Panorama general de las herramientas actuales de evaluación de las capacidades cibernéticas nacionales

GLOBAL FORUM ON CYBER EXPERTISE

Autores

El presente documento ha sido elaborado por el Equipo de Tareas sobre Estrategia y Evaluaciones del Grupo de Trabajo A del Global Forum on Cyber Expertise (GFCE), como proyecto en el marco de su Plan de Trabajo de 2020. Los miembros del equipo del proyecto son:

- Carolin Weisser Harris, del Centro Global de Capacitación de Seguridad Cibernética (GCSCC).
- Ian Wallace, Presidente del Grupo de Trabajo A sobre Estrategia y Política del GFCE.
- James Boorman, del Centro de Seguridad Cibernética de Oceanía (OCSC).
- Orhan Osmani y Marwan Ben Rached, de la Unión Internacional de Telecomunicaciones (UIT).
- Melissa Hathaway y Francesca Spidalieri, del Instituto Potomac de Estudios Políticos (PIPS).
- Radu Serrano, de la e-Governance Academy (eGA).
- Kerry-Ann Barrett, de la Organización de los Estados Americanos (OEA).

El equipo del proyecto desea expresar su gratitud al Instituto Australiano de Política Estratégica (ASPI), la Agencia de la Unión Europea para la Ciberseguridad (ENISA), MITRE Corporation y el Banco Mundial por sus comentarios y contribuciones; así como a Kathleen Bei, de la Secretaría del GFCE, por su apoyo en materia de diseño, logística y organización. Se agradece igualmente a la UIT la revisión y edición del presente documento y su traducción en árabe, francés, ruso y español.

Índice

Introducción

La comunidad mundial viene desplegando cada vez más esfuerzos para comprender las posturas de las naciones en materia de ciberseguridad a fin de analizar las deficiencias y adoptar decisiones mejor informadas sobre las intervenciones e inversiones que deben realizarse para mejorar las capacidades en dicha materia. Las instituciones de investigación, las organizaciones regionales y las empresas han elaborado marcos, modelos e índices y los han aplicado en todo el mundo, creando una base de conocimientos sobre el grado de madurez cibernética de los países y su nivel de preparación frente a las crecientes ciberamenazas para los gobiernos, la industria, las empresas y los ciudadanos.

En los comentarios positivos que se recibieron de la sesión sobre Evaluaciones de las capacidades cibernéticas, organizada en la quinta reunión del GFCE de abril de 2020, se destacó la necesidad de crear conciencia sobre las herramientas actuales de evaluación de las capacidades cibernéticas y proporcionar información sobre sus metodologías, resultados e impacto, a fin de ayudar a la comunidad del GFCE (beneficiarios, financiadores y encargados de la aplicación) a identificar herramientas y enfoques adecuados para atender las necesidades y lagunas de conocimiento prevalecientes.

Por consiguiente, este documento tiene por objeto ayudar en el proceso de toma de decisiones proporcionando un panorama completo de las diferentes herramientas, sus enfoques, beneficios y resultados, e indicando qué hacer y a quién contactar si un país desea someterse a dicha evaluación.

El Equipo de Tareas sobre Estrategia y Evaluaciones del GFCE seleccionó específicamente herramientas que sirven para evaluar las capacidades cibernéticas de un país. Sobre esta base, se han incluido las siguientes herramientas:

- Lucha contra la ciberdelincuencia: herramienta de fomento de capacidades, del Banco Mundial.
- Madurez cibernética en la región de Asia y el Pacífico, del Instituto Australiano de Política Estratégica (ASPI).
- Índice de Preparación Cibernética 2.0 (IPC), del Instituto Potomac de Estudios Políticos (PIPS).
- Modelo de Madurez de las Capacidades de Ciberseguridad para Naciones (MMC), del Centro Global de Capacitación de Seguridad Cibernética (GCSCC).
- Marco de Elaboración y Aplicación de la Estrategia Cibernética (EAEC), de la MITRE Corporation.
- Índice de Ciberseguridad Global (ICG), de la Unión Internacional de Telecomunicaciones (UIT).
- Marco de Evaluación de las Capacidades Nacionales (MECN), de la Agencia de la Unión Europea para la Ciberseguridad (ENISA); e
- Índice Nacional de Ciberseguridad (INC), de la e-Governance Academy (eGA).

A medida que se vayan identificando, se añadirán al documento otras herramientas que cumplan los criterios antes señalados.

A los efectos de este documento, se envió un cuestionario a las organizaciones encargadas de cada herramienta, a fin de recabar información sobre lo siguiente:

- Encargado(s) de la aplicación e información de contacto.
- Temas y asuntos.
- Indicadores.
- Metodología, recopilación de datos y control de calidad.
- Resultados y presentación.
- Impacto y beneficios; y
- Función en la coordinación de la actividad de fomento de la capacidad cibernética y el proceso de adecuación con el GFCE.

