Guía para el cuestionario sobre el Índice Mundial de Ciberseguridad (IMC) 2015/16

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 2015/16 junto con las mencionadas en la Cuestión 3 de la Comisión de Estudio 2 del UIT-D, y está dividido en tres secciones. Las preguntas de las dos primeras secciones deben contestarse por sí o no, y las de la última sección son abiertas. 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.

SECCIÓN 1

1. ¿Disponen de legislación sobre ciberseguridad?

1.1. ¿Disponen de legislación sobre ciberdelincuencia?

Explicación: *Leyes relativas a accesos no autorizados, interferencia o interceptación de datos y sistemas y utilización indebida de sistemas informáticos. Se incluyen leyes procesales y cualquier artículo sobre la conservación rápida de datos informáticos almacenados, órdenes de presentación, recopilación en tiempo real de datos informáticos, extradición, asistencia mutua, confidencialidad y limitación del uso, así como jurisprudencia sobre ciberdelitos o utilización indebida de computadores, además de delitos relacionados con el contenido. Las disposiciones pueden formar parte de leyes penales, de protección de datos, de libertad de información, de derecho de autor o de propiedad intelectual.*

1.1.1. ¿Existen leyes materiales en materia de ciberdelincuencia?

Exp: *Cualquier categoría del derecho público y privado, incluido el derecho de los contratos, patrimonio inmobiliario, delitos civiles, testamentos y derecho penal, así como leyes penales que crean, definen y regulan derechos.*

1.1.1.1. ¿Existen artículos sobre el acceso no autorizado a computadores, sistemas y datos?

Exp: *Acceso a computadores, sistemas y datos mediante contraseñas ajenas o medios indebidos, como adivinando o descifrando contraseñas o robando la identidad.*

1.1.1.2. ¿Existen artículos sobre interferencias o modificaciones no autorizadas en computadores, sistemas y datos?

Exp: *Las interferencias y modificaciones no autorizadas designan intromisiones ilegales en sistemas, computadores o datos durante las que se producen cambios en el estado inicial de estos, introduciendo, dañando, suprimiendo o en general alterando datos informáticos.*

1.1.1.3. ¿Existen artículos sobre la intercepción no autorizada de computadores, sistemas y datos?

Exp: *Esta se refiere a la captura ilícita de transmisiones de datos informáticos que no son de carácter público.*

1.1.2. ¿Existen leyes procesales sobre ciberdelincuencia?

Exp: *Las normas por las que se rige un tribunal para examinar y determinar qué sucede en causas civiles, penales o administrativas, formuladas para garantizar una aplicación justa y congruente del debido proceso y los principios de la justicia fundamental en todos los casos de los que conoce un tribunal.*

1.1.2.1. ¿Existen artículos sobre la conservación rápida de datos informáticos almacenados?

Exp: *La conservación de los datos es una obligación impuesta a personas y organizaciones por autoridades estatales, que exige la conservación de determinados tipos de datos para evitar su pérdida o modificación durante un periodo determinado*.

1.1.2.2. ¿Existen artículos sobre órdenes de presentación?

Exp: Dichas órdenes constituyen obligaciones impuestas a personas y organizaciones por autoridades estatales, y exigen la presentación de *datos informáticos específicos a los agentes del orden público en un plazo determinado.*

1.1.2.3. ¿Existen artículos sobre registro y confiscación de datos informáticos almacenados?

Exp: *El registro y la confiscación de datos designan las medidas legislativas y de otra índole que permiten a las autoridades registrar y acceder a sistemas y datos informáticos almacenados en su territorio.*

1.1.2.4. ¿Existen artículos sobre la recopilación en tiempo real de datos informáticos?

Exp: *La recopilación en tiempo real designa las medidas, legislativas y de otra índole, que permiten a las autoridades recopilar o registrar en tiempo real y en su territorio datos de tráfico de sistemas informáticos.*

1.1.2.5. ¿Existen artículos sobre la extradición de ciberdelincuentes?

