Programa de Ciberseguridad del UIT-D

Índice de Ciberseguridad Global – GCIv5

Cuestionario final revisado

Índice

Índice de Ciberseguridad Global GCIv5 – Registro de cambios y definiciones

Cuestionario revisado para el GCIv5, con inclusión de las medidas correspondientes adoptadas a raíz de las ediciones anteriores del Índice de Ciberseguridad Mundial, las definiciones de los términos clave, y la lógica subyacente de los indicadores/el marco.

Leyenda

***Código- [NÚMERO DE EDICIÓN]* –** Código correspondiente a la pregunta/sección que figura en el correspondiente número de edición.

Fundamento- [NÚMERO DE EDICIÓN] – Todo fundamento lógico o de fondo sobre el que se basa la pregunta en la correspondiente edición.

Indicadores del Índice de Ciberseguridad Global por pilar

Medidas legislativas

Fundamento-GCIv5: La legislación constituye una medida fundamental para proporcionar un marco armonizado en el que las entidades se adaptan a una base normativa común, ya sea con respecto a la prohibición de una determinada conducta delictiva o a la definición de requisitos reglamentarios mínimos. Los marcos legislativos establecen las funciones, obligaciones y responsabilidades de diversas partes interesadas. Se puede afirmar que la legislación en materia de ciberseguridad responde a cinco preguntas fundamentales: "1) ¿Qué se está protegiendo?; 2) ¿Dónde y a quién se está bridando protección?; 3) ¿De qué manera se está brindando protección?; 4) ¿En qué momento se brinda protección?; y 5) ¿Por qué se brinda protección[1]?" La seguridad de los datos es una parte importante de la ciberseguridad, pero no constituye su único componente, ya que la ciberseguridad abarca los "sistemas en los que se almacenan los datos y las redes por las que estos se transmiten[2]".

Las medidas legislativas también permiten a un país establecer mecanismos básicos de respuesta a los incumplimientos: por conducto de la investigación y el enjuiciamiento de delitos y la imposición de sanciones por incumplimiento o vulneración de la ley. Las leyes protegen la seguridad general, garantizan los derechos de los ciudadanos contra el abuso de terceros y aseguran la protección contra el uso indebido de las tecnologías más recientes. En un marco legislativo se establecen las normas mínimas de comportamiento en todos los ámbitos, aplicables a todos, y sobre las que se pueden desarrollar capacidades adicionales en materia de ciberseguridad. Por último, el objetivo que se persigue es permitir que los países dispongan de una legislación adecuada a fin de armonizar las prácticas en el plano supranacional y ofrecer un entorno propicio a las medidas interoperables, que facilite la lucha internacional contra la ciberdelincuencia.

El entorno jurídico se puede medir en función de la existencia y el número de instituciones y marcos jurídicos en materia de ciberseguridad y ciberdelincuencia. El subgrupo comprende los indicadores de desempeño siguientes:

1 La legislación en materia de ciberdelincuencia

Código-GCIv5: Legal1

Fundamento-GCIv5: En las leyes de ciberdelincuencia se definen el acceso no autorizado (sin derechos), la injerencia y la interceptación respecto de computadoras, sistemas y datos. Estas leyes pueden clasificarse bajo el derecho sustantivo y/o procesal, el derecho público o privado, el derecho anglosajón, la jurisprudencia, el derecho administrativo u otras categorías aplicables del Derecho.

1.1 Leyes sobre comportamientos en línea no autorizados

Código-GCIv5: Legal1.1

Fundamento-GCIv5: Diversos comportamientos en línea pueden incidir negativamente en la seguridad y la confianza de las actividades en línea. Algunos de estos comportamientos se han señalado en acuerdos internacionales, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia de 2011 ("Convenio de Budapest"). La legislación en vigor sobre estos comportamientos puede ofrecer orientaciones claras a los organismos encargados de hacer cumplir la ley, proporcionar claridad judicial y remitir a las personas afectadas por tales comportamientos.

[1] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

[2] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

1.1.1 ¿Tiene su país leyes en vigor en materia de acceso ilegal a dispositivos, sistemas informáticos y datos?

Código-GCIv5: Legal1.1.1

Fundamento-GCIv5: Diversos comportamientos en línea pueden incidir negativamente en la seguridad y la confianza de las actividades en línea. Una forma de hacer frente a tales comportamientos es por conducto de la legislación. Esta pregunta tiene por objeto medir si, en el momento en que se presentó el Cuestionario sobre el Índice de Ciberseguridad Mundial, un determinado país tenía leyes específicas en vigor que abordasen el acceso ilegal a dispositivos, sistemas informáticos y datos, que puede a su vez causar daños a la privacidad, los bienes, la dignidad personal y otro tipo de daños o perjuicios. Las leyes previstas o preparadas que no estén actualmente en vigor no se examinan en este punto.

1.1.2 ¿Tiene su país leyes en vigor en materia de injerencia ilegal (cometida por conducto del ingreso, la alteración o la supresión de datos) en dispositivos, datos y sistemas informáticos?

Código-GCIv5: Legal1.1.2

Fundamento-GCIv5: Diversos comportamientos en línea pueden incidir negativamente en la seguridad y la confianza de las actividades en línea. Una forma de hacer frente a tales comportamientos es por conducto de la legislación. Esta pregunta tiene por objeto medir si, en el momento en que se presentó el Cuestionario sobre el Índice de Ciberseguridad Mundial, un determinado país tenía leyes específicas en vigor que abordasen la injerencia ilegal (cometida por conducto del ingreso, la alteración o la supresión de datos) en dispositivos, datos y sistemas informáticos. Las leyes previstas o preparadas que no estén actualmente en vigor no se examinan en este punto.

1.1.3 ¿Tiene su país leyes en vigor en materia de interceptación ilegal de dispositivos, datos y sistemas informáticos?

Código-GCIv5: Legal1.1.3

Fundamento-GCIv5: Diversos comportamientos en línea pueden incidir negativamente en la seguridad y la confianza de las actividades en línea. Una forma de hacer frente a tales comportamientos es por conducto de la legislación. Esta pregunta tiene por objeto medir si, en el momento en que se presentó el Cuestionario sobre el Índice de Ciberseguridad Mundial, un determinado país tenía leyes específicas en vigor que abordasen la interceptación ilegal de dispositivos, datos y sistemas informáticos. Las leyes previstas o preparadas que no estén actualmente en vigor no se examinan en este punto.

1.1.4 ¿Tiene su país leyes sustantivas sobre la identidad en línea?

Código-GCIv5: Legal1.1.4

Fundamento-GCIv5: Dado el creciente número de actividades en línea, es necesario que las personas puedan identificarse en línea de manera fiable y segura. Las leyes, ya sean específicas de las actividades en línea o formen parte de otras leyes relacionadas con la identidad o de otro tipo, ayudan a proporcionar un fundamento jurídico respecto de la utilización y gestión de identidades y los comportamientos conexos.

1.2 ¿Tiene su país leyes en vigor relacionadas con la falsificación informática (piratería/vulneraciones de derechos de autor)?

Código-GCIv5: Legal1.2

Fundamento-GCIv5: La confianza es la base del ecosistema digital. La falsificación informática destruye dicha confianza. La falsificación informática abarca "la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean considerados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente[3]". "Esto ocurre, por ejemplo, cuando una persona modifica un correo electrónico auténtico de

[3] https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html

una institución financiera y envía la versión modificada a varios destinatarios (lo cual se conoce también como "suplantación de identidad"). Algunos países exigen que, para que haya falsificación, los datos informáticos originales guarden relación con la documentación con la que se pretende crear obligaciones jurídicas vinculantes. Otros solo exigen que el autor tenga la intención de que la versión modificada resultante sea considerada o utilizada con respecto a las obligaciones jurídicas[4]".

1.3 Leyes sobre la seguridad en línea

Código-GCIv5: Legal1.3

Fundamento-GCIv5: Dada la incidencia negativa de los comportamientos antisociales en las actividades en línea, que causan un sentimiento de menor seguridad a los usuarios y las comunidades, a continuación se mide la reglamentación de ciertos comportamientos. Con frecuencia, la reglamentación de estos comportamientos debe conciliar cuidadosamente los derechos humanos y otros valores refrendados por la Convención de Derechos Humanos de las Naciones Unidas, entre otros instrumentos. Téngase en cuenta que no es necesario que las leyes mencionen de manera explícita que se aplican a las circunstancias digitales/en línea, siempre que a nivel nacional, los órganos judiciales acepten que se apliquen a las circunstancias digitales/en línea.

1.3.1 ¿Tiene su país leyes en vigor aplicables al material racista y xenófobo en línea?

Código-GCIv5: Legal1.3.1

Fundamento-GCIv5: El material racista y xenófobo en línea tiene importantes efectos negativos en las comunidades en línea, ya que entre otras cosas reduce la diversidad, agrava las divisiones, y puede causar perjuicios a las personas. La legislación en vigor en materia de racismo y xenofobia ha de ser clara, de manera que las personas puedan comprenderla fácilmente y cumplirla. Se acepta la legislación neutral en cuanto al aspecto tecnológico; no es necesario que las leyes especifiquen que se aplican al material racista y xenófobo en línea si hay declaraciones judiciales conexas, alegatos, jurisprudencia, enjuiciamientos anteriores u otro material adecuado que demuestre su aplicabilidad a las circunstancias en línea.

1.3.2 ¿Tiene su país leyes en vigor aplicables al acoso y al abuso en línea contra la dignidad/integridad personal?

Código-GCIv5: Legal1.3.2

Fundamento-GCIv5: El acoso y el abuso contra la dignidad/integridad personal puede tener importantes efectos negativos en las personas, especialmente cuando tienen lugar en línea. La legislación en vigor ofrece orientaciones a los organismos encargados de hacer cumplir la ley respecto de los casos sobre los que han de actuar, a los miembros del sistema judicial sobre la manera de ocuparse de los casos, y brinda oportunidades de remisión a las personas afectadas, lo cual contribuye en última instancia a la seguridad y la confianza en línea. Se acepta la legislación neutral en cuanto al aspecto tecnológico; no es necesario que las leyes especifiquen que se aplican al material que constituya un acoso o abuso en línea si hay declaraciones judiciales conexas, alegatos, jurisprudencia, enjuiciamientos anteriores u otro material adecuado que demuestre su aplicabilidad a las circunstancias en línea.

---

[4] http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_questionnaires/Member_State_questionnaire.xls

2 Normativa en materia de ciberseguridad

Código-GCIv5: Legal2

Fundamento-GCIv2: La normativa en materia de ciberseguridad se refiere a las normas que tratan de la protección de datos, la notificación de infracciones, los requisitos de certificación/normalización en materia de ciberseguridad, la aplicación de medidas de ciberseguridad, los requisitos de las auditorías de ciberseguridad, la protección de la privacidad, la Protección de la Infancia en Línea (PIeL), las firmas digitales, las operaciones electrónicas y la responsabilidad de los proveedores de servicios de Internet. Con frecuencia, las normas constituyen el marco de aplicación de leyes, en el que se especifica la manera en que estas se deben cumplir. Los países pueden mejorar su compromiso con la ciberseguridad por conducto de normas claras, coherentes, aplicables y actualizadas.

2.1 ¿Tiene su país normas relacionadas con la protección de los datos personales?

Código-GCIv5: Legal2.1

Fundamento-GCIv5: La normativa sobre datos personales refuerza la gestión de datos, ya que en ella se destacan las responsabilidades de los titulares y los derechos de las personas. Puede ofrecer directrices por las que se exijan responsabilidades a los titulares de los datos respecto de la manera en que utilizan sus datos personales y garantizar que las organizaciones no abusen de los datos recopilados.

2.2 ¿Tiene su país normas relacionadas con la protección de la privacidad?

Código-GCIv5: Legal2.2

Fundamento-GCIv5: La normativa en materia de protección de la privacidad garantiza que los datos personales estén protegidos, que las organizaciones sean transparentes sobre la manera en que utilizan los datos, y que las personas tengan derecho a acceder a sus datos personales y a corregirlos. La normativa puede prohibir a las organizaciones la venta o la compartición de datos personales sin el consentimiento de la persona a la que correspondan. La protección de la privacidad puede garantizar que las personas puedan controlar sus datos personales. El uso indebido de los datos personales puede contribuir a la ciberdelincuencia y destruir la confianza en las tecnologías digitales.

2.3 ¿Tiene su país normas relacionadas con la filtración de datos/la notificación de incidentes que se apliquen a los actores del sector privado?

Código-GCIv5: Legal2.3

Fundamento-GCIv5: Una filtración de datos puede afectar negativamente a las personas, empresas y gobiernos, con motivo del robo financiero y la usurpación de identidad, los efectos negativos en la reputación y las consecuencias punitivas para los titulares de los datos. Una normativa eficaz puede abordar las notificaciones relativas a la filtración de datos y exigir a los actores que comuniquen tales actos a las personas, empresas y gobiernos de manera oportuna. Esto permitiría a las personas, empresas y gobiernos adoptar medidas para protegerse contra el daño que puede derivarse de una filtración de datos. Las normas sobre las notificaciones relativas a la filtración de datos pueden fomentar la adopción de buenas prácticas en materia de gestión de datos, exigir la notificación oportuna y proporcionar vías de recurso a los afectados.

2.4 ¿Tiene su país normas relacionadas con los requisitos de las auditorías de ciberseguridad, que se apliquen a los organismos públicos y departamentos nacionales o a sus contratistas?

Código-GCIv5: Legal2.4

Fundamento-GCIv5: La normativa sobre los requisitos de las auditorías de ciberseguridad puede fomentar la detección de los riesgos de ciberseguridad y alentar la adopción de mejores prácticas en materia de ciberseguridad al animar a los organismos, departamentos y contratistas a detectar y reparar las vulnerabilidades de sus sistemas. Además, esta normativa puede alentar a los organismos, departamentos y contratistas a seguir las mejores prácticas en materia de ciberseguridad y ajustarse a las normas internacionales.

2.5 ¿Tiene su país una normativa relacionada con las normas de ciberseguridad que se aplique a los actores nacionales del sector público?

Código-GCIv5: Legal2.5

Fundamento-GCIv5: Los actores del sector público son con frecuencia blanco de ciberataques. Por tanto, es importante que estos actores hayan instaurado medidas de protección sólidas para que puedan protegerse y proteger a sus ciudadanos. El hecho de tener una normativa relacionada con las normas de ciberseguridad aplicable a los actores nacionales del sector público puede ayudar a que dichos actores gocen de una mejor protección contra los ciberataques y sigan las mejores prácticas en materia de ciberseguridad.