Lucha contra la ciberdelincuencia: Herramienta de evaluación del fomento de la capacidad

El Banco Mundial

La herramienta del Banco Mundial titulada Lucha contra la ciberdelincuencia: herramienta de evaluación del fomento de la capacidad ("Herramienta de Evaluación") se creó bajo los auspicios del proyecto de Lucha contra la Ciberdelincuencia para ayudar a los países en desarrollo a definir esferas prioritarias a fin de facilitar la asignación de sus escasos recursos de creación de capacidades.

La Herramienta de Evaluación se diferencia de otros marcos de evaluación en el hecho de que es una herramienta de autodiagnóstico que abarca nueve dimensiones, a saber: 1) el Marco no jurídico; 2) el Marco jurídico; 3) el Derecho sustantivo; 4) el Derecho procesal; 5) las Pruebas digitales; 6) la Jurisdicción; 7) las Salvaguardias; 8) la Cooperación internacional; y 9) el Fomento de la capacidad.

La Herramienta de Evaluación puede utilizarse para una actividad independiente llevada a cabo por un país para sus propios fines y también como un instrumento de diligencia debida fundamental para que los equipos de tareas operacionales evalúen el grado de preparación de un país para luchar contra la ciberdelincuencia.

Panorama general

Fecha de la última actualización de la herramienta	La última actualización de la publicación se realizó en 2017. Actualmente se está llevando a cabo el proceso de actualización de la actual herramienta de evaluación, que se ha previsto que concluya para julio de 2021.
Denominación de la herramienta de evaluación	Lucha contra la ciberdelincuencia: herramienta de evaluación del fomento de la capacidad.
Nombre de la organización que mantiene la herramienta	El Banco Mundial
Responsables de llevar a cabo las evaluaciones	La herramienta se encuentra disponible como un bien público mundial. Toda persona puede consultar la herramienta a partir del sitio web (véase más abajo) y utilizarla. Ha sido diseñada para servir como herramienta de autoevaluación.
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional.	https://www.combattingcybercrime.org/
Persona(s) de contacto para examinar la posibilidad de organizar una evaluación	Sr. David Satola, asesor principal, Vicepresidencia jurídica del Banco Mundial
Cobertura geográfica	Mundial

Posibles usuarios de la herramienta	• Responsables de la formulación de políticas • Legisladores • Fuerzas del orden • La sociedad civil de países en desarrollo • Todas las personas interesadas
Temas o asuntos cubiertos	Desde el punto de vista conceptual, la evaluación se organiza en torno a las nueve dimensiones siguientes: • **El marco no jurídico**: esto abarca las estrategias y políticas nacionales y otras cuestiones de índole no jurídica como la cooperación con el sector privado; • **El marco jurídico:** esto abarca la legislación nacional y si un país se ha adherido o no a un tratado; • **El derecho sustantivo:** aquí se abordan las actividades que se han tipificado como delito; • **El derecho procesal**: esto abarca principalmente las cuestiones relativas a la investigación; • **Las pruebas digitales:** esto se centra en la admisibilidad y el tratamiento de las pruebas digitales en el contexto de la ciberdelincuencia; • **La jurisdicción:** este apartado se centra en la manera en que se determina la jurisdicción del delito; • **Las salvaguardias:** esto se centra en tres elementos: las "garantías procesales", la protección de datos y la libertad de expresión; • **La cooperación internacional**: se centra primeramente en la extradición y, en segundo lugar, en la asistencia judicial recíproca, tanto oficial como oficiosa; y • **La creación de capacidades**: aquí se analiza la creación de capacidades tanto institucionales (por ejemplo, las academias de formación de las fuerzas del orden) como humanas, con hincapié en las necesidades de formación de los miembros de las fuerzas del orden, la fiscalía y la judicatura.
Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☐ Medidas de fomento de la confianza y normas ☐ Ciberdiplomacia ☒ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☐ Captura y análisis de incidentes ☐ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos / legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☒ Formación en materia de ciberdelincuencia

	☒ Prevención de la ciberdelincuencia Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☐ Normas sobre la Internet abierta ☐ Internet de las cosas
Tipos de indicadores	Indicadores tanto cuantitativos como cualitativos.
Número de indicadores y método de aplicación	La Herramienta de Evaluación consta de **115** indicadores, agrupados en nueve dimensiones: el marco no jurídico, el marco jurídico, el derecho sustantivo, el derecho procesal, las pruebas digitales, la jurisdicción, las salvaguardias, la cooperación internacional y el fomento de la capacidad. En el Cuadro de Evaluación, las nueve dimensiones se dividen en cuatro niveles. El **nivel 1** designa cada tema (la dimensión). El **nivel 2** define un marco general para cada pregunta, que se formula en el **nivel 3** y que puede precisarse con más detalle en el **nivel 4**. La última columna (indicador) proporciona una respuesta de tipo "sí/no" o una única opción entre una serie de respuestas.
Metodología – tipo de evaluación utilizada	**Específica para el caso:** el equipo de Lucha contra la Ciberdelincuencia realiza una evaluación inicial de un país cliente con base en una investigación documental y a continuación comunica sus conclusiones y comprueba y valida las evaluaciones con las autoridades gubernamentales responsables del país cliente.
Método primario de recopilación de datos	• Información disponible públicamente • Documentos no publicados • Cuestionarios y sondeos • Observaciones • Documentos y registros • Entrevistas personales
¿Se realiza una recopilación secundaria de datos?	Sí. Tras la investigación documental inicial, el equipo realiza una visita al país cliente y consulta con las autoridades gubernamentales responsables para comprobar y validar la evaluación inicial. • Observaciones • Documentos y registros
Mecanismos adoptados para garantizar la exactitud de los datos recopilados.	Los miembros del equipo de Lucha contra la Ciberdelincuencia, dirigidos por el Asesor Principal de TIC del Banco Mundial, suelen tener experiencia/conocimientos especializados en materia de ciberdelincuencia y se ocupan de diversas cuestiones de TIC en el Banco Mundial. Además, la evaluación inicial realizada por los miembros del equipo es comprobada y validada por las autoridades gubernamentales responsables en los países cliente a fin de garantizar la exactitud de los datos recopilados.
Principales resultados de la evaluación	En cada versión se crea un "Informe de evaluación de la creación de capacidades en materia de ciberdelincuencia" para cada país cliente.

