseguridad. La creciente interconexión y correlación de las infraestructuras hacen que la ciberseguridad siga siendo una cuestión transnacional. La seguridad del ecosistema cibernético mundial no puede garantizarse ni gestionarse unilateralmente, por cuanto se requiere cooperar en los planos nacional, regional e internacional para ampliar su alcance e incidencia. En este pilar relativo a la cooperación, el cuestionario recoge los países que cuentan con un acuerdo bilateral y multilateral, y los que participan en asociaciones interinstitucionales y público-privadas. Los objetivos generales de cooperación en materia de ciberseguridad comprenden la armonización de las medidas de seguridad mínimas, el intercambio de información y buenas prácticas, y la codificación de normas de conducta.

Acuerdos bilaterales y multilaterales

Los acuerdos bilaterales y multilaterales son cruciales para codificar normas y conductas y mejorar la cooperación internacional en materia de ciberseguridad.

Figura 22: Países que participan en acuerdos bilaterales de ciberseguridad



Fuente: UIT

Los datos extraídos muestran que 90 países son parte en un acuerdo bilateral en materia de ciberseguridad. En el caso de los acuerdos que recoge el ICG, algunos países están concertando acuerdos de ciberseguridad en el ámbito de la capacitación. En algunos casos, el acuerdo consiste únicamente en el intercambio de información y la ciberseguridad no siempre es el aspecto fundamental del acuerdo, sino que forma parte de otros temas. Son 37 los países que en sus acuerdos bilaterales incluyen tanto medidas de intercambio de información como de capacitación, pero no contemplan la asistencia jurídica recíproca.

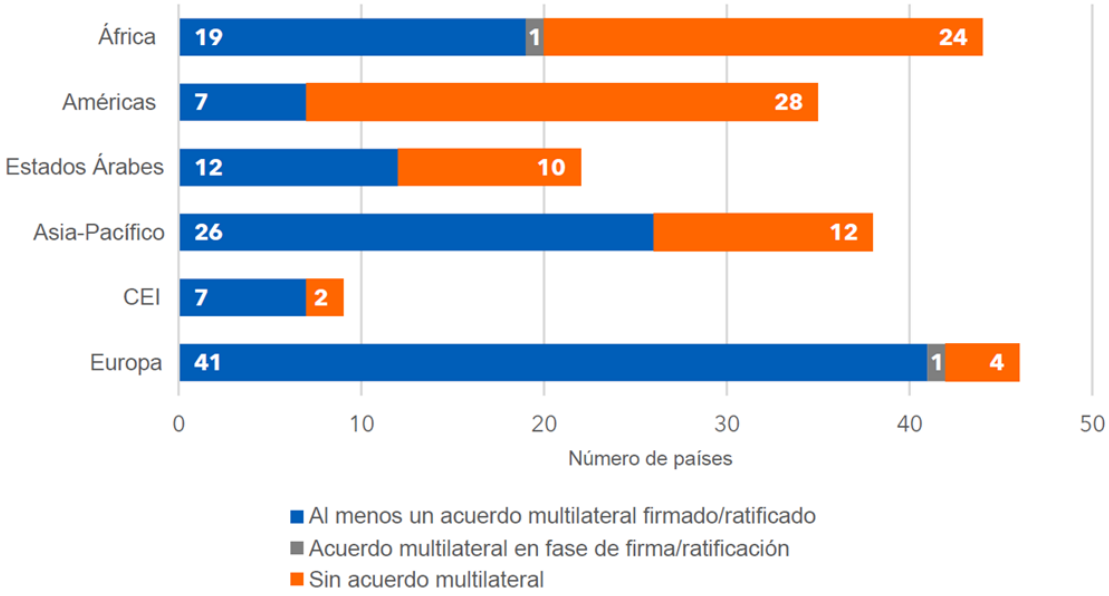
[24] https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019.

Figura 23: Países parte en un acuerdo bilateral de ciberseguridad (por temas tratados)

Fuente: UIT

Dado el problema de la acción colectiva de la ciberseguridad, algunos países procuran firmar no sólo de acuerdos bilaterales, sino también acuerdos multilaterales. En esta edición del Índice de Ciberseguridad Global se consideran acuerdos multilaterales aquellos firmados entre tres o más partes, incluidos gobiernos y organizaciones regionales, pero excluyendo los convenios internacionales, como el Convenio de Budapest sobre Ciberdelincuencia.

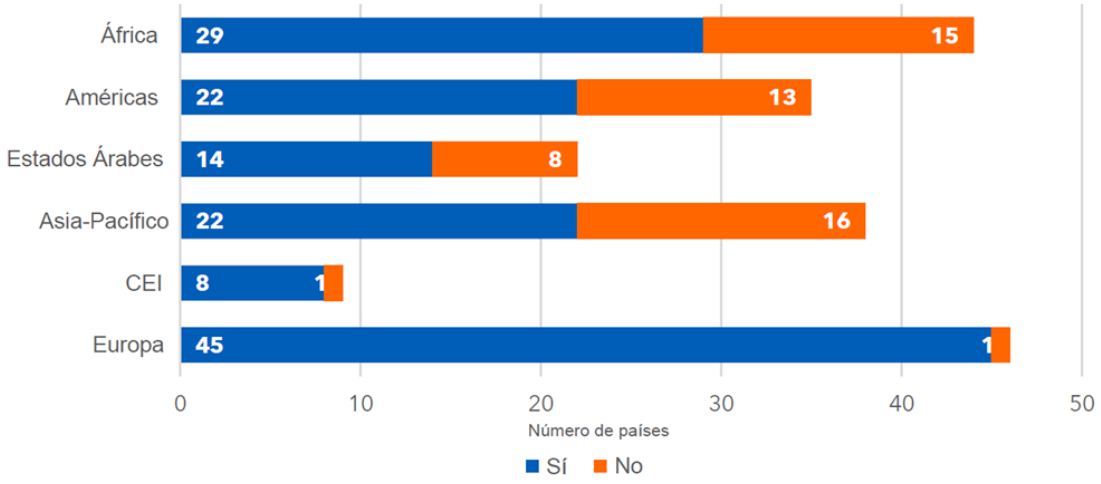
Figura 24: Número de países que son parte en acuerdos multilaterales de ciberseguridad (firmados y ratificados)



Fuente: UIT

La probabilidad de ser parte en un acuerdo multilateral es mayor que la de haber firmado un acuerdo bilateral, dado que casi el 57% de los países tienen firmado un acuerdo multilateral, mientras que el 46% han firmado un acuerdo bilateral. Asimismo, muchos países (99) han firmado o ratificado un acuerdo multilateral sobre intercambio de información y capacitación.

Figura 25: Participación en actividades internacionales



Fuente: UIT

Más allá de la cooperación oficial entre dos o más países, la participación en actividades internacionales ofrece a los países la oportunidad de comprender las buenas prácticas y los métodos para hacer frente a las amenazas a la ciberseguridad. En los dos últimos años, 140 países han participado en actividades internacionales en el ámbito de la ciberseguridad, como conferencias, talleres, alianzas y convenios con otros países.

Asociaciones público-privadas

Además de colaborar entre sí, los países colaboran también con actores del sector privado. Las asociaciones público-privadas (APP) son fundamentales para las actividades en materia de ciberseguridad, por cuanto permiten compartir información útil, intercambiar buenas prácticas y comunicar las necesidades y prioridades de I+D. En el Cuadro 2 se presenta el número de países que participan en APP internacionales y/o nacionales.

Cuadro 2: Países que participan en una APP nacional y/o internacional

	APP internacional	APP internacional en curso	Sin APP internacional
APP nacional	62	0	14
APP nacional en curso	1	0	0
Sin APP nacional	12	1	104

Fuente: UIT

A fin de implicarse en el ecosistema de ciberseguridad en general, algunos países organizan conferencias y talleres, mientras que otros contratan a empresas del sector privado para que impartan formación al sector público. Son cada vez más los países que crean parques científicos y tecnológicos para reforzar sus ecosistemas de ciberseguridad. Estas plataformas pueden servir de lugar de encuentro entre los sectores público y privado, para impartir formación, celebrar talleres, ayudar a empresas incipientes y organizar concursos. Este tipo de iniciativa intersectorial tiene por objeto desarrollar un ecosistema de ciberseguridad, compartiendo los conocimientos y competencias de las distintas partes interesadas, a saber, investigadores,

estudiantes, expertos en ciberseguridad, empresas incipientes, instituciones gubernamentales y empresas extranjeras. Según los datos recabados y recopilados, casi la mitad de los países cuentan al menos con algún tipo de asociación, siendo 86 el número de países que son o pronto serán parte en una APP internacional o nacional, de los cuales 60 participan tanto en asociaciones nacionales como en internacionales.

2.6 Protección de la infancia en línea

Figura 26: Informes de la UIT de la serie de protección de la infancia en línea

Fuente: UIT

Como se señala en las directrices de la UIT sobre la protección de la infancia en línea, proteger a los niños en línea es un reto mundial que requiere una colaboración también mundial.[25] Las directrices se publican en un momento en el que, a raíz de la enseñanza a distancia, los niños permanecen en línea más que nunca y, además, están más expuestos a los riesgos durante la pandemia de COVID-19. A diferencia de las generaciones anteriores, para las que la enseñanza a distancia debido a las pandemias tenía lugar por la radio[26], las tecnologías digitales permiten experiencias educativas interactivas y bidireccionales que, además de darles acceso a los materiales didácticos, permite a los estudiantes comunicarse entre sí.

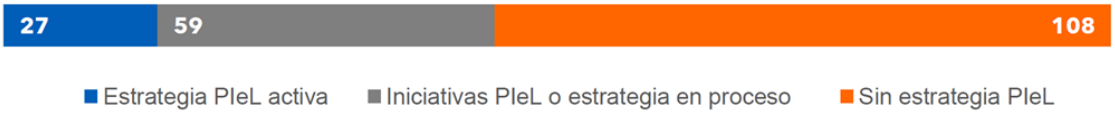
Las directrices de la UIT sobre la protección de la infancia en línea fueron concebidas para ayudar a los niños, los padres y los profesores a gestionar los riesgos en línea y, a su vez, a beneficiarse de las posibilidades que ofrece la tecnología digital y a reforzar sus aptitudes digitales. Asimismo, las directrices contienen recomendaciones dirigidas a los responsables políticos para acelerar el desarrollo y la adopción de una estrategia nacional de protección de la infancia en línea y de planes de acción eficaces, así como para promover la participación del sector privado en la elaboración de dichas políticas.

En este sentido, las preguntas relacionadas con la protección de la infancia en línea tienen por objeto medir el grado de preparación de los países para la generación digital a través de varios aspectos, como la existencia de legislación para proteger a los niños en línea, mecanismos para

25 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx.
26 https://www.washingtonpost.com/education/2020/04/03/chicago-schools-closed-during-1937-polio-epidemic-kids-learned-home-over-radio/.

notificar peligros en línea, campañas de sensibilización y planes de estudio para las escuelas, así como los países que han elaborado y aplican una estrategia para proteger a los niños en línea.

Figura 27: Países que han adoptado una estrategia de protección de la infancia en línea



Fuente: UIT

Del cuestionario se desprende que 86 de los 194 países declaran haber tomado medidas para proteger a los niños en línea. Sin embargo, los datos recogidos muestran que sólo el 13% de los 194 países aplican una estrategia independiente dedicada a la protección de la infancia en línea. Por otra parte, el 30% tiene integradas las iniciativas para proteger a la infancia en línea en estrategias, en la legislación o en iniciativas más generales sobre ciberdelincuencia.

Los resultados muestran que, concretamente, la región de Europa obtiene buenos resultados en cuestiones relacionadas con la protección de la infancia en línea, en la que el 89% de los países aplican plenamente leyes relacionadas con la protección de la infancia en línea. Por añadidura, se han registrado 101 mecanismos de notificación en todo el mundo, a través de servicios de atención telefónica, sitios web, direcciones de correo electrónico y redes sociales, y 81 países fueron más allá e informaron acerca de sus estrategias de protección de la infancia en línea e iniciativas más generales.

2.7 Conclusión

La ciberseguridad evoluciona sin cesar, tanto en lo que respecta a las conductas como a las prácticas. Ya se trate de una emergencia sanitaria mundial, del cambio climático, del envejecimiento de la población o de cualquier otro reto que nos depare el futuro, las tecnologías digitales constituyen una herramienta eficaz que contribuye al progreso del mundo. Cuando los Objetivos de Desarrollo Sostenible (ODS) lleguen a su vencimiento en 2030, se prevé que el 90% de la población mundial prevista, es decir, 7 500 millones de personas, estará en línea[27], con una cantidad estimada de entre 24 100[28] y 125 000[29] millones de dispositivos IoT (Internet de las cosas) conectados. Para que no decaigan los esfuerzos dedicados a los ODS, la ciberseguridad será imprescindible, por cuanto permitirá garantizar que las soluciones digitales sean seguras, fiables y dignas de confianza.

Una de las cosas que hemos aprendido de la COVID-19 es que los problemas de acción colectiva, ya sean de salud o de ciberseguridad, deben abordarse de manera interdisciplinaria y global. Para acometer todos los pilares del ICG – medidas legales, técnicas, institucionales, capacitación y cooperación – será indispensable conectar a las personas entre sí y generar confianza. Más allá de la colaboración interna en cada país, será preciso que los países ayuden a otros Estados menos capacitados para afrontar los retos de la ciberseguridad, como los países menos adelantados, los pequeños Estados insulares en desarrollo y los países en desarrollo sin litoral.

---

27 https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/.
28 https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030--generating-1-5-trillion-annual-revenue-301061873.html.
29 https://cdn.ihs.com/www/pdf/IoT_ebook.pdf.

Para avanzar, los países deben determinar sus puntos fuertes y débiles en materia de ciberseguridad y aprovechar sus ventajas competitivas para promover la cibercapacidad y la salud general. El Índice de Ciberseguridad Global puede ayudar a los países a iniciar este proceso. A tal efecto, los podrán considerar lo siguiente:

- evaluar periódicamente su grado de compromiso en materia de ciberseguridad, incluidas las métricas significativas;
- continuar la creación de EIII nacionales y de EIII sectoriales;
- supervisar y actualizar las estrategias nacionales de ciberseguridad con planes de implementación claros;
- velar por la inclusión y la diversidad, especialmente de los grupos subrepresentados, como las mujeres y los jóvenes, en lo que respecta al empleo en el sector de la ciberseguridad;
- participar periódicamente en actividades internacionales para compartir buenas prácticas y estudios de casos, y mejorar la preparación y la capacidad de respuesta;
- mejorar la capacidad de ciberseguridad de las microempresas y las pequeñas y medianas empresas (MIPYME);
- lograr la implicación periódica de todas las partes interesadas en la ciberseguridad, incluidos el sector privado, el mundo académico y la sociedad civil.

3 Resultados del ICG: Puntuación y clasificación

3.1 Puntuaciones globales y clasificación de los países

En el cuadro siguiente se indica la puntuación y la clasificación de cada país que ha participado en el cuestionario.

Cuadro 3: Resultados del ICG: Puntuación global y clasificación

Nombre del país	Puntuación	Clasificación
Estados Unidos de América**	100	1
Reino Unido	99,54	2
Arabia Saudí	99,54	2
Estonia	99,48	3
Corea (Rep. de)	98,52	4
Singapur	98,52	4
España	98,52	4
Federación de Rusia	98,06	5
Emiratos Árabes Unidos	98,06	5
Malasia	98,06	5
Lituania	97,93	6
Japón	97,82	7
Canadá**	97,67	8
Francia	97,6	9
India	97,5	10
Turquía	97,49	11
Australia	97,47	12
Luxemburgo	97,41	13
Alemania	97,41	13
Portugal	97,32	14
Letonia	97,28	15
Países Bajos**	97,05	16
Noruega**	96,89	17
Mauricio	96,89	17
Brasil	96,6	18
Bélgica	96,25	19

Nombre del país	Puntuación	Clasificación
Italia	96,13	20
Omán	96,04	21
Finlandia	95,78	22
Egipto	95,48	23
Indonesia	94,88	24
Viet Nam	94,59	25
Suecia	94,55	26
Qatar	94,5	27
Grecia	93,98	28
Austria	93,89	29
Polonia	93,86	30
Kazajstán	93,15	31
Dinamarca	92,6	32
China	92,53	33
Croacia	92,53	33
Eslovaquia	92,36	34
Hungría	91,28	35
Israel**	90,93	36
Tanzanía	90,58	37
Macedonia del Norte	89,92	38
Serbia	89,8	39
Azerbaiyán	89,31	40
Chipre	88,82	41
Suiza**	86,97	42
Ghana	86,69	43
Tailandia	86,5	44
Túnez	86,23	45

(continuación)

Nombre del país	Puntuación	Clasificación
Irlanda	85,86	46
Nigeria	84,76	47
Nueva Zelandia**	84,04	48
Malta	83,65	49
Marruecos	82,41	50
Kenya	81,7	51
México	81,68	52
Bangladesh	81,27	53
Irán (República Islámica de)	81,07	54
Georgia	81,06	55
Benin	80,06	56
Rwanda	79,95	57
Islandia	79,81	58
Sudáfrica**	78,46	59
Bahrein	77,86	60
Filipinas	77	61
Rumania	76,29	62
Moldova	75,78	63
Uruguay	75,15	64
Kuwait	75,07	65
República Dominicana	75,05	66
Eslovenia	74,93	67
República Checa	74,37	68
Mónaco	72,57	69
Uzbekistán	71,11	70
Jordania	70,96	71
Uganda	69,98	72
Zambia	68,88	73
Chile	68,83	74
Côte d'Ivoire	67,82	75
Costa Rica	67,45	76
Bulgaria	67,38	77
Ucrania	65,93	78
Pakistán	64,88	79
Albania	64,32	80
Colombia	63,72	81
Cuba	58,76	82
Sri Lanka	58,65	83
Paraguay	57,09	84
Brunei Darussalam	56,07	85
Perú	55,67	86
Montenegro	53,23	87
Botswana	53,06	88
Bielorrusia	50,57	89
Armenia**	50,47	90
Argentina	50,12	91
Kirguistán	49,64	92
Camerún	45,63	93
Nepal (República de)	44,99	94
Chad	40,44	95
Burkina Faso**	39,98	96
Malawi	36,83	97
Zimbabwe	36,49	98
Myanmar	36,41	99
Senegal	35,85	100
Liechtenstein**	35,15	101
Sudán	35,03	102
Panamá	34,11	103
Argelia	33,95	104
Togo	33,19	105
Jamaica**	32,53	106
Gambia	32,12	107
Suriname	31,2	108
Líbano**	30,44	109
Bosnia y Herzegovina	29,44	110
Samoa	29,33	111
Fiji	29,08	112
Libia	28,78	113
Guyana	28,11	114
Etiopía	27,74	115
Venezuela	27,06	116
Andorra**	26,38	117
Papúa Nueva Guinea**	26,33	118
Ecuador	26,3	119

(continuación)

Nombre del país	Puntuación	Clasificación
Mongolia	26,2	120
Sierra Leona	25,31	121
Estado de Palestina	25,18	122
Mozambique	24,18	123
Madagascar**	23,33	124
Trinidad y Tabago	22,18	125
República Árabe Siria**	22,14	126
Nauru**	21,42	127
Tonga**	20,95	128
Iraq**	20,71	129
Guinea**	20,53	130
Lao P.D.R.	20,34	131
Camboya**	19,12	132
Mauritania	18,94	133
Bután	18,34	134
Eswatini	18,23	135
Cabo Verde	17,74	136
Somalia	17,25	137
Tayikistán**	17,1	138
Barbados	16,89	139
Bolivia (Estado Plurinacional de)	16,14	140
Santo Tomé y Príncipe	15,64	141
Antigua y Barbuda	15,62	142
Congo (Rep. del)**	14,72	143
Turkmenistán**	14,48	144
Kiribati	13,84	145
San Marino	13,83	146
Bahamas	13,37	147
El Salvador**	13,3	148
Seychelles**	13,23	149
Guatemala	13,13	150
Angola	12,99	151
Vanuatu	12,88	152
Saint Kitts y Nevis**	12,44	153
San Vicente y las Granadinas**	12,18	154
Namibia	11,47	155
Níger	11,38	156
Gabón	11,36	157
Santa Lucía**	10,96	158
Belice	10,29	159
Malí**	10,14	160
Guinea-Bissau	9,85	161
Liberia	9,72	162
Granada	9,41	163
Lesotho	9,08	164
Nicaragua**	9	165
Islas Salomón	7,08	166
Haití	6,4	167
Tuvalu**	5,78	168
Sudán del Sur**	5,75	169
Rep. Dem. del Congo	5,3	170
Afganistán	5,2	171
Islas Marshall**	4,9	172
Timor-Leste**	4,26	173
Dominica	4,2	174
Comoras**	3,72	175
República Centroafricana **	3,24	176
Maldivas**	2,95	177
Honduras**	2,2	178
Djibouti	1,73	179
Burundi	1,73	179
Eritrea**	1,73	179
Guinea Ecuatorial**	1,46	180
Rep. Pop. Dem. de Corea**	1,35	181
Micronesia*	0	182
Vaticano*	0	182
Yemen*	0	182

* No se han recopilado datos
** No ha respondido al cuestionario

3.2 Puntuaciones regionales y clasificación de los países

Cuadro 4: Resultados del ICG: Región de África

Nombre del país	Puntuación global	Clasificación regional
Mauricio	96,89	1
Tanzanía	90,58	2
Ghana	86,69	3
Nigeria	84,76	4
Kenya	81,7	5
Benin	80,06	6
Rwanda	79,95	7
Sudáfrica**	78,46	8
Uganda	69,98	9
Zambia	68,88	10
Côte d'Ivoire	67,82	11
Botswana	53,06	12
Camerún	45,63	13
Chad	40,44	14
Burkina Faso**	39,98	15
Malawi	36,83	16
Zimbabwe	36,49	17
Senegal	35,85	18
Togo	33,19	19
Gambia	32,12	20
Etiopía	27,74	21
Sierra Leona	25,31	22
Mozambique	24,18	23
Madagascar	23,33	24
Guinea**	20,53	25
Eswatini	18,23	26
Cabo Verde	17,74	27
Santo Tomé y Príncipe	15,64	28
Congo (Rep. del)**	14,72	29
Seychelles**	13,23	30
Angola	12,99	31
Namibia	11,47	32
Níger	11,36	33
Gabón	11,38	34
Malí**	10,14	35
Guinea-Bissau	9,85	36
Liberia	9,72	37
Lesotho	9,08	38
Sudán del Sur**	5,75	39
Rep. Dem. del Congo	5,3	40
República Centroafricana**	3,24	41
Burundi	1,73	42
Eritrea**	1,73	42
Guinea Ecuatorial**	1,46	43

* Sin datos
** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

Cuadro 5: Resultados del ICG: Región de las Américas

Nombre del país	Puntuación global	Clasificación regional
Estados Unidos de América**	100	1
Canadá**	97,67	2
Brasil	96,6	3
México	81,68	4
Uruguay	75,15	5
República Dominicana	75,07	6
Chile	68,83	7
Costa Rica	67,45	8
Colombia	63,72	9
Cuba	58,76	10
Paraguay	57,09	11
Perú	55,67	12
Argentina	50,12	13
Panamá	34,11	14
Jamaica**	32,53	15
Suriname	31,2	16
Guyana	28,11	17

Cuadro 5: Resultados del ICG: Región de las Américas (continuación)

Nombre del país	Puntuación global	Clasificación regional
Venezuela	27,06	18
Ecuador	26,3	19
Trinidad y Tabago	22,18	20
Barbados	16,89	21
Bolivia (Estado Plurinacional de)	16,14	22
Antigua y Barbuda	15,62	23
Bahamas	13,37	24
El Salvador**	13,3	25
Guatemala	13,13	26
Saint Kitts y Nevis	12,44	27
San Vicente y las Granadinas**	12,18	28
Santa Lucía**	10,96	29
Belice	10,29	30
Granada	9,41	31
Nicaragua	9	32
Haití	6,4	33
Dominica	4,2	34
Honduras**	2,2	35

* Sin datos
** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

Cuadro 6: Resultados del ICG: Región de los Estados Árabes

Nombre del país	Puntuación global	Clasificación regional
Arabia Saudita	99,54	1
Emiratos Árabes Unidos	98,06	2
Omán	96,04	3
Egipto	95,48	4
Qatar	94,5	5
Túnez	86,23	6
Marruecos	82,41	7
Bahrein	77,86	8
Kuwait	75,05	9
Jordania	70,96	10
Sudán	35,03	11
Argelia	33,95	12
Líbano**	30,44	13
Libia	28,78	14
Estado de Palestina	25,18	15
República Árabe Siria**	22,14	16
Iraq**	20,71	17
Mauritania	18,94	18
Somalia	17,25	19
Comoras**	3,72	20
Djibouti	1,73	21
Yemen*	0	22

* Sin datos
** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

Cuadro 7: Resultados del ICG: Región de Asia-Pacífico

Nombre del país	Puntuación global	Clasificación regional
Corea (Rep. de)	98,52	1
Singapur	98,52	1
Malasia	98,06	2
Japón	97,82	3
India	97,49	4
Australia	97,47	5
Indonesia	94,88	6
Viet Nam	94,55	7
China	92,53	8
Tailandia	86,5	9
Nueva Zelandia**	84,04	10
Bangladesh	81,27	11
Irán (República Islámica de)	81,06	12
Filipinas	77	13
Pakistán	64,88	14
Sri Lanka	58,65	15
Brunei Darussalam	56,07	16

Cuadro 7: Resultados del ICG: Región de Asia-Pacífico (continuación)

Nombre del país	Puntuación global	Clasificación regional
Nepal (República de)	44,99	17
Myanmar	36,41	18
Samoa	29,33	19
Fiji	29,08	20
Papúa Nueva Guinea**	26,33	21
Mongolia	26,2	22
Nauru**	21,42	23
Tonga**	20,95	24
Lao P.D.R.	20,34	25
Camboya**	19,12	26
Bután	18,34	27
Kiribati	13,84	28
Vanuatu	12,88	29
Islas Salomón	7,08	30
Tuvalu**	5,78	31
Afganistán	5,2	32
Islas Marshall**	4,9	33
Timor-Leste**	4,26	34
Maldivas**	2,95	35
Rep. Pop. Dem. de Corea**	1,35	36
Micronesia*	0	37

* Sin datos
** Ninguna respuesta al cuestionario/datos recogidos por el Equipo ICG

Cuadro 8: Resultados del ICG: Región de la CEI

Nombre del país	Puntuación global	Clasificación regional
Federación de Rusia	98,06	1
Kazajstán	93,15	2
Azerbaiyán	89,31	3
Uzbekistán	71,11	4
Bielorrusia	50,57	5
Armenia**	50,47	6
Kirguistán	49,64	7
Tayikistán**	17,1	8
Turkmenistán**	14,48	9

* Sin datos
** Ninguna respuesta al cuestionario/datos recogidos por el Equipo ICG

Cuadro 9: Resultados del ICG: Región de Europa

Nombre del país	Puntuación global	Clasificación regional
Reino Unido	99,54	1
Estonia	99,48	2
España	98,52	3
Lituania	97,93	4
Francia	97,6	5
Turquía	97,5	6
Luxemburgo	97,41	7
Alemania	97,41	7
Portugal	97,32	8
Letonia	97,28	9
Países Bajos**	97,05	10
Noruega**	96,89	11
Bélgica	96,25	12
Italia	96,13	13
Finlandia	95,78	14
Suecia	94,59	15
Grecia	93,98	16
Austria	93,89	17
Polonia	93,86	18
Dinamarca	92,6	19
Croacia	92,53	20
Eslovaquia	92,36	21
Hungría	91,28	22
Israel**	90,93	23
La República de Macedonia del Norte	89,92	24
Serbia	89,8	25
Chipre	88,82	26

Cuadro 9: Resultados del ICG: Región de Europa (continuación)

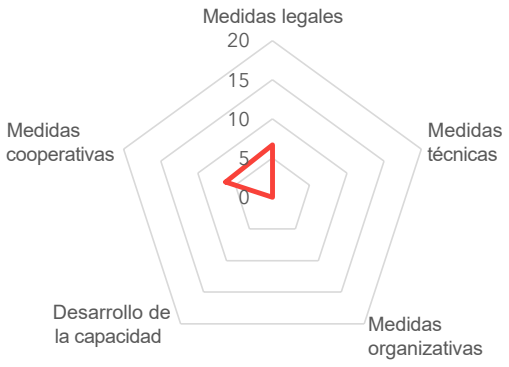
Nombre del país	Puntuación global	Clasificación regional
Suiza**	86,97	27
Irlanda	85,86	28
Malta	83,65	29
Georgia	81,07	30
Islandia	79,81	31
Rumania	76,29	32
Moldavia	75,78	33
Eslovenia	74,93	34
República Checa	74,37	35
Mónaco	72,57	36
Bulgaria	67,38	37
Ucrania	65,93	39
Albania	64,32	40
Montenegro	53,23	41
Liechtenstein**	35,15	42
Bosnia y Herzegovina	29,44	43
Andorra**	26,38	44
San Marino	13,83	45
Vaticano*	0	46