Entre esas normas están, 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), las relacionadas con los requisitos normativos de los sistemas de gestión de la seguridad informática de la ISO 27001, la ISO 28000 sobre la seguridad de la gestión de las cadenas de suministro, la ISA 62443 sobre la seguridad de los sistemas industriales de automatización y control, etc.

2.6 ¿Tiene su país normas relacionadas con la utilización de las firmas digitales y las operaciones electrónicas en los servicios y aplicaciones del Gobierno (e-govt)?

Código-GCIv5: Legal2.6

Fundamento-GCIv5: Los Gobiernos utilizan cada vez más las firmas digitales y las operaciones electrónicas en sus servicios y aplicaciones. Este cambio hacia la adopción de sistemas electrónicos ha aportado diversos beneficios, en particular un aumento de la eficacia y la seguridad. Sin embargo, si no hay una normativa adecuada, existe el riesgo de que dichos sistemas no se utilicen de manera segura o eficaz.

La normativa ayuda a garantizar que los ciudadanos puedan confiar en que sus datos están seguros, y que los sistemas del Gobierno sean eficaces y fiables.

2.7 ¿Tiene su país normas relacionadas con las comunicaciones no solicitadas, también conocidas como *spam*?

Código-GCIv5: Legal2.7

Fundamento-GCIv5: Al regular las comunicaciones no solicitadas, los países pueden crear una experiencia más segura y más agradable para todos. Estas normas ayudan a proteger a los ciudadanos contra los efectos nefastos del *spam*, y evitar que los generadores de *spam* se aprovechen de las personas.

2.8 ¿Tiene su país normas relacionadas con la detección y protección de infraestructuras nacionales críticas?

Código-GCIv5: Legal2.8

Fundamento-GCIv5: Al detectar y proteger las infraestructuras nacionales críticas, un país puede gestionar los riesgos relacionados con la ciberseguridad. Las normas de protección de las infraestructuras nacionales críticas ayudan a los países a planificar la manera de responder a una catástrofe o agresión importante, garantizando que puedan responder de manera rápida y eficaz a estos eventos. Asimismo, un país necesita tener un plan para recuperarse de una catástrofe o ataque importante.

2.9 ¿Tiene su país normas relacionadas con la Protección de la Infancia en Línea?

Código-GCIv5: Legal2.9

Fundamento-GCIv5: El hecho de abordar la Protección de la Infancia en Línea por conducto de normas pertinentes permite a los organismos y actores pertinentes adoptar medidas e implementar reglas y requisitos específicos para tratar y combatir los delitos en línea/cibernéticos contra los niños y los jóvenes. Es fundamental que dichas normas sean aplicadas por las diversas partes interesadas de todos los sectores y niveles de la sociedad – desde los operadores industriales hasta las fuerzas del orden y las partes interesadas de la sociedad civil – que deben actuar de manera colectiva para apoyar la consecución de un entorno digital seguro para los niños y los jóvenes.

Medidas técnicas

Fundamento-GCIv5: La tecnología es la primera línea de defensa contra las ciberamenazas y los agentes maliciosos en línea. Si no se dispone de medidas técnicas y capacidades adecuadas para detectar y responder a los ciberataques, los países y sus entidades respectivas siguen siendo vulnerables a dichos ataques. La aparición y el éxito de las TIC solo pueden prosperar realmente en un clima de confianza y seguridad. Por consiguiente, los países han de ser capaces de elaborar estrategias para establecer criterios de seguridad mínimos aceptados y esquemas de acreditación respecto de las aplicaciones y sistemas informáticos. Además de estas medidas, se debe crear una entidad nacional que se ocupe de los incidentes cibernéticos a nivel nacional, al menos con un organismo público responsable y un marco nacional que lo acompañe para supervisar, advertir y responder a los incidentes.

Las medidas técnicas se pueden medir sobre la base de la existencia y el número de instituciones y marcos técnicos que se ocupen de la ciberseguridad, avalados o creados por un país. El subgrupo comprende los indicadores de desempeño siguientes:

1 EIEI/EIII/EIISI o SOC nacionales

Código-GCIv5: Tech1

Fundamento-GCIv5: Se necesitan mecanismos y estructuras institucionales eficaces a nivel nacional para detectar, prevenir, responder y mitigar las amenazas e incidentes cibernéticos. Los Equipos de Intervención en caso de Incidente Informático (EIII), así como los Equipos de Intervención en caso de Incidente de Seguridad Informática (EIISI) y los Equipos de Intervención en caso de Emergencia Informática (EIEI) y Centros de Operaciones de Seguridad (SOC)[5] se encargan de la protección, detección y respuesta a los incidentes de ciberseguridad, y pueden mejorar la capacidad de un país para gestionar los incidentes de ciberseguridad. Los EIII o los SOC pueden servir para crear una base de conocimientos que respalde la aplicación por un país de una estrategia nacional de ciberseguridad, así como un método para la protección de infraestructuras críticas de información; apoyar la creación de una cultura y un ecosistema nacionales en materia de ciberseguridad, e iniciativas de sensibilización conexas; apoyar el desarrollo de plataformas nacionales conexas en materia de ciberseguridad, como los servicios electrónicos del Gobierno, la identidad nacional y los marcos de gestión de accesos; y seguir permitiendo que el país desarrolle y mejore su respuesta a los incidentes y sus capacidades de coordinación.

1.1 ¿Su país dispone de EIII/EIISI/EIEI o SOC nacionales o del Gobierno plenamente operativos?

Código-GCIv5: Tech1.1

Fundamento-GCIv5: Los Equipos de Intervención en caso de Incidente Informático (EIII), así como los Equipos de Intervención en caso de Incidente de Seguridad Informática (EIISI), los Equipos de Intervención en caso de Emergencia Informática (EIEI) y los Centros de Operaciones de Seguridad (SOC) se encargan de la protección, detección y respuesta a los incidentes de ciberseguridad. Se considera que los EIII/EIISI/EIEI y SOC son plenamente operacionales, en los siguientes casos:

- Disponen de una estructura organizacional definida y aprobada.
- Cuentan con personal formado y cualificado.
- Se han instaurado instalaciones seguras (se han implementado medidas adecuadas para proteger las instalaciones contra las amenazas físicas y del entorno).
- Se han elaborado e implementado procesos y procedimientos detallados para sus operaciones.
- Se ha adoptado e implementado la tecnología necesaria para sus operaciones.
- Se han implementado procesos para interactuar con partes interesadas y socios clave.

[5] https://ieeexplore.ieee.org/document/9296846

- Prestan servicios de manera eficaz y efectiva a su comunidad.

Los procesos iniciales para poner en marcha un EIII pueden abarcar la evaluación (medir el grado de preparación para crear un EIII, así como preparar a los interesados pertinentes para que presten la colaboración necesaria), el diseño (preparar el documento de diseño específico para el EIII) y el proceso de creación (implementar la infraestructura, establecer relaciones con las partes interesadas y los miembros de la comunidad, establecer procesos y servicios para los miembros de la comunidad, lanzar las operaciones, y solicitar la adhesión a una asociación internacional).

1.2 Actividades de los EIII/EIISI/EIEI o SOC nacionales

Código-GCIv5: Tech1.2

Fundamento-GCIv5: Los Equipos nacionales de Intervención en caso de Incidente Informático (EIII), así como los Equipos de Intervención en caso de Incidente de Seguridad Informática (EIISI), los Equipos de Intervención en caso de Emergencia Informática (EIEI) y los Centros de Operaciones de Seguridad (SOC) se encargan de la protección, detección y respuesta a los incidentes de ciberseguridad. Se trata de un punto central en lo que respecta a la comunicación de información sobre incidentes de ciberseguridad. También brindan información y asistencia técnica para ayudar a las organizaciones a prevenir, mitigar y responder a los incidentes cibernéticos. Además, un EIII o SOC nacional lleva a cabo investigaciones sobre cuestiones de ciberseguridad y elabora prácticas óptimas y directrices para responder a los incidentes cibernéticos.

1.2.1 ¿Su EIII/EIISI/EIEI o SOC nacional/del Gobierno desarrolla y lleva a cabo actividades de sensibilización en materia de ciberseguridad?

Código-GCIv5: Tech1.2.1

Fundamento-GCIv5: Los EIII o SOC nacionales pueden desempeñar un importante papel en la realización de campañas de sensibilización en materia de ciberseguridad; en su función de organismos de coordinación centrales, podrían adquirir cada vez más visibilidad sobre las ciberamenazas actuales y emergentes, los desafíos de ciberseguridad, las vulnerabilidades, la información sobre las principales tendencias de la ciberseguridad, los avances tecnológicos en el sector de la ciberseguridad y las prácticas idóneas para detectar y responder a las ciberamenazas. A fin de mejorar la cultura de la ciberseguridad y promover los conocimientos sobre las medidas, buenas prácticas y comportamientos en materia de ciberseguridad, los EIII/EIISI/EIEI o SOC deben diseñar, llevar a cabo y/o coordinar iniciativas de sensibilización en materia de ciberseguridad y actividades adaptadas a diversos interesados, que se basen en información recabada sobre la evolución del panorama de las amenazas, las principales tendencias en materia de ciberseguridad y las mejores prácticas.

1.2.2 ¿Su EIII/EIISI/EIEI o SOC nacional/del Gobierno lleva a cabo ejercicios periódicos en materia de ciberseguridad (cibersimulacros)?

Código-GCIv5: Tech1.2.2

Fundamento-GCIv5: Los ejercicios de ciberseguridad son eventos planificados en los que una organización simula un ciberataque a fin de desarrollar o poner a prueba competencias en materia de prevención, detección, mitigación, respuesta o recuperación tras el ataque. Los ejercicios de ciberseguridad que se llevan a cabo de manera periódica, en asociación con interesados pertinentes, son una medida proactiva para mejorar la preparación y resiliencia en materia de ciberseguridad. Los EIII/EIISI/EIEI o SOC deben desarrollar y llevar a cabo periódicamente ejercicios de gestión de crisis/incidentes en que también participen las entidades públicas o privadas pertinentes del país, a fin de poner a prueba sus capacidades de respuesta a incidentes.

1.2.3 ¿Su EIII/EIISI/EIEI o SOC nacional/del Gobierno emite avisos públicos en materia de ciberseguridad?

Código-GCIv5: Tech1.2.3

Fundamento-GCIv5: Los avisos públicos de ciberseguridad garantizan que los organismos y departamentos estén al corriente de las posibles amenazas a la ciberseguridad y puedan adoptar medidas. Además, los avisos pueden ayudar a promover respuestas coordinadas a las amenazas a la ciberseguridad.

1.3 ¿Los EIII/EIISI/EIEI o SOC nacionales o del Gobierno están afiliados al Foro de los equipos de intervención en caso de incidentes de seguridad (FIRST) y/o alistados por el Grupo Especial de EIISI?

Código-GCIv5: Tech1.3

Fundamento-GCIv5: Los EIII o SOC nacionales afiliados a FIRST gozan de los beneficios de una red mundial de EIII, formación y recursos, conocimientos técnicos del personal de FIRST y oportunidades para colaborar y compartir las mejores prácticas. Para formar parte de FIRST, se requiere la implicación activa de los países. La condición de miembro del Grupo Especial de EIISI se examinará para esta pregunta.

1.4 ¿Los EIII/EIISI/EIEI o SOC nacionales o del Gobierno antes señalados están afiliados a un EIII regional (como APCERT, PACSON, AFRICA CERT, ENSIA, OIC, OAS)?

Código-GCIv5: Tech1.4

Fundamento-GCIv5: La afiliación a un EIII regional abarca cualquier relación oficial o periódica con cualquier otro grupo de EIII regional. La afiliación a un EIII o EIEI regional ofrece muchas ventajas, por ejemplo, el intercambio de conocimientos y experiencias: con frecuencia, los EIII y EIEI son capaces de compartir conocimientos y experiencias pertinentes para las circunstancias de un país.

2 EIEI/EIII/EIISI o SOC sectoriales

Código-GCIv5: Tech2

Fundamento-GCIv5: Un EIEI/EIII/EIISI o SOC sectorial sirve a los miembros de su comunidad que trabajan en un determinado sector, como el sector financiero, las instituciones académicas, la energía, la salud, las telecomunicaciones, las instalaciones públicas, la infraestructura crítica, etc. Un EIII o SOC sectorial sirve a los miembros de su comunidad mediante información y servicios especializados en materia de amenazas. Los países pueden tener EIII o SOC sectoriales compartidos con otros países, en cuyo marco cada EIII o SOC sectorial sirve a los miembros de un sector específico en varios países. A los efectos de este indicador, no se aceptan los EIII militares.

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

Código-GCIv5: Tech2.1

Fundamento-GCIv5: Un EIEI/EIII/EIISI o SOC sectorial sirve a los miembros de su comunidad que trabajan en un determinado sector, como el sector financiero, las instituciones académicas, la energía, la salud, las telecomunicaciones, las instalaciones públicas, la infraestructura crítica, etc. Un EIII o SOC sectorial sirve a los miembros de su comunidad mediante información y servicios especializados en materia de amenazas. Los países pueden tener EIII o SOC sectoriales compartidos con otros países, en cuyo marco cada EIII sectorial sirve a los miembros de un sector específico en varios países. A los efectos de este indicador, no se aceptan los EIII militares. Se considera que los EIII/EIISI/EIEI y SOC sectoriales son plenamente operacionales, en los siguientes casos:

- Disponen de una estructura organizacional definida y aprobada.
- Cuentan con personal formado y cualificado.
- Se han instaurado instalaciones seguras (se han implementado medidas adecuadas para proteger las instalaciones contra las amenazas físicas y del entorno).

- Se han elaborado e implementado procesos y procedimientos detallados para sus operaciones.
- Se ha adoptado e implementado la tecnología necesaria para sus operaciones.
- Se han implementado procesos para interactuar con partes interesadas y socios clave.
- Prestan servicios de manera eficaz y efectiva a su comunidad.

Los EIII sectoriales parcialmente implementados pueden abarcar la evaluación (medir el grado de preparación para crear un EIII sectorial, así como preparar a los interesados pertinentes para que presten la colaboración necesaria), el diseño (preparar el documento de diseño específico para el EIII) y el proceso de creación (implementar la infraestructura, establecer relaciones con las partes interesadas y los miembros de la comunidad, establecer procesos y servicios para los miembros de la comunidad, lanzar las operaciones, y solicitar la adhesión a una asociación internacional).

2.2 Actividades de los EIII/EIISI/EIEI y SOC sectoriales

Código-GCIv5: Tech2.2

Fundamento-GCIv5: Los Equipos sectoriales de Intervención en caso de Incidente Informático (EIII), así como los Equipos sectoriales de Intervención en caso de Incidente de Seguridad Informática (EIISI), los Equipos de sectoriales Respuesta a Emergencias Informáticas (EIEI) y los Centros sectoriales de Operaciones de Seguridad (SOC) se encargan de la protección, detección y respuesta a los incidentes de ciberseguridad.