Formato de presentación de los resultados de la evaluación	• Informe de evaluación de la creación de capacidades en materia de ciberdelincuencia (PDF) • Herramienta de visualización (gráficos en Excel)
¿Se pueden publicar los resultados de la evaluación?	Sí. Sin embargo, queda a discreción del país cliente publicar los resultados de la evaluación.
Método de consulta de los informes anteriores	La consulta de los informes anteriores queda a discreción del país cliente.
Pruebas de impacto	El equipo ha llevado a cabo evaluaciones de la creación de capacidades en materia de ciberdelincuencia para países cliente en las regiones de África y Asia-Pacífico, como Namibia, Etiopía, Kenya, los Estados Federados de Micronesia y Myanmar. Además, el equipo ha recibido nuevas solicitudes de evaluación de 22 países (Benin, Burundi, la República Democrática del Congo, Gambia, Liberia, Malí, Níger, Sierra Leona, Tanzanía, Uganda, Zambia, Burkina Faso, Cabo Verde, Comoras, Marruecos, Camerún, Mauritania, Rwanda y Senegal). Asimismo, una de nuestras organizaciones asociadas, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), ha adoptado la herramienta de evaluación como su metodología de evaluación exclusiva para evaluar el grado de preparación en materia de ciberdelincuencia. Por último, el equipo ha presentado la herramienta de evaluación en los siguientes eventos: la reunión anual del GFCE en Singapur (2018) y las reuniones del grupo de trabajo en La Haya (2018 y 2019); la reunión anual del Consejo de Europa (CoE) en Estrasburgo (2019); las conferencias anuales de la Asociación Internacional de Fiscales (IAP) en Sudáfrica (2018) y Argentina (2019); las reuniones conjuntas del CoE y la Unión Africana (UA) sobre la creación de capacidades para luchar contra la ciberdelincuencia en África (2018); y el Coloquio sobre el Derecho Internacional en Hong Kong, China (2019).
Beneficios de llevar a cabo una evaluación	La herramienta de evaluación permite llevar a cabo una evaluación eficaz y universalmente aplicable del grado de preparación de una nación en materia de ciberdelincuencia, garantizando su objetividad, calidad y accesibilidad. La combinación de estas tres características de la herramienta de evaluación permite que los responsables de la formulación de políticas, la elaboración de leyes y la toma de decisiones estén en mejores condiciones de decidir la manera en que se deben asignar los recursos. • La **objetividad** se logra respondiendo a cada pregunta de la herramienta de evaluación con una respuesta binaria de tipo "sí/no" en la mayor medida posible o mediante la selección de una opción clara entre una limitada serie de opciones. • La calidad se consigue con la "ponderación" de cada criterio. La herramienta de evaluación utiliza unos 115 indicadores agrupados en nueve temas (o dimensiones).

	• La facilidad **de comprensión** se logra a través de representaciones gráficas de la evaluación en un único gráfico de tipo "radial". El gráfico ayuda al país cliente a determinar si su práctica actual se ajusta a las buenas prácticas internacionales. Cada dimensión del gráfico radial general también puede examinarse con mayor detalle mostrando los resultados obtenidos en cada uno de los diferentes subcriterios.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	Sí. Sin embargo, el proceso específico de cálculo del coeficiente de ponderación no se comunica a los usuarios para evitar que se manipule la herramienta de evaluación.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	No. No se establece ninguna puntuación o clasificación de los resultados.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	• ¿Se han implementado ya estrategias y políticas nacionales en materia de ciberseguridad? **(Marco no jurídico)** • ¿Se han elaborado leyes nacionales en materia de ciberdelincuencia? ¿El país se ha adherido a algún tratado en materia de ciberdelincuencia? **(Marco jurídico)** • ¿El país tipifica como delito los actos delictivos tradicionales cometidos mediante/a través de actividades informáticas o los nuevos ciberdelitos? **(Derecho sustantivo)** • ¿Existen leyes procesales por las que se rija la investigación y el enjuiciamiento de los ciberdelitos? (**Derecho procesal)** • ¿El país ha implementado normas específicas sobre la admisibilidad y el tratamiento de las pruebas digitales? (**Pruebas digitales)** • ¿Cómo determina el país la jurisdicción de un ciberdelito? **(Jurisdicción)** • ¿El país ofrece "garantías procesales" (protección de datos y libertad de expresión) a sus ciudadanos? **(Salvaguardias)** • ¿El país ha implementado procedimientos de extradición o principios oficiales/oficiosos para la asistencia judicial recíproca en el plano internacional? **(Cooperación internacional)** • ¿Existen instituciones o programas destinados a la capacitación en materia de ciberdelincuencia de las fuerzas del orden, los fiscales y los jueces? **(Capacitación)**
¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	• Inicio • Inventario y análisis • Elaboración de la estrategia • Implementación • Supervisión y evaluación Cuando se utilice por primera vez la herramienta de evaluación se conseguirá un punto de referencia, mientras que la actualización periódica de los resultados mediante la herramienta facilitará supervisar el progreso.