* Sin datos
** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

4 Índice de Ciberseguridad Global 2020: Perfiles de los países

Región de África

Angola (República de)



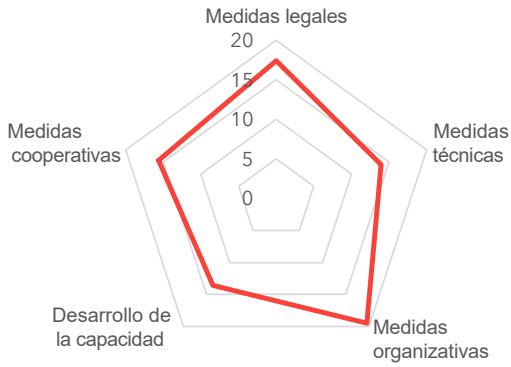
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, de desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
12,99	6,70	0,00	0,00	0,00	6,30

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Benin (República de)



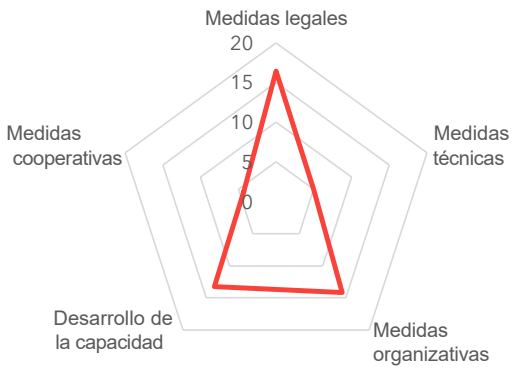
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
80,06	17,42	13,94	19,48	13,60	15,63

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Botswana (República de)



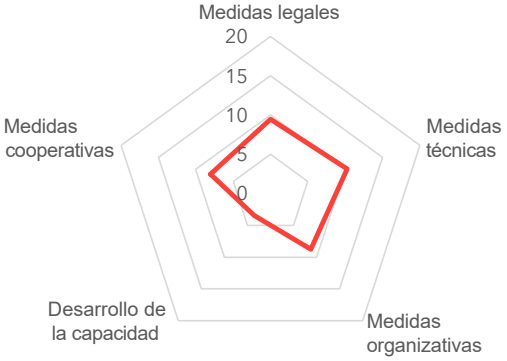
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas,
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
53,06	16,44	4,95	14,16	13,23	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Burkina Faso***



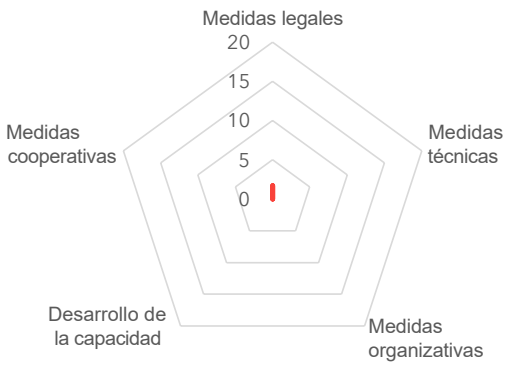
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
39,98	9,47	10,25	8,75	3,47	8,04

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Burundi (República de)



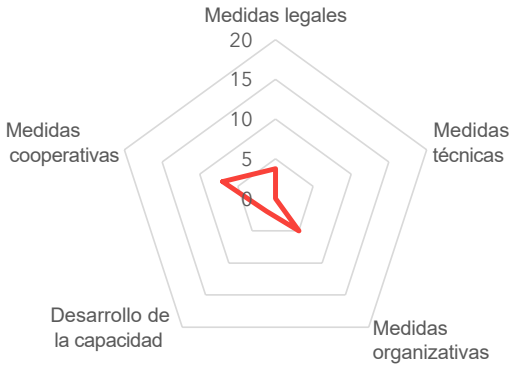
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
1,73	1,73	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Cabo Verde (República de)



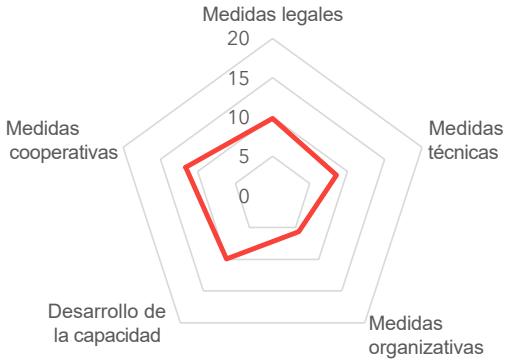
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
17,74	3,77	0,00	5,00	1,96	7,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Camerún (República de)



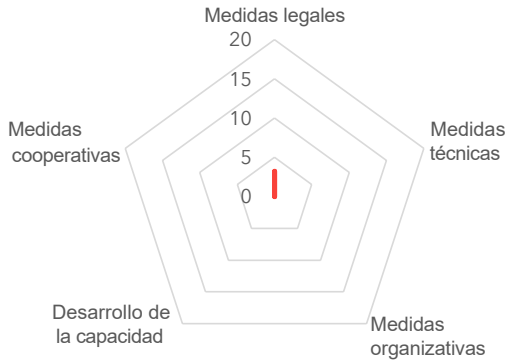
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
45,63	9,84	8,54	5,67	9,95	11,63

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*República Centroafricana***



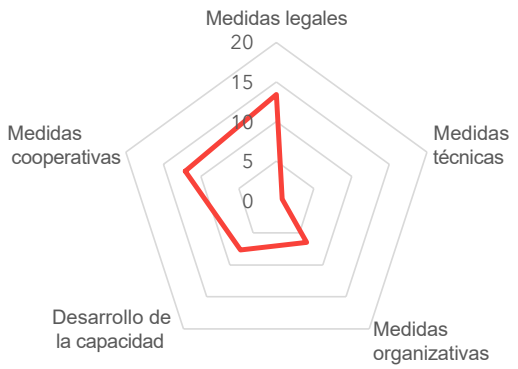
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Técnica, Organizativa, Desarrollo de la capacidad, Cooperativa

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
3,24	3,24	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Chad (República de)



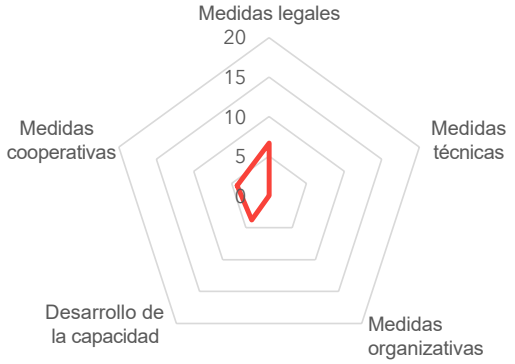
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
40,44	13,43	0,73	6,50	7,67	12,11

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Congo (República del)***



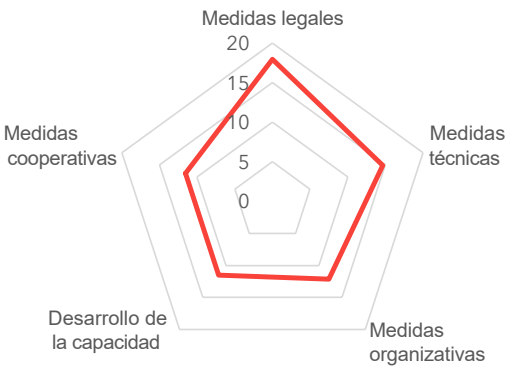
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
14,72	6,66	0,00	0,00	3,80	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Côte d'Ivoire (República de)



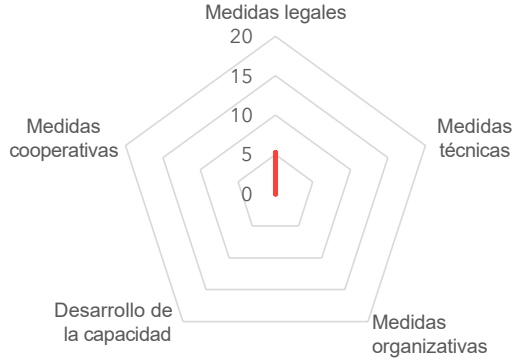
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad, Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
67,82	17,95	14,65	12,14	11,53	11,55

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Democrática del Congo



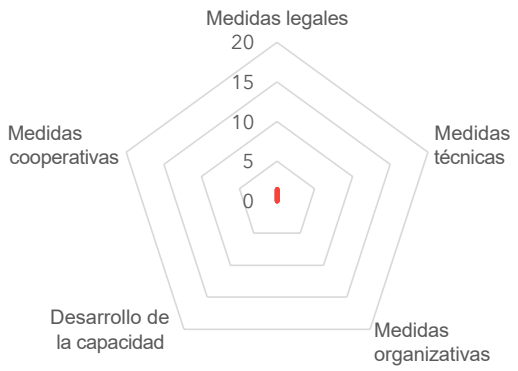
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativa, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
5,30	5,30	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Guinea Ecuatorial (República de)***



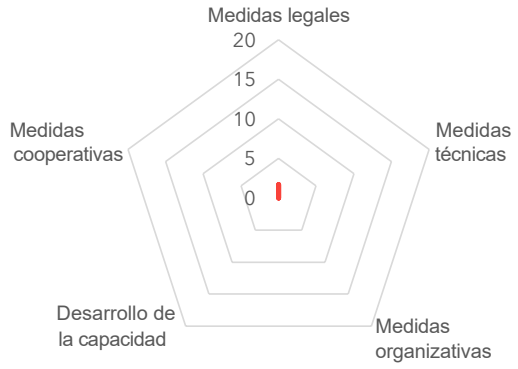
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
1,46	1,46	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Eritrea***



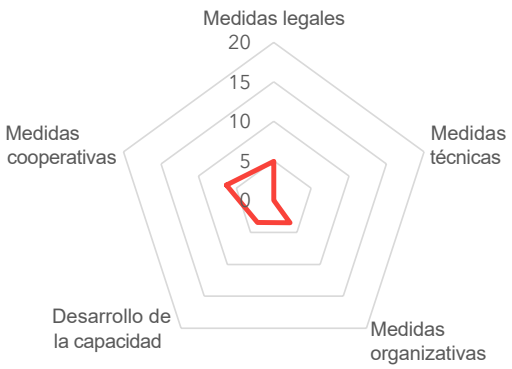
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
1,73	1,73	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Eswatini (Reino de)



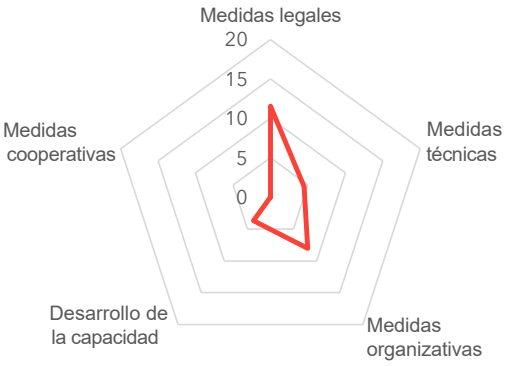
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
18,23	4,96	0,00	3,49	3,47	6,31

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Etiopía (República Democrática Federal de)



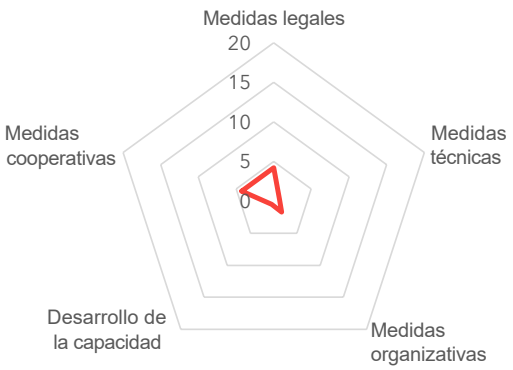
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
27,74	11,56	4,46	8,03	3,69	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Gabonesa



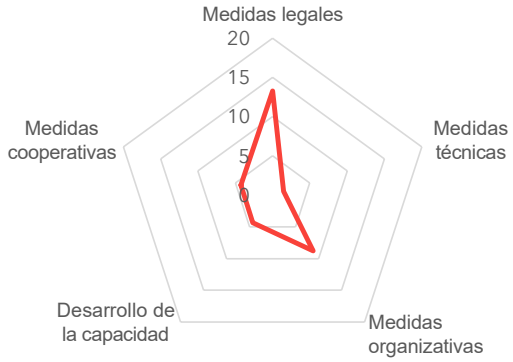
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
11,38	4,24	0,73	1,69	0,46	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Gambia (República de)



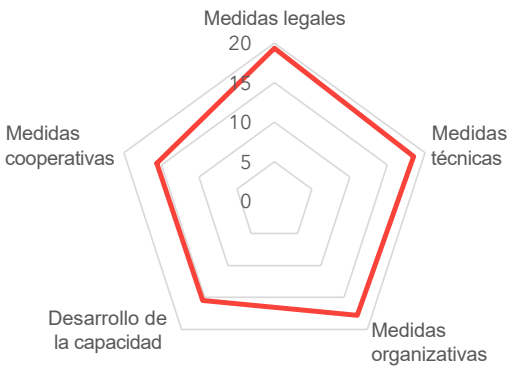
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
32,12	13,28	1,46	8,78	4,34	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Ghana



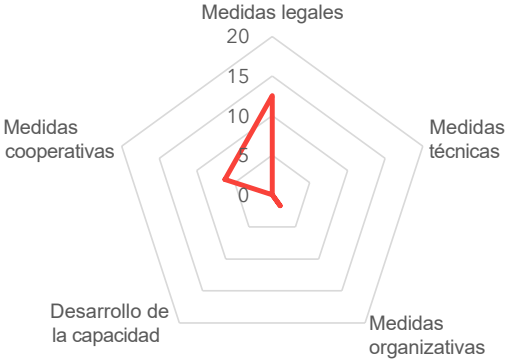
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, técnicas
Área(s) de posible crecimiento
Desarrollo de la capacidad, Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
86,69	19,35	18,48	17,78	15,44	15,63

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Guinea (República de)***



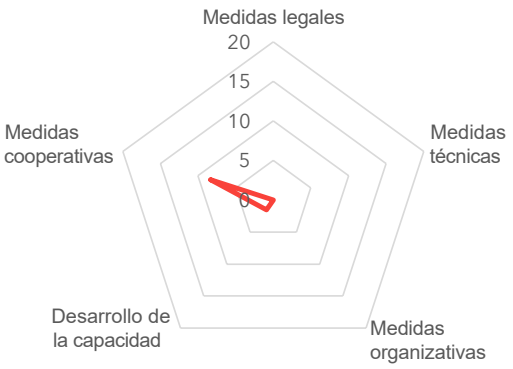
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
20,53	12,54	0,00	1,69	0,00	6,30

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Guinea-Bissau (República de)



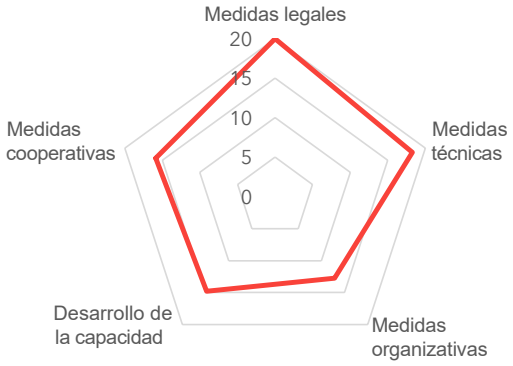
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas legales, técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
9,85	0,00	0,00	0,00	1,52	8,33

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Kenya (República de)



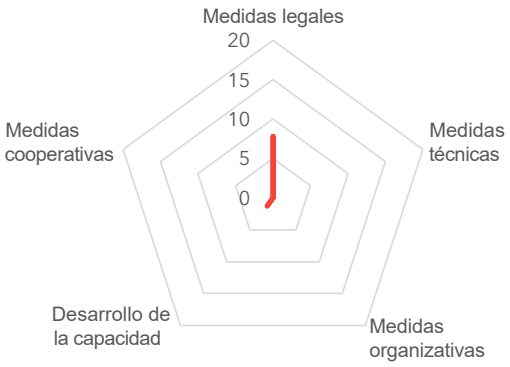
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, técnicas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
81,70	20,00	18,27	12,75	14,79	15,89

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Lesotho (Reino de)



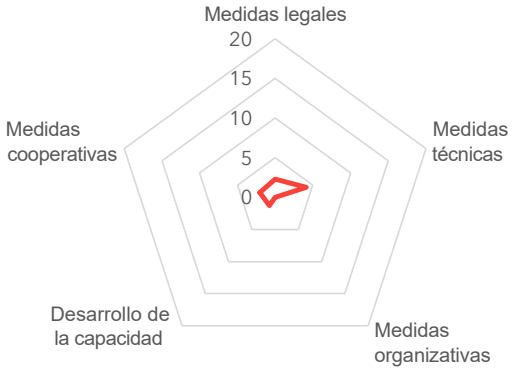
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
9,08	7,82	0,00	0,00	1,26	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Liberia (República de)



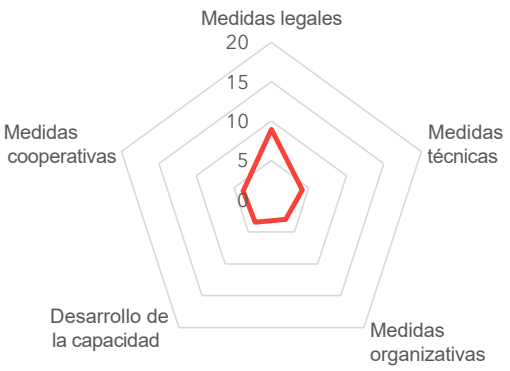
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
9,72	2,31	4,11	0,00	1,26	2,04

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Madagascar (República de)***



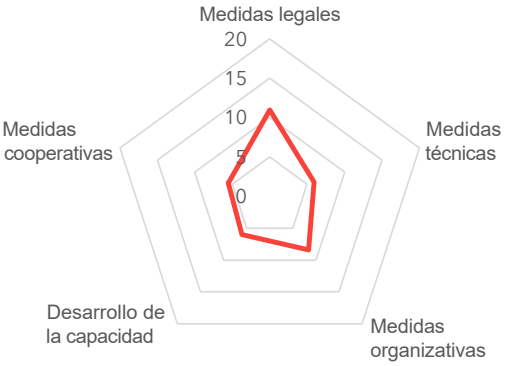
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
23,33	8,96	4,11	3,00	3,47	3,78

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Malawi



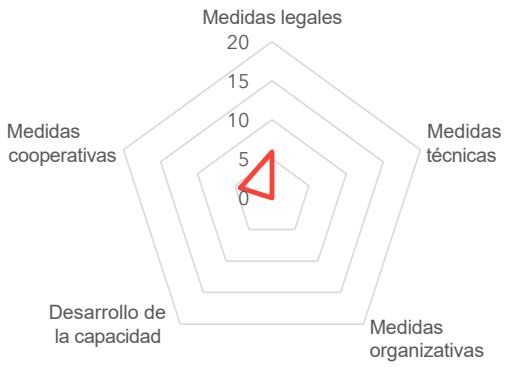
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, organizativas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
36,83	10,98	5,92	8,40	6,00	5,54

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Malí (República de)***



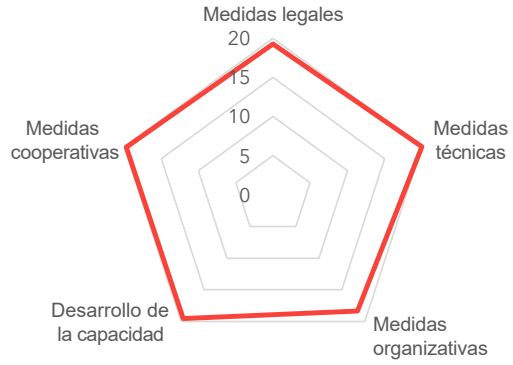
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
10,14	5,89	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Mauricio (República de)



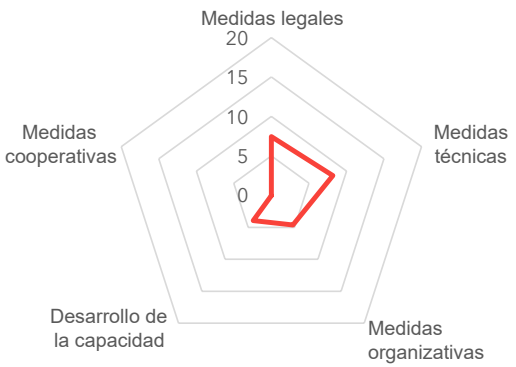
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas técnicas, Medidas cooperativas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas legales

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
96,89	19,27	20,00	18,38	19,54	19,70

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Mozambique (República de)



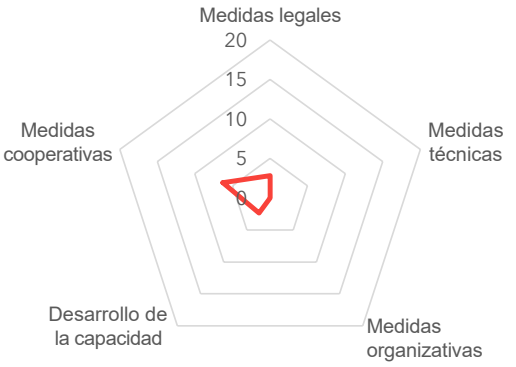
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas técnicas, legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
24,18	7,46	8,19	4,62	3,92	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Namibia (República de)



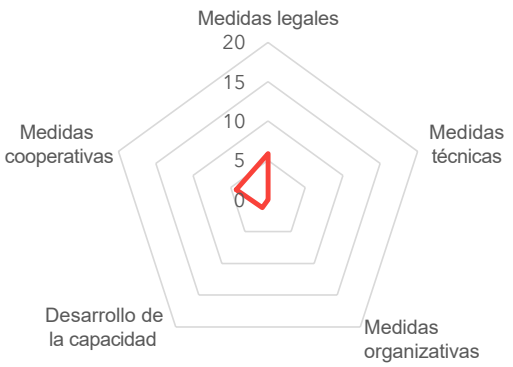
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
11,47	2,84	0,00	0,00	2,34	6,30

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Níger (República de)



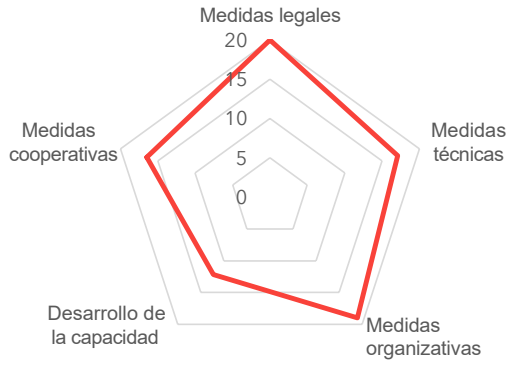
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, cooperativas
Área(s) de posible crecimiento
Medidas técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
11,36	5,87	0,00	0,00	1,23	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Nigeria (República Federal de)



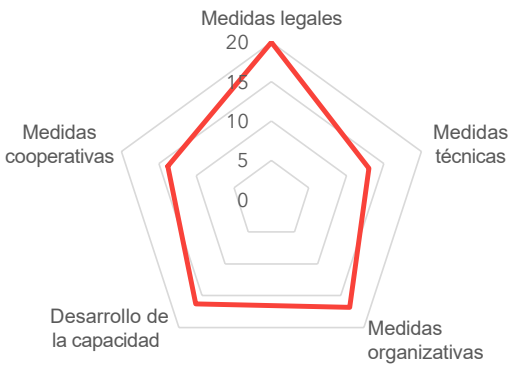
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
84,76	20,00	17,09	18,98	12,21	16,48

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Rwanda (República de)



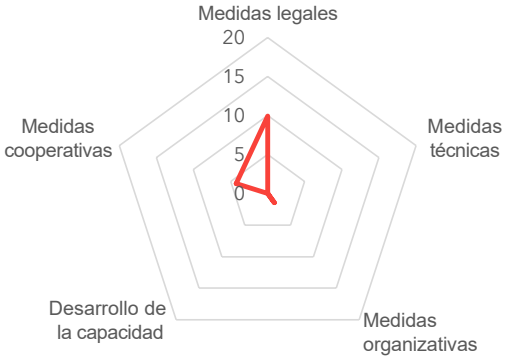
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
79,95	20,00	13,00	16,83	16,30	13,82

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Santo Tomé y Príncipe (República Democrática de)



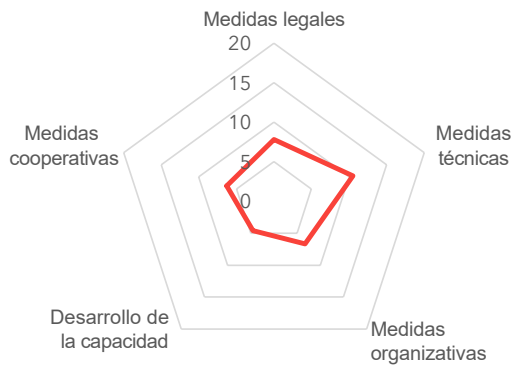
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
15,64	9,94	0,00	1,44	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Senegal (República de)



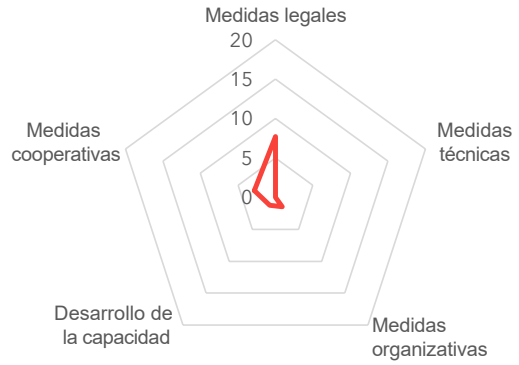
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
35,85	7,82	10,50	6,66	4,58	6,30

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Seychelles (República de)***



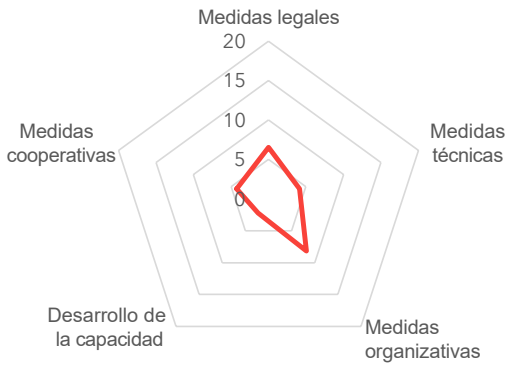
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
13,23	7,73	0,00	1,44	1,23	2,83

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Sierra Leona



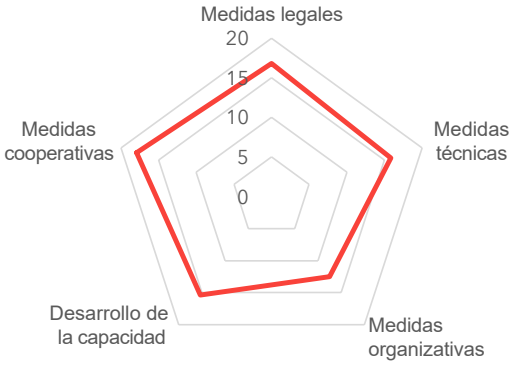
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
25,31	6,54	4,11	8,16	2,24	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Sudáfrica (República de)***



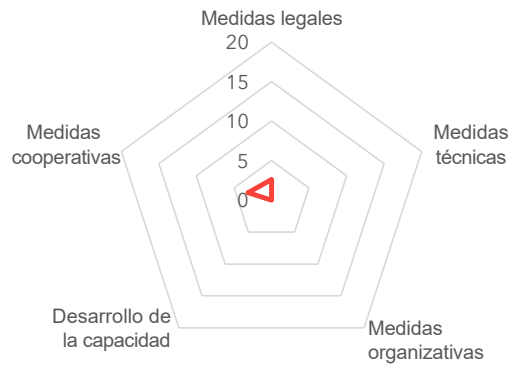
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
7,46	16,82	15,85	12,50	15,37	17,93

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Sudán del Sur (República de)***



