Guía para el cuestionario sobre el Índice Mundial de Ciberseguridad (IMC) 2018

El presente documento es únicamente informativo. El IMC evalúa el compromiso de los países en materia de ciberseguridad de acuerdo con los cinco pilares de la Agenda sobre Ciberseguridad Global: medidas jurídicas, medidas técnicas, medidas organizativas, capacitación y cooperación.

El presente cuestionario combina las preguntas preparadas para establecer la clasificación del IMC 2017/18 junto con las mencionadas en la Cuestión 3 de la Comisión de Estudio 2 del UIT-D, y está dividido en cinco secciones. Las preguntas de todas las secciones deben contestarse por sí o no, marcando las casillas que preceden cada elemento. El cuestionario debe realizarse en línea. Los participantes recibirán un correo electrónico oficial de la UIT con una url personal que deberán conservar. El cuestionario en línea permite a los participantes cargar en cada pregunta documentos (y url) pertinentes que servirán de información complementaria.

No está previsto que las respuestas al cuestionario facilitadas por los participantes sean confidenciales.

1 Medidas jurídicas

1.1 ¿Disponen de legislación sobre ciberdelincuencia?

Explicación: *Se entiende por legislación sobre ciberdelincuencia toda ley que proteja la confidencialidad, integridad y disponibilidad de los sistemas informáticos, las redes y los datos informáticos; los delitos informáticos; los delitos relacionados con los contenidos; los delitos de infracción a los derechos de autor y derechos conexos. También incluye la legislación procesal y la ayuda mutua. .*

- ☐ *Sí*
- ☐ *No*
- ☐ *De forma parcial (**Únicamente** proyectos de texto en fase de elaboración avanzada, preparados para su adopción o verificación)*

1.1.1 ¿Disponen de legislación sustantiva sobre…

Explicación*: Se entiende por legislación sustantiva aquella que crea, define y regula derechos.* **(Especifíquese marcando la casilla de un artículo aplicable a su país e indique las páginas y la cantidad de artículos en los que los artículos siguientes figuran en sus documentos)**

- ☐ Acceso no autorizado a computadores, sistemas y datos?
- ☐ Interferencias/intercepciones/modificaciones/destrucciones no autorizadas en computadores, sistemas y datos?
- ☐ Protección de datos/privacidad?

Proporcione enlaces/url
Proporcione documentos

Explique una ley o un artículo parcial proporcionando únicamente los proyectos de texto de los artículos anteriormente citados

1.1.2 ¿Existen leyes procesales sobre ciberdelincuencia relacionados con...

Explicación: *Se entiende por leyes procesales las reglas y formalidades que han de seguirse en un procedimiento legal a fin de garantizar una aplicación justa y coherente de la legislación en todos los casos que llegan a los tribunales.* **(Especifíquese marcando la casilla de un artículo aplicable a su país e indique las páginas y la cantidad de artículos en los que los artículos siguientes figuran en sus documentos)**

- ☐ Artículos sobre conservación rápida de datos informáticos almacenados
- ☐ Órdenes de presentación
- ☐ Registro y confiscación de datos informáticos almacenados
- ☐ Recopilación en tiempo real de datos informáticos
- ☐ Extradición de ciberdelincuentes
- ☐ Asistencia mutua
- ☐ Confidencialidad y limitación de uso

Proporcione enlaces/url
Proporcione documentos
Explique una ley o un artículo parcial proporcionando únicamente los proyectos de texto de los artículos anteriormente citados

1.2 ¿Existen reglamentos sobre ciberseguridad relacionados con…

Explicación: *Reglamentos: normas basadas en textos legislativos determinados que prevén la ejecución de estos. Son aplicados* ***por agencias reguladoras*** *encargadas de ejecutar las disposiciones de una ley. Por tanto, la regulación sobre seguridad se refiere a principios que deben respetar los diferentes interesados, que emanan y forman parte de su aplicación.* **(Especifíquese marcando la casilla de un artículo aplicable a su país e indique las páginas y la cantidad de artículos en los que los artículos siguientes figuran en sus documentos).** Obsérvese que esta sección está dedicada exclusivamente a la reglamentación, y no a las leyes/legislación que se mencionan en la pregunta 1.1.1**.**

