ÍNDICE MUNDIAL DE CIBERSEGURIDAD V4 2019/2020

Las preguntas de este cuestionario han sido preparadas y revisadas en la reunión del Grupo de Relator para la Cuestión 3/2 del UIT-D: Seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad. En la reunión se pidió la aprobación de los Miembros para lanzar el IMCv4 – 2019/2020. El presente cuestionario está dividido en cinco secciones. Las preguntas de todas las secciones deben contestarse con 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. Si el coordinador opta por formar un equipo para responder al cuestionario, todos deberán utilizar el mismo identificador para facilitar las respuestas.

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.

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

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.*

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.

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

2.5 Utilización de firmas digitales en servicios y aplicaciones gubernamentales (cibergobierno)?

***Explicación**: 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.*

☐ ***Sí***

☐ ***No***

Proporcione enlaces/URL

Proporcione documentos

2.6 contra los mensajes de correo electrónico indeseados?

***Explicación**: añádase información sobre toda legislación o normativa en virtud de la cual se restringen los mensajes de correo electrónico indeseados.*

☐ ***Sí***

☐ ***No***

Proporcione enlaces/URL

Proporcione documentos

2.7 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

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

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

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.*

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 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

MEDIDAS ORGANIZATIVAS

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.*

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

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

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

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

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

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 (ISC²), 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

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*
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.*

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 medidas de capacitación 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

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.*

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*

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 medidas de cooperación 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