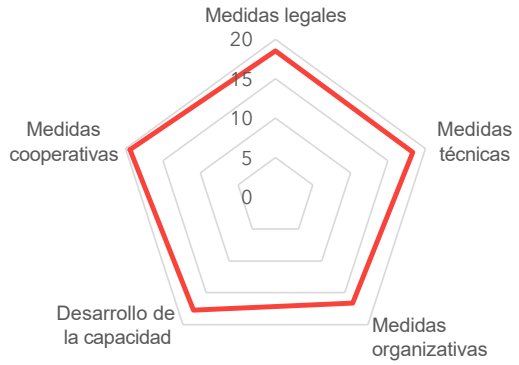
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas, organizativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
5,75	2,63	0,00	0,00	0,00	3,12

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Tanzanía (República Unida de)



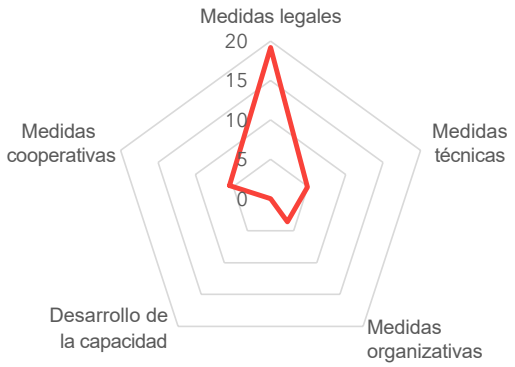
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
90,58	18,54	18,31	16,60	17,72	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Togolesa



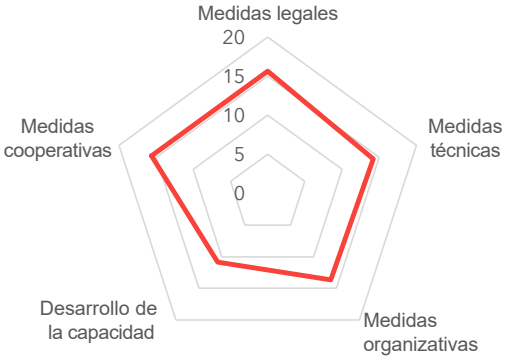
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
33,19	19,19	4,90	3,61	0,00	5,49

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Uganda (República de)



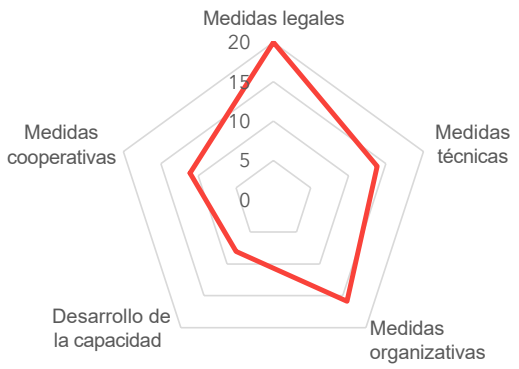
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
69,98	15,64	14,19	13,65	10,87	15,63

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Zambia (República de)



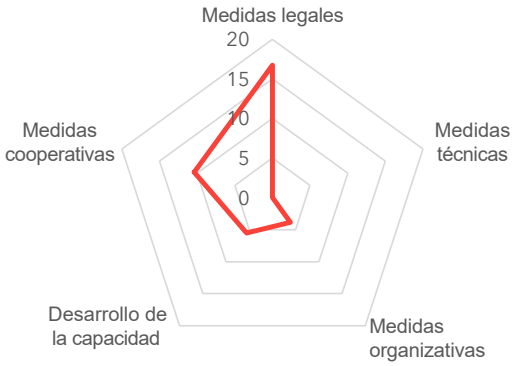
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
68,88	20,00	13,82	15,86	8,07	11,12

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Zimbabwe (República de)



Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
36,49	16,73	0,00	3,84	5,52	10,40

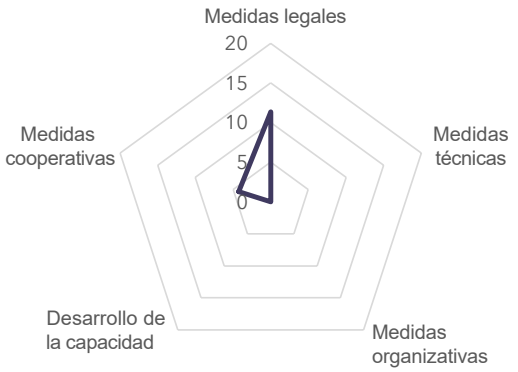
Fuente: Índice de Ciberseguridad Global v4, UIT 2020

** Sin respuesta al cuestionario/datos recogidos por el Equipo ICG

* Sin datos

Región de las Américas

Antigua y Barbuda



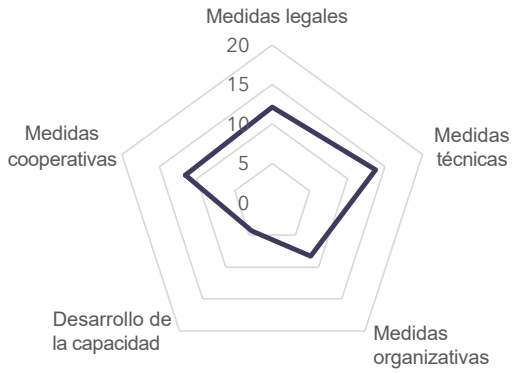
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
15,62	11,36	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Argentina



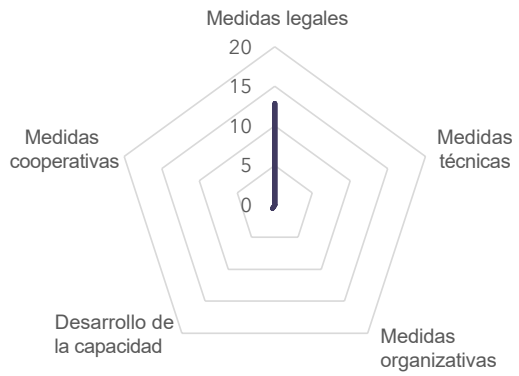
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
50,12	12,15	13,75	8,29	4,38	11,55

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bahamas (Commonwealth de las)



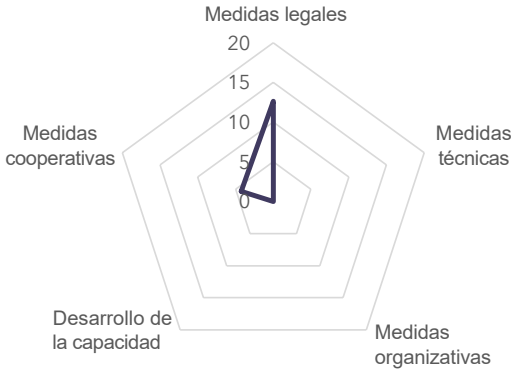
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas,
cooperativas, Desarrollo
de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
13,37	12,85	0,00	0,00	0,52	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Barbados



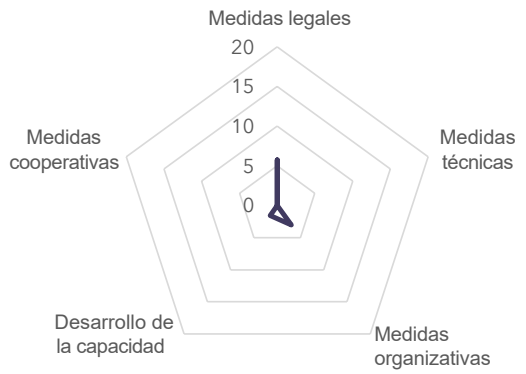
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas,
cooperativas, Desarrollo de
la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
16,89	12,63	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Belice



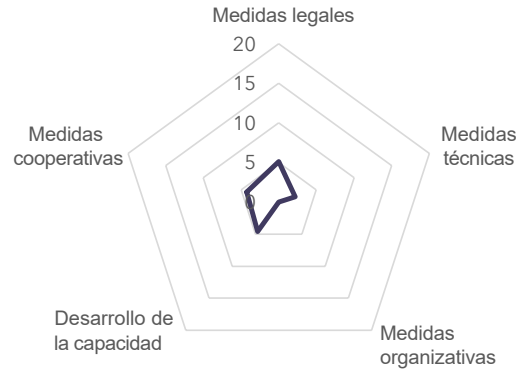
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
10,29	5,77	0,00	3,01	1,52	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bolivia (Estado Plurinacional de)



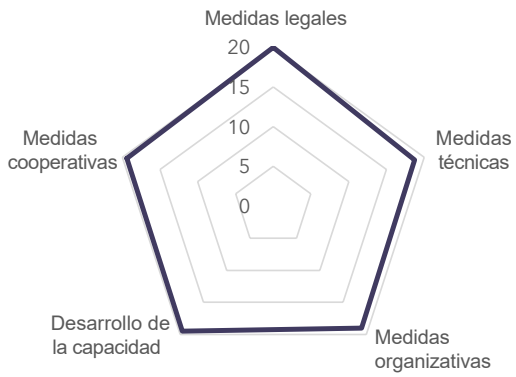
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, Medidas cooperativas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
16,14	5,13	2,18	0,00	4,58	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Brasil (República Federativa de)



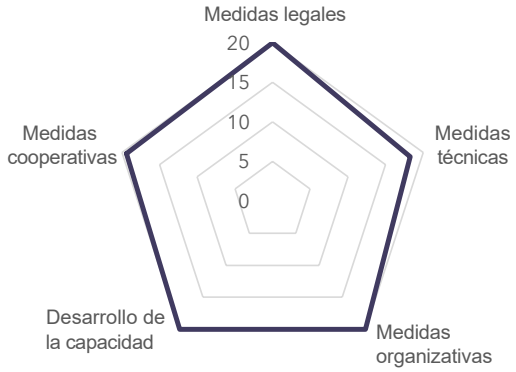
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
96,60	20,00	18,73	18,98	19,48	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Canadá***



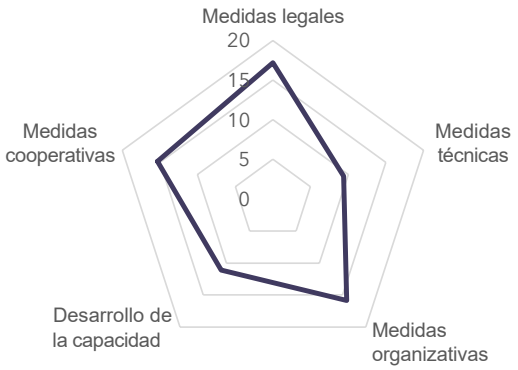
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, organizativas, cooperativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,67	20,00	18,27	20,00	20,00	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Chile



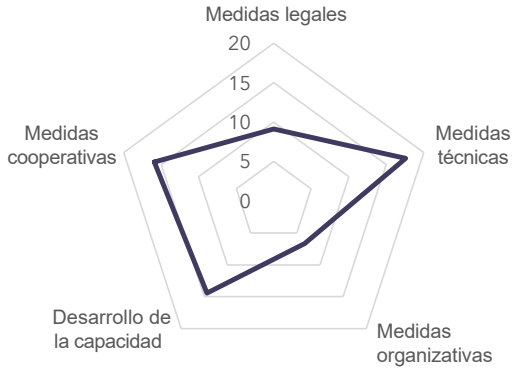
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
68,83	17,20	9,39	15,84	11,07	15,33

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Colombia (República de)



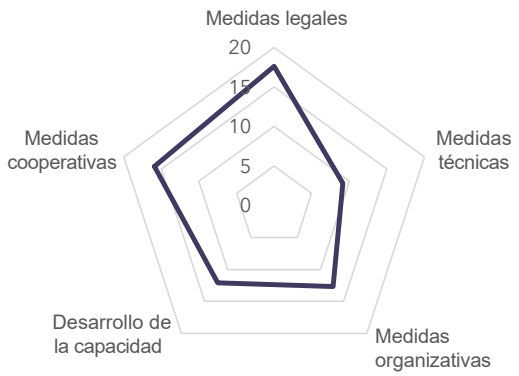
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
63,72	9,14	17,58	6,67	14,42	15,93

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Costa Rica



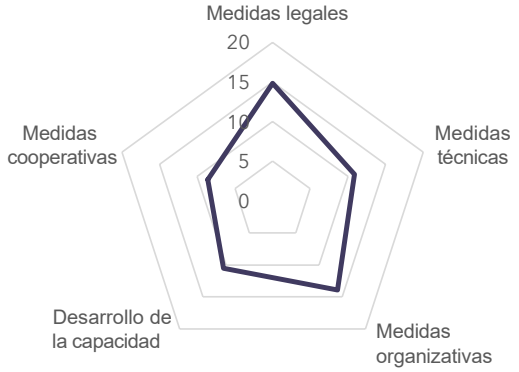
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
67,45	17,62	9,14	12,66	12,11	15,93

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Cuba



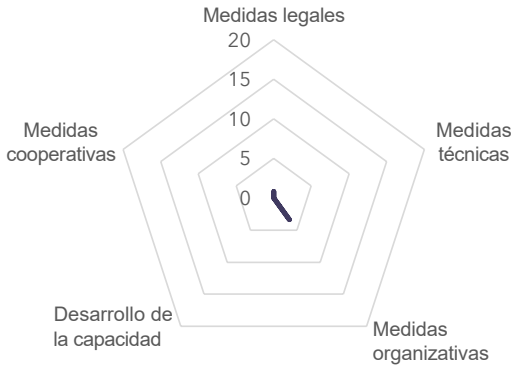
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
58,76	14,85	10,87	13,91	10,52	8,61

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Dominica (Commonwealth de)



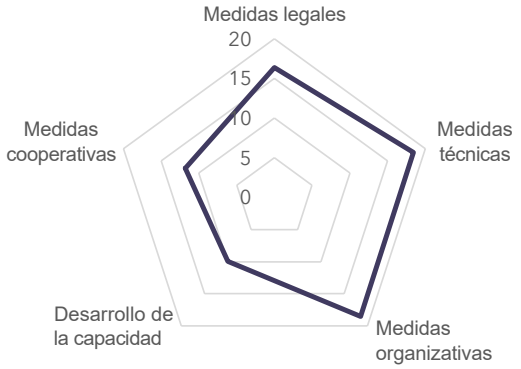
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Medidas técnicas cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
4,20	0,85	0,00	3,35	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Dominicana



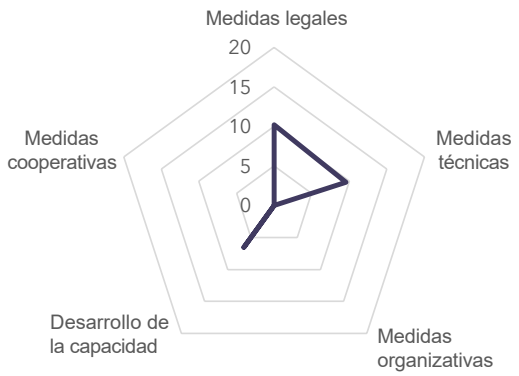
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
75,07	16,38	18,42	18,52	9,94	11,81

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Ecuador



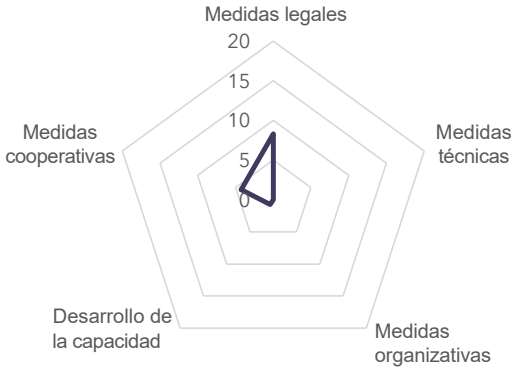
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas,
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
26,30	10,22	9,55	0,00	6,53	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*El Salvador (República de)***



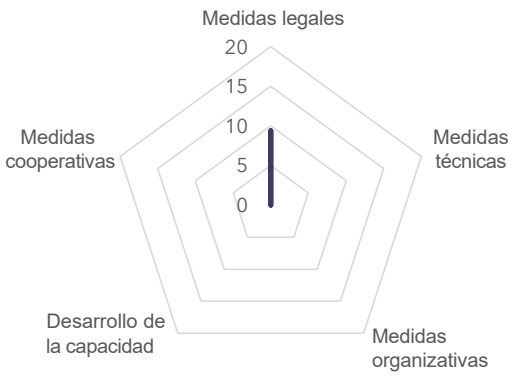
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, técnicas
Área(s) de posible crecimiento
Medidas organizativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
13,30	8,32	0,00	0,00	0,72	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Granada



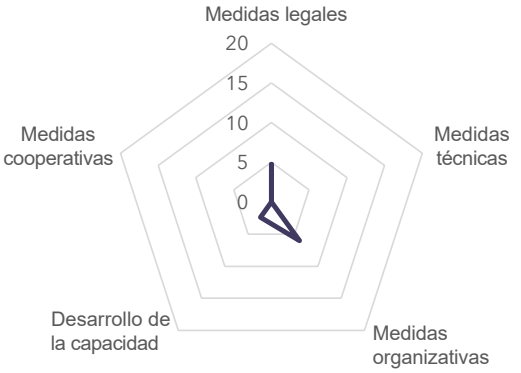
Nivel de desarrollo:
País en desarrollo, Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
9,41	9,41	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Guatemala (República de)



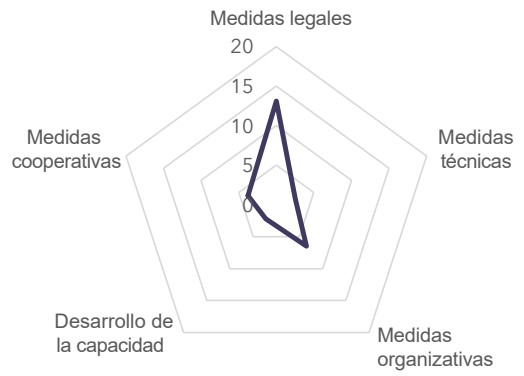
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Medidas técnicas, cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
13,13	4,76	0,00	6,01	2,36	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Guyana



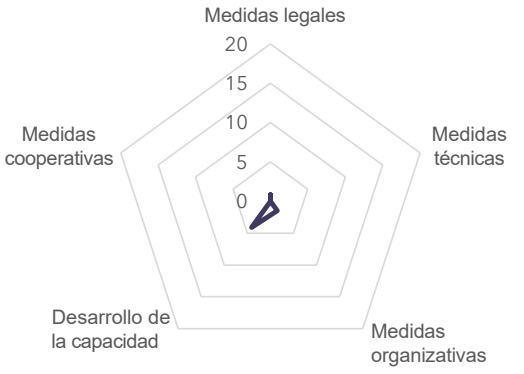
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
28,11	13,12	2,50	6,47	2,24	3,78

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Haití (República de)



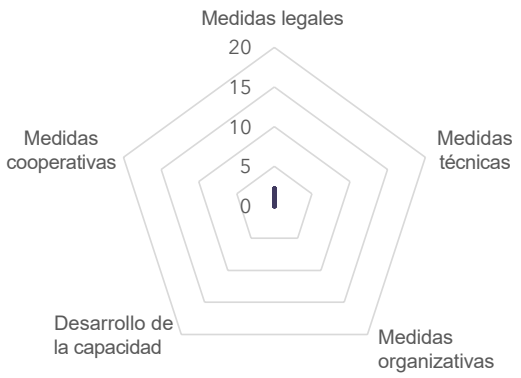
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas, Desarrollo
de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
6,40	0,85	0,00	1,46	4,09	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Honduras (República de)***



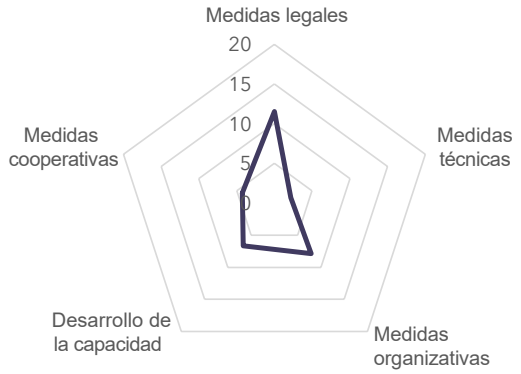
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
2,20	2,20	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Jamaica***



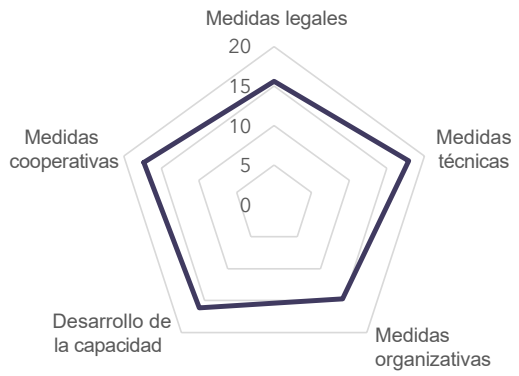
Nivel de desarrollo:
País en desarrollo, Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
32,53	11,54	2,18	7,87	6,68	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

México



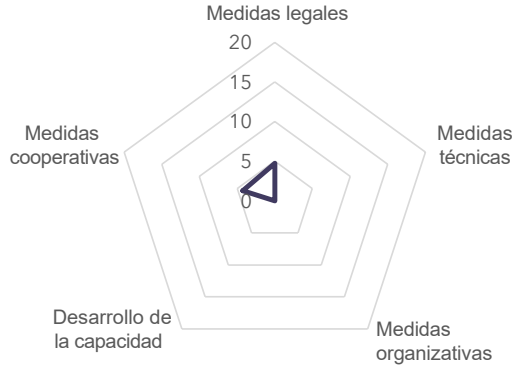
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
81,68	15,61	17,90	14,70	16,13	17,34

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Nicaragua***



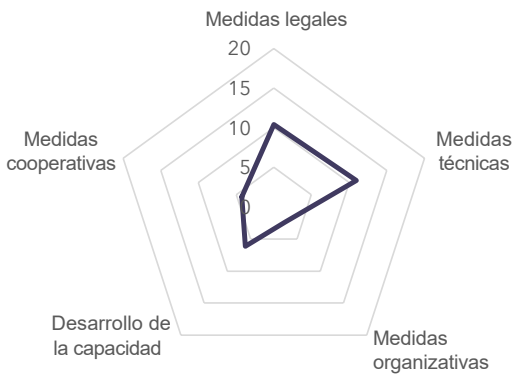
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
9,00	4,74	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Panamá (República de)



Nivel de desarrollo:
País en desarrollo

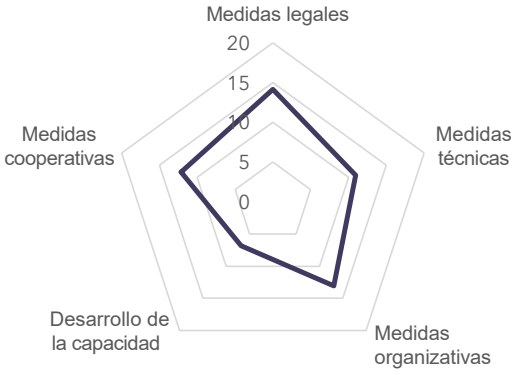
Área(s) de fortaleza relativa
Medidas técnicas,
Medidas legales

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
34,11	10,41	10,94	2,37	6,12	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Paraguay (República de)



Nivel de desarrollo:
País en desarrollo,
País sin litoral

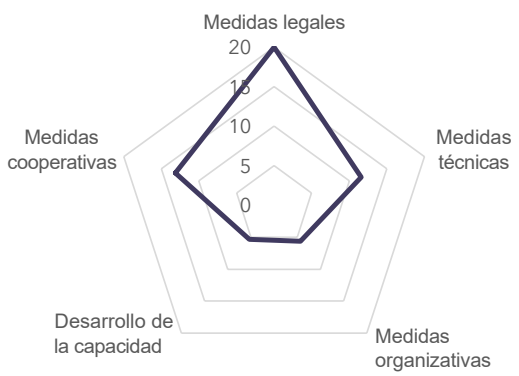
Área(s) de fortaleza relativa
Medidas legales

Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
57,09	14,15	10,94	13,06	6,79	12,14

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Perú



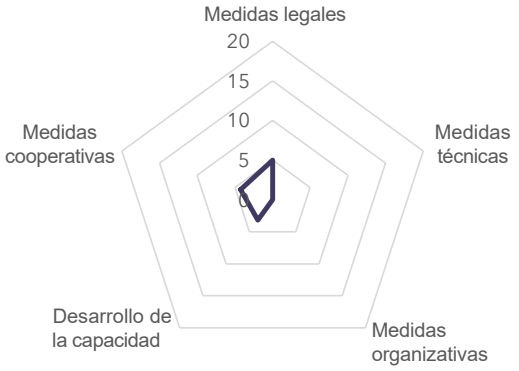
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
55,67	20,00	11,58	5,63	5,32	13,15

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Saint Kitts y Nevis (Federación de)



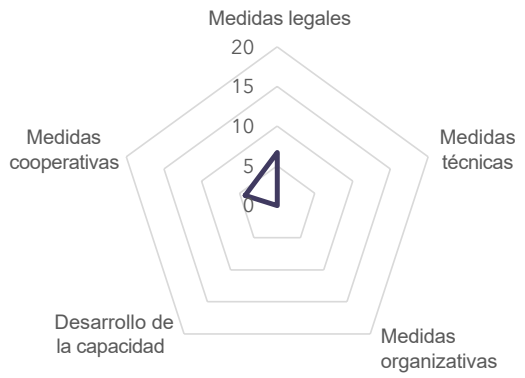
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
12,44	5,00	0,00	0,00	3,18	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Santa Lucía***



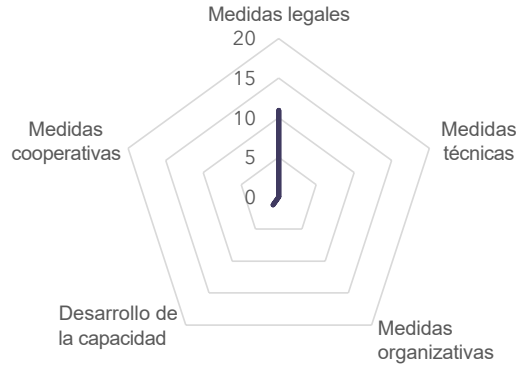
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Técnica, organizativa,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
10,96	6,70	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*San Vicente y las Granadinas***



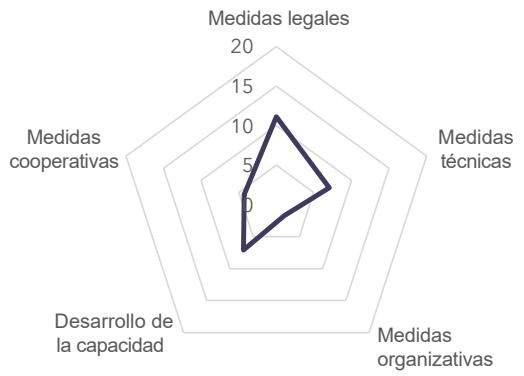
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Técnica, organizativa,
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
12,18	10,95	0,00	0,00	1,23	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Suriname (República de)



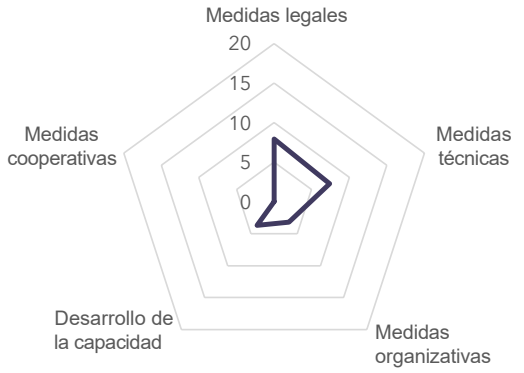
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
31,20	11,13	7,04	1,69	7,08	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Trinidad y Tabago



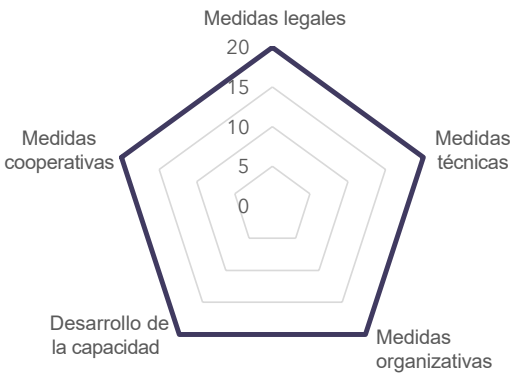
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
22,18	7,94	7,38	3,18	3,69	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Estados Unidos de América***



Nivel de desarrollo:
País desarrollado

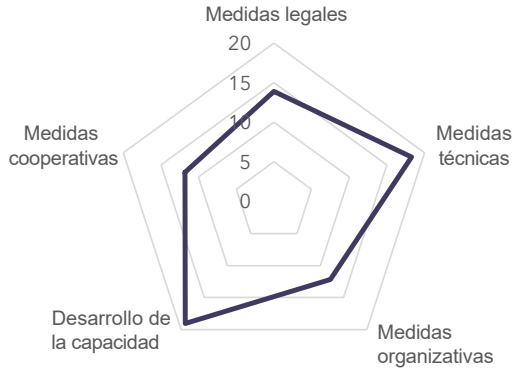
Área(s) de fortaleza relativa
Medidas legales, organizativas, cooperativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
N/A