Exp: *En un proceso de extradición, un estado o nación, a petición oficial de otro, entrega a dicha jurisdicción a las personas acusadas de ciberdelito en su jurisdicción, o condenadas por ello.*

1.1.2.6. ¿Existen artículos sobre la asistencia mutua?

Exp: *Se trata de acuerdos entre al menos dos países a fin de recopilar e intercambiar información para ejecutar leyes públicas o penales.*

1.1.2.7. ¿Existen artículos sobre confidencialidad y limitación de uso?

Exp: *Una Parte puede utilizar los datos obtenidos si respeta determinadas cláusulas de confidencialidad o utiliza los datos solo para fines específicos y convenidos.*

1.1.3. ¿Existe jurisprudencia sobre ciberdelitos o uso indebido de computadores?

Exp: *Los delitos aquí contemplados pueden incluir pirateo, acceso no autorizado a sistemas informáticos o propagación deliberada de software malintencionado y dañino (malware). El acceso sin autorización para introducir cambios en computadores puede referirse a alteraciones de software y datos, cambios de contraseñas o configuración para impedir que terceros accedan al sistema, o interferencias con el funcionamiento habitual del sistema en detrimento de este.*

1.2. ¿Existen leyes o reglamentos sobre ciberseguridad?

Exp: *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 seguridad 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.*

1.2.1. ¿Existen leyes o reglamentos sobre protección de datos?

Exp: *Reglamentos relativos a la protección de datos personales, comerciales y gubernamentales frente a posibles accesos no autorizados, alteraciones, eliminaciones o utilizaciones.*

1.2.2. ¿Existen leyes o reglamentos sobre protección de sistemas y redes?

Exp: *Medidas jurídicas destinadas a proteger sistemas y redes de interferencias dañinas.*

1.2.3. ¿Existen leyes o reglamentos sobre notificación de infracciones?

Exp: *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. Por lo general, estas leyes se promulgan para responder a la creciente cantidad de infracciones en bases de datos de clientes que contienen información personal identificable.*

1.2.3.1. ¿Sobre datos?

Exp: *Leyes sobre notificación de infracciones sobre datos.*

1.2.3.2. ¿Sobre sistemas y redes?

Exp: *Leyes sobre notificación de infracciones en sistemas y redes. Pueden incluir normas sobre ciberseguridad y otros requisitos básicos para proteger los datos de los consumidores, como la encriptación.*

1.2.4. ¿Existen leyes o reglamentos sobre certificación/normalización?

Exp: *La regulación sobre certificación/normalización prevé que las entidades que operan en el territorio de un país cumplan determinados criterios mínimos sobre certificación/normalización; estos pueden variar en función del sector de la economía. Las normas incluyen, entre otras, las elaboradas por las siguientes agencias: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.*

1.2.4.1. ¿Para el sector público?

Exp: Regulación relativa a certificación/normalización de carácter obligatorio para el sector público.

1.2.4.2. ¿Para el sector privado?

Exp: Regulación relativa a certificación/normalización de carácter obligatorio para el sector privado.

1.2.5. ¿Exigen las leyes o reglamentos la aplicación de medidas de ciberseguridad?

Exp: *Estas pueden incluir, entre otros, medidas técnicas y organizativas, como cortafuegos, listas de control de acceso, funciones y responsabilidades en materia de seguridad y seguros en caso de ciberdelitos (propios).*

1.2.5.1. ¿Para el sector público?

1.2.5.2. ¿Para los operadores de infraestructuras críticas?

Exp: *Las infraestructuras críticas son sistemas clave, fundamentales para la seguridad, la seguridad económica y la salud pública de un país. Entre otros, estos sistemas pueden incluir sistemas de defensa, banca y finanzas, telecomunicaciones, transporte, salud, energía, etc.*

1.2.5.3. ¿Para el sector privado?

1.2.6. ¿Exigen las leyes o reglamentos la organización de auditorías sobre ciberseguridad?

Exp: *evaluaciones sistemáticas y periódicas de la seguridad del sistema de información. Generalmente incluyen 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.*

1.2.6.1. ¿Para el sector público?

1.2.6.2. ¿Para los operadores de infraestructuras críticas?