Los EIII y los SOC sectoriales son el punto central en materia de comunicación de información sobre incidentes de ciberseguridad en un determinado sector. También brindan información y asistencia técnica para ayudar a las organizaciones del sector a prevenir, mitigar y responder a los incidentes cibernéticos. Además, un EIII o SOC sectorial lleva a cabo investigaciones sobre cuestiones de ciberseguridad y elabora prácticas óptimas y directrices para responder a los incidentes cibernéticos.

2.2.1 ¿Los EIII/EIISI/EIEI o SOC sectoriales desarrollan y llevan a cabo actividades de sensibilización en materia de ciberseguridad para el sector?

Código-GCIv5: Tech2.2.1

Fundamento-GCIv5: Los EIII o SOC sectoriales pueden desempeñar un importante papel en la realización de campañas de sensibilización en materia de ciberseguridad para un sector determinado. En su función de organismos de coordinación para el sector, tienen información sobre las tendencias en materia de ciberseguridad pertinentes para sus partes interesadas. Sobre la base de información relativa a amenazas generales y específicas del sector, los EIII sectoriales pueden ayudar a preparar y llevar a cabo actividades de sensibilización destinadas a diversos grupos de interesados a fin de mejorar los comportamientos seguros en el ámbito cibernético.

2.2.2 ¿Los EIII/EIISI/EIEI o SOC sectoriales participan periódicamente en ejercicios nacionales de ciberseguridad (cibersimulacros)?

Código-GCIv5: Tech2.2.2

Fundamento-GCIv5: Los ejercicios de ciberseguridad son eventos planificados en los que una organización simula un ciberataque a fin de desarrollar o poner a prueba competencias en materia de prevención, detección, mitigación, respuesta o recuperación tras el ataque. La participación de EIII sectoriales en ejercicios nacionales de ciberseguridad constituye una medida proactiva para mejorar las capacidades generales en materia de ciberseguridad.

2.2.3 ¿Los EIII/EIISI/EIEI o SOC sectoriales comparten incidentes relacionados con el sector a su comunidad?

Código-GCIv5: Tech2.2.3

Fundamento-GCIv5: El hecho de compartir información pertinente sobre amenazas puede permitir a las partes interesadas de un sector tener un mayor conocimiento de las amenazas y vulnerabilidades pertinentes y mejorar los tiempos y la eficacia de las respuestas. Además, esto puede ayudar a crear una respuesta más coordinada a los incidentes de ciberseguridad en todo el Gobierno, el sector privado y la población general.

3 Marco nacional para la aplicación de las normas de ciberseguridad

Código-GCIv5: Tech3

Fundamento-GCIv5: Los marcos nacionales para la aplicación de las normas de ciberseguridad implican la existencia de un marco (o marcos) aprobado(s) (o avalado(s)) por el Gobierno para la certificación y acreditación de profesionales conforme a normas de ciberseguridad internacionalmente reconocidas. Entre estas certificaciones, acreditaciones y normas están, 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), las relacionadas con los requisitos normativos de los sistemas de gestión de la seguridad informática de la ISO 27001, la ISO 28000 sobre la seguridad de la gestión de las cadenas de suministro, la ISA 62443 sobre la seguridad de los sistemas industriales de automatización y control, etc.

3.1 ¿Su gobierno tiene un marco para la aplicación/adopción de normas de ciberseguridad reconocidas en el plano nacional o internacional?

Código-GCIv5: Tech3.1

Fundamento-GCIv5: Los marcos nacionales para la aplicación de las normas de ciberseguridad implican la existencia de un marco (o marcos) aprobado(s) (o avalado(s)) por el Gobierno para la aplicación/adopción de normas de ciberseguridad reconocidas en el plano nacional o internacional. Un marco podría definir un plan o una hoja de ruta para la aplicación/adopción de normas, las partes interesadas implicadas, los procesos que se utilizarán para actualizaciones futuras y otros métodos por los que se orienta la aplicación.

Entre esas normas están, 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), las relacionadas con los requisitos normativos de los sistemas de gestión de la seguridad informática de la ISO 27001, la ISO 28000 sobre la seguridad de la gestión de las cadenas de suministro, la ISA 62443 sobre la seguridad de los sistemas industriales de automatización y control, etc.

3.2 ¿El marco para la aplicación/adopción de normas de ciberseguridad reconocidas en el plano nacional o internacional aborda infraestructuras críticas?

Código-GCIv5: Tech3.2

Fundamento-GCIv5: Es fundamental abordar las infraestructuras críticas como parte de todo marco para la aplicación/adopción de normas de ciberseguridad reconocidas en el plano nacional o internacional a fin de mejorar la protección y resiliencia de las infraestructuras críticas y ayudarlas a reducir las vulnerabilidades y a gestionar de manera eficaz los riesgos en materia de ciberseguridad.

Medidas organizacionales

Fundamento-GCIv5: Las medidas organizacionales son necesarias para el cumplimiento adecuado de la posición de un país en materia de ciberseguridad. El Gobierno debe determinar objetivos estratégicos, así como un plan exhaustivo respecto de la implementación, el cumplimiento y la medición. Se deben crear y habilitar estructuras del Gobierno que permitan llevar a la práctica su posición en materia de ciberseguridad, y supervisar la consecución y evaluación de los resultados. Si no se dispone de una red organizacional bien definida de socios, que trabajen en toda la industria, la sociedad civil y las instituciones académicas, las medidas adoptadas en los diferentes sectores e industrias serán dispares y no guardarán relación, lo que frustraría los esfuerzos realizados para alcanzar la armonización nacional en cuanto al desarrollo de capacidades de ciberseguridad.

Las estructuras organizacionales se pueden medir sobre la base de la existencia y el número de instituciones y estrategias que organizan el desarrollo de la ciberseguridad a escala nacional. La creación de una estructura organizacional eficaz es necesaria para promover el desarrollo de la ciberseguridad, luchar contra la ciberdelincuencia y fomentar la función de supervisión, alerta y respuesta a los incidentes a fin de garantizar una coordinación interinstitucional, intersectorial y transfronteriza entre las iniciativas actuales y nuevas. El subgrupo comprende los indicadores de desempeño siguientes:

1 Estrategia nacional de ciberseguridad

Código-GCIv5: Org1

Fundamento-GCIv5: Una estrategia nacional de ciberseguridad proporciona un marco de asignación de recursos[6] para determinar los objetivos nacionales en materia de ciberseguridad y priorizar los recursos destinados a su consecución con miras a mejorar la seguridad y resiliencia de un país[7]. También permite al Gobierno cooperar con todas las partes interesadas pertinentes en el plano nacional. Además, una estrategia nacional de ciberseguridad podría ayudar a promover la innovación y proteger la privacidad y las libertades civiles. En la estrategia se deben establecer claramente los objetivos nacionales de ciberseguridad y determinar la estructura de gobernanza que se ocupará de su implementación[8].

1.1 ¿Tiene su país una Estrategia o Política Nacional de Ciberseguridad, ya sea de autónoma o como parte de otro documento?

Código-GCIv5: Org1.1

Fundamento-GCIv5: No cabe duda de que la ciberseguridad es una cuestión fundamental para todas las naciones. Una Estrategia Nacional de Ciberseguridad proporciona un marco de asignación de recursos para proteger las infraestructuras críticas de una nación. También permite a los Gobiernos trabajar con el sector privado a fin de determinar y mitigar las ciberamenazas. Además, una estrategia nacional de ciberseguridad puede ayudar a promover la innovación y proteger la privacidad y las libertades civiles.

1.2 Prioridades estratégicas nacionales de ciberseguridad

Código-GCIv5: Org1.2

Fundamento-GCIv5: Una estrategia nacional con prioridades permite dar una respuesta coordinada a los riesgos cibernéticos. Dado que cada país se enfrenta a diferentes desafíos en materia de ciberseguridad, el hecho de centrarse en áreas específicas de la ciberseguridad ayuda a los países a priorizar sus recursos y coordinar una respuesta a las ciberamenazas. Es posible que la mayoría de las guías para elaborar una Estrategia Nacional de Ciberseguridad se centren en diferentes prioridades como "Desarrollar una Estrategia

---

6 https://www.enisa.europa.eu/topics/national-cyber-security-strategies

7 https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

8 https://ncsguide.org/the-guide/

Nacional de Ciberseguridad[9]". Asimismo, es posible que las áreas prioritarias también hagan referencia a las "Áreas de interés" respecto de algunas estrategias[10]. Las preguntas 1.2.1 a 1.2.4 incluyen áreas prioritarias que se podrían abordar en la Estrategia Nacional de Ciberseguridad de un país. Sin embargo, los países quizás tengan otras áreas prioritarias.

1.2.1 ¿En la Estrategia Nacional de Ciberseguridad de su país se aborda la protección de las infraestructuras nacionales críticas?

Código-GCIv5: Org1.2.1

Fundamento-GCIv5: Las infraestructuras nacionales críticas incluyen todo tipo de infraestructuras, desde la red eléctrica y los sistemas de abastecimiento de agua hasta las redes de transporte y las instituciones financieras. El fallo de alguna de ellas podría conducir a un país al caos. De esto se desprende la importancia de que una Estrategia Nacional de Ciberseguridad tenga un plan para garantizar que todas estén protegidas correctamente, dado que las infraestructuras críticas son fundamentales para mantener el orden y la seguridad públicos, importantes para la economía de un país y esenciales para la seguridad nacional.

1.2.2 ¿Incorpora la estrategia nacional de ciberseguridad de su país los principios de gestión del ciclo de vida, con seguimiento, evaluación y actualizaciones periódicas?

Código-GCIv5: Org1.2.3

Fundamento-GCIv5: La estrategia nacional de ciberseguridad de un país debe incorporar los principios de gestión del ciclo de vida[11], con seguimiento, evaluación y actualizaciones periódicas para asegurar que la estrategia siga siendo eficaz y pertinente. Esto ayuda a que se identifiquen y aborden los riesgos asociados a una determinada estrategia, y a que esta se adapte según sea necesario para reflejar los cambios del entorno. El enfoque de la gestión del ciclo de vida también ayuda a garantizar que todas las partes interesadas participen en el desarrollo y la aplicación de la estrategia, y a que todos comprendan claramente su función y sus responsabilidades. Esto propicia que la estrategia se aplique eficazmente y que todos trabajen con el mismo objetivo. Por último, al utilizar los principios de gestión del ciclo de vida, es posible supervisar la aplicación de la estrategia y evaluar sus resultados. Esto permite corregir a tiempo el rumbo cuando sea necesario y ayuda a garantizar que la estrategia siga siendo pertinente y eficaz con el paso del tiempo.

1.2.3 ¿Dispone la estrategia nacional de ciberseguridad de su país de un mecanismo que garantice la consulta periódica con los expertos en ciberseguridad y con las partes interesadas?

Código-GCIv5: Org1.2.4

Fundamento-GCIv5: El panorama de la ciberseguridad está en constante evolución y, por consiguiente, es importante contar con un mecanismo que garantice la actualización periódica de la estrategia nacional de ciberseguridad. Los expertos en ciberseguridad pueden aportar valiosa información sobre las amenazas más recientes y sobre la mejor manera de contrarrestarlas. Durante el proceso de la estrategia nacional de ciberseguridad, se debe consultar también a las partes interesadas, como las empresas y los ciudadanos, para que los resultados de las políticas sean más eficaces. Las partes interesadas pueden proporcionar información sobre el funcionamiento de la estrategia y formular sugerencias para mejorarla. Mediante la consulta a los expertos y a las partes interesadas, la estrategia nacional de ciberseguridad puede adaptarse a las necesidades del país.

---

9 http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf

10 https://ncsguide.org/the-guide/

11 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

1.2.4 ¿Dispone su país de un plan de acción o una hoja de ruta para la aplicación de su estrategia de ciberseguridad?

Código-GCIv5: Org1.2.5

Fundamento-GCIv5: La definición de un plan de acción o una hoja de ruta para la aplicación de una estrategia de ciberseguridad es parte fundamental de la protección de la infraestructura digital de un país y de sus ciudadanos. A falta de un plan, resulta difícil asignar recursos y medir los progresos, lo que puede mermar la eficacia y originar deficiencias de cobertura. Un plan de acción bien definido o una hoja de ruta puede propiciar que todas las partes interesadas sean conscientes de sus funciones y responsabilidades en la aplicación de la estrategia, y que el plan sea factible y realista. También puede ayudar a seguir y evaluar el impacto de la estrategia a largo plazo, con el fin de hacer los ajustes necesarios.

2 Organismo responsable

Código-GCIv5: Org2

Fundamento-GCIv5: Un organismo responsable es una autoridad competente con la responsabilidad de gestionar la ciberseguridad. Esta autoridad debe ser un dirigente (individuo o entidad) que ocupe un cargo elevado y profundamente arraigado en las altas instancias del gobierno para dar orientaciones, coordinar la acción y supervisar la ejecución de la estrategia. Esa autoridad nacional competente también debería actuar como entidad gestora para definir y aclarar las funciones, responsabilidades, procesos, potestades de decisión y tareas necesarias para garantizar una postura eficaz en materia de ciberseguridad.

2.1 ¿Existe en su país un organismo o ministerio responsable de la ciberseguridad a nivel nacional?

Código-GCIv5: Org2.1

Fundamento-GCIv5: Un organismo nacional o un ministerio con responsabilidades en materia de ciberseguridad a nivel nacional puede apoyar la gestión cohesiva de las amenazas contra la ciberseguridad y las acciones proactivas de ciberseguridad. Ese organismo o ministerio debería colaborar con otros departamentos gubernamentales, el sector privado, la sociedad civil y demás actores pertinentes para desarrollar y ejecutar una estrategia nacional de ciberseguridad.

2.2 ¿Existe en su país un organismo o ministerio con responsabilidades en materia de ciberseguridad relacionada con la protección nacional de las infraestructuras críticas?

Código-GCIv5: Org2.2

Fundamento-GCIv5: Un organismo o ministerio con responsabilidades en materia de infraestructuras esenciales a nivel nacional apoya la resiliencia y la continuidad de las operaciones. Las infraestructuras críticas pueden sustentar servicios esenciales como el agua, la electricidad y las telecomunicaciones, que son fundamentales para el funcionamiento de una sociedad. Un organismo nacional o un ministerio con responsabilidades en materia de infraestructuras críticas puede ayudar a prevenir o mitigar sus posibles alteraciones colaborando con las partes interesadas.