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
100,00	20.,00	20,00	20,00	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Uruguay (República Oriental del)



Nivel de desarrollo:
País en desarrollo

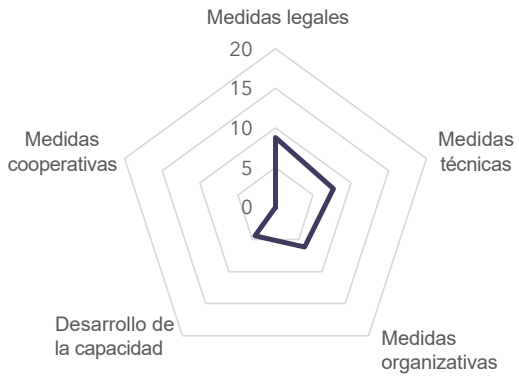
Área(s) de fortaleza relativa
Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
75,15	13,90	18,27	12,13	19,04	11,81

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Venezuela (República Bolivariana de)



Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
27,06	8,80	7,67	6,17	4,41	0,00

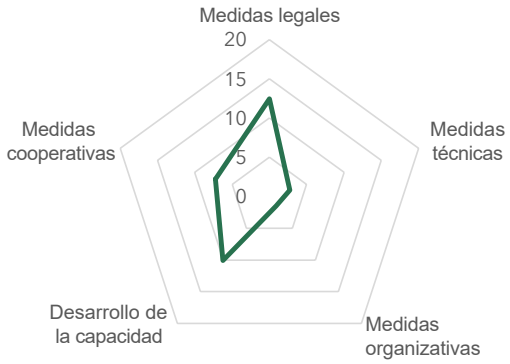
Fuente: Índice de Ciberseguridad Global v4, UIT 2020

** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

* Sin datos

Región de los Estados Árabes

Argelia (República Democrática Popular de)



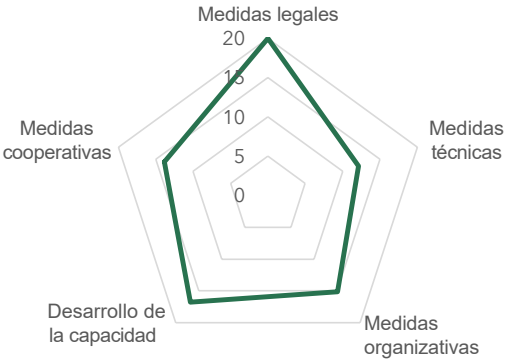
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
33,95	12,46	2,73	1,44	10,07	7,25

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bahrein (Reino de)



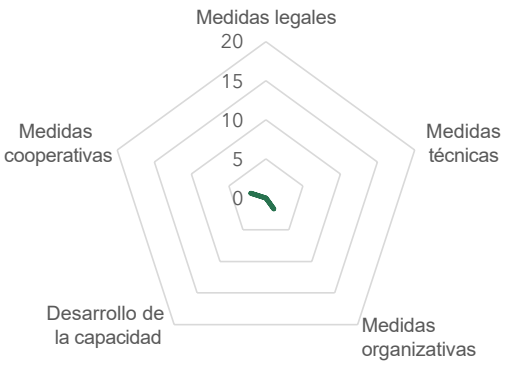
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
77,86	20,00	12,12	15,11	16,77	13,86

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Comoras (Unión de las)***



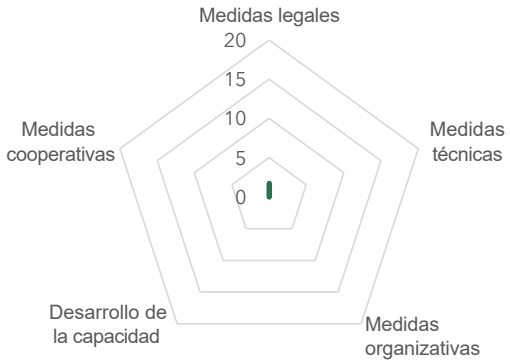
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas legales, técnicas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
3,72	0,00	0,00	1,69	0,00	2,04

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Djibouti (República de)



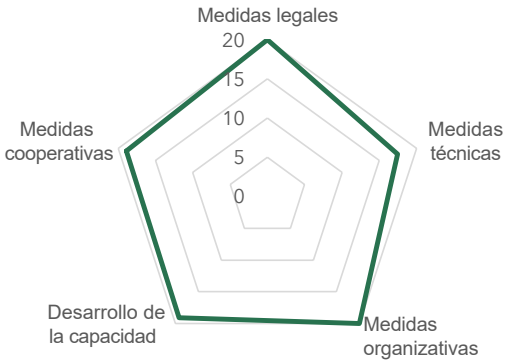
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas,
cooperativas, Desarrollo de
la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
1,73	1,73	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Egipto (República Árabe de)



Nivel de desarrollo:
País en desarrollo

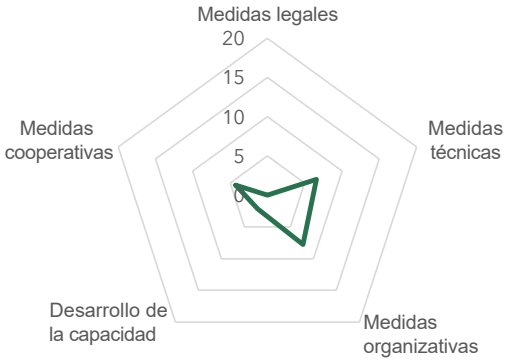
Área(s) de fortaleza relativa
Medidas legales, organizativas, Desarrollo de la capacidad

Área(s) de posible crecimiento

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
95,48	20,00	17,45	20,00	19,12	18,91

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Iraq (República de)***



Nivel de desarrollo:
País en desarrollo

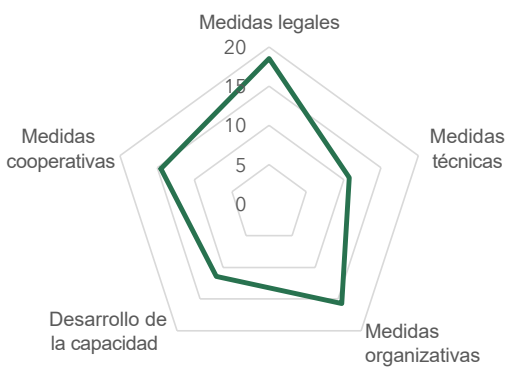
Área(s) de fortaleza relativa
Medidas organizativas

Área(s) de posible crecimiento
Medidas legales

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
20,71	0,00	6,56	7,75	2,14	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Jordania (Reino Hachemita de)



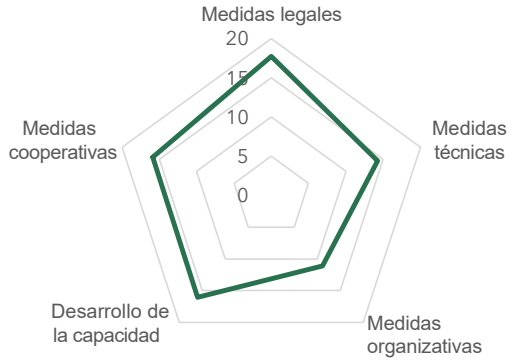
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
70,96	18,53	10,74	15,70	11,47	14,51

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Kuwait (Estado de)



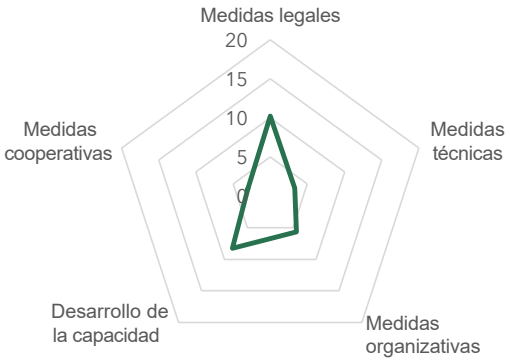
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
75,05	17,74	14,25	11,13	16,05	15,90

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Líbano***



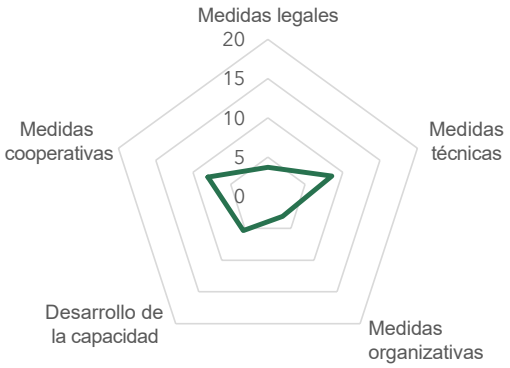
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
30,44	10,24	3,27	5,69	8,26	2,99

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Libia (Estado de)



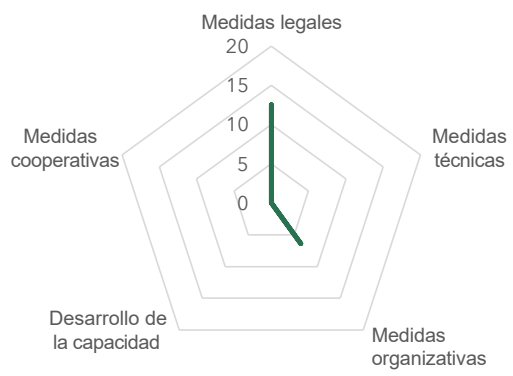
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas técnicas, cooperativas
Área(s) de posible crecimiento
Medidas legales, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
28,78	3,73	8,54	3,13	5,34	8,04

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Mauritania (República Islámica de)



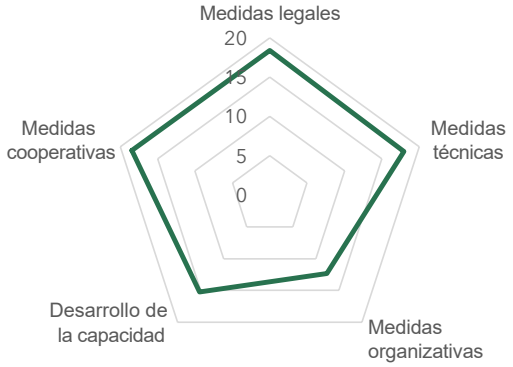
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
18,94	12,55	0,00	6,39	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Marruecos (Reino de)



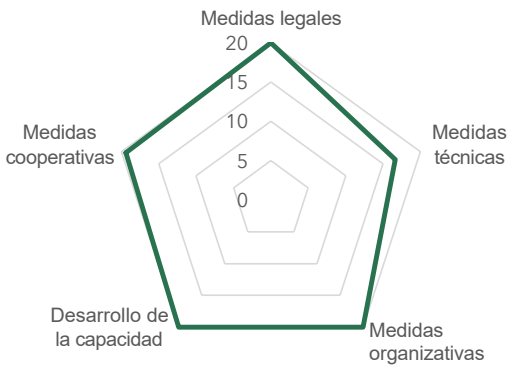
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
82,41	18,40	17,94	12,37	15,24	18,46

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Omán (Sultanato de)



Nivel de desarrollo:
País en desarrollo

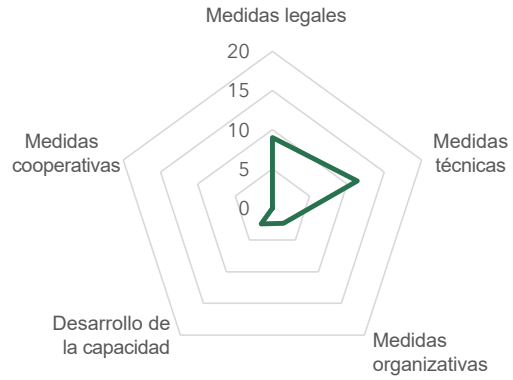
Área(s) de fortaleza relativa
Medidas legales, organizativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
96,04	20,00	16,64	20,00	20,00	96,04

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Estado de Palestina



Nivel de desarrollo:
País en desarrollo

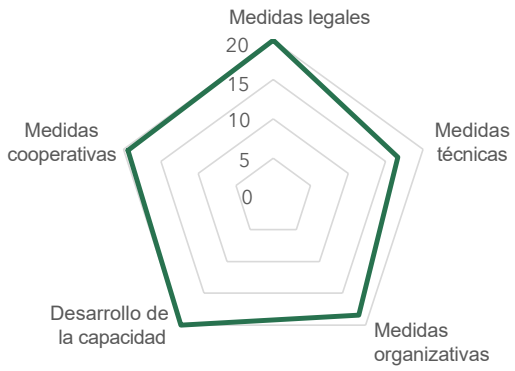
Área(s) de fortaleza relativa
Medidas técnicas

Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
25,18	9,02	11,36	2,34	2,46	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Qatar (Estado de)



Nivel de desarrollo:
País en desarrollo

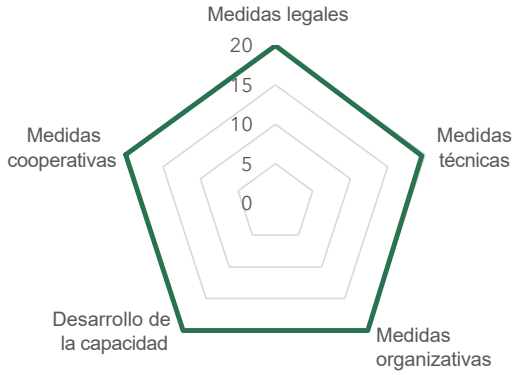
Área(s) de fortaleza relativa
Medidas legales, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
94,50	20,00	16,64	18,46	20,00	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Arabia Saudita (Reino de)



Nivel de desarrollo:
País en desarrollo

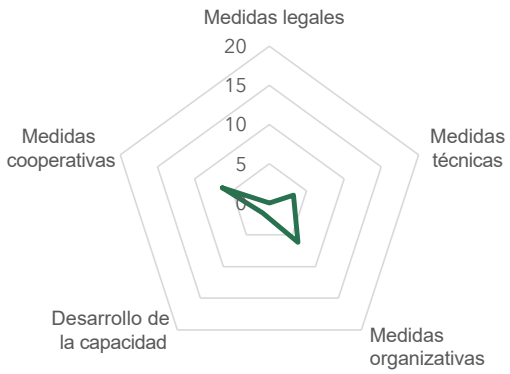
Área(s) de fortaleza relativa
Medidas legales, organizativas, cooperativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
99,54	20,00	19,54	20,00	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Somalia (República Federal de)



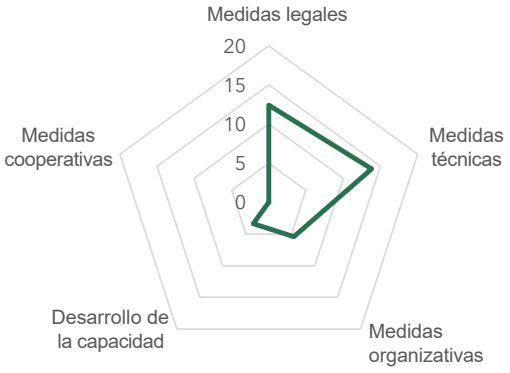
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas organizativas, cooperativas
Área(s) de posible crecimiento
Medidas legales

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
17,25	0,00	3,25	6,17	1,52	6,31

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Sudán (República de)



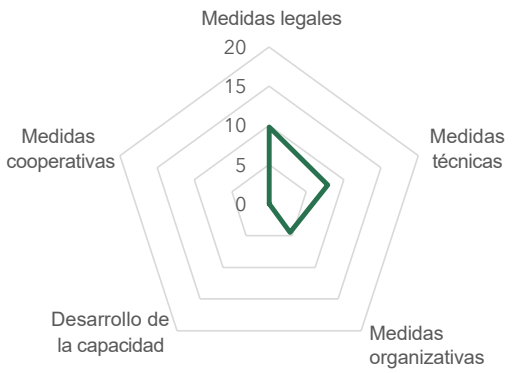
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
35,03	12,43	13,81	5,41	3,38	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*República Árabe Siria***



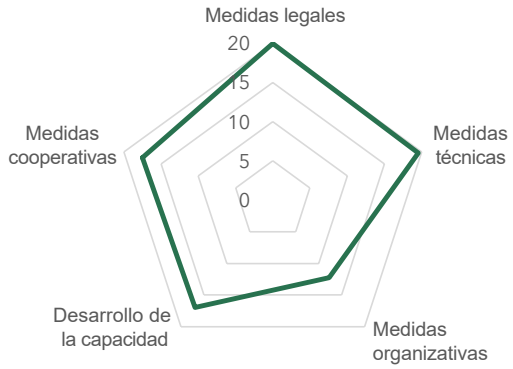
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad, Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
22,14	9,80	7,85	4,49	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Túnez



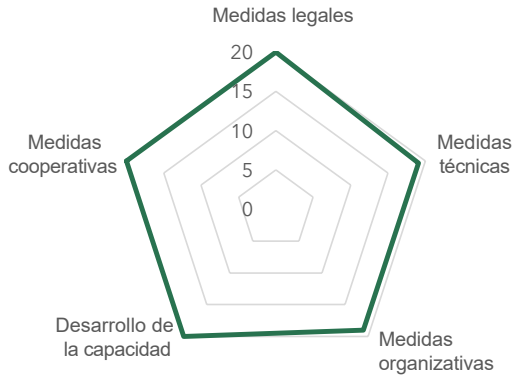
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, Medidas técnicas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
86,23	20,00	19,54	12,21	16,96	17,52

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Emiratos Árabes Unidos



Nivel de desarrollo:
País en desarrollo

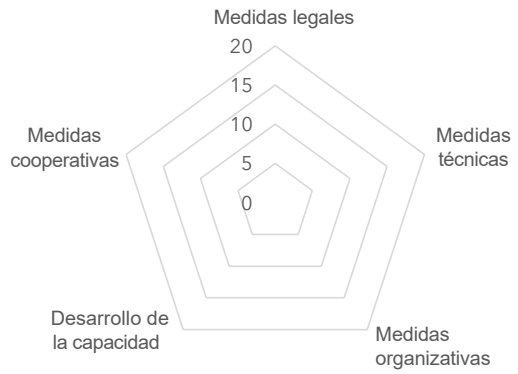
Área(s) de fortaleza relativa
Medidas legales, cooperativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,06	20,00	19,08	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Yemen (República de)**



Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
N/A

Área(s) de posible crecimiento
N/A

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
0	0	0	0	0	0

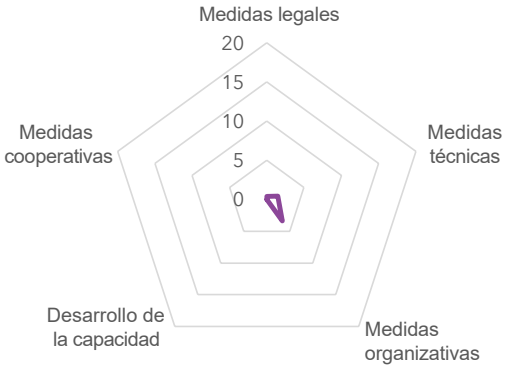
Fuente: Índice de Ciberseguridad Global v4, UIT 2020

** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

* Sin datos

Región de Asia-Pacífico

Afganistán



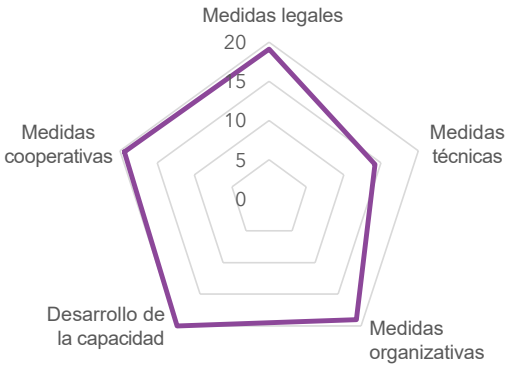
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Desarrollo de la capacidad,
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
5,20	0,40	1,46	3,35	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Australia



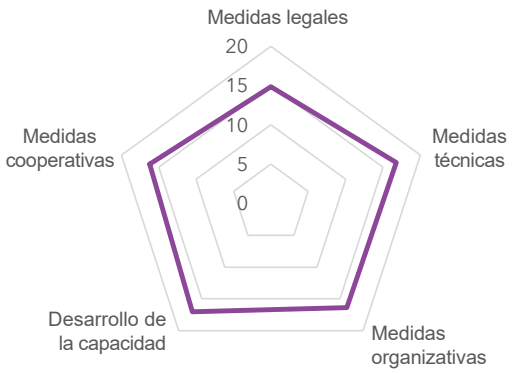
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Desarrollo de la capacidad,
Medidas cooperativas,
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,47	20,00	19,08	18,98	20,00	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bangladesh (República Popular de)



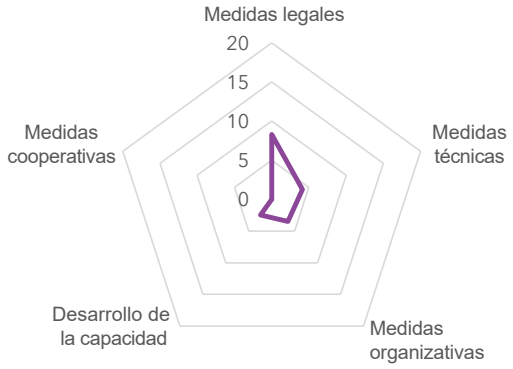
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Desarrollo de la capacidad,
Medidas técnicas
Área(s) de posible crecimiento
Medidas legales

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
81,27	14,86	16,77	16,39	17,03	16,22

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bután (Reino de)



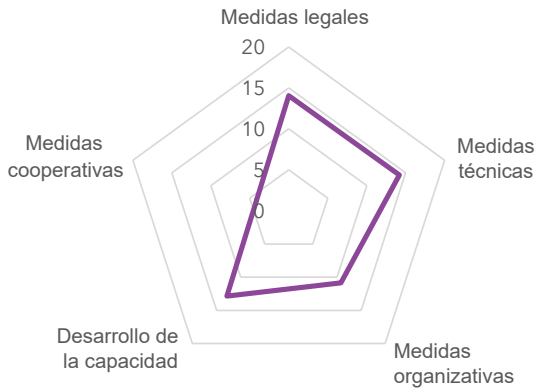
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
18,34	8,30	4,12	3,47	2,45	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Brunei Darussalam



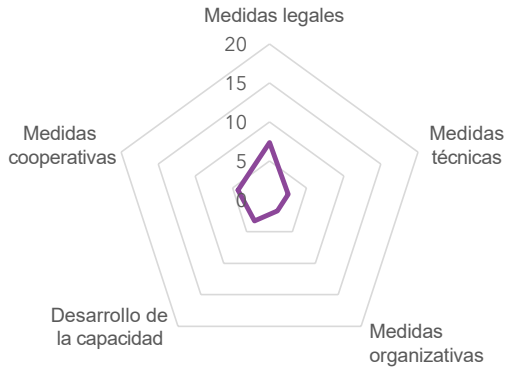
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
56,07	14,06	14,19	10,84	12,85	4,12

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Camboya (Reino de)***



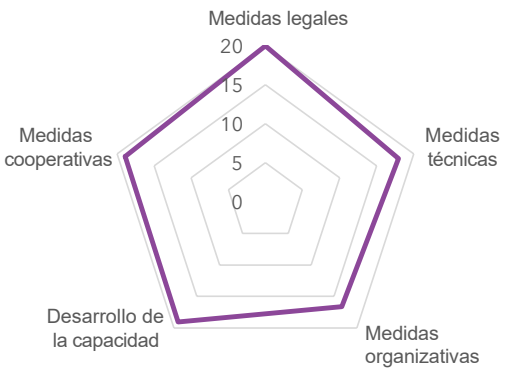
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
19,12	7,38	2,50	1,69	3,29	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

China (República Popular de)



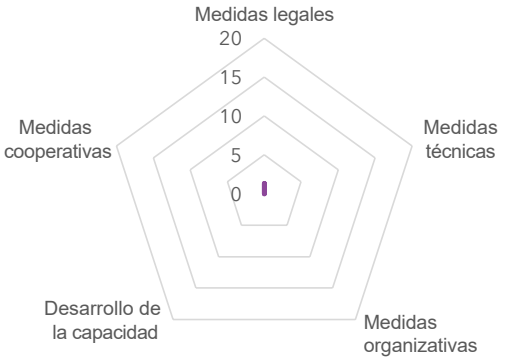
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
92,53	20,00	17,94	16,63	19,04	18,91

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*República Popular Democrática de Corea***



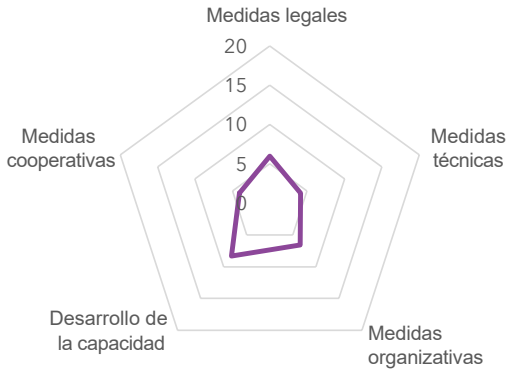
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas, cooperativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
1,35	1,35	0,00	0,00	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Fiji (República de)



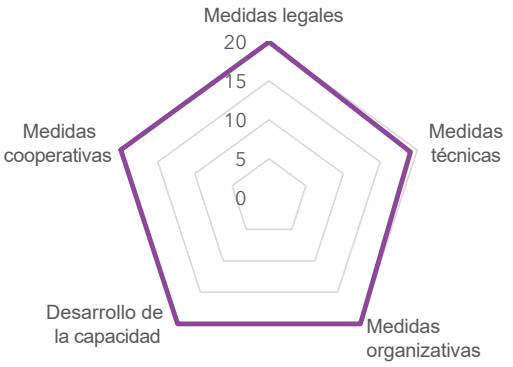
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas técnicas, cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
29,08	5,99	4,11	6,59	8,31	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

India (República de)



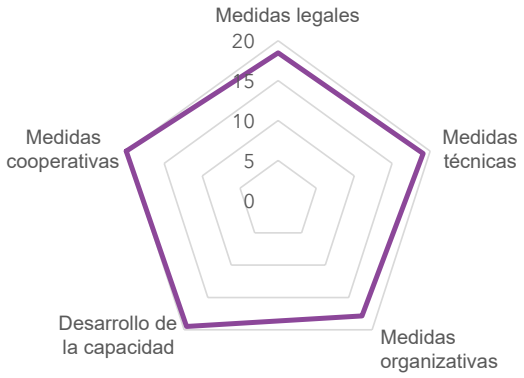
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, organizativas, cooperativas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,49	20,00	19,08	18,41	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Indonesia (República de)



Nivel de desarrollo:
País en desarrollo

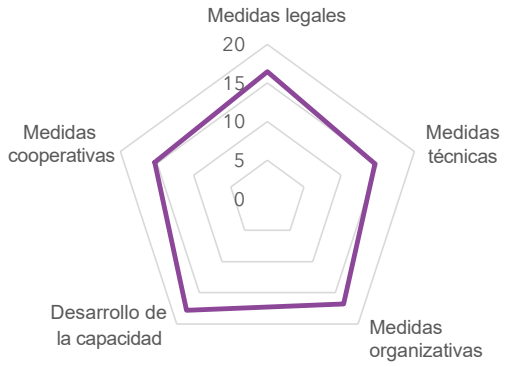
Área(s) de fortaleza relativa
Medidas cooperativas, técnicas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
94,88	18,48	19,08	17,84	19,48	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Irán (República Islámica de)



Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

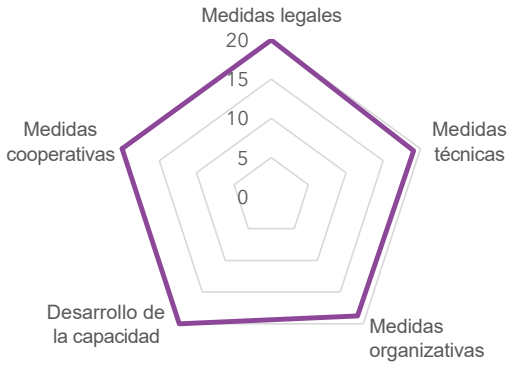
Área(s) de fortaleza relativa
Desarrollo de la capacidad, Medidas organizativas

Área(s) de posible crecimiento
Medidas técnicas, legales, cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
81,06	16,48	14,63	16,82	17,80	15,33

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Corea (República de)