- ☐ *Sí*
- ☐ *No*
- ☐ *De forma parcial*
- ☐ *Protección de datos?*
- ☐ *Notificación de infracciones?*
- ☐ *Requisitos en materia de auditorías sobre ciberseguridad y certificación/normalización de la ciberseguridad*
- ☐ *Protección de la privacidad*
- ☐ *Firmas digitales y transacciones electrónicas?*
- ☐ *Responsabilidad de los proveedores de servicios de Internet?*
- ☐ *Protección de sistemas y redes?*

Proporcione enlaces/url
Proporcione documentos

Explique una ley o un artículo parcial proporcionando únicamente los proyectos de texto de los artículos anteriormente citados

1.3 ¿Existen leyes o reglamentos sobre el control o la reducción del correo basura?

Explicación*: Legislación/reglamentos sobre protección frente a correos electrónicos no deseados como consecuencia de la utilización de Internet. (Sírvase facilitar la reglamentación o la legislación (ley) o ambas)*

- ☐ *Sí*
- ☐ *No*
- ☐ *De forma parcial*

Proporcione enlaces/url
Proporcione documentos
Explique una ley o un artículo parcial proporcionando únicamente los proyectos de texto de los artículos anteriormente citados

1.4 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. (Nota: las prácticas idóneas son aplicables únicamente a países que cuentan con legislación o reglamentos en materia de ciberseguridad)

Proporcione enlaces/url
Proporcione documentos
Enumere a continuación prácticas idóneas si no ha mencionado previamente ningún enlace o documento

2 ¿Disponen de medidas técnicas?

2.1 ¿Existe un CIRT, CSIRT o CERT?

Explicación: *Los CIRT son equipos de respuesta ante incidentes informáticos. Los CSIRT son equipos de respuesta ante incidentes de seguridad informática. Los CERT son equipos de respuesta ante emergencias informáticas. Estos términos se utilizan indistintamente para designar a la entidad que recibe información sobre vulneraciones de seguridad, lleva a cabo análisis de los informes y responde a los remitentes.*

- ☐ *Sí*
- ☐ *No*

2.1.1 Indique qué opción de las siguientes CERT, CSIRT o CERT es aplicable a su país

Explicación: *El CSIRT/CIRT/CERT nacional es un organismo cuyo mandato consiste en supervisar y gestionar incidentes de ciberseguridad a nivel nacional en colaboración con instituciones locales, como círculos académicos, policía, sociedad civil, sector privado (en grupos económicos o de reflexión), infraestructuras de información crítica (energía, salud, transporte, finanzas, etc.) y con el gobierno. También colabora con los CIRT nacionales de otros países y con instituciones regionales e internacionales para elaborar respuestas pertinentes y eficaces en caso de ataque.*

- ☐ CIRT, CSIRT o CERT nacional
- ☐ CIRT, CSIRT o CERT gubernamental
- ☐ CIRT, CSIRT o CERT sectorial

Proporcione enlaces/url
Proporcione documentos

2.2 ¿Organiza el CIRT, CSIRT o CERT con frecuencia ejercicios de seguridad de forma ininterrumpida?

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

2.3 ¿Está el CIRT, CSIRT o CERT anteriormente seleccionado afiliado/asociado a FIRST?

- ☐ FIRST
- ☐ CERTS (APCERT, ICCERT, AFRICACERT, TFCCERT) regionales
- ☐ Otras asociaciones CERT

Proporcione enlaces/url
Proporcione documentos

2.4 ¿Existe un marco para la aplicación de las normas de ciberseguridad?

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.*

- ☐ En el sector público
- ☐ En el sector privado

Proporcione enlaces/url
Proporcione documentos

2.5 ¿Existe un órgano de normalización en el país?