¿Cómo facilita la evaluación la adecuación con otras actividades?	La herramienta de evaluación sirve para identificar las esferas prioritarias de un país en las nueve dimensiones, lo que a su vez facilita asignar de manera específica y concreta los escasos recursos de capacitación a fin de establecer una estrategia nacional para fomentar la capacidad de un país de luchar contra la ciberdelincuencia. Por consiguiente, la herramienta de evaluación puede utilizarse tanto para una actividad independiente llevada a cabo por un país y como un instrumento de diligencia debida fundamental para que los equipos de tareas operacionales evalúen el grado de preparación de un país para luchar contra la ciberdelincuencia.
¿Qué función desempeña la evaluación en el proceso de adecuación con el GFCE?	La herramienta de evaluación contribuiría en el proceso de adecuación con el GFCE al ofrecer una referencia sólida y objetiva a partir de la cual se pueden planificar y llevar a cabo sus actividades de creación de capacidades cibernéticas.
¿De qué estudios de caso o testimonios se dispone en relación con los beneficios de la herramienta?	Como se indicó anteriormente, la herramienta de evaluación ha demostrado sus beneficios a través de la realización exitosa de evaluaciones de la creación de capacidades en materia de ciberdelincuencia en diversos países cliente, y mediante el reconocimiento de nuestra organización asociada, la UNODC, que ahora utiliza la herramienta de evaluación como su método de evaluación exclusivo para evaluar el grado de preparación en materia de ciberdelincuencia.
¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?	• La herramienta de evaluación ha sido evaluada y validada por nuestras organizaciones asociadas, como el CoE, la UIT, la UNODC, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), la Fiscalía Suprema de la República de Corea (KSPO) y el GCSCC (Universidad de Oxford). • Un grupo independiente de expertos contribuyó a determinar el coeficiente de ponderación de cada indicador en la herramienta de evaluación.

Madurez cibernética en la región de Asia y el Pacífico

Instituto Australiano de Política Estratégica (ASPI)

Madurez cibernética en la región de Asia y el Pacífico es el título de un informe anual publicado por el Instituto Australiano de Política Estratégica (ASPI) en que se examinan las tendencias en materia de madurez cibernética en Asia y el Pacífico. En él se analiza una amplia muestra representativa de la región, que abarca 25 países de Asia Meridional, Septentrional y Sudoriental, el Pacífico Sur y América del Norte.

La metodología de la "medida de la madurez cibernética" consiste en evaluar las diversas facetas de las capacidades cibernéticas de los Estados. El modelo se ha perfeccionado mediante la implicación de expertos y partes interesadas de la región de Asia-Pacífico, de manera que evalúa los cambios de los enfoques de los Estados y los avances tecnológicos. En este contexto, la "madurez" se demuestra a través de la presencia, la aplicación eficaz y el funcionamiento de estructuras, políticas, leyes y organizaciones relacionadas con la esfera cibernética. Estos indicadores de madurez cibernética abarcan las estructuras políticas y legislativas pangubernamentales, las respuestas a la ciberdelincuencia financiera, la organización militar, la solidez económica digital y de las empresas y los niveles de cibersensibilización en la sociedad.

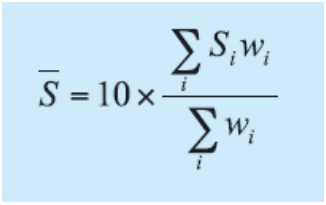
La base de investigación en que se fundan estos grupos de indicadores es una compilación de información procedente exclusivamente del ámbito público; en otras palabras, las conclusiones del informe se basan solo en datos públicos.

Panorama general

Fecha de la última actualización de la herramienta	2017
Denominación de la herramienta de evaluación	Madurez cibernética en la región de Asia y el Pacífico
Nombre de la organización que mantiene la herramienta	Instituto Australiano de Política Estratégica (ASPI)
Responsable de llevar a cabo las evaluaciones	Instituto Australiano de Política Estratégica (ASPI)
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017
Personas de contacto para examinar la posibilidad de organizar una evaluación	Sra. Danielle Cave, directora adjunta del Centro Internacional de Política Cibernética del ASPI; Sr. Tom Uren, analista superior de ese mismo centro; y Sr. Bart Hogeveen, Jefe de la Unidad de Creación de Capacidades Cibernéticas del ASPI.
Cobertura geográfica	Regional
Posibles usuarios de la herramienta	Cualquier persona. El informe se encuentra públicamente disponible.