1.2.6.3. ¿Para el sector privado?

1.2.7. ¿Existen leyes o reglamentos sobre protección de la privacidad?

Exp: *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.*

1.2.8. ¿Existen leyes o reglamentos sobre firmas digitales y transacciones electrónicas?

***Exp**: Las firmas digitales son técnicas matemáticas empleadas para validar la autenticidad e integridad de un mensaje, software o contenido de un documento digital. Las transacciones electrónicas son ventas o compras de bienes o servicios, realizadas entre empresas, hogares, particulares, gobiernos y otras organizaciones. Se incluyen aquí, por ejemplo, la Ley de comercio electrónico, la Ley de firmas electrónicas o la Ley de transacciones electrónicas, que pueden prever la creación de una entidad reguladora de las autoridades de certificación.*

1.2.9. ¿Existen leyes o reglamentos sobre la responsabilidad de los proveedores de servicios de Internet?

***Exp**: Proveedores de servicios de Internet responsables de infracciones de derecho de autor cometidos por sus usuarios. Proveedores obligados a notificar a la policía, los equipos de respuesta a las emergencias informáticas (CERT) o a otras agencias/autoridades nacionales toda ciberoperación ilegal iniciada en su infraestructura, un requisito de control activo de la red.*

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

1.3. ¿Se ofrece formación sobre ciberseguridad a los agentes de la policía y el personal judicial o similar?

***Exp**: Procesos oficiales para formar a los funcionarios judiciales sobre seguridad informática.*

1.3.1. ¿Para los agentes encargados de hacer cumplir la ley (agentes de policía o similar)?

1.3.2. ¿Para el personal judicial o similar (jueces, abogados, fiscales, procuradores, agentes parajudiciales, etc.)?

1.3.3. ¿Se ofrece la formación periódicamente?

Exp: La formación se ofrece periódicamente o varias veces.

2. ¿Disponen de medidas técnicas?

2.1. ¿Existe un CIRT, CSIRT o CERT con responsabilidad nacional?

Exp: 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. 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.*

2.1.1. ¿Cuenta con mandato gubernamental?

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

2.1.2. ¿Organiza el CIRT, CSIRT o CERT con frecuencia ejercicios de seguridad?

Exp: *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?*

2.1.3. ¿Está el CIRT, CSIRT o CERT afiliado a FIRST?

Exp: *Miembro titular o de enlace del Foro sobre los equipos de seguridad y respuesta ante incidentes.*

2.1.4. ¿Está el CIRT, CSIRT o CERT afiliado a otras comunidades de CERT? (CERT regionales)

Exp: Cualquier relación oficial u oficiosa con otros CERT de dentro o fuera del país, miembro de algún grupo de CERT regional.

2.2. ¿Existe un CERT gubernamental?

Exp: *Un CERT/CIRT/CSIRT gubernamental es una entidad que responde a los incidentes de seguridad informática o ciberseguridad que afectan únicamente a las instituciones gubernamentales. Además de servicios de respuesta puede también ofrecer servicios proactivos, como análisis de vulnerabilidad o auditorías de seguridad. Al contrario que los CERT nacionales, que ofrecen servicios tanto al sector privado como al público, los CERT gubernamentales ofrecen sus servicios únicamente a entidades del sector público.*

2.3. ¿Existen CERT sectoriales?

Exp: *Los CERT/CIRT/CSIRT 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, los servicios de emergencia y el sector financiero. Al contrario que los CERT gubernamentales, que ofrecen sus servicios al sector público, los CERT sectoriales trabajan con agencias de un único sector.*

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

Exp: *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.

2.4.1. ¿En el sector público?

2.4.2. ¿En el sector privado?

2.5. ¿Existe un marco para la certificación y acreditación de profesionales en materia de ciberseguridad?

Exp: *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.*

2.5.1. ¿En el sector público?

2.5.2. ¿En el sector privado?

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

2.7. ¿Existen herramientas o medidas técnicas para reforzar la ciberseguridad, como software anti-virus o contra correos basura, que estén disponibles para las personas con discapacidad?

3. ¿Disponen de medidas organizativas?