2.3 ¿Existe en su país un organismo, ministerio, grupo especial u otro órgano encargado de supervisar el desarrollo de la capacidad nacional de ciberseguridad?

Código-GCIv5: Org2.3

Fundamento-GCIv5: Un enfoque coordinado e integral para desarrollar las competencias y capacidades necesarias en materia de ciberseguridad puede reducir la probabilidad de incidentes de ciberseguridad y mejorar la resiliencia. La ciberseguridad es una preocupación multidimensional que requiere la coordinación y cooperación de diversos organismos gubernamentales y entidades del sector privado.

2.4 La coordinación de las iniciativas y actividades de Protección de la Infancia en Línea ¿es responsabilidad de algún organismo, ministerio, grupo especial u otro órgano en su país?

Código-GCIv5: Org2.5

Fundamento-GCIv5: La coordinación entre las partes interesadas y los grupos objetivo, así como la supervisión de las actividades, reviste importancia para asegurar la complementariedad de las intervenciones de Protección de la Infancia en Línea (PIeL). La responsabilidad de coordinar las iniciativas y actividades de PIeL a nivel nacional puede recaer en un organismo independiente, un ministerio, un grupo especial u otro órgano, o bien formar parte de un conjunto más amplio de responsabilidades de cualquiera de esas instituciones.

3 Métricas de ciberseguridad

Código-GCIv5: Org3

Fundamento-GCIv5: Las métricas de ciberseguridad consisten en cualquier ejercicio de referencia nacional o sectorial oficialmente reconocido o utilizado para cuantificar los avances en materia de ciberseguridad, estrategias de evaluación de riesgos, auditorías sobre ciberseguridad y otros instrumentos o actividades de calificación o evaluación del rendimiento resultante para tratar de lograr mejoras futuras. Por ejemplo, la norma ISO/CEI 27004[12] se ocupa de las mediciones relacionadas con la gestión de la seguridad de la información.

3.1 ¿Se realizan auditorías sobre ciberseguridad a nivel nacional?

Código-GCIv5: Org3.1

Fundamento-GCIv5: La realización de auditorías sobre ciberseguridad a nivel nacional puede estar motivada por preocupaciones de seguridad o puede ser el resultado de la aplicación de disposiciones reglamentarias u otros documentos orientativos. Cuando se aplica la normativa de auditoría sobre ciberseguridad, es necesario realizar auditorías efectivas a nivel nacional. Los informes de auditoría, resúmenes, presentaciones, memorandos u otros materiales similares pueden ser el resultado de esas auditorías.

La auditoría sobre ciberseguridad consiste en la identificación de posibles vulnerabilidades. Una vez identificados, se pueden evaluar y priorizar para determinar el nivel de riesgo que suponen para la organización. Existen diversas herramientas útiles para evaluar esas vulnerabilidades, como la exploración de vulnerabilidades, las pruebas de penetración y los ejercicios de equipo rojo. Como cada una de estas herramientas tiene sus propias fortalezas y debilidades, es importante seleccionar aquella que más se adecue a la situación. Una vez identificadas las vulnerabilidades, es importante determinar el nivel de riesgo que suponen para la organización.

3.2 ¿Existen métricas o herramientas para evaluar los riesgos de ciberseguridad a nivel nacional?

Código-GCIv5: Org3.2

Fundamento-GCIv5: Las métricas para evaluar los riesgos de ciberseguridad a nivel nacional variarán según los países y deberán reflejar las amenazas, las capacidades y los problemas específicos de cada país. Esto puede hacerse mediante diversas métricas, como los factores de impacto, los factores de probabilidad y los valores de los activos. A través de estas métricas es posible determinar el nivel y la gravedad del riesgo que supone cada vulnerabilidad y adoptar las medidas correctivas oportunas[13]. La norma ISO/CEI 27004[14] ofrece técnicas de seguridad que permiten supervisar, medir, analizar y evaluar los riesgos relacionados con la ciberseguridad.

---

12 https://www.iso.org/standard/64120.html

13 https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf

14 https://www.iso.org/standard/64120.html

3.3 ¿Existen medidas para evaluar el nivel de desarrollo de la ciberseguridad a nivel nacional con herramientas como el Modelo de Madurez de las Capacidades de Ciberseguridad, el Índice de Preparación Cibernética o cualquier otra herramienta de evaluación pertinente?

Código-GCIv5: Org3.3

Fundamento-GCIv5: La evaluación del nivel de desarrollo de la ciberseguridad puede permitir a los países conocer la madurez y la fiabilidad de su infraestructura de ciberseguridad. Las medidas específicas adoptadas a tal efecto pueden variar según los países. El Modelo de Madurez de la Ciberseguridad[15] y el Índice de Preparación Cibernética[16] son algunas de las herramientas que se suelen utilizar para evaluar el nivel de desarrollo de la ciberseguridad a nivel nacional, además de cualquier otro indicador que los países decidan adoptar. Entre las herramientas de evaluación comprendidas en esta pregunta no se incluye la participación de los países en el Índice Mundial de Ciberseguridad (GCI) de la UIT.

4 Estrategias e iniciativas de Protección de la Infancia en Línea

Código-GCIv5: Org4

Fundamento-GCIv5: La Protección de la Infancia en Línea (PIeL) es la expresión que engloba las estrategias e iniciativas destinadas a proteger a los niños de los daños o la explotación cuando acceden a Internet: desde velar por que los niños utilicen programas informáticos y herramientas de filtrado apropiados para su edad, hasta educar a los padres y a los niños sobre la seguridad en línea. Existen diversas estrategias e iniciativas de PieL, generalmente adaptadas a las necesidades específicas de los niños en el país de destino.

4.1 ¿Dispone su país de una estrategia nacional para la Protección de la Infancia en Línea, asociada a las actuales iniciativas de Protección de la Infancia en Línea?

Código-GCIv5: Org4.1

Fundamento-GCIv5: En las directrices de PieL se recomienda contar con una estrategia holística específica en esta materia, que abarque ámbitos relacionados con la infancia como la salud, el bienestar y el desarrollo de competencias. Cuando la estrategia de PieL se integra en otro ámbito, a menudo no es holística y suele centrarse únicamente en el abuso sexual o la pornografía infantil.

4.2 ¿Existen en su país mecanismos de información y capacidades gubernamentales a nivel nacional para ayudar a proteger a los niños en línea?

Código-GCIv5: Org4.2

Fundamento-GCIv5: Las personas físicas pueden señalar y denunciar los problemas que afectan a la infancia en línea a través de los mecanismos de denuncia accesibles al público en general con fines de identificación, seguimiento y vigilancia de las cuestiones relacionadas con la infancia en línea. Estos mecanismos también pueden abarcar capacidades técnicas como la alerta de contenidos. Los EIII y los organismos encargados de hacer cumplir la ley pueden habilitar otros mecanismos de denuncia. Lo ideal sería disponer de diversos sistemas, como líneas de ayuda nacionales o portales en línea con sistemas de derivación y apoyo.

---

15 https://gcscc.ox.ac.uk/cmm-2021-edition

16 https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Medidas de desarrollo de capacidades

Fundamento-GCIv5: El desarrollo de capacidades es intrínseco a las medidas jurídicas, técnicas y organizativas contempladas en el Índice de Ciberseguridad Global y constituye una fuerza motriz del desarrollo digital. Los programas de desarrollo de capacidades tienen como objetivo ampliar las competencias, los conocimientos y la confianza en el ámbito local, colmando la brecha de competencias y construyendo un ecosistema tecnológico más inclusivo. Además, la capacidad de prestar servicios digitales inclusivos depende cada vez más de la existencia de recursos humanos calificados. Los marcos de desarrollo de capacidades destinados a promover la ciberseguridad pueden incluir actividades de sensibilización y se cuantifican en función de la existencia y el número de programas de investigación y desarrollo, programas de educación y formación, y profesionales y organismos del sector público certificados.

1 Campañas públicas de sensibilización sobre ciberseguridad

Código-GCIv5: CapDev1

Fundamento-GCIv5: El principal objetivo de las campañas públicas de sensibilización sobre ciberseguridad es incentivar la adopción de un comportamiento seguro en línea. Para lograr un cambio de comportamiento significativo, las campañas públicas de sensibilización deben convencer a las personas de que la información es importante, ayudarles a entender cómo afrontar la cuestión y persuadirles de que lo hagan teniendo en cuenta otras prioridades[17]. Las campañas de sensibilización se enfrentan a numerosas dificultades, sobre todo porque requieren un esfuerzo ingente y numerosas competencias y porque "infundir miedo rara vez provoca cambios de comportamiento[18]". Las campañas de sensibilización específicas pueden adaptar las intervenciones para abordar mejor estas preocupaciones.

1.1 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas específicamente a las mipymes?

Código-GCIv5: CapDev1.1

Fundamento-GCIv5: Las microempresas y pequeñas y medianas empresas (mipymes) son una parte vital de la economía de un país y deben ser conscientes de las amenazas contra la ciberseguridad que podrían afectar a sus negocios. Se enfrentan a dificultades específicas en lo relativo a la mejora de la ciberseguridad, como la falta de recursos y de conocimientos técnicos. Se pueden abordar estos problemas concretos mediante intervenciones específicas que se centren en maximizar el impacto para las mipymes. Las campañas de sensibilización en materia de ciberseguridad, dirigidas específicamente a las pymes, pueden proporcionarles información sobre cómo protegerse de los ciberataques y cómo responder si sufren uno.

1.2 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas específicamente al sector privado en general?

Código-GCIv5: CapDev1.2

Fundamento-GCIv5: Cualquier actor del sector privado se enfrenta a problemas de ciberseguridad. Más allá de las necesidades específicas de las mipymes, las campañas públicas de sensibilización sobre los riesgos de ciberseguridad que afectan al sector privado pueden ayudar a mejorar las pautas de actuación.

---

[17] Rogers, R.W., Attitude change and information integration in fear appeals. Psychological Reports, 56 (1985) 183-188 Witte, K. Message and conceptual confounds in fear appeals: The role of threat, fear and efficacy. The Southern Communication Journal, 58(2) (1993) 147-155

[18] https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

1.3 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas específicamente a los organismos del sector público de ámbito local, municipal y nacional, y a los trabajadores del sector público?

Código-GCIv5: CapDev1.3

Fundamento-GCIv5: Los organismos del sector público pueden beneficiarse de las campañas de sensibilización sobre ciberseguridad. Estas campañas están concebidas específicamente para llegar a los trabajadores del sector público, y proporcionan información importante sobre cómo proteger los datos sensibles y las infraestructuras críticas.

1.4 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas específicamente a la sociedad civil?

Código-GCIv5: CapDev1.4

Fundamento-GCIv5: Las organizaciones de la sociedad civil pueden ser objeto de ciberataques. Estos ataques pueden ir acompañados de acoso en línea, sustracción de datos o robo de información financiera. Las organizaciones de la sociedad civil deben ser conscientes de los riesgos y protegerse mediante la impartición de formación al personal, el uso de contraseñas seguras y la actualización del *software* antivirus. Los países pueden mejorar la protección de esas organizaciones vitales frente a posibles daños mediante actividades de sensibilización que les ayuden a defender de forma segura sus organizaciones, redes y los datos de los ciudadanos.

1.5 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas a la población en general?

Código-GCIv5: CapDev1.5

Fundamento-GCIv5: La ciberseguridad no incumbe solamente a las empresas y los gobiernos. Los ciudadanos son las partes más vulnerables a la ciberdelincuencia, pero a menudo carecen de conocimientos y herramientas para protegerse. Los ciberdelincuentes buscan constantemente nuevas formas de robar datos, dinero o identidades. Pueden hacerlo pirateando sistemas informáticos, robando contraseñas o creando sitios web falsos. A nivel nacional, el gobierno puede sensibilizar a los ciudadanos y educarlos para que se protejan utilizando contraseñas seguras, teniendo cuidado al abrir los correos electrónicos y no facilitando nunca información personal en línea. Los ciudadanos también deben ser conscientes de las señales de alerta de una estafa o un ataque de suplantación de identidad (*phishing*). Los gobiernos deben comprometerse a sensibilizar a toda la ciudadanía sobre la ciberseguridad e instar a todas las personas a que adopten las medidas necesarias para protegerse en línea.

1.6 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas específicamente a las personas mayores (ancianos)?

Código-GCIv5: CapDev1.6

Fundamento-GCIv5: A medida que envejece nuestra población, crece el número de personas mayores que van a utilizar Internet y dispositivos electrónicos. Por desgracia, esto los convierte en un objetivo prioritario de los ciberdelincuentes. Las personas mayores son más vulnerables a las ciber amenazas por varias razones: puede que no sean tan conscientes de los peligros que conlleva el uso de Internet, que carezcan de conocimientos técnicos para protegerse, que sean más propensas a dejarse engañar por estafas y que tiendan menos a denunciar un ciberdelito.

Por esta razón, los gobiernos están desarrollando campañas de sensibilización en materia de ciberseguridad para que la población mayor se mantenga segura en Internet y proteja su información personal.

1.7 ¿Tiene su gobierno campañas públicas de sensibilización dirigidas a las personas con necesidades específicas, incluidas las personas con discapacidad?

Código-GCIv5: CapDev1.7

Fundamento-GCIv5: A medida que el modelo médico de discapacidad da paso a uno basado en los derechos humanos, la supresión de los obstáculos sociales a que se enfrentan las personas con necesidades especiales, como "las barreras arquitectónicas y comunicativas, las actitudes y las estructuras de la sociedad[19]", puede mejorar la capacidad y la seguridad de las personas con discapacidad. Existe también una mayor necesidad de sensibilización y formación en materia de ciberseguridad dirigida específicamente a esas personas. Las personas con discapacidad son más vulnerables a los ciberataques por varias razones, como su falta de familiaridad con la tecnología, su dependencia de la ayuda de los demás y su reticencia a pedirla. Por lo tanto, la educación y la sensibilización son esenciales, y los gobiernos deben velar por que todos los miembros de la comunidad estén incluidos en los esfuerzos de ciberseguridad. Abordar las necesidades de esta población mediante campañas públicas de sensibilización es importante para el desarrollo inclusivo y eficaz de capacidades en materia de ciberseguridad.

1.8 ¿Tiene su gobierno alguna campaña pública de sensibilización dirigida específicamente a padres, educadores y niños como parte de los esfuerzos de Protección de la Infancia en Línea (PieL)?

Código-GCIv5: CapDev1.8

Fundamento-GCIv5: El gobierno debe promover el desarrollo de campañas públicas de sensibilización dirigidas específicamente a padres y educadores para que amplíen sus conocimientos sobre los riesgos y daños a que se exponen los niños y jóvenes y aumentar las capacidades para hacer frente a los problemas relacionados con la PieL.