Temas o asuntos cubiertos	**1 Gobernanza** El tema de la gobernanza aborda el enfoque organizacional del Estado sobre las cuestiones cibernéticas, incluida la composición de los organismos gubernamentales que colaboran en estas cuestiones; la intención y las capacidades legislativas del Estado; y la implicación del Estado en las cuestiones internacionales en materia de política cibernética como la gobernanza de Internet, la aplicación del derecho internacional y la elaboración de normas o principios. Estos indicadores proporcionan orientaciones para la colaboración de los diplomáticos, el Gobierno, los socios para el desarrollo, las fuerzas del orden y el sector privado en los Estados de la región de Asia-Pacífico. **2 Aplicación de la ley en materia de ciberdelincuencia financiera** La ciberdelincuencia financiera es un problema crucial para todos los Estados de Asia y el Pacífico. El efecto de la ciberdelincuencia en la gente común de la región es importante e incluye considerables pérdidas financieras. Comprender la capacidad del Estado para afrontar la ciberdelincuencia financiera puede guiar la colaboración en materia de aplicación de la ley, por ejemplo, a través de la compartición de información y la ayuda al desarrollo de capacidades de los sectores público y privado. **3 Aplicación militar** Este tema aborda la estructura organizacional militar del Estado (en su caso) en relación con el ciberespacio y las opiniones conocidas del Estado sobre el uso del ciberespacio por sus fuerzas armadas. Esto puede guiar la colaboración militar entre Estados, así como la colaboración diplomática y político-militar. Los usos militares del ciberespacio, concretamente las capacidades nacionales, son un tema delicado para todos los países de la región de Asia-Pacífico, por lo que esta esfera debe examinarse detenidamente antes de que los Estados intenten o acepten colaborar entre sí. **4 Economía digital y empresas** El hecho de que el Estado comprenda la importancia del ciberespacio y la economía digital y la manera en que concibe estos factores como económicamente importantes constituye un indicador de madurez cibernética. Esto puede guiar la colaboración en materia de creación de capacidades, el establecimiento de relaciones comerciales regionales y la interacción entre el Gobierno y las empresas en la esfera de la ciberseguridad. **5 Implicación social** La concienciación y participación públicas sobre las cuestiones cibernéticas, como la gobernanza de Internet, la censura de Internet y la ciberdelincuencia indican la madurez del discurso público entre el Estado y sus ciudadanos. Los programas educativos sobre las TIC y las cuestiones cibernéticas también podrían indicar un alto grado de comprensión técnica basada en las cuestiones pertinentes. La parte de la población de un Estado que tiene acceso a Internet indica el tipo de implicación personal y de las empresas en el ciberespacio, la calidad de la infraestructura de TIC y el nivel de confianza de los ciudadanos en el comercio digital. Esto puede guiar a los organismos de desarrollo que buscan construir economías regionales y a las empresas que desean desarrollar el comercio en la región.

Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☒ Medidas de fomento de la confianza y normas ☒ Ciberdiplomacia ☒ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☐ Captura y análisis de incidentes ☐ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☐ Formación en materia de ciberdelincuencia ☐ Prevención de la ciberdelincuencia Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☐ Formación en materia de ciberdelincuencia ☐ Prevención de la ciberdelincuencia Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☐ Normas sobre la Internet abierta ☐ Internet de las cosas
Tipos de indicadores	Indicadores cuantitativos y cualitativos
Número de indicadores y método de aplicación	La "medida de la madurez cibernética" incluye diez indicadores. Los indicadores se ponderan con base en su importancia para la madurez cibernética del Estado. Un grupo de ciberexpertos y partes interesadas de los organismos gubernamentales y el sector privado los ponderaron con una escala del 1 al 10, donde 1 significa que el indicador no es "nada importante" y 10 "extremadamente importante". A continuación, se calculó el promedio de estas ponderaciones de expertos realizadas para cada categoría, a fin de conseguir un factor de ponderación que podría utilizarse en el cálculo de un resultado general. Así, en la última etapa, cada país fue evaluado con base en los diez factores, mediante una escala del 0 al 10 (donde 10 corresponde al mayor grado de madurez). Las evaluaciones se basaron en una investigación de datos públicos

	cualitativos y cuantitativos y, cuando fue posible, una comparación con la investigación y los resultados de 2014, 2015 y 2016. La puntuación general de cada país fue la suma de las puntuaciones obtenidas para cada factor ponderadas por la importancia media calculada. Para facilitar la interpretación, las puntuaciones generales se convirtieron a un porcentaje de la mayor puntuación posible, con base en los coeficientes de ponderación asignados:  donde $\overline{S}$ = puntuación ponderada, S = puntuación y w = ponderación.
Metodología – tipo de evaluación utilizada	Comparativa, con clasificación.
Método primario de recopilación de datos	Información pública
¿Se realiza una recopilación secundaria de datos?	• Entrevistas • Cuestionarios y sondeos • Observaciones • Grupos temáticos
Mecanismos adoptados para garantizar la exactitud de los datos recopilados.	Se invita a las embajadas y altos comisionados de los países cubiertos por el informe a que verifiquen los hechos del perfil de su país.
Principales resultados de la evaluación	• Perfiles individuales de países • Clasificación regional comparativa • Visión general de las tendencias regionales • Evaluación de oportunidades de colaboración internacional
Formato de presentación de los resultados de la evaluación	Informe
¿Se pueden publicar los resultados de la evaluación?	Sí. Los resultados se publican en un informe.
Método de consulta de los informes anteriores	https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2016 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2015 https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2014
Pruebas de impacto	Véase la respuesta en el apartado sobre los "testimonios" más abajo.