Nivel de desarrollo:
País en desarrollo

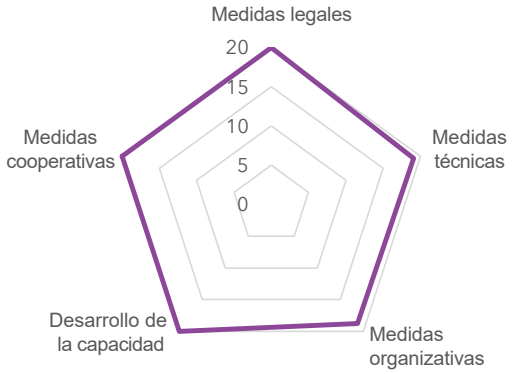
Área(s) de fortaleza relativa
Medidas legales, cooperativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,52	20,00	19,54	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Japón



Nivel de desarrollo:
País desarrollado

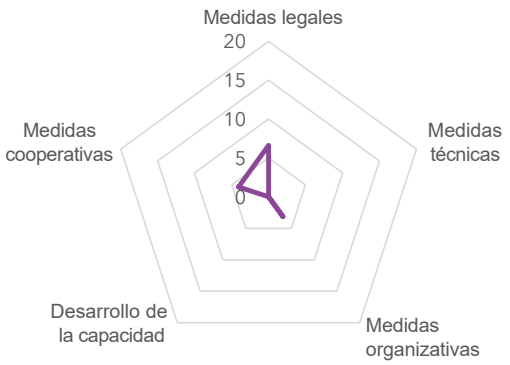
Área(s) de fortaleza relativa
Medidas legales, cooperativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,82	20,00	19,08	18,74	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Kiribati (República de)



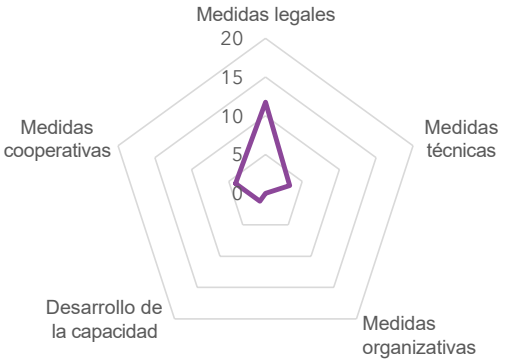
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, Desarrollo
de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
13,84	6,64	0,00	3,13	0,00	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Democrática Popular de Laos



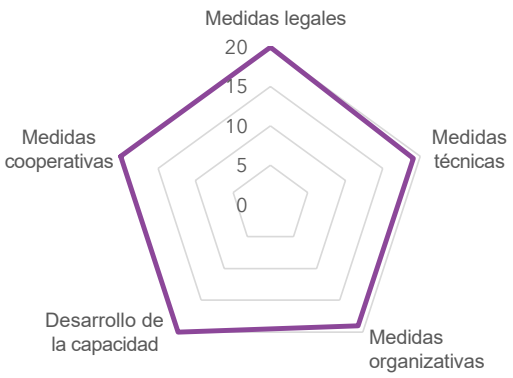
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
20,34	11,77	3,27	0,00	1,23	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Malasia



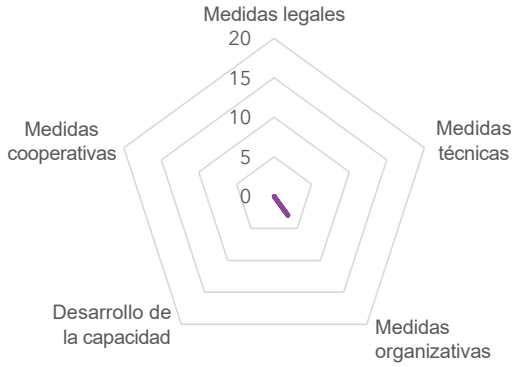
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,06	20,00	19,08	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Maldivas (República de)***



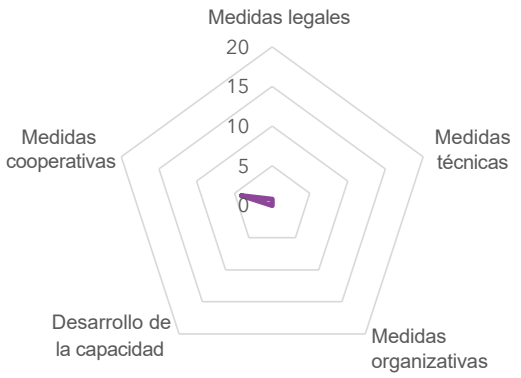
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Medidas legales, técnicas,
cooperativas, Desarrollo
de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
2,95	0,00	0,00	2,95	0,00	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Islas Marshall (República de las)***



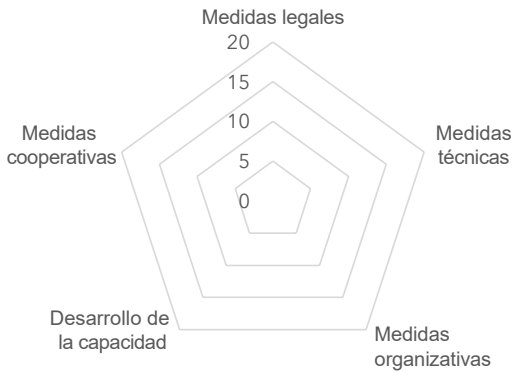
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas, organizativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
4,90	0,83	0,00	0,00	0,00	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Micronesia (Estados Federados de)**



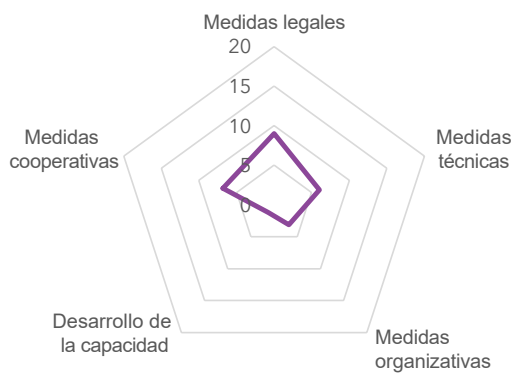
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
N/A
Área(s) de posible crecimiento
N/A

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
0	0	0	0	0	0

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Mongolia



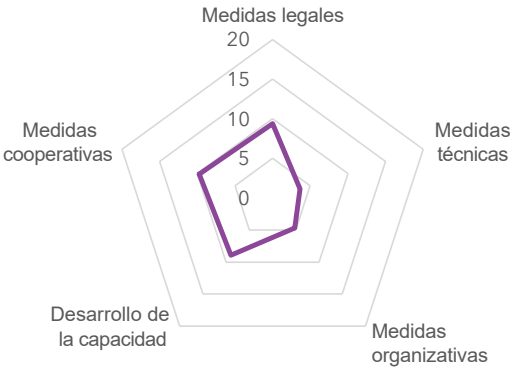
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
26,20	9,00	6,02	3,13	1,23	6,82

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Myanmar (Unión de)



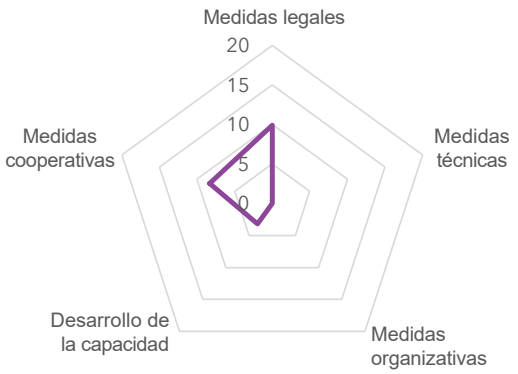
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA)

Área(s) de fortaleza relativa
Medidas cooperativas, legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
36,41	9,39	3,64	4,71	8,92	9,75

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Nauru (República de)***



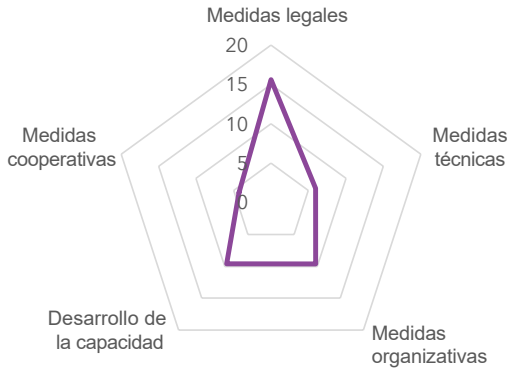
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
21,42	9,91	0,00	0,00	3,18	8,33

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Nepal (República Democrática Federal de)***



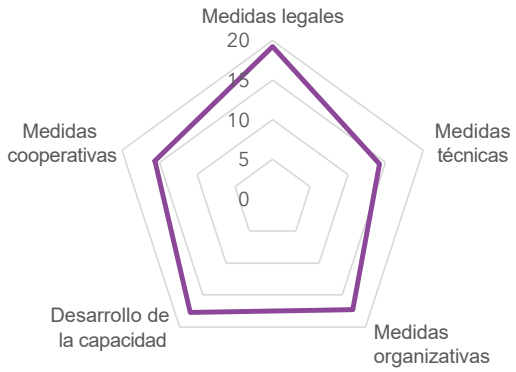
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
44,99	15,61	5,94	9,58	9,60	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Nueva Zelandia***



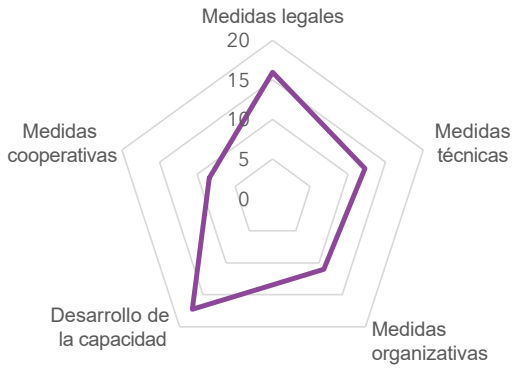
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
84,04	19,24	14,19	17,27	17,71	15,63

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Pakistán (República Islámica de)



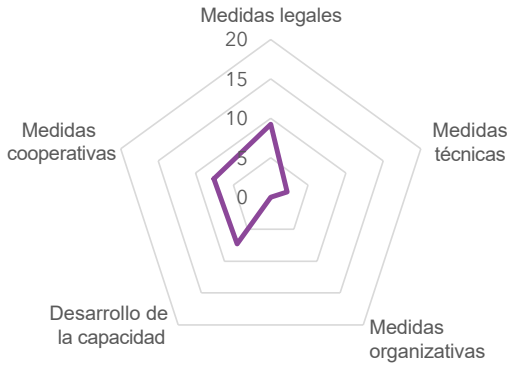
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
64,88	15,97	12,26	11,01	17,25	8,38

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Papúa Nueva Guinea***



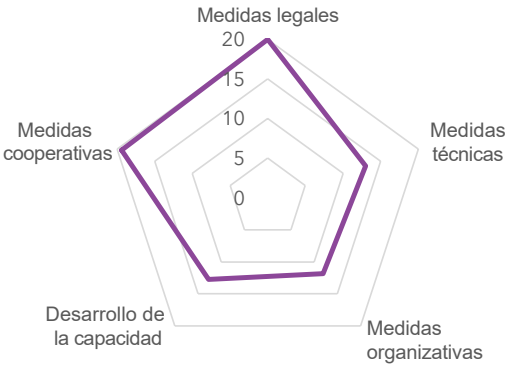
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
26,33	9,26	2,18	0,00	7,30	7,59

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Filipinas (República de)



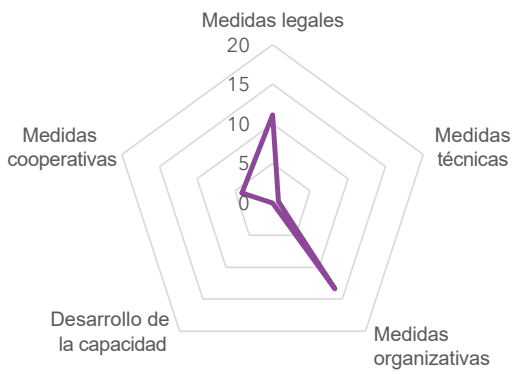
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
77,00	20,00	13,00	11,85	12,74	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Samoa (Estado independiente de)



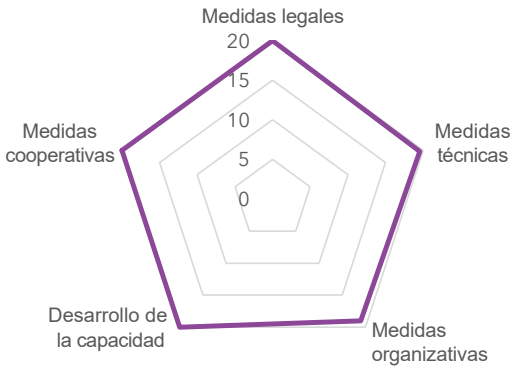
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Desarrollo de la capacidad, Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
29,33	11,15	0,73	13,37	0,00	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Singapur (República de)



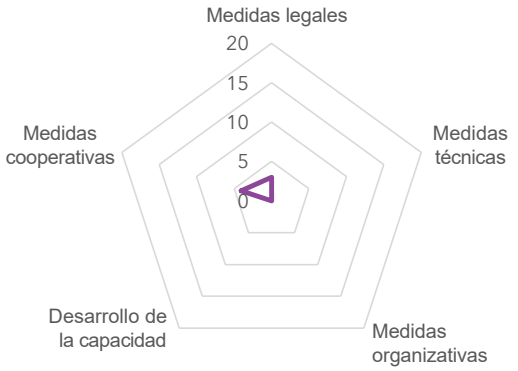
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas legales, cooperativas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,52	20,00	19,54	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Islas Salomón



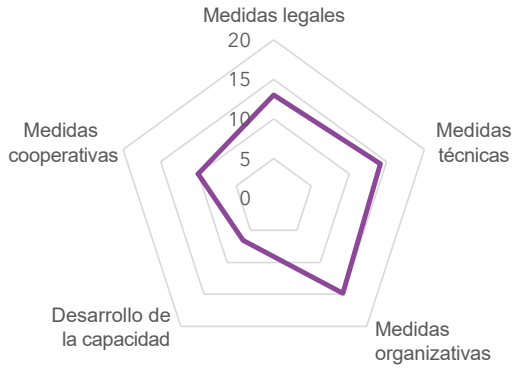
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas,
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
7,08	3,00	0,00	0,00	0,00	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Sri Lanka (República Socialista Democrática de)



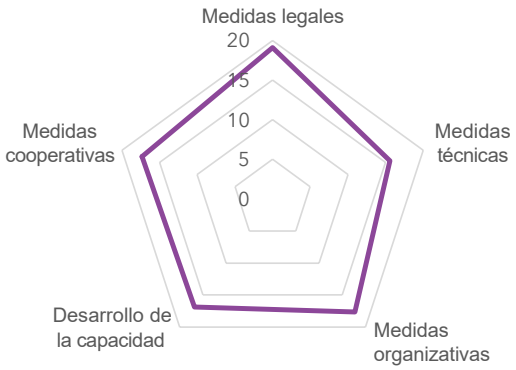
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas organizativas, técnicas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
58,65	13,05	14,15	14,82	6,58	10,04

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Tailandia



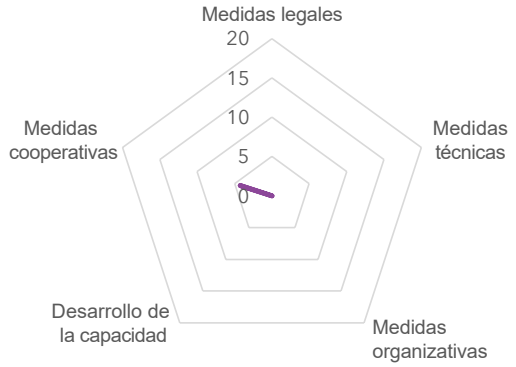
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
86,50	19,11	15,57	17,64	16,84	17,34

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Timor-Leste (República Democrática de)***



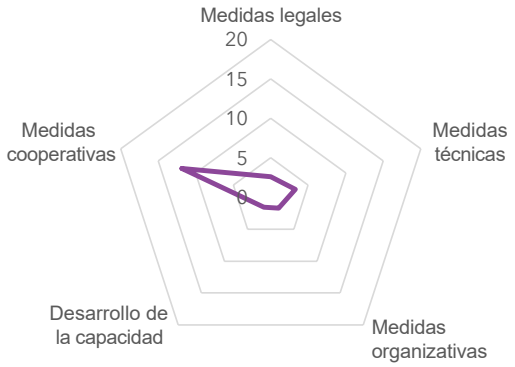
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas legales, técnicas,
organizativas, Desarrollo
de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
4,26	0,00	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Tonga (Reino de)***



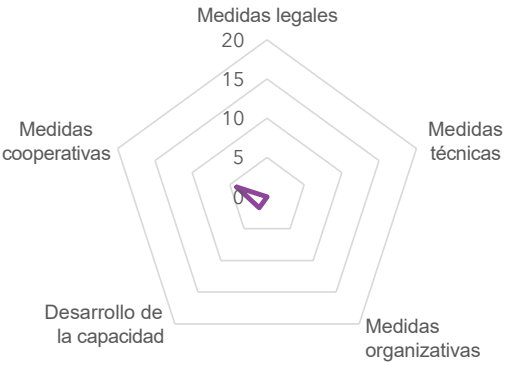
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Desarrollo de la capacidad,
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
20,95	2,63	3,27	1,69	1,52	11,85

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Tuvalu***



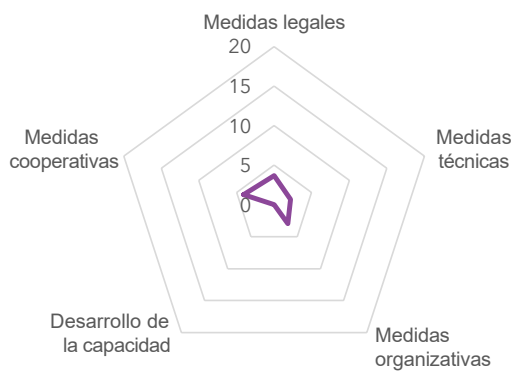
Nivel de desarrollo:
País en desarrollo,
Países menos adelantados (PMA),
Pequeños Estados insulares
en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas legales, técnicas,
organizativas, Desarrollo
de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
5,78	0,00	0,00	0,00	1,71	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Vanuatu (República de)



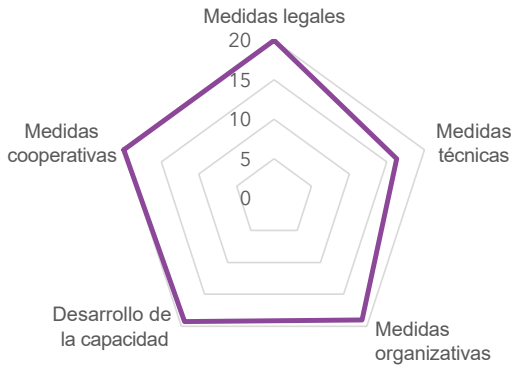
Nivel de desarrollo:
País en desarrollo,
Pequeños Estados insulares en desarrollo (PEID)

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
12,88	3,69	2,18	2,95	0,00	4,07

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Viet Nam (República Socialista de)



Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales, cooperativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
94,55	20,00	16,31	18,98	19,26	20,00

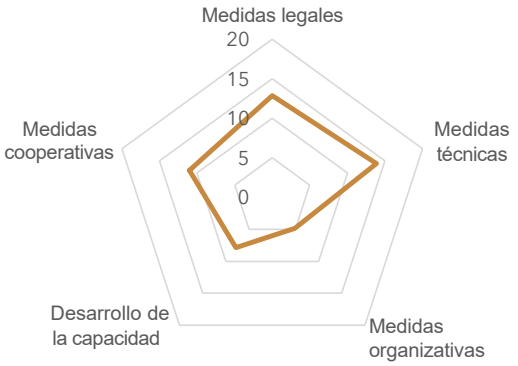
Fuente: Índice de Ciberseguridad Global v4, UIT 2020

** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

* Sin datos

Región de la Comunidad de Estados Independientes

*Armenia (República de)***



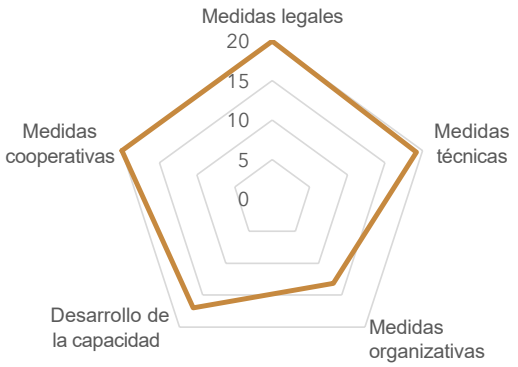
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
50,47	12,87	13,86	4,87	7,85	11,02

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Azerbaiyán (República de)



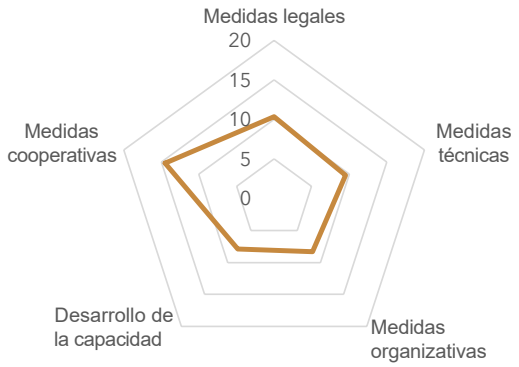
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
89,31	20,00	19,19	13,14	16,99	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bielorrusia (República de)



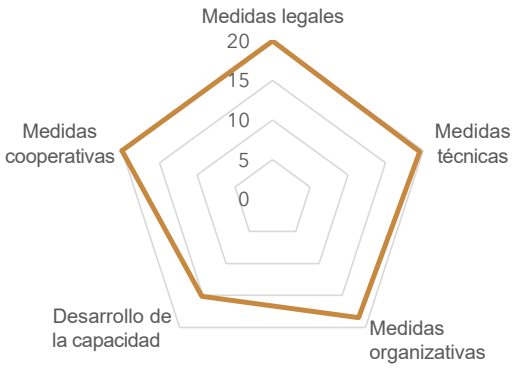
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
50,57	10,36	9,50	8,31	7,88	14,51

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Kazajstán (República de)



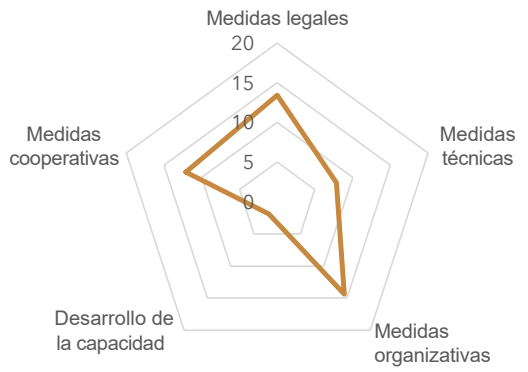
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas cooperativas, técnicas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
93,15	20,00	19,54	18,46	15,15	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Kirguisa



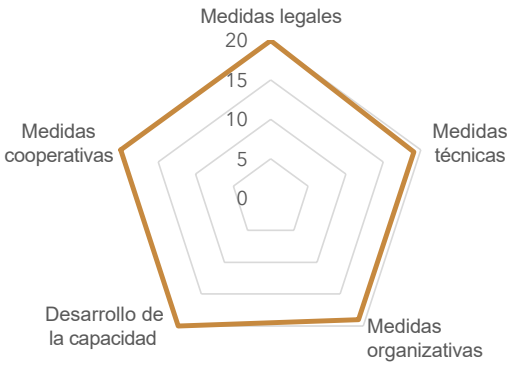
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas organizativas, legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
49,64	13,43	7,85	14,37	1,87	12,11

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Federación de Rusia



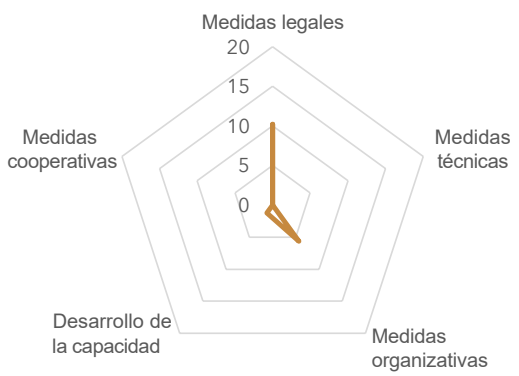
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, cooperativas,
Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,06	20,00	19,08	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Tayikistán (República de)***



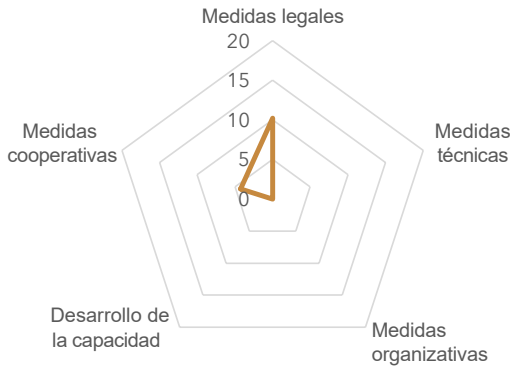
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
17,10	10,22	0,00	5,63	1,25	0,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Turkmenistán***



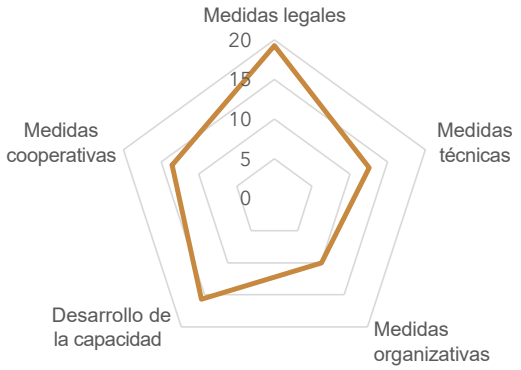
Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas, organizativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
14,48	10,22	0,00	0,00	0,00	4,26

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Uzbekistán (República de)



Nivel de desarrollo:
País en desarrollo,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, cooperativas,
Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas técnicas, organizativas

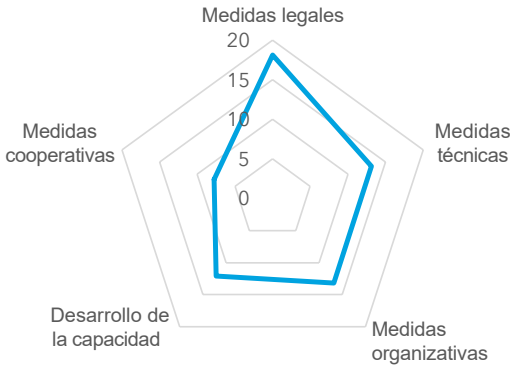
Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
71,11	19,27	12,56	10,05	15,68	13,56

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

** Sin respuesta al cuestionario/datos recabados por el Equipo ICG
* Sin datos

Europa

Albania (República de)



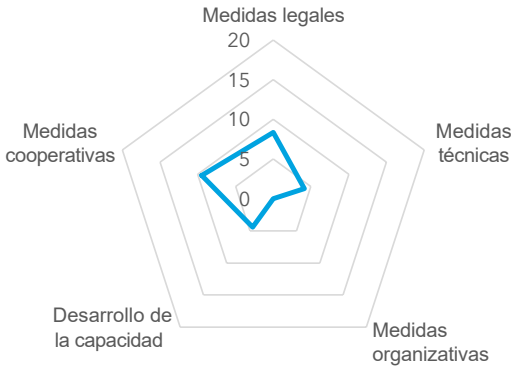
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
64,32	18,13	13,12	13,18	12,12	7,78

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Andorra (Principado de)***



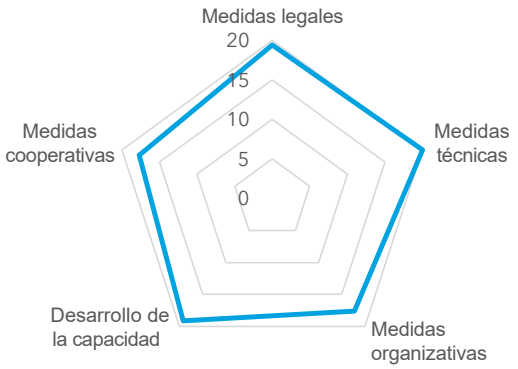
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
26,38	8,37	4,11	0,00	4,41	9,49