1.9 ¿Tiene su gobierno alguna campaña pública de sensibilización dirigida específicamente a los niños como parte de los esfuerzos de Protección de la Infancia en Línea (PieL)?

Código-GCIv5: CapDev1.9

Fundamento-GCIv5: La presencia en línea durante más tiempo aumenta la vulnerabilidad de los menores. Los menores son especialmente vulnerables a las ciberamenazas, ya que pueden no ser tan conscientes de los peligros y no tener el mismo nivel de conocimientos y experiencia en ciberseguridad que los adultos. Los gobiernos deberían promover el desarrollo de campañas públicas de sensibilización dirigidas a los menores para ayudarles a adquirir conocimientos sobre los diversos riesgos que pueden encontrar en línea, para mejorar sus capacidades de identificar y mitigar esos riesgos y promover la adopción de comportamientos responsables en línea.

2 Formación para profesionales de la ciberseguridad

Código-GCIv5: CapDev2

Fundamento-GCIv5: El desarrollo de competencias puede apoyar el desarrollo de recursos humanos capaces y bien informados en materia de ciberseguridad. La formación de trabajadores especializados en ciberseguridad requiere continuos esfuerzos para hacer frente a la evolución y a los cambios que se producen en este ámbito.

---

[19] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e777?rskey=sn89T4&result=201&prd=MPIL#

2.1 ¿Desarrolla o apoya su gobierno cursos de formación específicos para los profesionales de la ciberseguridad?

Código-GCIv5: CapDev2.1

Fundamento-GCIv5: A medida que crece el número de empresas que trasladan sus operaciones a Internet, la necesidad de profesionales de la ciberseguridad alcanza cotas nunca vistas. Sin embargo, a menudo estos profesionales carecen de la formación necesaria para proteger a sus empleadores de los ciberataques. La formación en ciberseguridad es importante por varias razones, entre ellas, para ayudar a los profesionales de la ciberseguridad a construir una base sólida en esa materia, a adquirir capacidades sobre cómo aplicar sus conocimientos en la práctica, a mantenerse al corriente de las últimas tendencias y novedades en materia de ciberseguridad, y a desarrollar las competencias necesarias para proteger las redes y los datos de sus organizaciones.

2.2 ¿Existen en su país programas de acreditación reconocidos a nivel nacional o internacional para los profesionales de la ciberseguridad?

Código-GCIv5: CapDev2.2

Fundamento-GCIv5: Los programas de acreditación en ciberseguridad son un instrumento útil para garantizar que los profesionales de este campo alcanzan un elevado nivel de competencia. Esto puede contribuir a mejorar la calidad general de los profesionales de la ciberseguridad y ayudar a proteger a las personas y organizaciones frente a posibles daños. Además, los países pueden generar confianza entre los profesionales de la ciberseguridad y sus clientes. Contar con un programa de acreditación universalmente reconocido puede ayudar a que todas las partes interesadas confíen en las calificaciones de los profesionales con los que trabajan.

2.3 Programas sectoriales nacionales de educación/formación en ciberseguridad para profesionales

Código-GCIv5: CapDev2.3

Fundamento-GCIv5: Los profesionales de cada país que trabajan en diversos sectores pueden beneficiarse de programas/formaciones de ciberseguridad que abordan las preocupaciones y situaciones específicas a las que se enfrentan dichos profesionales, además de dotarlos de las competencias adecuadas necesarias.

2.3.1 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a las fuerzas y cuerpos de seguridad del Estado?

Código-GCIv5: CapDev2.3.1

Fundamento-GCIv5: Las fuerzas y cuerpos de seguridad, como los agentes de policía, desempeñan una función primordial para ayudar a proteger a nuestro país de los ciberataques. Pueden contribuir a identificar e investigar la ciberdelincuencia y colaborar con las empresas y otras organizaciones para mejorar su postura en materia de ciberseguridad. Las fuerzas y cuerpos de seguridad deben estar dotadas de los conocimientos y herramientas necesarios para responder a esas amenazas cada vez mayores. La formación en ciberseguridad puede ayudarles a comprender mejor las amenazas más recientes, a identificar las actividades maliciosas y a proteger sus redes.

2.3.2 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a los funcionarios de la administración de justicia a nivel nacional?

Código-GCIv5: CapDev2.3.2

Fundamento-GCIv5: Los funcionarios de la administración de justicia nacional son imprescindibles para garantizar la seguridad de un país y, por lo tanto, deben estar dotados de los conocimientos y las herramientas necesarias para hacer frente a las amenazas de ciberseguridad. Al planificar las formaciones nacionales en materia de ciberseguridad, es necesario prever que se imparta este tipo de formación a los funcionarios de la administración de justicia y a otros actores del sistema judicial, además de impartir una

formación profesional y técnica que puede ser recurrente a jueces, procuradores, abogados, auxiliares jurídicos y demás profesionales de la administración de justicia y de las fuerzas y cuerpos de seguridad del Estado.

2.3.3 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a las mipymes? [NO PUNTUADO]

Código-GCIv5: CapDev2.3.3

Fundamento-GCIv5: Las mipymes necesitan formación en ciberseguridad porque poseen una gran cantidad de datos sensibles, que pueden ser robados o sufrir otro tipo de daños en caso de ciberataque. Además, las mipymes no suelen ser conscientes de los riesgos asociados al uso de la tecnología y pueden no disponer de las herramientas o recursos necesarios para proteger sus datos. La formación en ciberseguridad puede ayudar a las mipymes a entender los riesgos asociados al uso de la tecnología y cómo proteger sus datos. Además, puede ayudarles a identificar actividades sospechosas y a responder a los ciberataques. Al proporcionar a las mipymes las herramientas y los conocimientos necesarios para proteger sus datos, los países contribuyen también a proteger su propio desarrollo económico.

2.3.4 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos al sector privado en general?

Código-GCIv5: CapDev2.3.4

Fundamento-GCIv5: El sector privado se ve cada vez más expuesto a ciberriesgos de creciente alcance, magnitud y complejidad que afectan a las finanzas, a la reputación y a la propiedad de las empresas. Como la tecnología es solo un componente de la ciberseguridad, la aplicación de políticas y programas destinados a cambiar el comportamiento de las personas en el sector privado puede mejorar la resiliencia y reducir los ciberriesgos.

2.3.5 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a los funcionarios del sector público o del Estado en general?

Código-GCIv5: CapDev2.3.5

Fundamento-GCIv5: El sector público presta servicios esenciales a la ciudadanía y a las empresas. A fin de prestar esos servicios de forma segura, los actores del sector público deben conocer a fondo la ciberseguridad y la forma de protegerse a sí mismos y a los ciudadanos de las amenazas digitales. Los funcionarios del sector público que trabajan fuera de la judicatura y de las fuerzas y cuerpos de seguridad del Estado pueden beneficiarse de los programas educativos y la formación en materia de ciberseguridad.

2.3.6 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a los actores del sector financiero, sanitario, de las telecomunicaciones, del transporte y/o de la energía?

Código-GCIv5: CapDev2.3.6

Fundamento-GCIv5: Los problemas de ciberseguridad suelen variar según el sector. Dada la importancia de los sectores financiero, sanitario, de las telecomunicaciones, del transporte y de la energía, la formación dirigida a estos actores puede contribuir a la seguridad cibernética general de un país.

2.3.7 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a los jóvenes?

Código-GCIv5: CapDev2.3.8

Fundamento-GCIv5: Tradicionalmente, los gobiernos intervienen para corregir las externalidades negativas del mercado y para apoyar a grupos que, de otro modo, estarían desatendidos. Las medidas gubernamentales de apoyo y el fomento público de programas educativos y de formación en ciberseguridad abarcan un ámbito que el sector privado no cubre, ya que el retorno de la inversión puede no ser suficiente para incentivar la

participación. El gobierno puede proporcionar apoyo a través de subvenciones, apoyo a los estudios y apoyo al aprendizaje, entre otras opciones. Los jóvenes que aspiran a desarrollar su actividad profesional en el ámbito de la ciberseguridad pueden tener una mayor necesidad de apoyo, ya que carecen de capital financiero para invertir en educación por su cuenta.

2.3.8 ¿Desarrolla o apoya su gobierno programas educativos o formaciones de ciberseguridad dirigidos a los educadores, como los programas educativos de Protección de la Infancia en Línea?

Código-GCIv5: CapDev2.3.9

Fundamento-GCIv5: Los educadores están en condiciones de inculcar en niños y jóvenes hábitos de conducta positivos en el ámbito de la ciberseguridad, gracias a la influencia que ejercen en la educación de los menores. Cuando los países imparten formación a los educadores sobre temas relacionados con la ciberseguridad, como la Protección de la Infancia en Línea, demuestran sus esfuerzos por adoptar medidas de ciberseguridad a largo plazo, apoyando a los educadores que trabajan con la próxima generación de usuarios de Internet a medida que se incorporan al universo en línea.

3 Programas educativos de ciberseguridad como parte de los planes académicos nacionales

Código-GCIv5: CapDev3

Fundamento-GCIv5: La integración de los principios esenciales de la ciberseguridad en los programas académicos nacionales puede preparar a los estudiantes de todas las edades para afrontar mejor los riesgos en línea, con el fin de propiciar que la población esté más capacitada en esta materia.

3.1 ¿Desarrolla o apoya su gobierno algún programa educativo de ciberseguridad que forme parte de los planes de estudio académicos en la educación primaria?

Código-GCIv5: CapDev3.1

Fundamento-GCIv5: Los menores de la escuela primaria, o los del nivel CINE 1, comienzan su escolarización aprendiendo las competencias fundamentales de lectura, escritura y matemáticas[20]. La integración de actividades en esta etapa para construir una base de comportamiento ciberseguro puede ayudar a promover la conciencia de los riesgos y la seguridad cibernética de por vida. Sin embargo, es posible que los niños de este nivel aún no tengan la capacidad de pensamiento crítico y la agencia para poder evaluar de forma independiente los riesgos de ciberseguridad, y eso los expone a riesgos específicos[21]. Las actividades a este nivel podrían incluir actividades de Protección de la Infancia en Línea.

3.2 ¿Desarrolla o apoya su gobierno algún programa educativo de ciberseguridad que forme parte de los planes de estudio académicos en la educación secundaria?

Código-GCIv5: CapDev3.2

Fundamento-GCIv5: Los estudiantes de educación secundaria, en los programas de escolarización de los niveles CINE 2 y 3, suelen participar en actividades educativas cuyo objetivo es "sentar las bases para el desarrollo humano y el aprendizaje a lo largo de la vida sobre las cuales los sistemas educativos puedan expandir oportunidades de educación adicionales", y que están diseñadas para "consolidar la educación secundaria como preparación a la educación terciaria, o bien proporcionar destrezas pertinentes al empleo o ambos[22]". Introducir la ciberseguridad en esta etapa no solo puede impartir a los estudiantes competencias que les den mayor seguridad en línea, sino también promover un interés que culmine en una carrera profesional dentro del campo de la tecnología y la ciberseguridad.

---

20 http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

21 https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/

22 http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

3.3 ¿Desarrolla o apoya su gobierno algún programa educativo de ciberseguridad que forme parte de los planes de estudio académicos en la educación superior?

Código-GCIv5: CapDev3.3

Fundamento-GCIv5: Los estudiantes de educación terciaria, también conocidos como CINE 5-8, suelen haber completado los cursos de educación obligatoria. Los programas de educación terciaria pueden incluir cursos con los siguientes objetivos: impartir a los participantes conocimientos, habilidades y competencias profesionales (CINE 5); impartir a los participantes conocimientos, destrezas y competencias académicas o profesionales intermedias que conduzcan a un primer título o a una certificación equivalente (CINE 6); impartir a los participantes competencias académicas y/o profesionales avanzadas que conduzcan a un segundo título o a una certificación equivalente, como un máster o un nivel equivalente (CINE 7); o, conducir a un título de investigación avanzada, como una titulación de nivel de doctorado (CINE 8)[23]. Abordar la ciberseguridad en estos niveles educativos puede formar trabajadores conscientes y capacitados en esa materia, además de promover la capacitación con fines de investigación y desarrollo.

4 Programas de investigación y desarrollo (I+D) en ciberseguridad

Código-GCIv5: CapDev4

Fundamento-GCIv5: La investigación y el desarrollo en los sectores público, privado y académico pueden apoyar los esfuerzos de ciberseguridad a través de la capacitación humana, el desarrollo de nuevas técnicas y productos, y una mejor comprensión de los riesgos y mitigaciones. La investigación y el desarrollo pueden abarcar soluciones de carácter técnico o no técnico.

4.1 ¿Realizan los actores del sector privado de su país actividades de I+D relacionadas con la ciberseguridad?

Código-GCIv5: CapDev4.1

Fundamento-GCIv5: La investigación y el desarrollo de iniciativa privada demuestran la voluntad del sector privado de invertir en un mayor crecimiento e innovación en el ámbito de la ciberseguridad y de mejorar las soluciones de ciberseguridad disponibles en el mercado.

4.2 ¿Realizan los actores del sector público nacional de su país actividades de I+D relacionadas con la ciberseguridad?

Código-GCIv5: CapDev5.2

Fundamento-GCIv5: La participación activa de los actores del sector público en las actividades de I+D relacionadas con la ciberseguridad puede contribuir a una mejor identificación y corrección de las vulnerabilidades de la infraestructura de ciberseguridad de un país. También puede promover el desarrollo de soluciones de ciberseguridad que protejan las infraestructuras críticas del país. Las actividades públicas de I+D relacionadas con la ciberseguridad también pueden preparar para los ciberataques. En el marco de esta pregunta, los actores del sector público deben pertenecer al gobierno nacional, y no a un gobierno estatal o local.

4.3 ¿Realizan las instituciones académicas de su país actividades de I+D relacionadas con la ciberseguridad?

Código-GCIv5: CapDev5.3

Fundamento-GCIv5: Las instituciones académicas desempeñan una función primordial en la I+D relacionada con la ciberseguridad. Contribuyen a la investigación de vanguardia y a la generación de nuevas ideas, forman a la próxima generación de profesionales y actúan como puente entre los sectores público y privado.

---

[23] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

4.4 ¿Se emprenden programas o iniciativas para evaluar la ciberseguridad de los productos TIC, como sistemas de etiquetado o certificación, en su país?

Código-GCIv5: CapDev4.2

Fundamento-GCIv5: Los sistemas de certificación y etiquetado con los que se evalúa la ciberseguridad de los productos TIC pueden elevar los niveles de ciberseguridad de los fabricantes, proporcionar un marco de rendición de cuentas y facilitar a los consumidores la selección de productos. Los países pueden aplicar diferentes tipos de planes en función de sus contextos y necesidades nacionales.