Beneficios de llevar a cabo una evaluación	Véase la respuesta en el apartado sobre el "momento del ciclo de vida de la estrategia" más abajo.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	Sí. Véase la respuesta sobre los "indicadores y su método de aplicación" indicada anteriormente.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	Sí. Véase la respuesta sobre los "indicadores y su método de aplicación" indicada anteriormente.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	¿Cuáles son las tendencias regionales en materia de madurez cibernética en la región de Asia-Pacífico? ¿De qué manera comparan los países de Asia y del Pacífico los cinco temas de política que constituyen la madurez cibernética? ¿Qué oportunidades de colaboración internacional hay con los países de la región de Asia-Pacífico?
¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	La medida analiza la región de Asia-Pacífico desde una perspectiva comparativa. Para desarrollar una ciberestrategia nacional, los informes son más adecuados en las fases de inicio, inventario, y supervisión y evaluación. Cuando se desarrolla un enfoque regional o una "imagen" regional, la herramienta es idónea para la definición de programas, los análisis en el plano estratégico y las comparaciones de prácticas nacionales. El ciclo anual del informe es útil para las labores de supervisión y evaluación y los análisis de tendencias.
¿Cómo facilita la evaluación la adecuación con otras actividades?	El informe proporciona una fuente autorizada de análisis basados en hechos y pruebas en beneficio de los responsables de la formulación de políticas de los sectores público y privado en los planos nacional, regional y público.
¿Qué función desempeña la evaluación en el proceso de adecuación con el GFCE?	El informe proporciona posibles puntos de acceso para las conversaciones entre los destinatarios y los proveedores de las actividades de creación de capacidades cibernéticas.
¿De qué estudios de caso o testimonios se dispone en relación con los beneficios de la herramienta?	El informe tiende a ser seleccionado por los medios de comunicación: • https://www.zdnet.com/article/only-us-tops-australia-in-asia-pacific-cyber-maturity-aspi/ • https://www.theaustralian.com.au/commentary/opinion/threat-posed-by-evil- nations-and-criminals-in-cyberland-is-rising/news-story/fdebd93f3dc0206afe0705e6f6ec045c • https://vovworld.vn/en-US/spotlight/vietnam-ranks-9th-in-cyber-maturity-in- asiapacific-region-379580.vov

	• https://theaseanpost.com/article/cyberattack-malaysia-imminent-or-imagined Se hace referencia al informe en discursos, como los de líderes políticos (de Australia): • https://www.rusi.org.au/resources/Documents/2015_10_05%20Brodtman.pdf El informe se utiliza como fuente en otras publicaciones políticas y académicas, como por ejemplo: • https://www.austcyber.com/resources/sector-competitiveness-plan/executive- summary • https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Maurer_Tim_Web.pdf • https://www.standards.org.au/getmedia/952ea009-ffc2-490a-905f-8f731fa84a52/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx
¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?	En su condición de grupo de reflexión reconocido, el ASPI se rige por su carta en la que se consagran los principios de independencia y antipartidismo. Además, el informe se elabora con base en fuentes públicas y verificables. Las observaciones o conclusiones no están sujetas a la aprobación de ningún gobierno o financiador y siguen las prácticas normativas habituales de rigor analítico.
Sírvanse añadir información adicional	El informe se publicó por última vez en diciembre de 2017 en previsión de una nueva financiación y una reevaluación de los posibles resultados de la investigación.

Índice de Preparación Cibernética 2.0 (IPC)

Instituto Potomac de Estudios Políticos (PIPS)

El *Índice de Preparación Cibernética 2.0* (IPC) proporciona una metodología exhaustiva, comparativa y basada en las experiencias para evaluar el compromiso y la madurez de los países a la hora de garantizar su infraestructura y servicios digitales nacionales de que dependen su crecimiento económico y su resistencia nacional. El IPC 2.0 se basa en el Índice de Preparación Cibernética de 2013 1.0, que fue el primer marco metodológico disponible para evaluar el grado de preparación cibernética. La herramienta de evaluación del IPC puede ayudar a los países a determinar las deficiencias existentes, fortalecer su posición actual en materia de ciberseguridad y gestionar mejor los riesgos cibernéticos a nivel nacional.

Desde 2013, el IPC se ha aplicado a más de 100 países y se han elaborado 14 informes exhaustivos.