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Austria



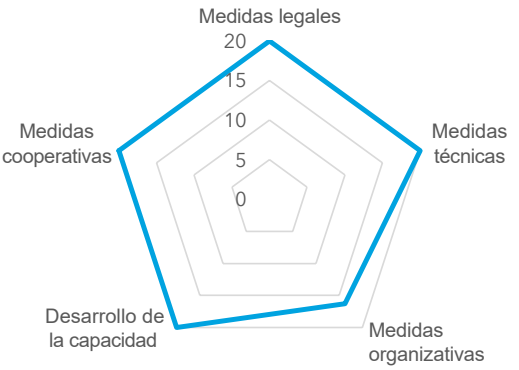
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
93,89	19,43	20,00	17,64	19,13	17,70

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bélgica



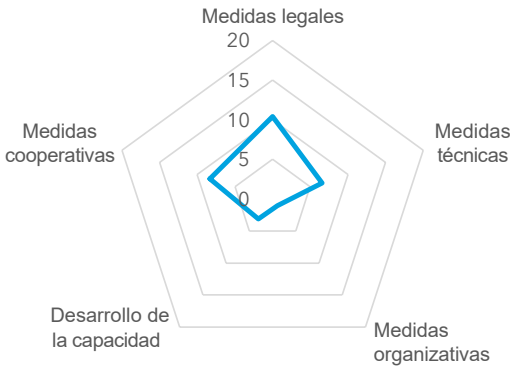
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
96,25	20,00	20,00	16,25	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bosnia y Herzegovina



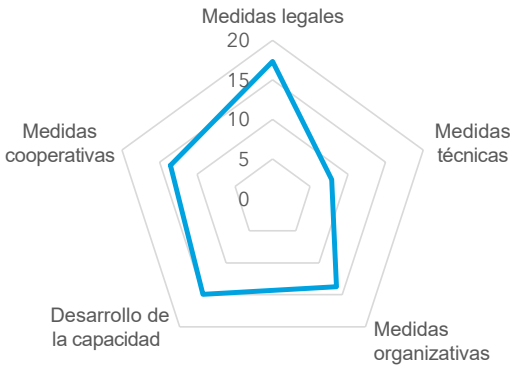
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
29,44	10,41	6,56	1,02	3,12	8,33

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Bulgaria (República de)



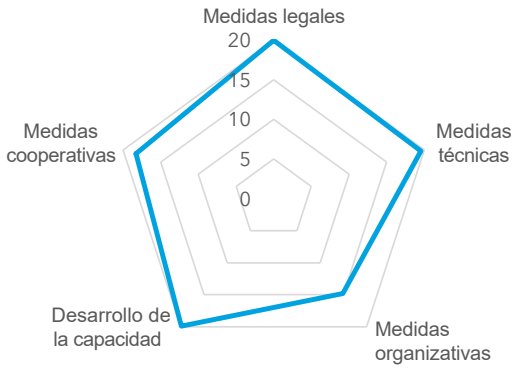
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
67,38	17,34	7,84	13,72	14,92	13,57

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Croacia (República de)



Nivel de desarrollo:
País desarrollado

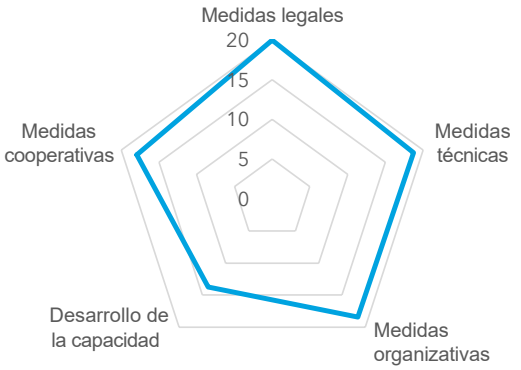
Área(s) de fortaleza relativa
Medidas legales, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas, técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
92,53	20,00	19,54	14,80	19,89	18,29

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Chipre (República de)



Nivel de desarrollo:
País desarrollado

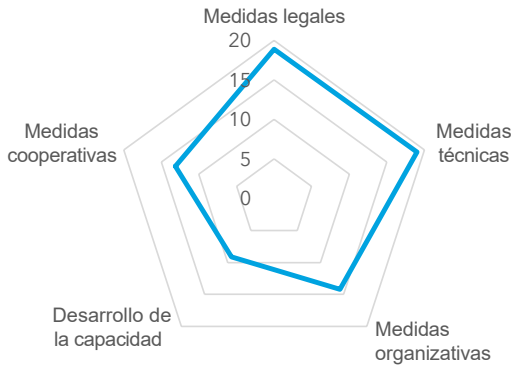
Área(s) de fortaleza relativa
Medidas legales

Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
88,82	20,00	18,73	18,41	13,73	17,94

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Checa



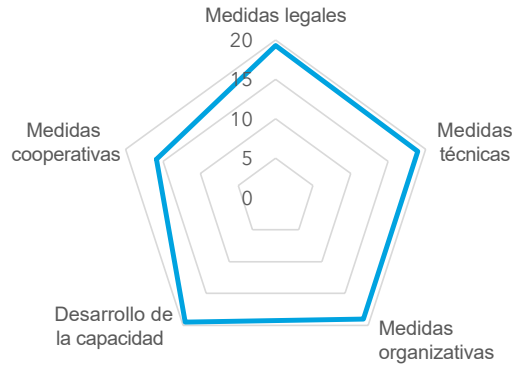
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas técnicas, legales
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
74,37	18,89	19,00	14,20	9,14	13,14

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Dinamarca



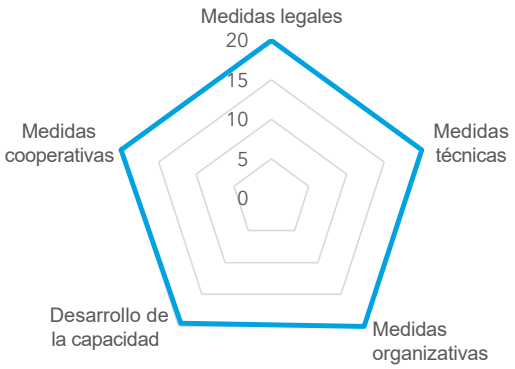
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Desarrollo de la capacidad, Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
92,60	19,30	18,94	18,98	19,48	15,89

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Estonia (República de)



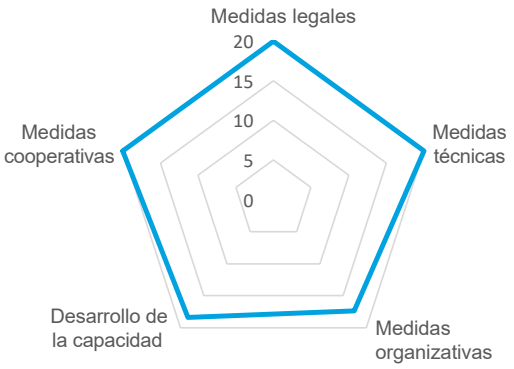
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
99,48	20,00	20,00	20,00	19,48	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Finlandia



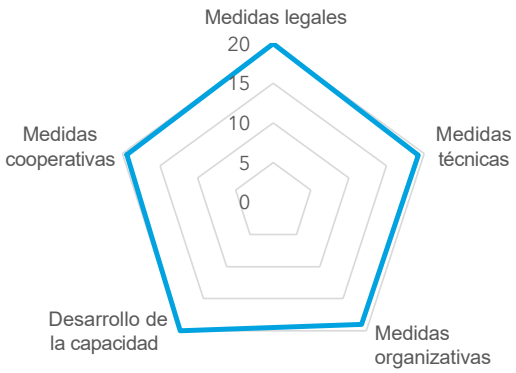
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
92,07	20,00	20,00	14,33	17,74	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Francia



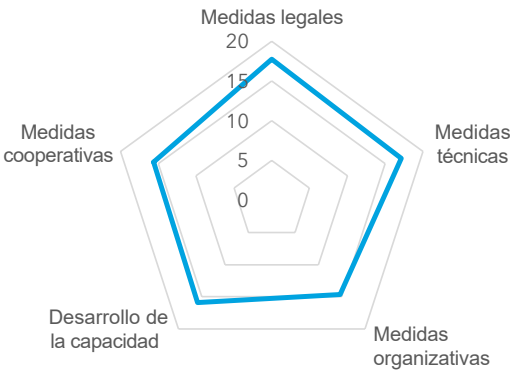
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,60	20,00	19,21	18,98	20,00	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Georgia



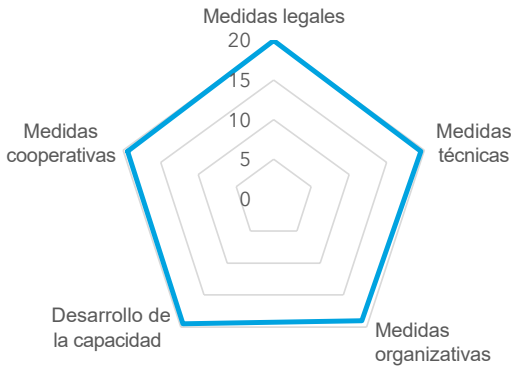
Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas cooperativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
81,07	17,75	17,13	14,67	15,89	15,63

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Alemania (República Federal de)



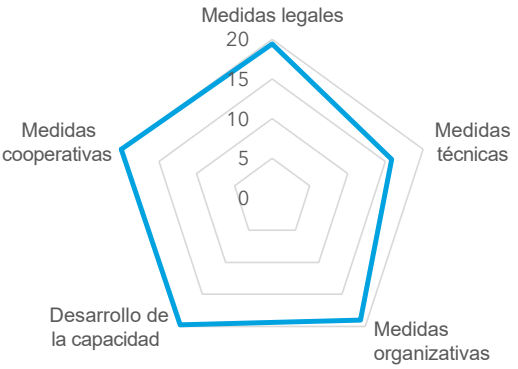
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, Desarrollo de la capacidad, Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,41	20,00	19,54	18,98	19,48	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Grecia



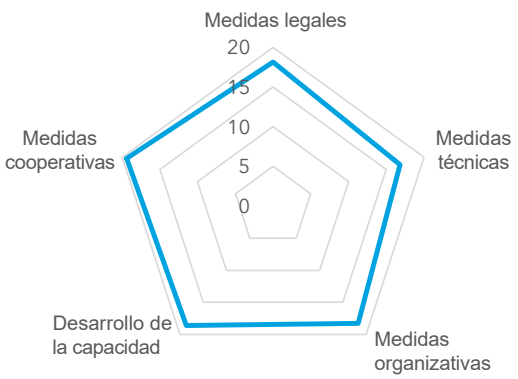
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas, Desarrollo de la capacidad, Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
93,98	19,43	15,83	18,98	19,74	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Hungría



Nivel de desarrollo:
País desarrollado

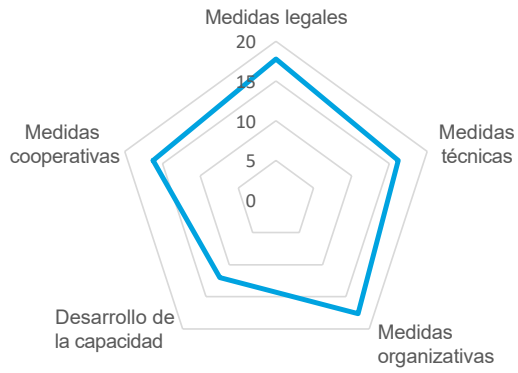
Área(s) de fortaleza relativa
Medidas cooperativas, Desarrollo de la capacidad, Medidas legales

Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
91,28	18,16	16,82	18,29	18,60	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Islandia



Nivel de desarrollo:
País desarrollado

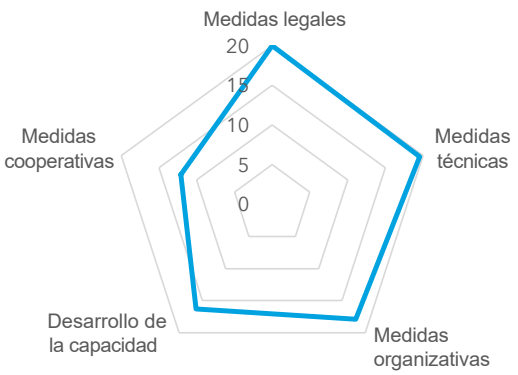
Área(s) de fortaleza relativa
Medidas legales, organizativas

Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
79,81	17,78	16,17	17,62	11,99	16,25

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Irlanda



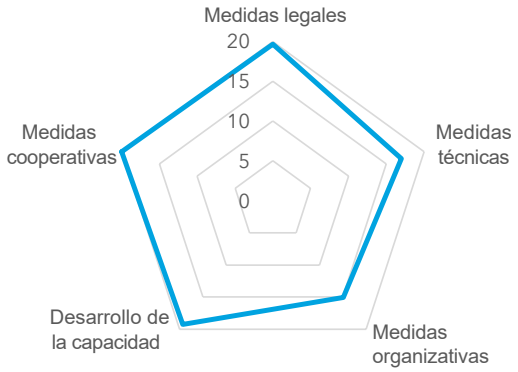
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
85,86	20,00	19,54	17,89	16,32	12,11

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Israel (Estado de)***



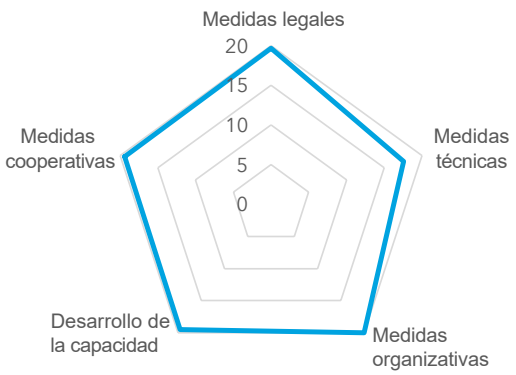
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas técnicas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas legales, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
90,93	19,68	16,99	15,02	19,24	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Italia



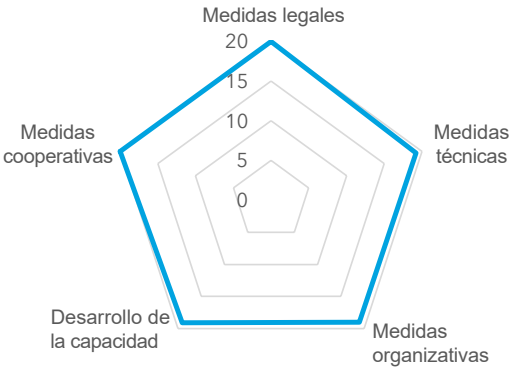
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas organizativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
96,13	19,68	17,56	20,00	19,48	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Letonia (República de)



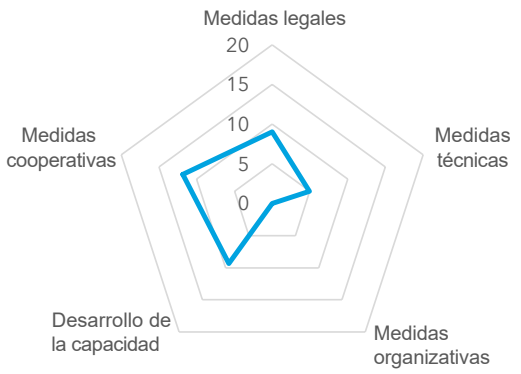
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas, Desarrollo de la capacidad
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,28	20,00	19,21	18,98	19,09	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Liechtenstein (Principado de)***



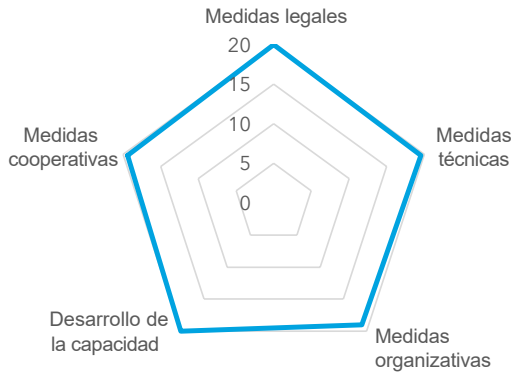
Nivel de desarrollo:
País desarrollado,
País sin litoral

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
35,15	9,04	4,93	0,00	9,34	11,85

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Lituania (República de)



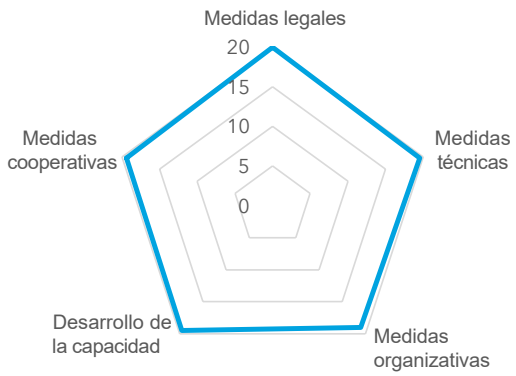
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, Desarrollo de la capacidad, Medidas técnicas, cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,93	20,00	19,54	18,98	20,00	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Luxemburgo



Nivel de desarrollo:
País desarrollado

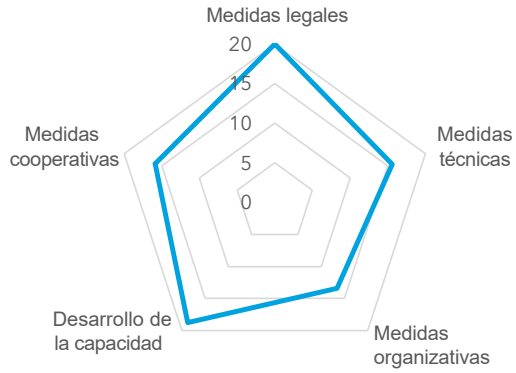
Área(s) de fortaleza relativa
Medidas legales, Desarrollo de la capacidad, Medidas técnicas, cooperativas

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,41	20,00	19,54	18,98	19,48	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Malta



Nivel de desarrollo:
País desarrollado

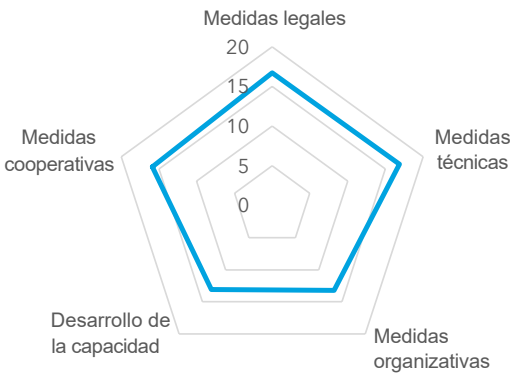
Área(s) de fortaleza relativa
Medidas legales

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
83,65	20,00	15,59	13,41	18,76	15,89

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Moldavia (República de)



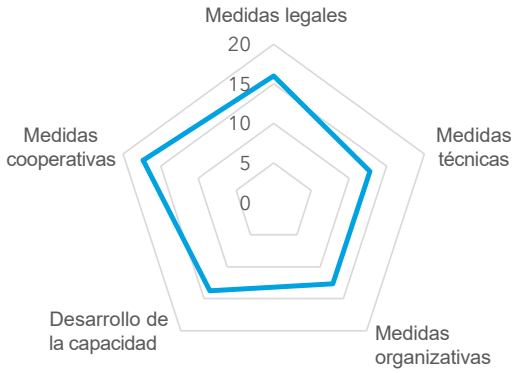
Nivel de desarrollo:
País desarrollado,
País sin litoral

Área(s) de fortaleza relativa
Medidas técnicas
Área(s) de posible crecimiento
Medidas organizativas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
75,78	16,73	16,86	13,21	13,09	15,89

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Mónaco (Principado de)



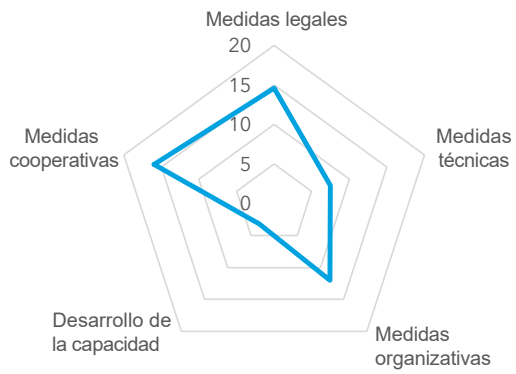
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas, organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
72,57	16,00	12,77	12,70	13,75	17,34

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Montenegro



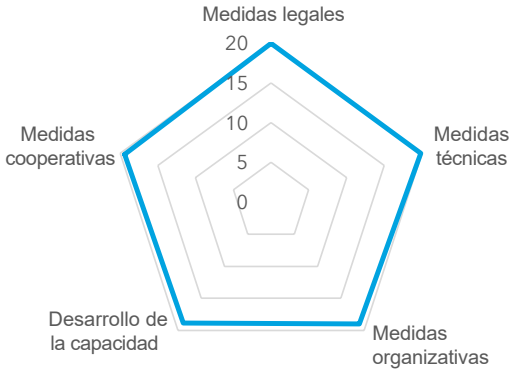
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
53,23	14,61	7,48	12,00	3,18	15,97

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Países Bajos (Reino de los)***



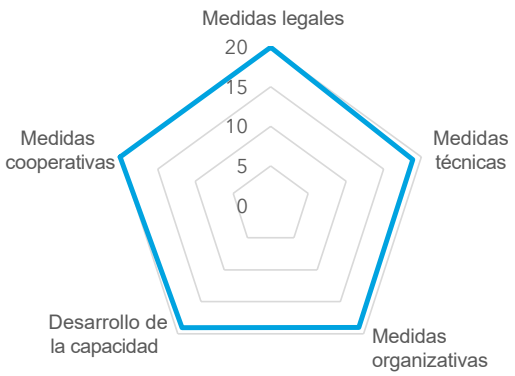
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas
Área(s) de posible crecimiento
Medidas organizativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,05	20,00	19,84	18,98	18,82	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Noruega***



Nivel de desarrollo:
País desarrollado

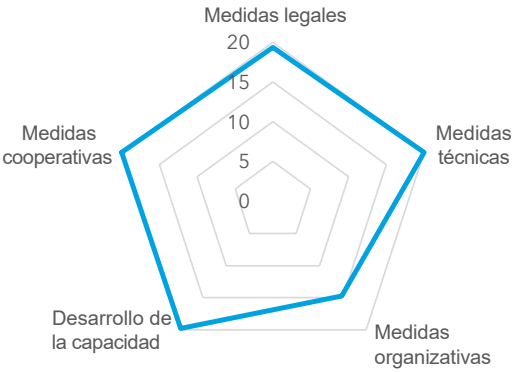
Área(s) de fortaleza relativa
Medidas legales,
Medidas cooperativas

Área(s) de posible crecimiento
Desarrollo de la capacidad,
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
96,89	20,00	18,86	18,98	19,04	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Polonia (República de)



Nivel de desarrollo:
País desarrollado

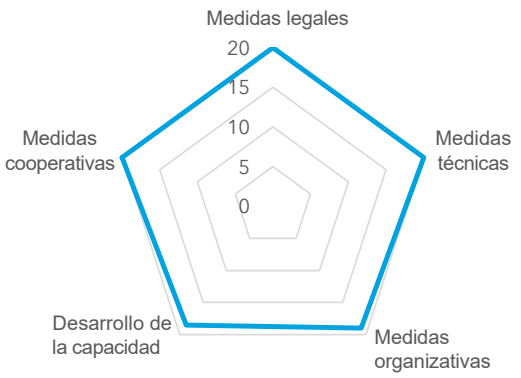
Área(s) de fortaleza relativa
Medidas técnicas, cooperativas,
legales, Desarrollo de
la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
93,86	19,35	20,00	14,74	19,77	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Portugal



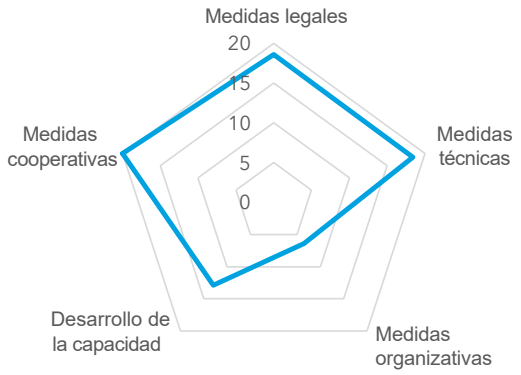
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas, cooperativas
Área(s) de posible crecimiento
Medidas organizativas, Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,32	20,00	20,00	18,98	18,34	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Rumania



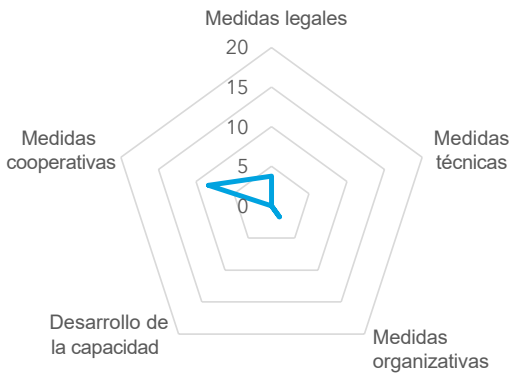
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
76,29	18,60	18,40	6,42	12,88	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

San Marino (República de)



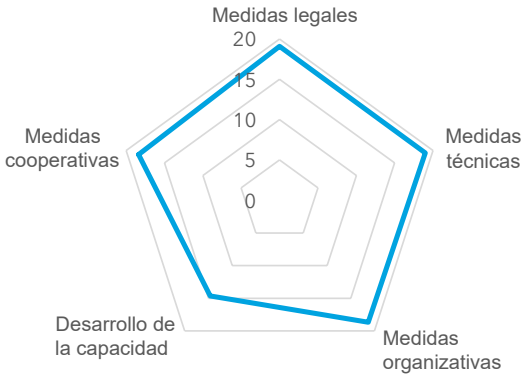
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas técnicas,
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
13,83	3,77	0,00	1,69	0,00	8,37

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Serbia (República de)



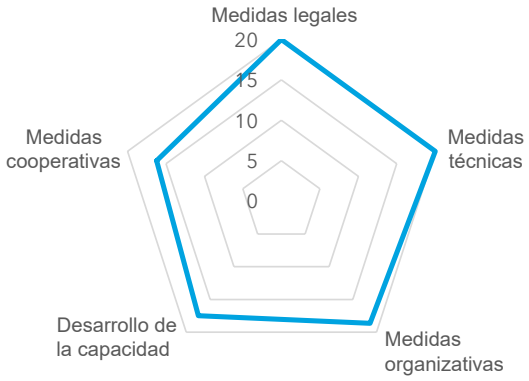
Nivel de desarrollo:
País desarrollado

Área(s) de fortaleza relativa
Medidas legales, técnicas,
organizativas, cooperativas
Área(s) de posible crecimiento
Desarrollo de la capacidad

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
89,80	19,10	18,99	18,67	14,66	18,38

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

República Eslovaca



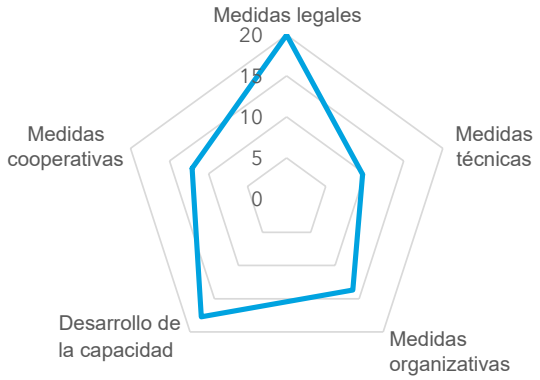
Nivel de desarrollo:
País desarrollado,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, técnicas
Área(s) de posible crecimiento
Medidas cooperativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
92,36	20,00	20,00	18,64	17,50	16,22

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Eslovenia (República de)



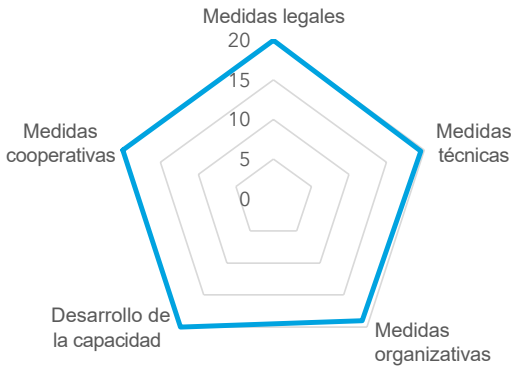
Nivel de desarrollo
País desarrollado

Área(s) de fortaleza relativa
Medidas legales
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
73,27	20,00	11,38	13,71	17,72	12,11

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

España



Nivel de desarrollo:
País desarrollado

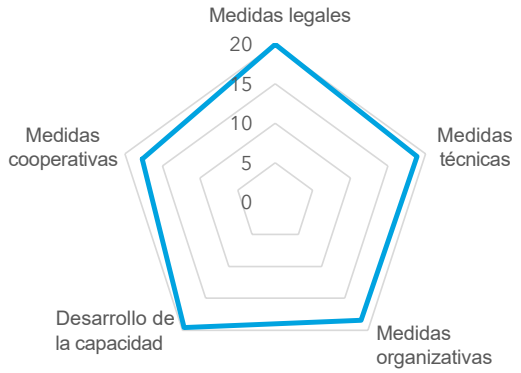
Área(s) de fortaleza relativa
Medidas legales, cooperativas, Desarrollo de la capacidad, Medidas técnicas