5 Industria nacional de la ciberseguridad

Código-GCIv5: CapDev5

Fundamento-GCIv5: El desarrollo y el fomento de una industria nacional de ciberseguridad pueden apoyar la capacidad nacional para abordar y mejorar los problemas de ciberseguridad y propiciar una gestión proactiva en esta materia.

5.1 ¿Existe una industria nacional de ciberseguridad en su país?

Código-GCIv5: CapDev5.1

Fundamento-GCIv5: Un entorno económico, político y social favorable que apoye el desarrollo de la ciberseguridad incentivará el crecimiento de un sector privado dedicado a la ciberseguridad. La existencia de campañas públicas de sensibilización, el desarrollo de recursos humanos, la creación de capacidades y los incentivos gubernamentales impulsarán un mercado de productos y servicios de ciberseguridad. La existencia de una industria nacional de ciberseguridad atestigua la existencia de ese entorno favorable y fomenta la creación de empresas del sector y el mercado conexo de las ciberaseguradoras.

5.2 ¿Existen en su país organizaciones o asociaciones que promuevan el desarrollo de la industria de la ciberseguridad en su país?

Código-GCIv5: CapDev5.4

Fundamento-GCIv5: Algunas organizaciones y asociaciones pueden potenciar una industria de la ciberseguridad activa y comprometida a través de la promoción del intercambio de conocimientos, el desarrollo del talento, el acceso a la inversión y la financiación, entre otras cosas. Esas organizaciones y asociaciones pueden contar con el apoyo de la industria o de los gobiernos nacionales u otros organismos.

6 Mecanismos de incentivos gubernamentales

Código-GCIv5: CapDev6

Fundamento-GCIv5: La inversión en seguridad puede tener externalidades positivas que no tienen en cuenta quienes realizan la inversión o el esfuerzo. Para hacer frente a la posible falta de inversión o esfuerzo en ciberseguridad, los gobiernos pueden intervenir, ofreciendo incentivos destinados a mejorar la ciberseguridad, como la financiación, la regulación u otros mecanismos. Esto puede aumentar el nivel de ciberseguridad de un país más allá del nivel que podría haberse alcanzado sin apoyo.

6.1 ¿Existen mecanismos de incentivos gubernamentales para fomentar el desarrollo de capacidades en el ámbito de la ciberseguridad?

Código-GCIv5: CapDev6.1

Fundamento-GCIv5: Los mecanismos de incentivos gubernamentales pueden fomentar el desarrollo de capacidades de ciberseguridad, como la realización de estudios, la participación en la formación continua o el desarrollo de nuevos programas de desarrollo de capacidades, mecanismos de incentivos como subvenciones, becas, exoneración de tasas, préstamos u oportunidades de empleo.

6.2 ¿Existe algún mecanismo de incentivo gubernamental para el desarrollo o el fomento de la industria de la ciberseguridad?

Código-GCIv5: CapDev6.2

Fundamento-GCIv5: Dada la naturaleza de los bienes de información como la ciberseguridad, pueden crearse monopolios[24]. Con el fin de promover la aparición de nuevas ideas y prácticas en las organizaciones nuevas y existentes, y animar a una diversidad de actores y partes interesadas a participar en la ciberseguridad, los gobiernos pueden ofrecer incentivos en forma de subvenciones monetarias, reducción de impuestos o tasas, beneficios para la reputación, condiciones contractuales ventajosas o incentivos para que las empresas, organizaciones y personas participen en un ecosistema de ciberseguridad.

6.3 ¿Existen en su país mecanismos de incentivos gubernamentales para fomentar las actividades de I+D relacionadas con la ciberseguridad?

Código-GCIv5: CapDev6.3

Fundamento-GCIv5: Los mecanismos de incentivos gubernamentales son útiles cuando las fuerzas del mercado existentes no generan los resultados deseados. Dado que los beneficios de las actividades de I+D relacionadas con la ciberseguridad pueden tener externalidades positivas para la sociedad en su conjunto, los gobiernos pueden fomentar ese tipo de actividades de diversas maneras, por ejemplo, mediante subvenciones, mecanismos de préstamo, entornos comerciales y empresariales favorables, contratos, apoyo a las actividades universitarias, entre otros.

[24] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

Medidas de cooperación

Fundamento-GCIv5: La ciberseguridad precisa que contribuyan todos los sectores y disciplinas y necesita que se adopte un enfoque multipartito. La cooperación mejora el diálogo y la coordinación, y facilita la creación de un campo de aplicación más completo de la ciberseguridad. Dado que la ciberseguridad abarca diferentes sectores, ámbitos geográficos y niveles de recursos, es necesaria una cooperación a nivel privado, público, regional e internacional. Unas iniciativas de cooperación más amplias pueden permitir el desarrollo de capacidades de ciberseguridad mucho más sólidas, lo que contribuye a evitar las amenazas que se producen de forma reiterada y persistente en la red, y permite una mejor investigación, captura y procesamiento de los sujetos malintencionados.

La cooperación nacional e internacional puede medirse en base a la existencia y al número de asociaciones, marcos de cooperación y redes de intercambio de información.

1 Acuerdos bilaterales de ciberseguridad

Código-GCIv5: Coop1

Fundamento-GCIv5: Los acuerdos bilaterales (acuerdos entre dos partes) designan cualquier asociación nacional oficialmente reconocida para compartir de manera transfronteriza recursos de ciberseguridad (por ejemplo, el intercambio de información, conocimientos especializados, políticas, tecnologías u otros recursos), establecida por un gobierno con otro gobierno extranjero, o una organización internacional, para hacer frente a los riesgos transfronterizos de los conflictos de ciberseguridad. El indicador también mide si el acuerdo es legalmente vinculante o está pendiente de ratificación. Los recursos pueden designar el intercambio de profesionales (comisiones de servicio, estancias u otras adscripciones temporales de empleados), instalaciones, equipos y otras herramientas y servicios.

1.1 Acuerdos bilaterales de ciberseguridad con otros países

Código-GCIv5: Coop1.1

Fundamento-GCIv5: Los acuerdos bilaterales (acuerdos entre dos partes) designan cualquier asociación nacional oficialmente reconocida para compartir de manera transfronteriza recursos de ciberseguridad (por ejemplo, el intercambio de información, conocimientos especializados, políticas, tecnologías u otros recursos), establecida por un gobierno con otro gobierno extranjero. Compartir los conocimientos especializados y la experiencia entre países puede ayudar a crear unas capacidades sólidas de respuesta a los incidentes, así como a desarrollar medidas proactivas para hacer frente a los riesgos de ciberseguridad.

1.1.1 ¿Comparte su país información de ciberseguridad en el marco de uno o varios acuerdos bilaterales con otros países?

Código-GCIv5: Coop1.1.1

Fundamento-GCIv5: Los acuerdos de ciberseguridad que contemplan el intercambio de información demuestran un mayor compromiso de los países en materia de ciberseguridad, ya que facilitan hacer frente a los posibles riesgos, llevar a cabo evaluaciones de las amenazas y cooperar en las acciones relacionadas con la ciberseguridad.

1.1.2 ¿Forma parte de los acuerdos bilaterales de su país con otros países el desarrollo de capacidad en materia de ciberseguridad?

Código-GCIv5: Coop1.1.2

Fundamento-GCIv5: Los acuerdos que promueven el desarrollo bilateral de capacidad en materia de ciberseguridad mejoran las capacidades de los países para hacer frente de forma proactiva a los ciberriesgos a través del intercambio de prácticas idóneas, el perfeccionamiento del personal, la mejora de la colaboración, el aumento de la concienciación y el desarrollo y la puesta en marcha de procedimientos operativos relacionados con la ciberseguridad.

1.2 Acuerdos de ciberseguridad con organizaciones internacionales o regionales

Código-GCIv5: Coop1.2

Fundamento-GCIv5: Dada la importancia de las organizaciones intergubernamentales regionales, los países están suscribiendo cada vez más acuerdos de cooperación en materia de ciberseguridad para compartir de manera transfronteriza recursos de ciberseguridad, como el intercambio de información, conocimientos especializados, tecnologías y otros recursos, ya sea de manera individual, como países, o como parte de su pertenencia a una organización regional intergubernamental con otras organizaciones regionales intergubernamentales, como la Unión Europea, la ASEAN, la CEDEAO, la OEA y la UA, entre otras.

1.2.1 ¿Tiene su país, o las organizaciones intergubernamentales regionales de las que su país es miembro, intercambio de información de ciberseguridad como parte de los acuerdos bilaterales con otras organizaciones regionales e internacionales?

Código-GCIv5: Coop1.2.1

Fundamento-GCIv5: Los acuerdos de ciberseguridad que contemplan el intercambio de información demuestran un mayor compromiso de los países en materia de ciberseguridad, ya que facilitan hacer frente a los posibles riesgos, compartir datos sobre las evaluaciones de las amenazas y cooperar en las acciones relacionadas con la ciberseguridad.

1.2.2 ¿Forma parte de los acuerdos bilaterales de su país o de las organizaciones intergubernamentales regionales de las que su país es miembro, con otras organizaciones regionales e internacionales, el desarrollo de capacidad en materia de ciberseguridad?

Código-GCIv5: Coop1.2.2

Fundamento-GCIv5: Los acuerdos bilaterales que contemplan el desarrollo de capacidad en materia de ciberseguridad entre países y organizaciones regionales intergubernamentales pueden mejorar las capacidades en materia de ciberseguridad a través del intercambio de prácticas idóneas, el perfeccionamiento del personal, la mejora de la colaboración, el aumento de la concienciación y el desarrollo y la puesta en marcha de procedimientos operativos relacionados con la ciberseguridad

2 Acuerdos multilaterales de ciberseguridad con otros países

Código-GCIv5: Coop2

Fundamento-GCIv5: La participación en acuerdos multilaterales escritos requiere un acuerdo sobre las definiciones y los parámetros más importantes relacionados con la ciberseguridad y establecer una agenda común para avanzar en dicho ámbito. También pueden impulsar las medidas de creación de confianza como parte de la creación de mecanismos de respuesta positiva para la construcción de relaciones pacíficas.

2.1 ¿Forma su país parte de un acuerdo multilateral de ciberseguridad que incluye el intercambio de información de ciberseguridad?

Código-GCIv5: Coop2.1.1

Fundamento-GCIv5: Los acuerdos de ciberseguridad que contemplan el intercambio de información demuestran un mayor compromiso de los países en materia de ciberseguridad, ya que facilitan hacer frente a los posibles riesgos, compartir datos sobre la realización de las evaluaciones de las amenazas y cooperar en las acciones relacionadas con la ciberseguridad.

2.2 ¿Forma su país parte de un acuerdo multilateral de ciberseguridad que incluye el intercambio de desarrollo de capacidad?

Código-GCIv5: Coop2.1.2

Fundamento-GCIv5: La participación en acuerdos multilaterales escritos que incluyen el desarrollo de capacidad pueden apoyar dicho desarrollo en los países con situaciones de ciberseguridad más precarias, y apoyar las medidas de creación de confianza.

3 Tratados de asistencia jurídica mutua[25] relacionados con la ciberseguridad

Código-GCIv5: Coop3

Fundamento – GCIv5: Dada la naturaleza transnacional de la ciberseguridad, la adopción de medidas contra las amenazas que afectan a la soberanía de otro Estado requiere mecanismos claros de cooperación, especialmente en materia judicial. La asistencia jurídica mutua en forma, por ejemplo, de tratados de asistencia jurídica mutua, puede variar entre la entrega de documentos y la transmisión de pruebas hasta la asistencia en investigaciones, entre otras formas de asistencia[26].

3.1 ¿Participa su país en tratados de asistencia legal mutua en materia de ciberseguridad a través de acuerdos bilaterales o multilaterales con otros países u organizaciones regionales o intergubernamentales?

Código-GCIv5: Coop3.1

Fundamento-GCIv5: Dada la naturaleza transnacional de la ciberseguridad, la adopción de medidas contra las amenazas que afectan a la soberanía de otro Estado requiere mecanismos claros de cooperación, especialmente en materia judicial. La asistencia jurídica mutua en forma, por ejemplo, de tratados de asistencia jurídica mutua, puede variar entre la entrega de documentos y la transmisión de pruebas hasta la asistencia en investigaciones, entre otras formas de asistencia[27].

4 Asociaciones público-privadas (APP)

Código-GCIv5: Coop4

Fundamento-GCIv5: Las asociaciones público-privadas han sido parte de una tendencia impulsada tanto por razones ideológicas como por una búsqueda de la rentabilidad[28]. Especialmente en el ámbito de la ciberseguridad, en el que las nuevas innovaciones suelen originarse en el sector privado, la participación en las APP puede ayudar a los gobiernos a beneficiarse más rápidamente de estas nuevas innovaciones y de las mejoras potenciales en materia de ciberseguridad. Sin embargo, las APP también conllevan una serie de dificultades, como los problemas del agente principal, la gestión de las externalidades, la complejidad de la negociación de los contratos, la flexibilidad de los mismos y la realización de evaluaciones efectivas[29].

4.1 ¿Participa su gobierno en APP en materia de ciberseguridad con empresas nacionales?

Código-GCIv5: Coop4.1

Fundamento-GCIv5: Debido a los efectos de red que conllevan, las APP con empresas nacionales pueden impulsar un ecosistema nacional de ciberseguridad, permitiendo a los actores nacionales del sector privado desarrollar y ampliar sus competencias, sus sistemas y sus servicios.

---

25 https://www.unodc.org/e4j/es/organized-crime/module-11/key-issues/mutual-legal-assistance.html

26 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL

27 https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL

28 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page5

29 https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page66

4.2 ¿Participa su gobierno en APP en materia de ciberseguridad con empresas extranjeras en su país?

Código-GCIv5: Coop4.2

Fundamento-GCIv5: La ciberseguridad, como bien de información, está sujeta a los efectos de red y a los conocimientos que se obtienen por la escala[30]. Los actores internacionales que cuentan con conocimientos de ciberseguridad adquiridos en diferentes entornos y contextos nacionales pueden ofrecer beneficios adicionales a los gobiernos que buscan mejorar la ciberseguridad de sus países. Los gobiernos que participan en APP con actores extranjeros pueden aprovechar esta experiencia para su propio crecimiento y seguridad.

5 Asociaciones entre organismos

Código-GCIv5: Coop5

Fundamento-GCIv5: Cualquier asociación nacional oficial entre diferentes organismos gubernamentales de un país puede facilitar la capacidad de respuesta del gobierno ante los riesgos de ciberseguridad. Las asociaciones pueden consistir en las de intercambio de información o de recursos entre ministerios, departamentos, programas y otras instituciones del sector público. A efectos de este apartado, no se consideran las asociaciones entre organismos de diferentes países o entre organizaciones intergubernamentales.