3.1. ¿Existe una estrategia nacional de ciberseguridad?

Exp: *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.*

3.1.1. ¿Es autónoma la estrategia nacional?

Exp: *La estrategia nacional sobre ciberseguridad puede recogerse en un documento independiente de la estrategia nacional de información, tecnología o seguridad.*

3.1.1.1. ¿Incluye al sector privado?

Exp: *La estrategia define las funciones y responsabilidades en materia de ciberseguridad de los representantes del sector privado.*

3.1.1.2. ¿Incluye al sector público?

Exp: *La estrategia define las funciones y responsabilidades en materia de ciberseguridad de los representantes del sector público.*

3.1.1.3. ¿Existe una sección sobre la protección de la infraestructura de información crítica?

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

3.1.1.4. ¿Existe una hoja de ruta sobre gobernanza?

Exp: *La estrategia incluye una hoja de ruta con fases para lograr la aplicación completa de esta.*

3.1.1.5. ¿Se revisa la estrategia con regularidad?

Exp: *La estrategia se actualiza conforme a los avances nacionales, tecnológicos, sociales, económicos y políticos que le pueden afectar.*

3.1.1.6. ¿Está abierta la estrategia a consultas públicas?

Exp: *La estrategia está abierta a consultas con todos los interesados, incluidos operadores de infraestructura, proveedores de servicios de Internet, círculos académicos, etc.*

3.1.1.7. ¿Incluye la estrategia un plan nacional de resiliencia?

Exp: *Este plan prevé 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.*

3.1.2. ¿Se enmarca la estrategia nacional de ciberseguridad en otra estrategia nacional de carácter más general?

3.1.2.1. ¿Existe una sección sobre la protección de la infraestructura de información crítica?

Exp: *Las infraestructuras críticas 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.

3.1.2.2. ¿Existe una hoja de ruta sobre la gobernanza de la sección de ciberseguridad?

3.1.3. ¿Define las prioridades del sector público?

3.1.4. ¿De no existir una estrategia de ciberseguridad en vigor, se está preparando alguna?

3.1.5. ¿Incluye la actual estrategia o la que se encuentra en fase de preparación acciones relativas a personas con discapacidad?

3.2. ¿Existe algún organismo o agencia nacional encargado de la ciberseguridad?

Exp: *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.*

3.2.1. ¿Existe alguna agencia responsable de la protección de la infraestructura de información crítica?

3.2.2. ¿Existe alguna agencia nacional que actúe como punto focal sobre asuntos relacionados con el correo basura?

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

Exp: *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.*

3.3.1. ¿Se realizan periódicamente evaluaciones de riesgo para la ciberseguridad?

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

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

3.3.1.2. ¿Se analizan o evalúan los riesgos para integrar mejoras futuras?

3.3.2. ¿Se realizan con frecuencia auditorías de ciberseguridad?

Exp: *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.*

3.3.2.1. ¿Son obligatorias?

Exp: *Impuestas por reglamentos internos o sectoriales, o de conformidad con las normas de certificación ISO270001.*

4. ¿Disponen de actividades de capacitación?

4.1. ¿Existe en el país un órgano de normalización?

Exp: *La normalización es un buen indicador del nivel de madurez de una tecnología, y la aparición de nuevas normas en áreas fundamentales pone de manifiesto la vital importancia de las normas. Si bien la ciberseguridad siempre ha sido importante para la seguridad nacional y recibe un trato diferente según los países, los planteamientos comunes se recogen en normas reconocidas por todos. Estas normas incluyen, entre otras, las elaboradas por las entidades siguientes: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc. Este indicador evalúa la existencia de un organismo nacional de normalización en materia de ciberseguridad y las actividades para desarrollar y aplicar las normas correspondientes.*

4.1.1. ¿Elabora sus propias normas sobre ciberseguridad?