- ☐ que facilite sus propias normas sobre ciberseguridad
- ☐ o que las adopte con arreglo a normas internacionales

Proporcione enlaces/url
Proporcione documentos

2.6 ¿Existe algún mecanismo o función técnica para luchar contra el correo basura?

Explicación: *¿Existen herramientas o medidas técnicas para reforzar la ciberseguridad, como software anti-virus o contra correos basura?*

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

2.7 ¿Su gobierno/organización utiliza la nube con fines de ciberseguridad en el sector público?

Explicación: *Programas informáticos que permiten realizar una copia de seguridad de los datos en caso de interferencia informática indeseada a través de Internet o una computadora, que no sean software antivirus, ni aplicaciones informáticas de seguridad de Internet, lucha contra programas informáticos dañinos o encriptación, con objeto de mejorar los sistemas de ciberseguridad del gobierno. El sistema en la nube permite la utilización de documentos/datos propios, o de cualquier otro tipo de archivos, así como el acceso a los mismos, en cualquier lugar y en cualquier momento evitando los daños causados por dicha interferencia informática. (De nuevo, la finalidad de la pregunta es entender la posible utilización de la nube para mejorar la posición de la ciberseguridad a nivel nacional sin ninguna especificación de un software específico en la nube)*

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

2.8 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. (Nota: las prácticas idóneas son aplicables únicamente a países con CIRT, CSIRT o CERT)

Proporcione enlaces/url
Proporcione documentos

3 ¿Disponen de medidas organizativas?

3.1 ¿Existe una estrategia (política) nacional de ciberseguridad?

Explicación: *Las políticas sobre estrategias nacionales de ciberseguridad o los planes nacionales para la protección de las infraestructuras de información son definidos y respaldados oficialmente por un país, y pueden incluir los compromisos siguientes: delimitar con precisión las responsabilidades en materia de ciberseguridad a todos los niveles de gobierno (local, regional y federal o nacional), con funciones y obligaciones bien definidas; comprometerse a velar por la ciberseguridad de forma pública y transparente; fomentar la participación del sector privado y su inclusión en iniciativas gubernamentales de promoción de la ciberseguridad, y elaborar una hoja de ruta sobre gobernanza que identifique a los principales interlocutores. (**Si está en fase de elaboración, marque la casilla "de forma parcial" y pase directamente al punto 3.8, y si no se dispone de ninguna estrategia, pase asimismo directamente a la pregunta 3.8**)*

- ☐ *Sí*
- ☐ *No*
- ☐ *De forma parcial (**Únicamente** proyectos de texto en fase de elaboración avanzada, preparados para su adopción o verificación)*

Proporcione enlaces/url
Proporcione documentos
Explique un proyecto de texto parcial proporcionando los proyectos de texto relativos a la estrategia nacional

3.2 ¿Es la estrategia nacional

Explicación: *La estrategia nacional sobre ciberseguridad puede recogerse en un documento independiente de la estrategia nacional de información, tecnología o seguridad. (**Si ha especificado la estrategia en la pregunta anterior, no es necesario hacerlo nuevamente; indique únicamente el número de página en el que figure información pertinente para las preguntas siguientes, hasta la 3.5**)*

- ☐ autónoma
- ☐ o forma parte de otra estrategia nacional más amplia?

Proporcione el número de página

3.3 ¿Incluye

Explicación: *La estrategia define las funciones y responsabilidades en materia de ciberseguridad de los representantes de los sectores privado o público.*

- ☐ el sector privado?
- ☐ el sector público?

Proporcione el número de página

3.4 ¿Existe una sección sobre

Explicación*: La estrategia incluye planes para la protección de la infraestructura de información crítica.*

Explicación*: El plan de resiliencia nacional permite la recuperación de un país tras una catástrofe (natural o provocada por el hombre) de manera rápida y eficiente, protegiendo y reconstruyendo por ejemplo sus estructuras y funciones básicas.*

- ☐ la protección de la infraestructura de información crítica?
- ☐ un plan nacional de resiliencia?