Panorama general

Fecha de la última actualización de la herramienta	Se añaden periódicamente nuevas preguntas e indicadores a cada uno de los siete elementos fundamentales de la herramienta.
Denominación de la herramienta de evaluación	Índice de Preparación Cibernética 2.0
Nombre de la organización que mantiene la herramienta	Institut Potomac d'études politiques (PIPS)
Responsables de llevar a cabo las evaluaciones	Miembros del equipo de Preparación Cibernética (Sras. Melissa Hathaway y Francesca Spidalieri)
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional	• Página web del PIPS: https://www.potomacinstitute.org/academic-centers/cyber- readiness-index • Portal Cybil: https://cybilportal.org/tools/cyber-readiness-index-2-0/
Personas de contacto para examinar la posibilidad de organizar una evaluación	• Melissa Hathaway, investigadora superior del PIPS e investigadora principal del IPC: hathawayglobal@icloud.com • Francesca Spidalieri, investigadora coprincipal del IPC: francescaspidalieri@gmail.com
Cobertura geográfica	Mundial
Posibles usuarios de la herramienta	• Líderes mundiales • Gobiernos nacionales/regionales • Ministerios y organismos públicos • Organismos de ciberseguridad/responsables de la formulación de políticas • Instituciones académicas • Expertos en ciberseguridad • Investigadores particulares

Temas o asuntos cubiertos	El IPC 2.0 utiliza más de 70 indicadores únicos sobre siete elementos esenciales para discernir las actividades operacionalmente preparadas e identificar las esferas de mejora en las siguientes categorías: 1) **Estrategia nacional:** publicación de una estrategia nacional; designación de una autoridad competente; identificación de las entidades gubernamentales clave y las entidades comerciales clave encargadas de la aplicación; mecanismos para garantizar la infraestructura crítica; identificación de servicios críticos; identificación de normas nacionales para la continuidad del servicio. 2) **Respuesta a incidentes:** publicación de un plan de respuesta a incidentes; identificación de dependencias intersectoriales; pruebas de que el plan se aplica y actualiza; publicación de una evaluación de amenazas cibernéticas; establecimiento de un equipo de intervención en caso de incidentes de seguridad informática (EIISI); recursos financieros y humanos. 3) **Ciberdelincuencia y aplicación de la ley:** ratificación de tratados internacionales en materia de ciberdelincuencia; medidas adoptadas para reducir la ciberdelincuencia; capacidad institucional para luchar contra la ciberdelincuencia; compromiso de revisar las leyes y mecanismos existentes; medidas adoptadas para limpiar las infraestructuras infectadas; capacitación de las fuerzas del orden y desarrollo de capacidades. 4) **Compartición de la información:** política sobre la compartición de la información; estructura institucional para compartir información con los organismos gubernamentales y/o la industria; pruebas de la presencia de mecanismos de coordinación entre sectores y entre partes interesadas; posibilidad de que el Gobierno desclasifique información de inteligencia y procesos a tales efectos. 5) **Inversión en I+D, educación y capacidad:** mecanismos de incentivos del Gobierno para alentar la innovación y las inversiones en la ciberseguridad; recursos financieros y humanos para la I+D y la transmisión de tecnologías; maestrías sobre ciberseguridad; patrocinio de campañas de concienciación y programas educativos en materia de ciberseguridad. 6) **Diplomacia y comercio:** identificación de la ciberseguridad como un elemento esencial de la política extranjera y las negociaciones económicas internacionales; definición del personal dedicado a la diplomacia cibernética en una oficina del país en el extranjero; participación en los acuerdos internacionales, multinacionales y regionales en materia de ciberseguridad y aplicación de esos acuerdos. 7) **Defensa y respuesta a crisis:** establecimiento de una organización militar y/o no militar para la defensa cibernética en el plano nacional; pruebas de que se realizan ejercicios cibernéticos a nivel nacional con los asociados comerciales y/o internacionales; definición de normas relativas al comportamiento del Estado en el ciberespacio; establecimiento de mecanismos de asistencia rápida. Se puede consultar una descripción completa de cada elemento esencial en la metodología expuesta por completo en: https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☒ Medidas de fomento de la confianza y normas ☒ Ciberdiplomacia ☒ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☒ Captura y análisis de incidentes ☒ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☒ Formación en materia de ciberdelincuencia ☒ Prevención de la ciberdelincuencia Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☒ Normas internacionales y/o nacionales
Tipos de indicadores	El método de recopilación de datos en el marco del IPC 2.0 es cualitativo y cada indicador se evalúa con base en cuatro categorías clave: 1) declaraciones/estrategias/políticas; 2) organización/autoridad competente; 3) recursos; y 4) aplicación.
Número de indicadores y método de aplicación	El IPC 2.0 utiliza más de 70 indicadores sobre siete elementos esenciales para evaluar la madurez de un país en materia de ciberseguridad y discernir las áreas que están plenamente operacionales, parcialmente operacionales o respecto de las que no hay pruebas suficientes. Todos los indicadores del IPC 2.0 tienen la misma estructura en común, y las preguntas formuladas en una versión de la metodología son comparables a preguntas similares de las versiones anteriores o futuras. Cada indicador recibe la misma ponderación y a continuación se describe en el informe de país como parte de un contexto más amplio basado en las necesidades, capacidades, prioridades y objetivos del país.
Metodología – tipo de evaluación utilizada	El IPC 2.0 utiliza fuentes primarias, como las estrategias nacionales, políticas, leyes, declaraciones oficiales de líderes, evaluaciones e informes nacionales, etc. para evaluar la madurez cibernética de los países y elaborar perfiles exhaustivos de estos. ⇒ No se establece una clasificación de los países.