Exp: *Las normas sobre ciberseguridad son técnicas presentadas generalmente en publicaciones y cuyo objetivo es proteger el ciberentorno de un usuario u organización. Dicho entorno incluye a los propios usuarios junto con redes, dispositivos, software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas que pueden conectarse directa o indirectamente a redes. El objetivo principal es reducir los riesgos y prevenir o atenuar los ataques a la ciberseguridad. Algunos países se basan en normas internacionales adaptadas a su entorno local, convirtiéndolas en normas nacionales. Otros (con programas avanzados de I+D) crean normas que en función de su aceptación van cobrando reconocimiento internacional y sirven de base para nuevas normas internacionales*.

4.1.2. ¿Adopta normas internacionales sobre ciberseguridad ya existentes?

Exp: *Las normas sobre ciberseguridad son técnicas presentadas generalmente en publicaciones cuyo objetivo es proteger el ciberentorno de un usuario u organización. Dicho entorno incluye a los propios usuarios junto con redes, dispositivos, software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas que pueden conectarse directa o indirectamente a redes. El objetivo principal es reducir los riesgos y prevenir o atenuar los ataques a la ciberseguridad. Algunos países se basan en normas internacionales adaptadas a su entorno local, convirtiéndolas en normas nacionales. Otros (con programas avanzados de I+D) crean normas que en función de su aceptación van cobrando reconocimiento internacional y sirven de base para nuevas normas internacionales*.

4.2. ¿Se recopilan buenas prácticas nacionales o sectoriales sobre ciberseguridad? ¿Se elaboran directrices al respecto?

Exp: *Las buenas prácticas son métodos o procedimientos cuyo éxito ha quedado demostrado. La adopción de buenas prácticas no solo reduce los posibles fallos, sino que aumenta la eficiencia.*

4.3. ¿Se invierte en programas de investigación y desarrollo sobre ciberseguridad?

Exp: *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 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.*

4.3.1. ¿En el sector público?

4.3.2. ¿En centros de educación superior?

4.3.3. ¿Existe algún órgano institucional reconocido a nivel nacional que supervise las actividades de I+D en materia de ciberseguridad?

4.4. ¿Se preparan y llevan a cabo campañas públicas sobre ciberseguridad?

Exp: *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.*

4.4.1. ¿Para organizaciones?

Exp: *Campañas públicas de sensibilización dirigidas a organizaciones.*

4.4.2. ¿Para la sociedad civil?

Exp: *Campañas destinadas al público en general.*

4.4.2.1. ¿Para adultos (>18 años)?

4.4.2.2. ¿Para jóvenes (12-17 años)?

4.4.2.3. ¿Para niños (<12 años)?

4.4.3. ¿Se informa al público durante estas campañas de los beneficios de utilizar software, hardware o soluciones basadas en servicios para mejorar la ciberseguridad?

4.4.4. ¿Se pone a disposición del público algún software, hardware o solución basada en servicios?

Exp: *Disponible de forma gratuita o a un precio reducido, por ejemplo, en el marco de una campaña de sensibilización.*

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

Exp: *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.*

4.5.1. ¿Para organizaciones?

4.5.2. ¿Para el sector público?

4.5.3. ¿Para la sociedad civil?

4.6. ¿Desarrolla su organización/gobierno algún programa educativo o programa de estudios sobre ciberseguridad o fomenta su preparación?

Exp: *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.*

4.6.1. ¿En centros de educación primaria?

4.6.2. ¿En centros de educación secundaria?

4.6.3. ¿En centros de educación superior?

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

Exp: *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.*

4.7.1. ¿Existe un organismo institucional con reconocimiento nacional que supervise las actividades existentes sobre capacitación?

4.8. ¿Existe una industria nacional de la ciberseguridad?

Exp: *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.*

4.8.1. ¿Existe un mercado de ciberaseguradoras?

Exp: *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.*

4.8.1.1 ¿Se ofrecen subvenciones a las empresas y otras entidades que carecen de medios para contratar ciberseguros en el mercado abierto?

4.8.2. ¿Se ofrecen incentivos para desarrollar la industria de la ciberseguridad?

Exp: *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.*

4.8.2.1. ¿Se brinda apoyo a las nuevas empresas del sector?

Exp*: 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).*

5. ¿Disponen de medidas de cooperación?