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
98,52	20,00	19,54	18,98	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Suecia



Nivel de desarrollo:
País desarrollado

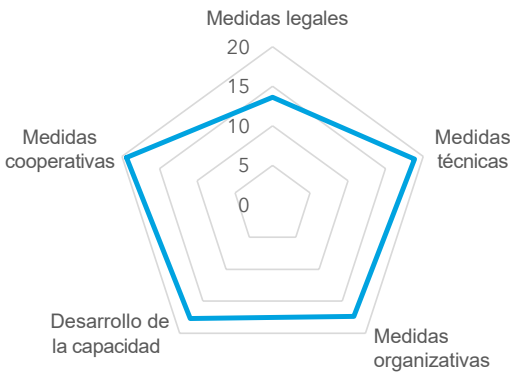
Área(s) de fortaleza relativa
Medidas legales

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
94,59	20,00	18,86	18,46	19,57	17,70

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Suiza (Confederación de)***



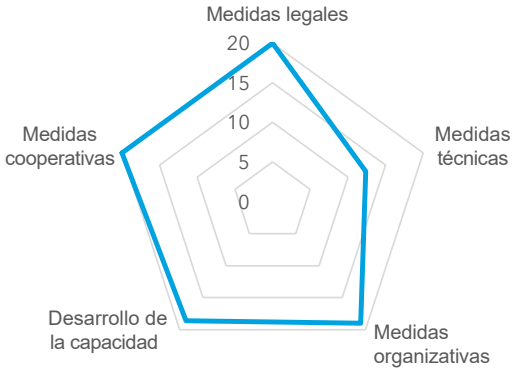
Nivel de desarrollo:
País desarrollado,
País sin litoral

Área(s) de fortaleza relativa
Medidas técnicas,
Medidas cooperativas
Área(s) de posible crecimiento
Medidas legales

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
86,97	13,62	18,85	17,40	17,69	19,41

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Macedonia del Norte (República de)



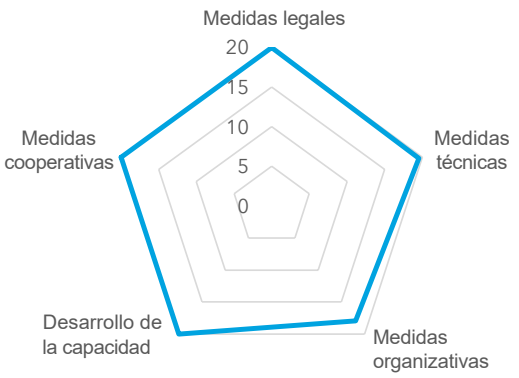
Nivel de desarrollo:
País desarrollado,
País sin litoral

Área(s) de fortaleza relativa
Medidas legales, cooperativas
Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
89,92	20,00	12,37	18,98	18,57	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Turquía



Nivel de desarrollo:
País en desarrollo

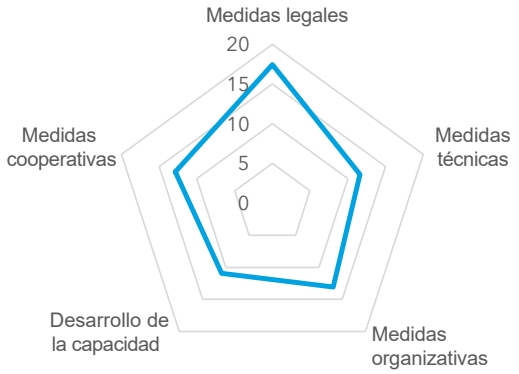
Área(s) de fortaleza relativa
Medidas legales, cooperativas, técnicas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
97,50	20,00	19,54	17,96	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Ucrania



Nivel de desarrollo:
País desarrollado

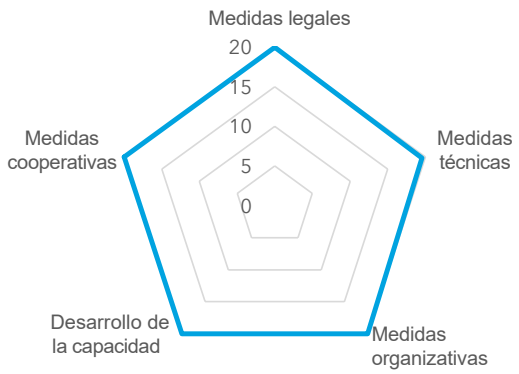
Área(s) de fortaleza relativa
Medidas cooperativas

Área(s) de posible crecimiento
Medidas legales

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
65,93	17,46	11,60	13,06	10,94	12,87

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

Reino Unido de Gran Bretaña e Irlanda del Norte



Nivel de desarrollo
País desarrollado

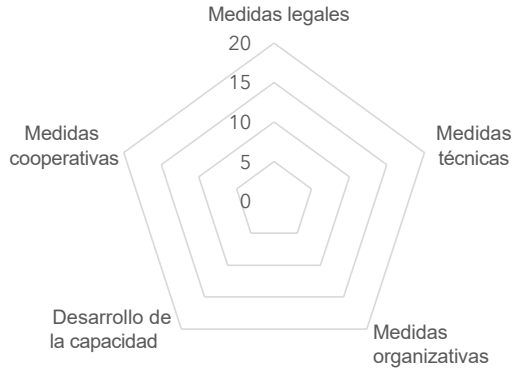
Área(s) de fortaleza relativa
Medidas legales, organizativas, cooperativas, Desarrollo de la capacidad

Área(s) de posible crecimiento
Medidas técnicas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
99,54	20,00	19,54	20,00	20,00	20,00

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

*Vaticano**



Nivel de desarrollo:
País desarrollado,
País sin litoral

Área(s) de fortaleza relativa
N/A

Área(s) de posible crecimiento
N/A

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
0	0	0	0	0	0

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

** Sin respuesta al cuestionario/datos recabados por el Equipo ICG

* Sin datos

Glosario

Abreviatura	Definición
APP	Asociación público-privada
CI	Infraestructuras esencial
DPP	Protección de datos y privacidad
EIEI	Equipo de intervención en caso de emergencia informática, marca registrada por la Universidad Carnegie Mellon
EIII*	Equipo de intervención en caso de incidente Informático, *ver términos relacionados CSIRTs, CERTs*
EIISI	Equipo de intervención en caso de incidente de seguridad informática
ENC	Estrategia Nacional de Ciberseguridad
GCI-1/2/3/4	Versión del Índice de Ciberseguridad Global
GDPR	Reglamento general de protección de datos (UE)
MIPYME	Microempresas, pequeñas y medianas empresas
MLAT	Tratado de asistencia jurídica mutua
ODC	Otros países en desarrollo
ONG	Organización no gubernamental
ONU	Naciones Unidas
OT	Tecnología operativa
PDSL	Países en desarrollo sin litoral
PEID	Pequeños Estados Insulares en Desarrollo
PMA	Países menos adelantados
PYME	Pequeñas y medianas empresas
TIC	Tecnología de la información y la comunicación
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones

Anexo A: Metodología

A1 Ámbito y marco del ICG

El mandato del Índice Mundial de Ciberseguridad (GCI) se deriva de la Resolución 130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios de la UIT relativa al Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC). En concreto, se invita a los países *a "a apoyar las iniciativas de la UIT sobre ciberseguridad, incluido el Índice de Ciberseguridad Global, con el fin de promover las estrategias gubernamentales y el intercambio de información acerca de los esfuerzos en todas las industrias y sectores*". El objetivo del ICG es fomentar una cultura global de ciberseguridad y su integración en el núcleo de las TIC.

Cuadro A1: Participación en el Índice de Ciberseguridad Global y años en los que se han recabado datos

	GCI-1	GCI-2	GCI-3	GCI-4
Países que han designado un coordinador	105	136	155	169
Años en que se recopilaron datos	2013-2014	2016	2017-2018	2020
Año de publicación	2015	2017	2019	2021

El ICG se obtiene de los datos facilitados por los Miembros de la UIT, incluidos particulares interesados, expertos y actores del sector que constituyen asociados colaboradores con el Instituto de Política Estratégica de Australia, FIRST (Foro de Respuesta a Incidentes y Equipo de Seguridad), la Universidad de Grenoble (Francia), la Universidad de Indiana, INTERPOL, el Centro de Ciberseguridad UIT para la Región Árabe en Omán, la Agencia de Internet y Seguridad de Corea, ANRT de Egipto, Red Team Cyber, el Instituto Potomac de Estudios Políticos, UNICRI, la Universidad de Tecnología de Jamaica, la ONUDD y el Banco Mundial.

Ámbito de aplicación del ICG

El Índice de Ciberseguridad Global (ICG) es un índice compuesto de indicadores, que evoluciona en cada iteración, y que sirve para determinar el nivel de compromiso con la ciberseguridad con arreglo a los cinco pilares de la Agenda de Ciberseguridad Global (ACG), y cuyos principales objetivos son medir:

- El tipo, el nivel y la evolución del grado de compromiso con la ciberseguridad dentro de los países y en relación con otros países.
- El progreso del compromiso de los países con la ciberseguridad desde una perspectiva global.
- El progreso del compromiso con la ciberseguridad desde una perspectiva regional.
- La brecha en el compromiso con la ciberseguridad (es decir, la diferencia entre los países en cuanto a su nivel de compromiso con las iniciativas de ciberseguridad).

El objetivo del ICG es ayudar a los países a determinar los aspectos susceptibles de mejora en el campo de la ciberseguridad e instarles a tomar medidas al respecto. De este modo, se contribuye a elevar el nivel general de compromiso con la ciberseguridad en todo el mundo, a armonizar las prácticas y a fomentar una cultura global de ciberseguridad. El ICG tiene por objeto aportar ejemplos exitosos en materia de ciberseguridad que puedan servir de buenas prácticas y directrices a países con entornos nacionales similares.

A2 Marco de cooperación en materia de ciberseguridad de la UIT

La ciberseguridad es un campo que abarca múltiples disciplinas y su aplicación implica a todos los sectores, industrias y partes interesadas, tanto vertical como horizontalmente. A fin de aumentar la capacitación en el plano nacional, es indispensable que se impliquen las fuerzas políticas, económicas y sociales, ya sea mediante las fuerzas del orden, los departamentos de justicia, las instituciones docentes, los ministerios, los operadores del sector privado, los creadores de tecnología, las asociaciones público-privadas y la cooperación intraestatal.

El marco de la UIT para la cooperación multipartita internacional en materia de ciberseguridad tiene por objeto crear sinergias entre las iniciativas presentes y futuras y se articula en torno a los siguientes cinco pilares, que constituyen los componentes básicos inherentes a una cultura nacional de ciberseguridad.

Cuadro A2: Descripción de los pilares del ICG 2020

Medidas jurídicas	
	Medidas basadas en la existencia de marcos jurídicos relativos a la ciberseguridad y la ciberdelincuencia.
	Las medidas jurídicas (como legislación, reglamentación y normativa contra el spam) autorizan al estado a establecer mecanismos básicos de respuesta mediante la investigación y el enjuiciamiento de los delitos y la imposición de sanciones por incumplimiento o infracción de la ley. El marco legislativo establece los fundamentos mínimos de actuación sobre los que se asientan otras capacidades de ciberseguridad. Esencialmente, el objetivo es disponer de una legislación suficiente que permita armonizar las prácticas a escala regional e internacional y simplificar la lucha internacional contra la ciberdelincuencia.
Medidas técnicas	
	Medidas basadas en la existencia de instituciones y marcos técnicos que se ocupan de la ciberseguridad.
	El desarrollo y utilización eficiente de las TIC sólo puede prosperar en un entorno de confianza y seguridad. Por consiguiente, los países deben crear y aplicar criterios mínimos de seguridad y regímenes de acreditación aceptados para las aplicaciones y sistemas informáticos. Estos esfuerzos deben complementarse con la implantación de un organismo nacional que se ocupe de los incidentes cibernéticos, una entidad gubernamental autorizada y un marco nacional para vigilar, advertir y responder a los incidentes.
Medidas institucionales	

Cuadro A2: Descripción de los pilares del ICG 2020 (continuación)

	Medidas basadas en la existencia de instituciones, políticas y estrategias de coordinación para el desarrollo de la ciberseguridad en el plano nacional.
	Las medidas institucionales consisten en determinar los planes estratégicos y los objetivos de ciberseguridad, así como en definir de manera oficial las funciones institucionales, las responsabilidades y la rendición de cuentas para garantizar su aplicación. Estas medidas son indispensables para refrendar la elaboración y aplicación de una postura eficaz de ciberseguridad. Es necesario que el Estado establezca objetivos y metas estratégicas amplias, además de un plan integral en para la aplicación, ejecución y medición. Los organismos nacionales deben estar representados para aplicar la estrategia y evaluar los resultados. Sin una estrategia nacional, un modelo de gobernanza y un organismo de supervisión, los esfuerzos de los distintos sectores entran en conflicto, lo que impide lograr una armonización eficaz en el desarrollo de la ciberseguridad.
Medidas de capacitación	
	Medidas basadas en la existencia de programas de investigación y desarrollo, educación y formación, profesionales certificados y organismos del sector público encargados de fomentar la capacitación.
	La capacitación consiste en campañas de sensibilización pública, la creación de marco de certificación y acreditación de los profesionales de la ciberseguridad, cursos de formación profesional en ciberseguridad, programas educativos o planes de estudios académicos, etc. Este pilar es intrínseco a los tres primeros (jurídico, técnico e institucional). La ciberseguridad suele abordarse desde una perspectiva tecnológica, pese a que son numerosas las repercusiones socioeconómicas y políticas. Reforzar las capacidades humanas e institucionales resulta esencial para la sensibilización y los conocimientos teóricos y prácticos en todos los sectores, para encontrar soluciones sistemáticas y adecuadas, y para promover la formación de profesionales cualificados.
Medidas de cooperación	
	Medidas basadas en la existencia de asociaciones, marcos de cooperación y redes de intercambio de información.
	La interconexión entre los Estados ha alcanzado niveles sin precedentes, por lo que la ciberseguridad es una responsabilidad colectiva y un reto transnacional. La mayor cooperación permitirá desarrollar capacidades de ciberseguridad mucho más sólidas, reduciéndose así los riesgos cibernéticos y mejorando además la investigación, arresto y enjuiciamiento de los malhechores.

A3 Principales cambios, desglosados por pilar

Medidas jurídicas

Las medidas jurídicas evalúan las intervenciones jurídicas en el ámbito de la ciberseguridad y se han actualizado para que se correspondan mejor con el derecho sustantivo nacional relacionado con la ciberseguridad.

- En virtud de las recomendaciones del Grupo Consultivo de la Dirección de la BDT, el Índice de Ciberseguridad Global ya no mide el derecho procesal. En su lugar, se insisten en una mayor claridad en diversas esferas, como la usurpación de identidad, el acoso en línea o el racismo.
- Las preguntas relativas a las medidas jurídicas se elaboraron inicialmente conforme a las recomendaciones de convenios tales como el de Budapest sobre la ciberdelincuencia. Sin embargo, las respuestas se ciñen ahora en destacar únicamente las leyes nacionales

aplicadas, y ya no recogen la ratificación de dichos convenios. No obstante, dada la importancia de los convenios internacionales y su papel en la creación de compromisos vinculantes, los convenios internacionales como el Convenio de Budapest se consideran ahora en el marco de las actividades de cooperación internacional.

- Con el aumento de personas en línea, y a fin de crear un ciberespacio de confianza que además promueva la diversidad y la inclusión, resulta indispensable examinar cuestiones tales como la privacidad, el acoso, la intimidación, la corrupción de menores, la pornografía infantil y el racismo. En esta versión del Índice de Ciberseguridad Global se ha añadido preguntas sobre estos temas.

Medidas técnicas

El pilar técnico se ha reestructurado para que se corresponda mejor con el funcionamiento de los EIII, en particular:

- Equipo de intervención en caso de incidente informático - Los EIII gubernamentales y nacionales se han combinado en un único indicador.
- La certificación de los EIII es un factor importante para determinar la capacidad de hacer frente a los incidentes cibernéticos. Para evaluar los niveles de madurez[1] de los EIII nacionales, se añadió el sistema de certificación SIM3. El TF-CSIRT/Trusted Introducer utiliza el SIM3 para la evaluación y los miembros "certificados" tienen el mayor grado de madurez. En las futuras ediciones del Índice de Ciberseguridad Global se profundizará en la exploración de los modelos de madurez de seguridad para los EIII.

Medidas institucionales

- Dado que la ciberseguridad es un proceso continuo, se insta a los países a volver a examinar y revisar periódicamente las estrategias nacionales de ciberseguridad (al menos una vez cada cinco años) para evaluar si la ENC sigue siendo pertinente en vista de la evolución del entorno de riesgo, si continúa estando en consonancia con los objetivos nacionales y qué ajustes son necesarios. Habida cuenta de esta recomendación, los países que no han reafirmado o actualizado su ENC en los últimos cinco años recibieron una puntuación reducida en los indicadores sobre ENC.
- El desarrollo de mecanismos para proteger a los niños en línea debería ser una de las principales prioridades de los países, especialmente ahora que los niños se han visto obligados a estudiar en línea debido a la pandemia de la COVID-19. Si bien Internet presenta importantes ventajas para la educación y el crecimiento de los niños, también los expone a riesgos en línea. La mayoría de los países han emprendido iniciativas para la protección de la infancia en línea que consisten, por ejemplo, en la creación de sitios web y redes sociales con material educativo especializado, juegos informativos y guías para niños, padres y educadores. Para distinguir entre las intervenciones *ad hoc* y las estructuradas integradas en una estrategia más amplia y definida, se concedió a estas últimas la máxima puntuación, mientras que los países con iniciativas puntuales o esporádicas recibieron una puntuación reducida.

Medidas de capacitación

Este pilar se ha mantenido estable con sus indicadores desde la segunda edición del ICG. En la presente edición, se amplió su alcance para incluir la sensibilización acerca de la necesidad de que los gobiernos apoyen a las pequeñas y medianas empresas (PYME), por cuanto desempeñan un papel importante en la economía digital y las cadenas de suministro, especialmente en este

[1] También conocidos como EIISI/EIDI, los EIII son entidades institucionales a las que se les asigna la responsabilidad de coordinar y ayudar en la respuesta a problemas o incidentes de seguridad informática a escala nacional.

período de evolución hacia el comercio electrónico, por lo que las PYME necesitan ayuda en la gestión de riesgos cibernéticos.

Medidas de cooperación

Este pilar se refiere a si la firma o ratificación de acuerdos, con independencia de si son jurídicamente vinculantes. Se han aclarado lo que se entiende por acuerdos bilaterales y multilaterales. El Convenio de Budapest, que antes se consideraba un acuerdo multilateral, se considera ahora una actividad internacional.

A4 Metodología de cálculo

El cuestionario utilizado para el ICG asigna un valor a cada uno de los 20 indicadores construidos a través de 82 preguntas. Así se consigue el nivel de granularidad requerido y se mejora la exactitud y la calidad de las respuestas. Los indicadores se encuentran en el Cuestionario ICG (Anexo B).

Los indicadores utilizados para calcular el ICG se seleccionaron en función de:

- su relevancia para los cinco pilares de la GCA;
- su relevancia para el marco conceptual y los principales objetivos del ICG;
- la disponibilidad y la calidad de los datos; y
- la posibilidad de verificación cruzada mediante datos secundarios.

El ICG se basa en un mapa de desarrollo de la ciberseguridad que los países pueden tener en cuenta a la hora de mejorar su compromiso con la ciberseguridad. El cuestionario se articula en torno a cinco pilares diferentes que se diferencian con cinco colores distintos. En los gráficos de este informe, cuanto mayor es la trayectoria, mayor es el nivel de desarrollo del compromiso.

Este informe describe las tendencias regionales y mundiales. En aras de la exactitud, se pidió a los países que adjuntaran a su respuesta documentos o una dirección URL, mediante una función de transmisión. En cada pilar se ha añadido una sección de comentarios para que los países puedan facilitar buenas prácticas que expliquen cómo ha evolucionado su ciberseguridad.

Para cada una de las 82 preguntas de los 20 indicadores de los 5 pilares, los países pudieron elegir entre dos o tres respuestas, y utilizar la sección de comentarios para explicar en qué fase de proyecto o implementación se encuentra un determinado aspecto pendiente.

Una vez recibidos los cuestionarios, se les sometió a dos procesos de validación diferentes y, en caso de que la respuesta se refiriera a un aspecto en proyecto o en fase de implementación, o si no respondió concretamente a todos los aspectos de la pregunta, se asignó una puntuación reducidos. Este modo de evaluación ternaria evita realizar evaluaciones basadas subjetivas o de opinión mediante un cuadro con aspectos específicos que se han de cumplir para que las respuestas se consideren positivas o parciales.

A tal efecto, la Secretaría de la BDT presentó la cuarta edición del cuestionario del Índice de Ciberseguridad Global, y toda la documentación correspondiente, durante la reunión del Grupo Relator para la Cuestión 3 de la Comisión de Estudio 2, de octubre de 2019, en la que se aprobó el cuestionario antes de su distribución. En marzo de 2020, con ocasión de la reunión de la CE2, la BDT actualizó la Cuestión 3 y pidió a los países que designaran expertos en el ámbito de la ciberseguridad para que participaran en el proceso de distribución de ponderaciones.

Proceso general del ICG

1) Se envía una carta de invitación a todos los Estados Miembros de la UIT y al Estado de Palestina, informándoles de la iniciativa y solicitando un coordinador responsable de recopilar todos los datos pertinentes y responder al cuestionario del ICG en línea. Durante la encuesta en línea, el la UIT invita oficialmente al coordinador designado a responder al cuestionario.
2) Recopilación de datos primarios (para los países que no responden al cuestionario):

    - La UIT elabora un proyecto inicial de respuesta al cuestionario utilizando datos disponibles públicamente e investigaciones en línea.
    - El proyecto de cuestionario se envía a los coordinadores para su revisión.
    - Los coordinadores corrigen las respuestas y devuelven el borrador del cuestionario.
    - El proyecto de cuestionario corregido se envía a cada coordinador para su aprobación final.
    - El cuestionario validado se utiliza para el análisis, la puntuación y la clasificación.

3) Recopilación de datos secundarios (para los países que responden al cuestionario):

    - La UIT identifica las respuestas que faltan, la documentación justificante, los enlaces, etc.
    - El coordinador corrige, si procede, las respuestas.
    - El proyecto de cuestionario corregido se envía a cada coordinador para su aprobación final.
    - El cuestionario validado se utiliza para el análisis, la puntuación y la clasificación.

Nota: Si un país no designa a un punto coordinador el cuestionario del ICG, la UIT se pondrá en contacto con el coordinador institucional en el Directorio Global de la UIT.

Ponderación

A diferencia de las ediciones anteriores, cuya escala era de 0 a 1, la presente edición del ICG tiene una escala de 0 a 100 y a cada pilar se le asigna una ponderación de 20 puntos.

Al tratarse de un índice ponderado compuesto, a cada indicador, subindicador y microindicador se le asigna una ponderación en función de su importancia relativa para el grupo de indicadores. La ponderación puede tener un repercutir considerablemente en la puntuación final y la clasificación obtenida variará según la técnica empleada.

Para el ICG se ha adoptado un método participativo, utilizando la técnica de proceso de asignación presupuestaria (PAB). En esta técnica se considera que las ponderaciones son, fundamentalmente, juicios de valor, y por ende, se han de tener en cuenta muy diversas aportaciones de expertos.

Según la técnica de asignación presupuestaria, los expertos disponen de un "presupuesto" dado que pueden asignar a un grupo de indicadores, de modo que asignan mayor cantidad a los indicadores que se consideran más importantes. Se pidió a los expertos que formularan recomendaciones sobre la ponderación para los pilares de su competencia.

Como todas las respuestas de los países se basan los datos derivados de encuestas y verificados por el equipo de la UIT, en la ponderación no se tiene en cuenta la calidad estadística de los datos.

Participación del grupo de expertos en ponderación

En octubre de 2020, se invitó mediante circular a los Estados Miembros de la UIT y a los Miembros del sector privado, a designar expertos para participar en esta edición del Índice de Ciberseguridad Global. Los expertos designados pertenecían a instituciones académicas, grupos de reflexión, ministerios de TIC, reguladores y organizaciones de normalización.

También se invitó a los expertos que participaron las ediciones anteriores del Índice de Ciberseguridad Global a que formularan recomendaciones en materia de ponderación.

En total participaron 84 expertos, a los que se pidió que formularan recomendaciones sobre la ponderación para los pilares de su competencia.

Combinación

Los grupos de indicadores se combinaron utilizando la media aritmética ponderada. Es decir, un país con una puntuación baja en un ámbito puede recuperar parte de su puntuación en otro ámbito.

Como se señala en el Manual de Índices Compuestos de la OCDE, *"la utilidad marginal de un aumento de la puntuación absoluta baja sería mucho mayor que la de una puntuación absoluta alta con una combinación geométrica. En consecuencia, los países tendrían un gran incentivo para mejorar aquellos sectores/actividades/alternativas cuya puntuación ha sido baja si la combinación fuera geométrica en lugar de lineal"* (33). Sin embargo, en aras de la claridad y la comprensión, se consideró que un enfoque lineal era más comprensible y viable.

Análisis de la sensibilidad

Habida cuenta de la importancia de la ponderación en las puntuaciones finales de los países, se realizaron análisis de la sensibilidad, en particular:

- la inclusión/exclusión de indicadores individuales;
- diferentes criterios de ponderación (ponderación equitativa, método de asignación presupuestaria, extremos de las recomendaciones de los expertos);
- diferentes sistemas de combinación (promedios ponderados, agregados).

Clasificación

Los países se han clasificado por su puntuación final, utilizando un método de clasificación "denso", a saber, los países con puntuaciones iguales obtienen la misma clasificación y el siguiente país, después de dos o más países con la misma puntuación, recibe el siguiente número ordinal.

Anexo B: Cuestionario del Índice de Ciberseguridad Global (4ª edición)

El presente cuestionario han sido preparado y examinado en la reunión del Grupo de Relator para la Cuestión 3/2 del UIT-D: Seguridad en las redes de información y comunicación: buenas prácticas para el desarrollo de una cultura de ciberseguridad. En la reunión se pidió la aprobación por los Estados Miembros para publicar la 4ª edición del Índice de Ciberseguridad Global de la UIT.

El presente cuestionario está dividido en cinco secciones. Las preguntas de todas las secciones deben contestarse con sí o no, marcando las casillas correspondientes. El cuestionario fue concebido para rellenarlo en línea. Se envió a cada participante una dirección URL personal (por correo electrónico oficial de la UIT) y con la información para abrir la sesión para responder a las preguntas.

Los participantes también tienen la opción de colgar documentos pertinentes (y direcciones URL) para cada pregunta, que servirán de información complementaria. No está previsto que las respuestas al cuestionario facilitadas por los participantes sean confidenciales.

Cuadro B1: Cuestionario ICG – Medidas jurídicas

1 Legislación sustantiva en materia de ciberdelincuencia

Explicación: Legislación sustantiva alude a derecho público o privado, incluido el derecho de los contratos, patrimonio inmobiliario, delitos civiles, testamentos y leyes penales que crean, definen y regulan derechos.

1.1 ¿Dispone de legislación sustantiva sobre comportamientos ilegales en línea?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.1 ¿Dispone de legislación sustantiva sobre acceso ilegal a dispositivos, sistemas informáticos y datos?

Explicación: **Acceso** – capacidad y medios para comunicar con un sistema o interactuar con él; para utilizar los recursos del sistema para manejar información, conocer la información que contiene el sistema o controlar sus componentes y funciones (NICCS).

Sistema informático o **sistema** – un aparato o grupo de aparatos interconectados o relacionados en que uno o varios de ellos llevan a cabo, con arreglo a un programa, el procesamiento automático de datos (COE – Convention on Cybercrime).

Datos informáticos – toda representación de hechos, información o conceptos de una forma que permita su procesamiento en un sistema informático, incluido un programa capaz de provocar que un sistema informático realice una función (COE – Convention on Cybercrime).

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B1: Cuestionario ICG – Medidas jurídicas (continuación)

1.1.2 ¿Dispone de legislación sustantiva sobre la injerencia ilegal (mediante ingreso, alteración o supresión de datos) en dispositivos, datos y sistemas informáticos?

Explicación: Injerencia en sistemas informáticos – perturbación grave, intencionada y no autorizada del funcionamiento de un sistema informático. Comprende el ingreso, la transmisión, el daño, la eliminación, el deterioro, la alteración o la supresión de datos informáticos.