5.1 ¿Existen en su país procesos específicos de coordinación en materia de ciberseguridad entre diferentes organismos gubernamentales nacionales?

Código-GCIv5: Coop5.1

Fundamento-GCIv5: Cualquier asociación nacional oficial entre diferentes organismos gubernamentales de un país puede facilitar la capacidad de respuesta del gobierno ante los riesgos de ciberseguridad. Las asociaciones pueden consistir en las de intercambio de información o de recursos entre ministerios, departamentos, programas y otras instituciones del sector público. A efectos de este apartado, no se consideran las asociaciones entre organismos de diferentes países o entre organizaciones intergubernamentales.

[30] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

Definiciones

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Mundo académico		Mundo de la educación universitaria.	Diccionario de inglés de Oxford		Tech2; CapDev4.1.3; CapDev6.2
Instituciones académicas		Instituciones que forman parte del mundo de la educación universitaria.	Diccionario de inglés de Oxford		CapDev4.1.3
Acuerdo		Compromisos recíprocos entre Estados u otras partes en formato escrito y regido por el derecho internacional, ya conste en un instrumento único o en dos o más instrumentos conexos.	Adaptado de la Convención de Viena sobre el Derecho de los Tratados		
Acuerdo bilateral		Acuerdo escrito entre dos partes, incluyendo Estados, organismos regionales u organizaciones, firmado por los responsables pertinentes.	GCIv2		Coop1; Coop1.1; Coop1.1.1; Coop1.1.2; Coop1.1.3
Desarrollo de capacidad		El desarrollo de capacidad, es un proceso de cambio. A menudo se equipara con la incorporación de personal adicional, la formación y los talleres. Aunque la formación individual y los talleres pueden formar parte de un plan global de desarrollo de capacidad, no son suficientes como tales. Formar a una persona, por ejemplo, no garantiza que esta formación se aplique posteriormente en el lugar de trabajo. El desarrollo de capacidades debe ser más amplio para abordar las mejoras en los sistemas para la salud con el fin de mejorar el rendimiento y garantizar la sostenibilidad. Es necesario evaluar cómo funciona el sistema en un momento determinado y qué áreas necesitan soporte; por ejemplo: desarrollar e implantar sistemas de información sanitaria, formar a personal en el análisis de datos, desarrollar políticas y procedimientos para una gestión financiera sólida o mejorar el suministro y la distribución de los productos sanitarios más importantes.	PNUD https://www.undp-capacitydevelopment-health.org/en/capacities/		Org2.3; CapDev1; CapDev6.1; Coop1.1.2

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Protección de la Infancia en Línea	PIeL	La Protección de la Infancia en Línea (PIeL) tiene como objeto proteger a los niños y los jóvenes de las amenazas y los riesgos que se encuentran en línea. El concepto de Protección de la Infancia en Línea abarca la adopción de un enfoque integral para construir espacios digitales seguros, adecuados a la edad, inclusivos y participativos para los niños y los jóvenes, caracterizados por: • una respuesta, un soporte y autoayuda frente a las amenazas; • la prevención de daños; • un equilibrio dinámico entre proporcionar protección y ofrecer oportunidades para que los niños sean ciudadanos digitales; • la defensa de los derechos y las responsabilidades tanto de los niños como de la sociedad.	https://www.itu-cop-guidelines.com/		Legal1.3.3; Tech1.2.4; Tech4; Org1.3; Org2.4; CapDev1.6
Infraestructura esencial (véase también: Infraestructura esencial nacional)		Sistemas, servicios y funciones fundamentales cuya destrucción o interrupción del funcionamiento podría tener unas repercusiones perjudiciales sobre la seguridad y la salud pública, el comercio y la seguridad nacional, o cualquier combinación de estos sectores.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf	Estos sistemas pueden incluir, pero sin limitarse a ellos: los sistemas de defensa, la banca y las finanzas, las telecomunicaciones, el transporte, la salud, la energía, etc.	Tech1.2
Infraestructura esencial de la información	CII	Activos materiales y digitales, redes, servicios e instalaciones que, en el caso de que se interrumpa su funcionamiento o se destruyan, tendrían unas repercusiones perjudiciales sobre la salud, la seguridad o el bienestar económico de los ciudadanos y en el funcionamiento eficaz del gobierno de un país.	International CIIP Handbook 2008/2009	Estos sistemas pueden incluir, pero sin limitarse a ellos: centrales telefónicas, centrales de Internet, redes inalámbricas, satélites, etc.	

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Legislación sobre ciberdelincuencia		La legislación sobre ciberdelincuencia establece reglas de conducta y normas de comportamiento para la utilización de Internet, las computadoras y las tecnologías digitales asociadas, así como para las acciones de los ciudadanos, el gobierno y las organizaciones privadas; normas en materia de pruebas y procedimientos penales, y otras cuestiones del enjuiciamiento de los delitos en el ciberespacio; y la reglamentación...	https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html		Legal1
Requisitos para auditorías de ciberseguridad		Una auditoría de seguridad significa la evaluación sistemática y periódica de la seguridad de un sistema de información. Una auditoría normal puede incluir una evaluación de la seguridad de la configuración física y el entorno del sistema, el *software*, el tratamiento de la información y las prácticas de los usuarios.	GCIv4		Legal2.3n
Ecosistema de ciberseguridad		Comunidad de actores en el ámbito de la ciberseguridad y en torno a la misma, con funciones y responsabilidades que evolucionan conjuntamente.	Adaptado de Moore, James, *The Death of Competition*, 1996	Ejemplo: profesionales legales, técnicos, de empresas y de políticas que trabajan juntos en temas relacionados con la ciberseguridad	CapDev5.1, CapDev6.2
Resiliencia de la ciberseguridad		Capacidad para recuperarse de ataques contra la seguridad o de situaciones de riesgo para la misma. Un plan nacional de resiliencia de ciberseguridad asegura que el país tiene la capacidad de 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 apoyándose en servicios externos.	https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc		Tech1.3
Tratados y acuerdos de ciberseguridad		Tratado o acuerdo entre dos países, organizaciones u otros grupos relacionado específicamente con la ciberseguridad.	https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478		

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Notificación de violación de datos		Las leyes y los reglamentos sobre notificación de las violaciones de datos requieren que una entidad que ha sido víctima de una violación de sus datos 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 al creciente número de infracciones en las bases de datos de consumidores que contienen información identificable personalmente.	GCIv2		Legal2.2
Acceso ilegal		Acceso a la totalidad o a una parte de un sistema informático sin derecho cuando se comete intencionadamente. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.	GCIv2		Legal1.1.1
Interceptación ilegal		Interceptación realizada de manera deliberada e ilegítima, por medios técnicos, de datos informáticos de transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporten dichos datos informáticos.	GCIv2		Legal1.1.3
Interferencia ilegal		"Acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos" y "la obstaculización grave, realizada de manera deliberada e ilegítima, del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos".	GCIv2		Legal1.1.2
Notificación de incidente		Notificación a las partes interesadas, por parte de un EIII o de otra entidad, de un incidente de ciberseguridad.			Legal2.2

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Asociaciones/ acuerdos entre organismos		Cualquier asociación oficial a nivel nacional entre diferentes organismos gubernamentales de un país puede facilitar la capacidad de respuesta del gobierno ante los riesgos de ciberseguridad. Las asociaciones pueden incluir las que permiten compartir información o recursos entre ministerios, departamentos, programas y otras instituciones del sector público. A efectos de esta sección, no se consideran las asociaciones entre organismos de diferentes países o las organizaciones intergubernamentales.	GCIv2		Coop5
Procesos de coordinación entre organismos		Coordinación entre dos o más organismos gubernamentales sobre cuestiones para trabajar con objetivos y actividades armonizados.			Coop5.1
Microempresas, pequeñas y medianas empresas	mipyme	Las definiciones de las microempresas y las pequeñas y las medianas empresas pueden variar según el país. En la medida de lo posible, se deben utilizar las definiciones recogidas por el Foro de Financiación de las pymes.		https://www.smefinanceforum.org/data-sites/msme-country-indicators	CapDev1.1; CapDev2.3.3
Acuerdo multilateral		Los acuerdos multilaterales (entre una parte y múltiples partes) designan alianzas nacionales o sectoriales reconocidas oficialmente y destinadas a compartir información y recursos sobre ciberseguridad de manera transfronteriza, concluidos por un gobierno con varios 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, entre otros.	GCIV2		Coop3; Coop3.1.1; Coop3.1.2

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Infraestructura esencial nacional (véase también: infraestructura esencial)		Sistemas, servicios y funciones fundamentales cuya destrucción o interrupción del funcionamiento podría tener unas repercusiones perjudiciales sobre la seguridad y la salud pública, el comercio y la seguridad nacional, o cualquier combinación de dichos sectores.	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf		Legal2.7; Org1.1.1
EIII nacional		Un EIII (equipo de intervención en caso de incidentes informáticos), EIEI (equipo de intervención en caso de emergencia informática) o EIISI (equipo de intervención en caso de incidente de seguridad informática) son entidades de una organización a quienes se asigna la responsabilidad de coordinar y ayudar en las respuestas en caso de eventos o incidentes de seguridad informática a escala nacional. Tienen la responsabilidad a nivel nacional de proporcionar capacidades para identificar, defender, responder y gestionar las ciberamenazas y mejorar la seguridad del espacio digital en el país. Esta capacidad debe ir acompañada de la recopilación de su propia información en lugar de depender de las notificaciones secundarias de los incidentes de seguridad, ya sea de las circunscripciones del EIII o de otras fuentes. Pueden ser militares o civiles.	De GCI2		
Abuso en línea					Legal1.3.2
Ciberacoso		Mensajes enviados por correo electrónico, mensajería o sitios web malintencionados destinados a acosar a una persona o grupo de personas con ataques personalizados.	GCIv4		Legal1.3.2
Seguridad en línea		Maximizar la seguridad de Internet frente a los diversos riesgos que afectan a la información privada y personal o relativa a la propiedad, mejorando también la autoprotección de los usuarios frente a los ciberdelitos.	GCIv4		Legal1.3

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Personas con necesidades especiales		Necesidades particulares derivadas de discapacidades físicas, dificultades de aprendizaje o de comportamiento, etc. (especialmente en contextos educativos).	Diccionario de inglés de Oxford	"special needs, n. y adj.". OED en línea. Junio de 2021. Oxford University Press. https://www.oed.com/view/Entry/253889?redirectedFrom=special+needs (acceso del 30 de agosto de 2021)	
Protección de datos personales		Los datos personales son cualquier información relacionada con una persona física identificada o identificable. La protección de los datos personales es el proceso de asegurar la seguridad de los datos personales.	https://gdpr-info.eu/issues/personal-data/ Definición del RGPD	La norma voluntaria, UIT-T X.1058 | ISO/CEI 29151, ofrece un valioso punto de referencia a los gobiernos y a la industria a la hora de intensificar su apuesta por garantizar la protección de los datos personales. La norma X.1058 establece los objetivos de los controles de la protección de datos, especifica los controles necesarios y proporciona directrices para su aplicación. Muestra cómo las disposiciones de estos controles pueden cumplir los requisitos identificados por las evaluaciones de las organizaciones de los riesgos y los efectos en relación con la protección de los datos personales.	Legal2.1a

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Políticas		Las políticas son normas, principios, directrices o estructuras adoptadas o diseñadas por una organización o un país para alcanzar objetivos a largo plazo. Suelen definirse en un formato escrito de fácil acceso. Las políticas se formulan para impulsar e influir en todas las decisiones importantes que se tomen dentro de la organización y mantener todas las actividades dentro de un conjunto establecido de límites.	Nuevo		Org1.1
Educación postsecundaria no terciaria (nivel CINE 4)	Nivel CINE 4	La educación postsecundaria no terciaria refuerza los conocimientos adquiridos en educación secundaria, prepara para el mercado laboral y para la educación terciaria. Las destrezas, competencias y conocimientos impartidos en este nivel se encuentran debajo del nivel de complejidad que caracteriza a la educación terciaria. Los programas de nivel CINE 4, o educación postsecundaria no terciaria están generalmente diseñados para proporcionar a las personas que han concluido el nivel CINE 3 las certificaciones no terciarias requeridas para avanzar a la educación terciaria, o bien para insertarse en el mercado laboral en el caso que sus certificaciones de nivel CINE 3 no otorgaran acceso a este nivel…	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.4n
Educación primaria (nivel CINE 1)		Los programas del nivel CINE 1, o educación primaria, están principalmente destinados a proporcionar a los estudiantes destrezas básicas en lectura, escritura y matemáticas (es decir, alfabetismo y utilización de números – numeracy) y sentar una sólida base para el aprendizaje y la comprensión de las áreas esenciales del conocimiento y el desarrollo personal y social como preparación a la educación secundaria baja. Estos programas privilegian el aprendizaje a un nivel de complejidad básico con muy poca o ninguna especialización…	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.1

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
		Usualmente, en este nivel el único requisito de ingreso es la edad. En general, la edad habitual o legal de ingreso no es inferior a los 5 años de edad ni superior a los 7 años de edad.			
Protección de la privacidad		La privacidad en Internet se refiere al nivel de seguridad de los datos personales que se publican en Internet. Se trata de un concepto amplio, que abarca muchos factores, técnicas y tecnologías que se empelan para para proteger los datos, las comunicaciones y las preferencias sensibles y privados. Como ejemplo de este tipo de legislación se puede citar la Ley de protección de datos.	GCIv2		Legal2.1b
Asociación público-privada	APP	Contrato a largo plazo entre una parte privada y una entidad gubernamental, para el suministro de un bien o un servicio público, en el que la parte privada asume un riesgo y una responsabilidad de gestión importantes, y la remuneración está vinculada al rendimiento. NOTA: Sin una definición legal formal, las APP suelen caracterizarse por su función. El Secretario General de la ONU ha sugerido dos tipologías. 11 La primera identifica cinco funciones principales: a) diálogo político, como por ejemplo, el Grupo de Tareas sobre la tecnología de la información y las comunicaciones, la Comisión Mundial sobre Represas, la Alianza GAVI (la Alianza mundial para el fomento de la vacunación y la inmunización); b) sensibilización, por ejemplo, la asociación ONUSIDA-medios de comunicación para divulgar la problemática del VIH/SIDA; c) movilización de fondos privados, como por ejemplo, la Fundación pro Naciones Unidas y el Fondo de las Naciones Unidas para la Colaboración Internacional, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) y el proyecto de inversión extranjera de la Cámara de Comercio Internacional;	https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1084?rskey=CTIBOr&result=1&prd=MPIL		