Proporcione el número de página

3.5 ¿Existe un claro plan de acción para la implantación a nivel gubernamental de la gobernanza sobre ciberseguridad?

Explicación*: La estrategia incluye una hoja de ruta/estrategia con hitos para el logro y la aplicación de la estrategia.*

- ☐ *SÍ*
- ☐ *No*

Proporcione el número de página

3.6 ¿La estrategia

- ☐ se revisa de forma ininterrumpida?
- ☐ puede ser objeto de consulta pública?

Explicación*: La estrategia se actualiza de acuerdo con los avances en los planos nacional, tecnológico, social, económico y político pertinentes.*

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

Proporcione el número de página o
el enlace en el que se especifique la consulta pública

3.7 ¿Existe algún organismo o agencia nacional encargado de:

- ☐ la ciberseguridad y la protección de la infraestructura de información crítica?
- ☐ coordinación/agencia/iniciativas para hacer frente a la lucha contra el correo basura?

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 CIRT 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.*

- ☐ *SÍ*
- ☐ *No*

Proporcione los enlaces/url
Proporcione documentos

3.8 ¿Disponen de parámetros para evaluar los avances en materia de ciberseguridad a nivel nacional?

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 gestión de la seguridad de la información.*

☐ *SÍ*
☐ *No*
Proporcione los enlaces/url
Proporcione documentos

3.9 ¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?

Explicación*: Un proceso sistemático que incluye identificación, análisis y evaluación de riesgos.*

☐ *SÍ*
☐ *No*
Proporcione los enlaces/url
Proporcione documentos

3.10 ¿Existe una referencia en materia de ciberseguridad para evaluar los riesgos?

☐ *SÍ*
☐ *No*
Proporcione los enlaces/url
Proporcione documentos

3.11 ¿Se realizan con frecuencia auditorías de ciberseguridad?

Explicación*: Se trata de 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.*

☐ *SÍ*
☐ *No*
Proporcione los enlaces/url
Proporcione documentos

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

Proporcione los enlaces/url
Proporcione documentos

4 Actividades de capacitación

4.1 ¿Se preparan y llevan a cabo 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, establecimientos informático, 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 concienciar sobre la ciberseguridad.*

- ☐ *Sí*
- ☐ *No*

Proporcione los enlaces/url
Proporcione documentos

4.2 ¿Se dirigen las campañas públicas de sensibilización a:

- ☐ Organizaciones?
- ☐ La sociedad?
- ☐ Adultos?
- ☐ Jóvenes y niños?
- ☐ Otros órganos conexos?

Proporcione enlaces/url numerados para cada casilla que haya seleccionado anteriormente
Proporcione documentos numerados para cada casilla que haya seleccionado anteriormente

4.3 ¿Existe un marco para la homologación y acreditación de profesionales en materia de ciberseguridad?

Explicación: *Existencia de uno o varios marcos aprobados (o respaldados) por el gobierno para la certificación y acreditación de profesionales con arreglo a normas de ciberseguridad reconocidas internacionalmente. Estas certificaciones, acreditaciones y normas incluyen, entre otras, las siguientes: Conocimientos sobre seguridad en la nube (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Analista Forense de Ciberseguridad (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Consejo de la CE), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Certificación en Ingeniería de Seguridad de Software (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), Técnico certificado en incidentes de seguridad informática-CERT (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc.*

- ☐ En el sector público
- ☐ En el sector privado

Proporcione enlances/url
Proporcione documentos

4.4 ¿Desarrolla su gobierno/organización algún cursillo de formación sobre ciberseguridad o fomenta su preparación...