5.1. ¿Existen acuerdos bilaterales de cooperación en materia de ciberseguridad?

Exp: *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).*

5.1.1. ¿Con otros Estados?

5.1.1.1. ¿Es el acuerdo jurídicamente vinculante?

Exp: *Expresión jurídica habitual que indica que el acuerdo se ha realizado deliberadamente y que determinadas acciones son obligatorias o están prohibidas por ley*.

5.1.1.1.1. ¿Para compartir información?

Exp: *La información designa aquí datos sobre posibles amenazas.*

5.1.1.1.2. ¿Para compartir recursos?

Exp: *Los recursos designan aquí tanto a profesionales (traslados, prácticas y otros cesiones temporales de empleados), instalaciones, equipos y otros instrumentos y servicios.*

5.1.1.2. ¿El acuerdo es oficioso, su ratificación está pendiente o no es jurídicamente vinculante?

5.1.1.2.1. ¿Para compartir información?

5.1.1.2.2. ¿Para compartir recursos?

Exp*: Los recursos incluyen recursos humanos, instalaciones, equipos, etc.*

5.1.2. ¿Con organizaciones internacionales?

5.1.2.1. ¿Es el acuerdo jurídicamente vinculante?

5.1.2.1.1. ¿Para compartir información?

5.1.2.1.2. ¿Para compartir recursos?

Exp: *Los recursos incluyen recursos humanos, instalaciones, equipos, etc*.

5.1.2.2. ¿El acuerdo es oficioso, su ratificación está pendiente o no es jurídicamente vinculante?

5.1.2.2.1. ¿Para compartir información?

5.1.2.2.2. ¿Para compartir recursos?

Exp: *Los recursos incluyen recursos humanos, instalaciones, equipos, etc*.

5.2. ¿Existen acuerdos multilaterales o internacionales de cooperación en materia de ciberseguridad?

Exp: *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.

5.2.1. ¿Es el acuerdo jurídicamente vinculante?

5.2.1.1. ¿Para compartir información?

5.2.1.2. ¿Para compartir recursos?

Exp: *Los recursos incluyen recursos humanos, instalaciones, equipos, etc*.

5.2.2. ¿El acuerdo es oficioso, su ratificación está pendiente o no es jurídicamente vinculante?

5.2.2.1. ¿Para compartir información?

5.2.2.2. ¿Para compartir recursos?

Exp: *Los recursos incluyen recursos humanos, instalaciones, equipos, etc*.

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

5.4. ¿Han concluido acuerdos público-privados?

Exp: *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.*

5.4.1. ¿Con empresas nacionales?

5.4.1.1. ¿Para compartir información?

5.4.1.2. ¿Para compartir recursos?

5.4.2. ¿Con empresas extranjeras?

5.4.2.1. ¿Para compartir información?

5.4.2.2. ¿Para compartir recursos?

Exp: *Los recursos incluyen recursos humanos, instalaciones, equipos, etc.*

5.5. ¿Disponen de acuerdos entre agencias?

Exp: *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.*

5.5.1. ¿Para compartir información?

5.5.2. ¿Para compartir recursos?

Exp: *Los recursos incluyen recursos humanos, instalaciones, equipos, etc.*

SECCIÓN 2

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

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

Exp: *En líneas generales, resulta necesaria la existencia de 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 resultar necesario elaborar leyes nuevas o adaptar las existentes para ilegalizar determinados comportamientos que solo 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).*

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

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

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

Exp: *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.*

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

1.2.3. ¿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?

1.2.4. ¿Existen programas educativos de protección de los menores en Internet?

1.2.4.1. ¿Para educadores?

1.2.4.2. ¿Para padres?

1.2.4.3. ¿Para niños?

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

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

1.4.1.1. ¿Para adultos (>18 años)?

1.4.1.2. ¿Para jóvenes (12-17 años)?

1.4.1.3. ¿Para niños (<12 años)?

SECCIÓN 3

Addéndum: Encuesta

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.
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
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
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
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
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 temas relacionados con la ciberseguridad se abordaron.
    b. En caso negativo, ¿por qué y cómo podríamos ser de ayuda?