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
		d) información y aprendizaje, por ejemplo, los proyectos conjuntos de investigación y formación; y e) ejecución operativa, por ejemplo, la iniciativa "El primero en llegar" de las Naciones Unidas y LM Ericsson, el proyecto de registro de refugiados entre las Naciones Unidas y Microsoft (Directrices de las Naciones Unidas 18-32). 12 La segunda identifica cuatro funciones: a) apoyo, como por ejemplo, la Alianza Mundial para Mejorar la Nutrición, la APP mundial para promover el lavado de manos con jabón; b) desarrollo de normas y reglas, por ejemplo, la Iniciativa mundial de presentación de informes, el proyecto "Who Cares Wins" sobre responsabilidad corporativa en las industrias financieras; c) compartición de recursos y conocimientos expertos, como el programa de logística del Programa Mundial de Alimentos y TNT "Moving the world"; y d) aprovechamiento de los mercados para el desarrollo, por ejemplo, la Iniciativa de producción de manteca de karité de UNIFEM–L'Occitane, el proyecto ONUDI-FIAT de componentes para automóviles en la India (AGNU, "Informe del Secretario General sobre intensificación de la cooperación entre las Naciones Unidas y todos los colaboradores pertinentes, en particular el sector privado" [*10 de agosto de 2005*] 5) 13 Las Directrices de las Naciones Unidas definen varias modalidades de cooperación y los acuerdos legales normalizados que se utilizan en cada una de ellas o que se definen simplemente como empresas entre el sector público y el privado. Este indicador de resultados puede medirse por el número de APP nacionales o sectoriales reconocidas oficialmente para compartir información de ciberseguridad (inteligencia sobre amenazas) y recursos (personas, procesos, herramientas) entre el sector público y el sector privado (es			

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
		decir, asociaciones oficiales para la cooperación o el intercambio de información, conocimientos especializados, tecnología y/o recursos), ya sea a nivel nacional o internacional.			
Reglamentación		Norma o principio que rige un comportamiento o una práctica; especialmente una directiva de este tipo establecida y mantenida por una autoridad.	Diccionario de inglés de Oxford	"regulation, n. y adj.". OED en línea. Junio de 2021. Oxford University Press. https://www.oed.com/view/Entry/161427?redirectedFrom=regulation (acceso del 30 de agosto de 2021)	Legal2, Legal2.1, Legal2.2
Investigación y desarrollo	I+D	La investigación y el desarrollo (I+D) incluyen el trabajo creativo y sistemático que se lleva a cabo para aumentar el conjunto de los conocimientos −incluyendo el conocimiento de la humanidad, la cultura y la sociedad− y para concebir nuevas aplicaciones de los conocimientos disponibles. El término I+D abarca tres tipos de actividades: la investigación básica, la investigación aplicada y el desarrollo experimental. Para que una actividad sea de I+D, debe satisfacer cinco criterios fundamentales. La actividad debe ser • novedosa (estar orientada a obtener nuevos descubrimientos) • creativa (basarse en conceptos e hipótesis originales y no evidencias) • incierta (no tener certeza sobre el resultado final) • sistemática (estar planificada y presupuestada) • transferible y/o reproducible (conducir a resultados que puedan reproducirse).	OCDE (2015), Manual de Frascati 2015: *Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental* http://uis.unesco.org/en/glossary-term/research-and-experimental development-rd		CapDev4.1; CapDev4.1.1; CapDev4.1.2; CapDev4.1.3

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Educación secundaria (niveles CINE 2 y 3)	CINE 2 y 3	Los programas del nivel CINE 2, o educación secundaria baja, suelen estar destinados a reforzar los resultados de aprendizaje del nivel CINE 1. En general, el objetivo que se persigue es sentar las bases para el desarrollo humano y el aprendizaje a lo largo de la vida sobre las cuales los sistemas educativos puedan expandir oportunidades de educación adicionales. Es probable que algunos sistemas educativos ya ofrezcan programas vocacionales en el nivel CINE 2 orientados a proporcionar a las personas destrezas relevantes para el acceso al mercado laboral. Los programas del nivel CINE 3, o educación secundaria alta, suelen tener como principal objetivo consolidar la educación secundaria como preparación a la educación terciaria, o bien proporcionar destrezas pertinentes al empleo o ambos. El nivel CINE 3 comienza después de 8 a 11 años de educación a partir del inicio del nivel CINE 1.	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.2
Educación terciaria (niveles CINE de 5 a 8)	Niveles CINE de 5 a 8	Los programas de nivel CINE 5, o educación terciaria de ciclo corto, suelen estar destinados a proporcionar al participante conocimientos, habilidades y competencias profesionales. Estos programas se caracterizan por estar basados en un componente práctico o, estar orientados a ocupaciones específicas y preparar al estudiante para el mercado laboral. Sin embargo, también pueden facilitar el ingreso a otros programas de educación terciaria… Con frecuencia, los programas de nivel CINE 6, o grado en educación terciaria o nivel equivalente, están destinados a impartir conocimientos, destrezas y competencias académicas o profesionales intermedias que conducen a un primer título o a una certificación equivalente. Los programas de nivel CINE 7, o nivel de maestría, especialización o equivalente, suelen tener como	http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf	http://uis.unesco.org/en/isced-mappings	CapDev3.3

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
		principal objetivo impartir al participante competencias académicas y/o profesionales avanzadas que conduzcan a un segundo título o a una certificación equivalente… Los programas de nivel CINE 8, o nivel de doctorado o equivalente, suelen tener como principal objetivo conducir a un título de investigación avanzada. Los programas de este nivel CINE están dedicados a estudios avanzados e investigaciones originales, en tanto que suelen ser ofrecidos exclusivamente por instituciones de educación superior (universidades) dedicadas a la investigación. Se imparten programas de doctorado tanto en el campo académico como en el profesional.			
Xenófobo		Aversión o prejuicios hacia las personas, las culturas y las costumbres extranjeras, o que se perciben como extranjeras.	Diccionario de inglés de Oxford	"xenophobia, n.". OED en línea. Junio de 2021. Oxford University Press. https://www.oed.com/view/Entry/230996?redirectedFrom=xenophobia (acceso del 30 de agosto de 2021)	Legal1.3.1
Iniciativas nacionales		Actividades realizadas a nivel nacional para abordar una preocupación específica de forma sistemática.	GCIv2	Las iniciativas nacionales suelen estar diseñadas para abordar un área específica que preocupa a la organización. Algunos ejemplos son los derechos humanos, la educación o el medio ambiente. Pueden ser metas u objetivos asignados a uno o varios miembros a través de la interfaz "crear proyecto".	

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Falsificaciones informáticas		Las falsificaciones informáticas consisten en la suplantación en línea de personas, autoridades, organismos y otras entidades legítimas con fines fraudulentos.	https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html#:~:text=Computer%2Drelated%20forgery%20involves%20impersonation,entities%20online%20for%20fraudulent%20purposes		Legal1.2
Comunicaciones no solicitadas o *spam*		Comunicación electrónica, como un correo electrónico, un SMS, una red social o una llamada telefónica, no solicitada por el destinatario. El *spam* designa al tipo de comunicaciones no solicitadas que se envían de forma masiva.	GCIv2		Legal2.7
Firma digital		Una firma digital es una técnica matemática empleada para validar la autenticidad y la integridad de un mensaje, un *software* o el contenido de un documento digital.	GCIv2		Legal2.6
Transacción electrónica		Una transacción electrónica es la venta o la compra de bienes o servicios, realizadas entre empresas, hogares, particulares, gobiernos y otras organizaciones públicas o privadas, por redes de comunicación, a través de ordenadores. Ejemplos de documentos legislativos son, por ejemplo, la Ley de comercio electrónico, la Ley de firmas electrónicas o la Ley de transacciones electrónicas, que pueden incluir reglamentaciones relativas a la creación de una entidad controladora de las autoridades de certificación.	GCIv2		

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Normas de ciberseguridad		Existencia de un marco aprobado (o respaldado) por el gobierno para la aplicación de normas de ciberseguridad, reconocidas a nivel internacional, dentro del sector público (agencias gubernamentales), y en las infraestructuras esenciales (incluso si la operación depende del 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.; o La reglamentación de ciberseguridad sobre certificación/normalización requiere que las entidades que operan en el territorio de un país cumplan determinados criterios mínimos de certificación y normalización; estos pueden variar en función del sector de la economía. Dichas 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.		Definición GCIv4 y GCIv2	Legal2.5
Ejercicios de ciberseguridad (por ejemplo, cibersimulacros)		Actividades planificadas durante las cuales una entidad simula un ciberataque a fin de desarrollar o poner a prueba competencias como la prevención, detección, mitigación, respuesta o recuperación tras el ataque.	GCIv4		Tech1.2.2

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Cibersimulacro		Un cibersimulacro es un evento anual durante el cual se simulan ciberataques, incidentes relacionados con la seguridad de la información y problemas de diversa índole, a fin de poner a prueba las capacidades de ciberseguridad de una organización, desde su capacidad para detectar un incidente de seguridad hasta su capacidad para responder de manera adecuada y minimizar cualquier repercusión conexa. Los participantes en un cibersimulacro pueden validar las políticas, los planes, los procedimientos, los procesos y las capacidades que permiten la preparación, la prevención, la respuesta, la recuperación y la continuidad de las actividades.	Definición de la UIT	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx	Tech1.2.2
Avisos de ciberseguridad		Avisos de EIII: compartición pública de información sobre ciberamenazas emergentes y sobre el comportamiento recomendado.	GCIv4		Tech1.2.3
Afiliación al FIRST		Miembro titular o miembro de enlace del Foro sobre los equipos de seguridad y respuesta ante incidentes. www.first.org	GCIv4		Tech1.3
Afiliación a un EIII/EIEI/EIISI regional		Relación formal o informal con otros EIEI de fuera del país, como miembro de algún grupo regional de EIEI. Ejemplos de grupos regionales de EIEI son APCERT, AFRICACERT, EGC, OIC y OAS.	GCIv4		Tech1.4
EIII/EIEI/EIISI sectoriales		Los EIII/EIISI/EIEI sectoriales son entidades que responden a incidentes de seguridad informática o de ciberseguridad que afectan a un sector determinado. Los EIEI sectoriales suelen crearse para sectores críticos como el sanitario, las infraestructuras de suministros públicos, los servicios de emergencia y el sector financiero. Al contrario que los EIEI gubernamentales que dan servicio al sector público, los EIEI sectoriales dan servicio a los componentes de un único sector.	GCIv2		Tech2.1

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
Cooperación internacional en el ámbito de la ciberseguridad		Colaboración entre dos o más gobiernos, organismos nacionales, organismos reguladores nacionales, EIII nacionales, organizaciones de la sociedad civil o el mundo académico.			Org1.8
Mecanismos y capacidades de presentación de informes		Como las líneas de asistencia y las líneas de ayuda nacionales conectadas a los sistemas internacionales de asistencia. Es necesario que estén conectados con los sistemas de seguimiento y soporte.			Org4.3
Campañas públicas de concienciación sobre ciberseguridad		La sensibilización de los ciudadanos incluye acciones para promover campañas que alcancen al mayor número posible de personas, así como la utilización de ONG, instituciones, organizaciones, proveedores de servicios de Internet, bibliotecas, organizaciones locales de comercio, centros comunitarios, centros universitarios y programas de formación de adultos, escuelas y organizaciones de padres y profesores para difundir mensajes sobre comportamientos seguros en línea. También incluyen medidas como la creación de portales y sitios web para promover conocimientos, difundir material de apoyo y realizar otras actividades pertinentes.	GCIv4		CapDev1.
Centro de operaciones de seguridad	SOC	"El SOC es una unidad organizativa que actúa en el centro de todas las operaciones de seguridad. Por lo general, no se ve como una entidad o un sistema único, sino más bien como una estructura compleja para gestionar y mejorar la situación general de seguridad de una organización. Su función es detectar, analizar las amenazas y los incidentes de ciberseguridad y responder a los mismos mediante el empleo de personas, procesos y tecnología. Esas actividades pueden formalizarse en siete dimensiones o áreas funcionales de un SOC. Aunque se acepta ampliamente que son absolutamente imprescindibles	https://ieeexplore.ieee.org/document/9296846		

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
		para la seguridad de una empresa, los SOC siguen considerándose un mecanismo de defensa pasivo y reactivo". "Equipo de intervención en caso de incidentes de seguridad informática: esta expresión se utiliza a menudo como equivalente de SOC, aunque se centra principalmente en la parte de actuación una vez que se ha producido un ataque. Un EIISI es una unidad organizativa responsable de coordinar y dar soporte a la respuesta a un incidente de seguridad informática. Un EIISI se puede considerar como un equipo independiente o como parte de un SOC". "Centro de Operaciones de Red": un Centro de Operaciones de Red (NOC) se ocupa de la identificación, investigación, priorización, escalado y resolución de los problemas. Sin embargo, en los NOC, los problemas que se abordan son diferentes, ya que un NOC se centra en los incidentes que afectan al rendimiento y la disponibilidad de la red de una organización. Como los incidentes pueden producirse en todos los sistemas, no solo en las redes, es beneficioso para las organizaciones que los equipos del NOC y del SOC trabajen juntos". "Centro de Inteligencia de Seguridad": el término Centro de Inteligencia de Seguridad (SIC) se utilizó por primera vez en 2017 para describir al sucesor de los SOC. Su objetivo es proporcionar una visión más completa e integrada que la de un SOC y puede visualizar y gestionar completamente la inteligencia de seguridad en un solo lugar. Por ello, se combinan varias tecnologías (por ejemplo, la gestión del conocimiento de la seguridad de la información (IS), el procesamiento de macrodatos)". "Gestión de la información de seguridad y de los eventos: este			

Término	Abreviatura	Definición	Fuente	Ejemplos	Cuestiones referenciadas (GCIv4)
		sistema forma parte de muchos SOC para cubrir gran parte de las necesidades tecnológicas. Se encarga de la recopilación de los datos relevantes para la seguridad de forma centralizada. De este modo, proporciona capacidades de análisis de la seguridad mediante la correlación de los eventos del registro. Otras funcionalidades permiten el enriquecimiento con datos de contexto, la normalización de los datos heterogéneos, la elaboración de informes y las alertas [73]. Para permitir el intercambio de información sobre amenazas, el SIEM proporciona una conexión con las plataformas de intercambio de información sobre ciberamenazas, e incluye a los analistas de seguridad humanos ofreciendo capacidades de análisis de seguridad en formato visual. Incluye capacidades de gestión de registros mediante el almacenamiento a largo plazo de los datos de los eventos.			