Explicación*: Existencia de programas de formación profesional nacionales o sectoriales para promover la ciberseguridad en el trabajo (ámbito técnico, ciencias sociales, etc.) y promoción de la certificación de profesionales del sector público y privado.*

- ☐ Para los órganos encargados del cumplimiento de la ley (policías y agentes encargados del cumplimiento de la ley)
- ☐ Para instancias u órganos jurídicos (jueces, abogados, personal parajurídico, etc.)
- ☐ Para organizaciones?
- ☐ Para el sector público?
- ☐ Para la sociedad?
- ☐ Otros

Proporcione enlaces/url numerados para cada casilla que haya seleccionado anteriormente
Proporcione documentos numerados para cada casilla que haya seleccionado anteriormente

4.5 ¿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. Estos conocimientos incluyen, entre otros, saber crear contraseñas seguras o no revelar en línea información personal. 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.*

- ☐ En centros de educación primaria?
- ☐ En centros de educación secundaria?
- ☐ En centros de educación superior?
- ☐ Otros

Proporcione enlaces/url numerados para cada casilla que haya seleccionado anteriormente
Proporcione documentos numerados para cada casilla que haya seleccionado anteriormente

4.6 ¿Se realizan inversiones en programas de investigación y desarrollo sobre seguridad?

Explicación*: Estos 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 anti-intrusión, 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.*

- ☐ En el sector público
- ☐ En el sector privado
- ☐ En instituciones educativas superiores (sector académico)
- ☐ Un organismo institucional reconocido a nivel nacional que supervisa la actividad de I+D en ciberseguridad

- ☐ Un organismo institucional reconocido que supervisa las actividades de capacitación en seguridad cibernética
- ☐ Otros

Proporcione enlaces/url numerados para cada casilla que haya seleccionado anteriormente
Proporcione documentos numerados para cada casilla que haya seleccionado anteriormente

4.7 ¿Ofrece el gobierno medidas de estímulo para fomentar la capacitación en el ámbito de la ciberseguridad?

Explicación: *Todos los estímulos ofrecidos por el gobierno para fomentar la capacitación en el ámbito de la ciberseguridad, como 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.*

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

4.8 ¿Existe una 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.*

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

4.9 ¿Existe un mercado de ciberaseguradoras?

Explicación: *Los ciberseguros se utilizan para proteger a empresas y particulares de los riesgos de Internet, así como de aquellos relacionados con las infraestructuras y actividades vinculadas a las tecnologías de la información.*

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

4.10 ¿Se brinda apoyo a las nuevas empresas del sector y a su desarrollo?

Explicación*: Mecanismos destinados a fomentar el desarrollo de nuevas empresas del sector (ventajas fiscales, parques tecnológicos, zonas de libre comercio) y de las PYMES (pequeñas y medianas empresas).*

☐ *Sí*
☐ *No*

Proporcione enlaces/url
Proporcione documentos

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

Proporcione enlaces/url
Proporcione documentos
Enumere a continuación prácticas idóneas si no ha mencionado previamente ningún enlace o documento

5 Medidas de cooperación

5.1 ¿Existen acuerdos bilaterales de cooperación en materia de ciberseguridad con

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).*

- ☐ Estados o Estados Miembros
- ☐ Organizaciones internacionales
- ☐ Otros

5.2 Existen acuerdos

- ☐ jurídicamente vinculantes
- ☐ para compartir información
- ☐ para compartir recursos
- ☐ oficiosos (informales)
- ☐ cuya ratificación está pendiente

5.3 ¿Existen acuerdos multilaterales de cooperación 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). 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.*

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

5.4 Existen acuerdos

- ☐ jurídicamente vinculante
- ☐ para compartir información
- ☐ para compartir recursos
- ☐ oficiosos (informales)
- ☐ cuya ratificación está pendiente

5.5 ¿Participa su gobierno/organización en foros/asociaciones internacionales sobre ciberseguridad?

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

5.6 ¿Han concluido acuerdos público-privados...

Explicación*: Estos designan las alianzas entre el sector público y el privado. Este indicador de rendimiento puede evaluarse a partir de la cantidad de acuerdos público-privados nacionales o sectoriales y reconocidos oficialmente para compartir información sobre ciberseguridad (datos sobre amenazas) y recursos (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.*

- ☐ Con empresas nacionales?
- ☐ Con empresas extranjeras?