Injerencia en datos – dañar, eliminar, deteriorar, alterar o suprimir datos informáticos de manera intencionada o no autorizada.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.3 ¿Dispone de legislación sustantiva sobre intercepción ilegal de dispositivos, sistemas *informáticos y datos?*

Explicación: Intercepción ilegal – transmisión intencionada, no autorizada y no pública de datos informáticos desde o en un ordenador u otro tipo de sistema electrónico por medios técnicos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.4 ¿Dispone de legislación sustantiva sobre robo de datos e identidades?

Explicación: Robo de identidad en línea – robo de la información personal, como el nombre, la dirección, la fecha de nacimiento, la información de contacto o la cuenta bancaria. Puede ocurrir como resultado de peska, pirateo de cuentas en línea, extracción de información de medios sociales o acceso ilegal a bases de datos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.2 ¿Hay disposiciones sobre falsificación informática (piratería/violación de derechos de autor)?

Explicación: Ingreso, alteración o eliminación no autorizados de datos informáticos que corrompe su veracidad para hacerlos valer como auténticos con fines jurídicos a fin de perpetuar actos fraudulentos o deshonestos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.3 ¿Dispone de legislación sustantiva sobre seguridad en línea?

Explicación: Seguridad en línea – maximizar la seguridad de Internet frente a los diversos riesgos a que se expone la información privada y personal o relativa a la propiedad, mejorando también la protección de los usuarios contra los ciberdelitos.

Cuadro B1: Cuestionario ICG – Medidas jurídicas (continuación)

1.3.1 ¿Hay disposiciones/medidas jurídicas contra los delitos relacionados con el material racista y xenófobo en línea?

Explicación: Medidas para prevenir distintas formas de odio en línea y otro tipo de intolerancia por raza, color, religión, origen, nacionalidad o etnia, orientación sexual, identidad de género, discapacidad, clase social, etc.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.3.2 ¿Hay disposiciones/medidas jurídicas contra el acoso en línea y el abuso contra la dignidad/integridad personal?

Explicación: Ciberacoso – mensajes enviados por correo electrónico, mensajería o sitios web destinados a acosar a una persona o grupo de personas con ataques personalizados.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.3.3 ¿Existe legislación relativa a la protección de menores en Internet?

Explicación: Se refiere a un cuerpo de leyes que estipule que todos los delitos que pueden cometerse contra un menor en el mundo real pueden también cometerse, mutatis mutandis, en Internet o en cualquier otra red electrónica. Es necesario elaborar leyes nuevas o adaptar las existentes para ilegalizar determinados comportamientos que sólo pueden producirse en Internet, como por ejemplo instigar a menores a realizar o ver actos sexuales o captar a menores para encontrarse con ellos en el mundo real con fines sexuales (UIT, Directrices destinadas a las instancias decisorias sobre la protección de los niños en el ciberespacio).

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2 ¿Existen leyes o reglamentos sobre ciberseguridad en materia de...

Explicación: Los reglamentos son normas basadas en textos legislativos determinados que prevén la ejecución de estos. Por lo general, son aplicados por agencias reguladoras creadas o encargadas de ejecutar las disposiciones de una ley.

Por tanto, la regulación sobre ciberseguridad se refiere a principios que deben respetar los diferentes interesados, que emanan y forman parte de la aplicación de leyes sobre protección de datos, notificación de infracciones, requisitos de certificación/normalización, aplicación de medidas de ciberseguridad, criterios para auditorías de ciberseguridad, protección de privacidad, protección de menores en línea, firmas digitales, transacciones electrónicas y obligaciones de los proveedores de servicios de Internet.

Cuadro B1: Cuestionario ICG – Medidas jurídicas (continuación)

2.1 ¿Protección de datos personales/privacidad?

Explicación: Reglamentación sobre protección de datos personales contra el acceso, la alteración, la destrucción o la utilización no autorizados. La privacidad en Internet se refiere al nivel de seguridad de los datos personales que se publican en línea. Se trata de un concepto amplio, que abarca muchos factores, técnicas y tecnologías empleados para proteger datos sensibles y privados, comunicaciones y preferencias. Como ejemplo cabe citar la Ley de protección de datos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.2 ¿Notificación de infracciones/incidentes de datos?

Explicación: Las leyes y reglamentos sobre notificación de infracciones son aquellos que prevén que una entidad víctima de una infracción lo notifique a las autoridades, sus clientes y terceras partes, y que tome las medidas necesarias para reparar los daños causados. Estas leyes se promulgan para responder a la creciente cantidad de infracciones en bases de datos de clientes que contienen información de identificación personal.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.3 ¿Requisitos para auditorías de ciberseguridad?

Explicación: Por auditoría de seguridad se entiende la evaluación sistemática y periódica de la seguridad de un sistema de información. Generalmente incluye una evaluación de la seguridad de la configuración física del sistema y entorno, el software, los procesos de administración de la información y las prácticas de los usuarios.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.4 ¿Aplicación de las normas?

Explicación: Existencia de uno o varios marcos aprobados (o respaldados) por el gobierno para la aplicación de normas de ciberseguridad reconocidas a nivel internacional dentro del sector público (agencias gubernamentales), e integrados en la infraestructura crítica (incluso si los ejecuta el sector privado). Estas normas incluyen, entre otras, las elaboradas por las agencias siguientes: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B1: Cuestionario ICG – Medidas jurídicas (continuación)

2.5 ¿Identificación y protección de infraestructuras informáticas esenciales a nivel nacional?

Explicación: Las infraestructuras esenciales son sistemas fundamentales para la seguridad, seguridad económica y salud pública de una nación. Pueden incluir, entre otros, sistemas de defensa, banca y finanzas, telecomunicaciones, transporte, salud, energía, etc. Adjúntese enlaces o documentos que describan las infraestructuras esenciales o documentos/noticias que confirmen su definición.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de esferas jurídicas asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad.

Utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración.

O demuestre con documentos con enlaces.

Cuadro B2: Cuestionario ICG – Medidas técnicas

1 EIII/EIISI/EIEI nacionales/gubernamentales

Explicación: EIII/EIISI/EIEI: los equipos de intervención en caso de incidente informático son entidades a cuyo personal se asigna la responsabilidad de coordinar y dar apoyo a las intervenciones en caso de eventos o incidentes de seguridad informática a nivel nacional o gubernamental.

NOTA: En ocasiones hay que distinguir los EIII nacionales de los gubernamentales: los EIII gubernamentales intervienen en los organismos gubernamentales y los EIII nacionales prestan servicio a toda la población, incluido el sector privado y los particulares. En ocasiones se consideran una misma entidad.

1.1 ¿Existe un EIII/EIISI/EIEI nacional/gubernamental?

Explicación: Respaldado por una decisión gubernamental o integrado en estructuras gubernamentales.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.2 Su EIII/EIISI/EIEI nacional gubernamental …

1.2.1 ¿Prepara y lleva a cabo actividades de sensibilización en materia de ciberseguridad?

Explicación: Campañas publicitarias de gran alcance sobre el comportamiento seguro en línea.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B2: Cuestionario ICG – Medidas técnicas (continuación)

1.2.2 ¿Realiza periódicamente ejercicios de ciberseguridad, como cibersimulacros?

Explicación: Actividades durante las que una entidad simula un ciberataque a fin de desarrollar o poner a prueba competencias en materia de prevención, detección, mitigación, respuesta o recuperación tras el ataque. ¿Se organiza el ejercicio periódicamente o en varias ocasiones?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.2.3 ¿Emite avisos públicos?

Explicación: Avisos EIII: publicación de información sobre ciberamenazas inminentes y sobre el comportamiento recomendado.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.2.4 ¿Participa en la Protección de la Infancia en Línea?

Explicación: El EIII/EIISI/EIEI presta su apoyo con campañas de sensibilización, comunicando incidentes relacionados con los niños, ofreciendo material docente sobre la Protección de la Infancia en Línea, etc.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.3 ¿Está el EIII (EIISI o EIEI) afiliado a FIRST?

Explicación: Miembro titular o de enlace del Foro sobre los equipos de seguridad y respuesta ante incidentes. www.first.org

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.4 ¿Está el EIII (EIISI o EIEI) afiliado a otras comunidades de EIEI (EIEI regionales)?

Explicación: Cualquier relación oficial u oficiosa con otros EIEI de dentro o fuera del país, miembro de algún grupo de EIEI regional. Ejemplos de EIEI regionales son APCERT, AFRICACERT, EGC, OIC y OAS.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B2: Cuestionario ICG – Medidas técnicas (continuación)

1.5 ¿Cuenta con certificación TF-CSIRT-SIM3 la evolución de los servicios EIII, EIISI y EIEI anteriormente mencionados?

***Explicación**:* SIM3 es el fundamento de la certificación de EIII.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2 EIII/EIISI/EIEI sectoriales

Explicación: Los EIII/EIISI/EIEI sectoriales responden a incidentes de seguridad informática o ciberseguridad que afectan a un sector determinado. Se suelen crear para sectores tan importantes como el sanitario, las infraestructuras públicas, las instituciones académicas los servicios de emergencia y el sector financiero. Los EIEI sectoriales trabajan con agencias de un único sector.

2.1 ¿Hay en su país EIII/EIISI/EIEI sectoriales?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.2 Sus EIII/EIISI/EIEI sectoriales:

2.2.1 ¿Preparan y llevan a cabo actividades de sensibilización para un sector?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.2.2 ¿Participan activamente en los cibersimulacros nacionales?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.2.3 ¿Dan a conocer los incidentes acaecidos en el sector?

Explicación: Publicación de información sobre ciberamenazas inminentes y sobre el comportamiento recomendado.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3 Marco nacional para la aplicación de las normas de ciberseguridad

Explicación: Existencia de uno o varios marcos aprobados por el gobierno para la aplicación de normas de ciberseguridad reconocidas a nivel internacional dentro del sector público (agencias gubernamentales), e integrados en la infraestructura esencial (incluso si los ejecuta el sector privado). Estas normas incluyen, entre otras, las elaboradas por las agencias siguientes: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

Cuadro B2: Cuestionario ICG – Medidas técnicas (continuación)

3.1 ¿Existe un marco para la aplicación/adopción de las normas de ciberseguridad?

□ *Sí*

□ *No*

Proporcione enlaces/URL

Proporcione documentos

3.2 ¿Incluye el marco normas internacionales o de otro tipo conexas?

Explicación: UIT-T, ISO/CEI, NIST, ANSI/ISA, etc.

□ *Sí*

□ *No*

Proporcione enlaces/URL

Proporcione documentos

4 Protección de la Infancia en Línea

Explicación: Este indicador mide la existencia de una agencia nacional dedicada a la Protección de la Infancia en Línea; la disponibilidad de un número de teléfono nacional para denunciar problemas relacionados con la infancia en línea; la inversión de medios y capacidades técnicos para proteger a la infancia en línea, y la ejecución de actividades por el gobierno o entidades no gubernamentales para dar información y ayudar a los interesados a proteger a la infancia en línea y comunicarles los números de teléfonos, direcciones de correo electrónico, páginas web, etc. donde pueden denunciar problemas o incidentes relacionados con la Protección de la Infancia en Línea (PIeL).

4.1 ¿Hay en pie mecanismos o capacidades de comunicación para proteger a la infancia en línea?

Explicación: Números gratuitos, líneas de ayuda, etc.

□ *Sí*

□ *No*

Proporcione enlaces/URL

Proporcione documentos

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de esferas jurídicas asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad.

Utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración.

O demuestre con documentos con enlaces.

Cuadro B3: Cuestionario ICG – Medidas institucionales

1 Estrategia nacional de ciberseguridad

Explicación: Definición de políticas para fomentar la ciberseguridad como una de las principales prioridades nacionales. Una estrategia nacional de ciberseguridad debe definir el mantenimiento de infraestructuras de información esenciales resilientes y fiables, incluida la seguridad de la población; la protección de los bienes materiales e inmateriales de la población, las organizaciones y la nación; la respuesta a ciberataques contra infraestructuras esenciales y su prevención; y la minimización de los daños y el tiempo de recuperación tras un ciberataque.

Cuadro B3: Cuestionario ICG – Medidas institucionales (continuación)

1.1 ¿Dispone su país de una estrategia/política nacional de ciberseguridad?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.1 ¿Comprende la protección de infraestructuras de información esenciales nacionales, incluidas las del sector de telecomunicaciones?

Explicación: Todo sistema de información físico o virtual que controle, procese, transmita, reciba o almacene información electrónica de cualquier tipo, incluidos datos, voz o vídeo, vital para el funcionamiento de la infraestructura esencial, tan vital que la incapacidad o destrucción de esos sistemas debilitaría la seguridad nacional, la seguridad económica nacional o la seguridad sanitaria del país.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.2 ¿Hace referencia a la resiliencia de ciberseguridad nacional?

Explicación: Un plan de resiliencia de ciberseguridad nacional permite al país poder resistir y absorber los efectos de una catástrofe (natural o provocada por el hombre) y adaptarse y recuperarse de los mismos de manera rápida y eficiente, protegiendo y reconstruyendo por ejemplo sus estructuras y funciones básicas dependientes de servicios externos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.3 ¿Se revisa y actualiza periódicamente la estrategia de ciberseguridad nacional?

Explicación: El ciclo de gestión de la estrategia está definido. La estrategia se actualiza en función de la evolución de factores nacionales, tecnológicos, sociales, económicos y políticos que puedan afectar a la ciberseguridad nacional.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.4 ¿Está la estrategia de ciberseguridad abierta a la consulta con expertos nacionales en ciberseguridad?

Explicación: La estrategia puede ser objeto de consulta de todas las partes interesadas pertinentes, incluidos los operadores de infraestructuras esenciales, proveedores de servicios de Internet, instituciones académicas, etc.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B3: Cuestionario ICG – Medidas institucionales (continuación)

1.2 ¿Hay un plan de acción/hoja de ruta definido para la implementación de la gobernanza de ciberseguridad?

Explicación: Un plan estratégico que define los resultados de la ciberseguridad nacional, incluidas las fases y resultados intermedios necesarios para alcanzarlos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.3 ¿Hay una estrategia nacional de Protección de la Infancia en Línea?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2 Agencia responsable

Explicación: Las agencias encargadas de la aplicación de políticas o estrategias nacionales sobre ciberseguridad pueden ser comités permanentes, grupos de trabajo oficiales, comités asesores o centros interdisciplinarios. Estos organismos pueden ser además responsables directos del EIII nacional. La agencia responsable puede estar integrada en el gobierno y tener autoridad para obligar a otras agencias y entidades nacionales a aplicar políticas y aprobar normas.

2.1 ¿Hay una agencia responsable de la coordinación de la ciberseguridad a nivel nacional?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.1.1 ¿Se ocupa esa agencia de la protección de la infraestructura de información esencial nacional?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.2 ¿Hay una agencia nacional responsable de la capacitación en materia de ciberseguridad nacional?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B3: Cuestionario ICG – Medidas institucionales (continuación)

2.3 ¿Hay una agencia responsable de las iniciativas de Protección de la Infancia en Línea a nivel nacional?

Explicación: Existencia de una agencia nacional dedicada supervisar y fomentar la Protección de la Infancia en Línea.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3 Medición de la ciberseguridad

Explicación: Existencia de estudios comparativos o de referencia oficiales, nacionales o sectoriales, empleados para evaluar los avances en materia de ciberseguridad, estrategias de evaluación del riesgo, auditorías sobre ciberseguridad y otros instrumentos o actividades para valorar o evaluar en función del rendimiento para mejoras futuras. Por ejemplo, a partir de la norma ISO/CEI 27004, relativa a la medición de la gestión de la seguridad de la información.

3.1 ¿Se realizan auditorías de ciberseguridad a nivel nacional?

Explicación: Las auditorías de ciberseguridad son evaluaciones sistemáticas de la seguridad de un sistema de información para determinar si respeta los criterios establecidos. Las auditorías completas suelen evaluar la seguridad de la configuración y el entorno físico del sistema, el software, los procesos de gestión de la información y las prácticas de los usuarios. Los organismos de reglamentación pueden exigir a las infraestructuras esenciales de gestión privada la realización de evaluaciones periódicas de la seguridad y la presentación de sus resultados.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3.2 ¿Hay un sistema de medición para la evaluación de los riesgos del ciberespacio a nivel nacional?

Explicación: Proceso sistemático que incluye la identificación, el análisis y la evaluación de los riesgos.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3.3 ¿Se realizan mediciones para evaluar el nivel de desarrollo de la ciberseguridad a nivel nacional?

Explicación: Proceso de medición del nivel de desarrollo de la ciberseguridad en un país.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B3: Cuestionario ICG – Medidas institucionales (continuación)

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de esferas técnicas asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad.

Utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración.

O demuestre con documentos con enlaces.

Cuadro B4: Cuestionario ICG – Medidas de capacitación

1 Campañas públicas sobre ciberseguridad

Explicación: La sensibilización de los ciudadanos supone promover campañas publicitarias de gran alcance, así como colaborar con ONG, instituciones, organizaciones, proveedores de servicios de Internet, bibliotecas, organizaciones locales de comercio, centros comunitarios, centros universitarios y de formación de adultos, escuelas y organizaciones de padres y profesores para difundir mensajes sobre comportamientos seguros en línea. Se incluyen medidas como la creación de portales y sitios web para promover conocimientos, difundir material de apoyo y realizar otras actividades pertinentes.

1.1 ¿Se llevan a cabo campañas de sensibilización públicas específicas para sectores como las PYME, las empresas privadas y las agencias estatales?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.2 ¿Se llevan a cabo campañas de sensibilización públicas para la sociedad civil?

Explicación: ONG, organizaciones comunitarias.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.3 ¿Se llevan a cabo campañas de sensibilización públicas para la población en general?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.4 ¿Se llevan a cabo campañas de sensibilización públicas para los ancianos?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.5 ¿Se llevan a cabo campañas de sensibilización públicas para las personas con necesidades especiales?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.6 ¿Se llevan a cabo campañas de sensibilización públicas para padres, docentes y niños (relacionadas con la PIeL)?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B4: Cuestionario ICG – Medidas de capacitación (continuación)

2 Formación para profesionales de la ciberseguridad

Explicación: Existencia de programas de formación profesional sectoriales para sensibilizar al público en general (por ejemplo, día, semana o mes de la ciberseguridad nacional), fomentar la formación en ciberseguridad de la mano de obra con distintos perfiles (técnico, ciencias sociales, etc.) y fomentar la certificación de profesionales de los sectores público y privado.

Comprende también la formación en ciberseguridad de las fuerzas del orden, el sector judicial y demás actores del sector. La formación profesional y técnica puede ser continua para los agentes de policía, agentes de aplicación, jueces, fiscales, abogados, personal auxiliar y demás involucrados en el sector judicial y de aplicación de la legislación. Este indicador comprende también la existencia de un marco aprobado (o apoyado) por el gobierno para la certificación y acreditación de profesionales conforme a normas de seguridad internacionalmente reconocidas. Estas certificaciones, acreditaciones y normas pueden ser, entre otras, las siguientes: Seguridad en la nube (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, analista de ciberseguridad forense (ISC^2), etc.

2.1 ¿Prepara/apoya su gobierno cursos de formación profesional en ciberseguridad?

Explicación: Fomento de la formación de la mano de obra (técnica, ciencias sociales, etc.) en ciberseguridad y fomento de la certificación de profesionales del sector público o privado.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.2 ¿Existe un programa de acreditación para profesionales de la ciberseguridad en su país?

Explicación: Institutos de acreditación de profesionales de la ciberseguridad o cualquier otro mecanismo relacionado.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.3 ¿Hay programas/formaciones/cursos sectoriales nacionales para profesionales de la ciberseguridad?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.3.1 ¿Hay programas/formaciones/cursos sectoriales nacionales para las fuerzas del orden?

Explicación: Proceso oficial de formación de las fuerzas de seguridad (policía y agentes de aplicación) en seguridad informática.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B4: Cuestionario ICG – Medidas de capacitación (continuación)

2.3.2 ¿Hay programas/formaciones/cursos sectoriales nacionales para el personal judicial y jurídico?

Explicación: Formación técnica o en ciberseguridad continua para policías, fuerzas del orden, jueces, fiscales, abogados, personal auxiliar y profesionales afines.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.3.3 ¿Hay programas/formaciones/cursos sectoriales nacionales para PYME/empresas privadas?

Explicación: Formación/capacitación en prácticas idóneas de ciberseguridad para la protección de empresas, etc. mediante la utilización adecuada de servicios en línea.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2.3.4 ¿Hay programas/formaciones/cursos sectoriales nacionales para funcionarios públicos/miembros del gobierno?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3 ¿Desarrolla su gobierno/organización algún programa educativo o programa de estudios sobre ciberseguridad o fomenta su preparación...

Explicación: Existencia y promoción de cursillos y programas educativos a escala nacional para formar a las nuevas generaciones en conocimientos y profesiones relacionadas con la ciberseguridad en escuelas, institutos, universidades y otros centros educativos. Las profesiones vinculadas a la seguridad incluyen, entre otras, criptoanalistas, expertos en informática forense, expertos en respuestas a incidentes, arquitectos de seguridad informática o expertos en pruebas de penetración informática.

3.1 ¿En la enseñanza primaria?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3.2 ¿En la enseñanza secundaria?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Cuadro B4: Cuestionario ICG – Medidas de capacitación (continuación)

3.3 ¿En la enseñanza superior?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

4 Programas de investigación y desarrollo en ciberseguridad

Explicación: Este indicador mide la inversión en programas nacionales de investigación y desarrollo en ciberseguridad de instituciones privadas, públicas, académicas, no gubernamentales o internacionales. También considera la presencia de un organismo reconocido a nivel nacional que supervise el programa. Los programas de investigación en ciberseguridad incluyen, entre otros, análisis de programas informáticos dañinos o investigaciones sobre criptografía, vulnerabilidades de los sistemas y modelos y conceptos de seguridad. Los programas de desarrollo de la ciberseguridad se refieren a la elaboración de soluciones de hardware o software que incluyen, entre otras cosas, cortafuegos, sistemas antiintrusión, sistemas de señuelos y módulos de seguridad del hardware. La existencia de un órgano nacional supervisor mejorará la coordinación entre las instituciones y la distribución de recursos.

4.1 ¿Se realizan actividades de I+D en ciberseguridad a nivel nacional?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

4.1.1 ¿Hay programas de I+D en ciberseguridad del sector privado?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

4.1.2 ¿Hay programas de I+D en ciberseguridad del sector público?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

4.1.3 ¿Participan las instituciones de enseñanza superior, como instituciones académicas y universidades, en las actividades de I+D?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

5 Industria nacional de la ciberseguridad

Explicación: Un entorno económico, político y social propicio que fomente el desarrollo de la ciberseguridad favorece el crecimiento del sector privado. Las campañas de sensibilización, el desarrollo de la mano de obra, la capacitación y los incentivos gubernamentales impulsarán un mercado de productos y servicios de ciberseguridad. La presencia de una industria nacional de la ciberseguridad testimonia un entorno adecuado y fomenta la creación de empresas del sector y del mercado conexo de las ciberaseguradoras.

Cuadro B4: Cuestionario ICG – Medidas de capacitación (continuación)

5.1 ¿Hay una industria nacional de la ciberseguridad?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

6 ¿Hay mecanismos estatales de incentivos para ...

Explicación: Este indicador evalúa los incentivos que ofrece el gobierno para fomentar la capacitación en el sector de la ciberseguridad, mediante ventajas fiscales, subvenciones, financiación, préstamos, instalaciones y otros incentivos económicos y financieros, como actividades de capacitación específicas o nacionales. Los incentivos incrementan la demanda de servicios y productos relacionados con la ciberseguridad, lo que mejora la protección ante ciberataques.

6.1 ¿Fomentar la capacitación en ciberseguridad?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

6.2 ¿El desarrollo de la industria de ciberseguridad?

Explicación: Apoyo a las nuevas empresas de servicios de ciberseguridad a través de instituciones académicas o de otro tipo.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de esferas técnicas asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad.

Utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración.

O demuestre con documentos con enlaces.

Cuadro B5: Cuestionario ICG – Medidas de cooperación

1 Acuerdos bilaterales de cooperación en materia de ciberseguridad con otros países

Explicación: Los acuerdos bilaterales (acuerdos entre dos partes) designan alianzas nacionales o sectoriales reconocidas oficialmente y destinadas a compartir información y recursos sobre ciberseguridad. Son concluidos por un gobierno y otro gobierno extranjero, entidad regional u organización internacional (por ejemplo, cooperación o intercambio de información, conocimientos expertos, tecnología y otros recursos). Este indicador mide también si se comparte información sobre amenazas. Por capacitación se entiende la compartición de herramientas profesionales, investigaciones avanzadas de expertos, etc.

1.1 ¿Se han establecido acuerdos bilaterales de cooperación en materia de ciberseguridad con otros países?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.1 ¿Comprenden esos acuerdos la compartición de información?

Explicación: Por compartición de información se entiende la compartición de información no clasificada.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.2 ¿Comprenden esos acuerdos la capacitación?

Explicación: Capacidad para fomentar la formación destinada a aumentar los conocimientos, competencias y capacidades de los profesionales nacionales en ciberseguridad mediante la cooperación con miras a la intervención colectiva contra ciberamenazas.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

1.1.3 ¿Comprenden esos acuerdos la asistencia jurídica mutua?

Explicación: Asistencia mutua entre al menos dos países a fin de recopilar e intercambiar información para ejecutar leyes públicas o penales.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

2 Participación del gobierno en mecanismos internacionales relacionados con la ciberseguridad

Explicación: También pueden incluir la ratificación de acuerdos internacionales sobre ciberseguridad, como la Convención de la Unión Africana sobre ciberseguridad y protección de datos personales o el Convenio sobre la Ciberdelincuencia de Budapest.

Cuadro B5: Cuestionario ICG – Medidas de cooperación (continuación)

2.1 ¿Participa su gobierno/organización en mecanismos internacionales relacionados con la ciberseguridad?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3 Acuerdos multilaterales en materia de ciberseguridad

Explicación: Los acuerdos multilaterales (entre varias partes) designan alianzas nacionales o sectoriales reconocidas oficialmente y destinadas a compartir información y recursos sobre ciberseguridad. Son concluidos por un gobierno y otros gobiernos extranjeros u organizaciones internacionales (por ejemplo, cooperación o intercambio de información, conocimientos expertos, tecnología y otros recursos).

3.1 ¿Ha concluido su gobierno acuerdos multilaterales sobre cooperación en materia de ciberseguridad?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3.1.1 ¿Comprenden esos acuerdos la compartición de información?

Explicación: Por compartición de información se entiende la compartición de información no clasificada.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

3.1.2 ¿Comprenden esos acuerdos la capacitación?

Explicación: Capacidad para fomentar la formación destinada a aumentar los conocimientos, competencias y capacidades de los profesionales nacionales en ciberseguridad mediante la cooperación con miras a la intervención colectiva contra ciberamenazas.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

4 Acuerdos con el sector privado

Explicación: Se trata de alianzas entre el sector público y el privado. Este indicador de rendimiento mide el número de acuerdos público-privados nacionales o sectoriales y reconocidos oficialmente para compartir información y recursos de ciberseguridad (personal, procesos, instrumentos) entre el sector público y el privado (por ejemplo, alianzas oficiales sobre cooperación o intercambio de información, conocimientos expertos, tecnología y/o recursos), ya sea a escala nacional o internacional.

Cuadro B5: Cuestionario ICG – Medidas de cooperación (continuación)

4.1 ¿Ha concluido su gobierno acuerdos con empresas locales?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

4.2 ¿Ha concluido su gobierno acuerdos con empresas extranjeras ubicadas en el país?

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

5 Acuerdos entre agencias

Explicación: Este indicador de rendimiento designa cualquier colaboración oficial entre diferentes agencias gubernamentales y el estado (no incluye las alianzas internacionales). Puede incluir colaboraciones entre ministerios, departamentos, programas y otras instituciones del sector público.

5.1 ¿Se han concluido acuerdos/alianzas entre distintos órganos estatales en materia de ciberseguridad?

Explicación: Cooperación entre ministerios y organismos especializados.

☐ *Sí*

☐ *No*

Proporcione enlaces/URL

Proporcione documentos

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de esferas técnicas asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad.

Utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración.

O demuestre con documentos con enlaces.

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
Ethiopía

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 des Almadies
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
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe
Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

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: ituteguciglapa@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
Thailand Post Training Center, 5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia
Correo-e: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia
Correo-e: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 55521

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: itumoscow@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
Place des Nations
CH-1211 Ginebra 20
Suiza

ISBN 978-92-61-33923-4

Publicado en Suiza
Ginebra, 2021