5.7 ¿Se han establecido asociaciones, en particular:

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.*

- ☐ asociaciones entre organismos?
- ☐ asociaciones en organismos?

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

Proporcione enlaces/url
Proporcione documentos

6 Encuesta suplementaria: Protección de la Infancia en Línea

6.1 ¿Disponen de medidas para proteger a los menores en Internet?

- ☐ *SÍ*
- ☐ *No*

6.1.1 ¿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. También puede referirse a legislación 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 a protección de los niños en el ciberespacio).*

- ☐ *SÍ*
- ☐ *No*
- ☐ *De forma parcial (**Únicamente** proyectos de texto en fase de elaboración avanzada, preparados para su adopción o verificación)*

Proporcione enlaces/url
Proporcione documentos

6.2 ¿Existe alguna agencia/entidad encargada de la protección de los menores en Internet?

Explicación: *Existencia de una agencia nacional dedicada a la protección de los menores en Internet.*

- ☐ *SÍ*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

6.2.1 ¿Se ha creado algún mecanismo público para denunciar problemas relacionados con la protección de menores en Internet?

Explicación: *Número de teléfono, dirección de correo electrónico o formulario web a través de los cuales se pueda informar de incidentes o inquietudes relativas a la protección de los niños.*

- ☐ *SÍ*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

6.2.2 ¿Se han desplegado capacidades y mecanismos técnicos para proteger a los menores en Internet?

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

6.2.3 ¿Han llevado a cabo el gobierno y las instituciones no gubernamentales actividades para ofrecer información y ayuda a los interesados para proteger a los menores en Internet?

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

6.2.4 ¿Existen programas educativos de protección de los menores en Internet?

- ☐ Para educadores
- ☐ Para padres
- ☐ Para niños

Proporcione enlaces/url
Proporcione documentos

6.3 ¿Existe una estrategia nacional para la protección de los niños en Internet?

- ☐ *Sí*
- ☐ *No*

Proporcione enlaces/url
Proporcione documentos

6.4 ¿Organizan campañas públicas sobre la protección de los menores en Internet?

- ☐ Para adultos
- ☐ Para jóvenes
- ☐ Para niños

Proporcione enlaces/url
Proporcione documentos

7 Addéndum: Encuesta

7.1 ¿Cree que concienciar sobre la ciberseguridad es una medida básica para conseguir un ciberespacio más seguro?

a) No es importante
b) Es relativamente importante
c) Es importante
d) Es muy importante

7.2 ¿A qué grupos están dirigidas las campañas de concienciación sobre la ciberseguridad en su país?

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

7.3 ¿Cuál de los grupos siguientes es prioritario? Sírvase clasificarlos del 1 a 6 en función de su importancia

a) Niños
b) Jóvenes
c) Estudiantes
d) Personas mayores
e) Personas con discapacidad
f) Instituciones privadas
g) Agencias gubernamentales
h) Otros

7.4 ¿Cuáles son los temas relacionados con la ciberseguridad que se abordan en las campañas existentes? (Pueden seleccionarse varias respuestas)

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

7.5 ¿Qué nivel de importancia recibe cada tema? Sírvase clasificar los temas de mayor a menor importancia y justificar el orden

a) Seguridad en Internet
b) Privacidad
c) Fraude
d) Suplantación de identidad
e) Programas informáticos dañinos
f) Protección de menores
g) Otros

7.6 ¿Ha recibido asistencia de la UIT o colaborado con la organización en el ámbito de la ciberseguridad?

a) En caso afirmativo, explique en qué ha consistido y dé su opinión sobre la eficacia de la asistencia/colaboración. Indique qué ámbitos específicos de la ciberseguridad se abordaron.

b) En caso negativo, ¿por qué e indique cómo podríamos ser de ayuda?

_____