Método primario de recopilación de datos	• Información pública • Documentos confidenciales oficiales o no publicados • Entrevistas/observaciones • Documentos y registros
¿Se realiza una recopilación secundaria de datos?	Sí. La recopilación secundaria de datos se realiza para corroborar, corregir o ampliar la información recabada durante nuestro análisis de fuentes primarias y las entrevistas con los funcionarios y expertos del país.
Mecanismos adoptados para garantizar la exactitud de los datos recopilados	Toda nuestra investigación se basa en fuentes primarias y documentación oficial, y a continuación es corroborada por funcionarios del país y/o expertos en la materia.
Principales resultados de la evaluación	En la página web del PIPS se publican informes de países exhaustivos, que se ponen a disposición del público en las seis lenguas de las Naciones Unidas. Estos informes pueden ayudar a los Gobiernos que aún están elaborando sus prácticas y políticas de ciberseguridad y proporcionarles un plan viable de las prioridades necesarias para reforzar su posición en la esfera de la ciberseguridad, permitiéndoles así determinar las medidas que se deben adoptar para reducir los riesgos con independencia de sus conocimientos técnicos internos.
Formato de presentación de los resultados de la evaluación	• Informes de países exhaustivos • Herramienta de visualización (gráfico de tipo radial y "bolas de Harvey") • Presentación en PowerPoint, si el país lo solicita.
¿Se pueden publicar los resultados de la evaluación?	Sí. Todos los informes de países del IPC están a disposición del público en la sección web dedicada al IPC de la página del PIPS: https://www.potomacinstitute.org/academic-centers/cyber-readiness-index.
Método de consulta de los informes anteriores	Véase más arriba.
Pruebas de impacto	El IPC ha influido directamente en las políticas de preparación cibernética y en el pensamiento de líderes de los siguientes países y organizaciones: Alemania, Arabia Saudita, Australia, Azerbaiyán, Bangladesh, Bosnia y Herzegovina, Bulgaria, Canadá, China, Egipto, Eslovaquia, Estonia, Filipinas, Francia, Georgia, India, Indonesia, Islandia, Israel, Italia, Japón, Jordania, Kirguistán, Lituania, México, Nueva Zelandia, Omán, Países Bajos, Polonia, Reino Unido, República Checa, Rumania, Serbia, Sudáfrica, Suecia, Suiza, Ucrania; el foro africano de equipos de intervención en caso de incidentes informáticos (Africa CERT), el grupo de equipos de respuesta a emergencias informáticas en la región de Asia-Pacífico (APCERT), la UIT, el Banco Interamericano de Desarrollo (BID), la Organización del Tratado del Atlántico Norte (OTAN), el Consejo Nórdico, la Organización de los Estados Americanos (OEA) y el Banco Mundial.

	El IPC sigue teniendo un impacto mundial y su principal investigador, Melissa Hathaway, ha reforzado la formación de líderes de todo el mundo sobre estas cuestiones. Se la invita habitualmente a participar en colaboraciones y debates internacionales de alto nivel, aparece en múltiples publicaciones internacionales y sigue informando a los líderes nacionales sobre la viabilidad de utilizar el IPC 2.0 como herramienta para planificar/comparar y garantizar la participación de varios interesados en las medidas y procesos nacionales en materia de ciberseguridad, y para aumentar la financiación destinada al fomento de la capacidad en la esfera de la ciberseguridad.
Beneficios de llevar a cabo una evaluación	La evaluación del IPC 2.0 puede ayudar a los países a identificar las lagunas existentes entre su postura actual en materia de ciberseguridad y las capacidades cibernéticas nacionales que se necesitan para apoyar su futuro digital. La herramienta también puede utilizarse para determinar la posición de un país en la curva de madurez desde un punto de vista pangubernamental y pannacional. Cuando se analizan conjuntamente, los indicadores pueden ayudar a los gobiernos a evaluar y armonizar sus iniciativas digitales y de seguridad nacional. A través de los datos recopilados, el IPC también puede destacar las mejores prácticas que los países pueden implementar para facilitar y contribuir a llevar a cabo las medidas de preparación cibernética implementadas en las industrias y sectores. El IPC 2.0 hace hincapié en las herramientas que los líderes nacionales pueden utilizar, como las políticas, las leyes, los reglamentos, las normas, los incentivos de mercado y otras iniciativas, a fin de proteger el valor de sus inversiones digitales y hacer frente a la constante erosión económica causada por la ciberinseguridad. Esta evaluación puede ayudar a los líderes nacionales a reconocer que para aprovechar todo el potencial de la economía digital en términos de crecimiento económico, aumento de la productividad y la eficiencia, mejora de las destrezas de la fuerza de trabajo y mejora del acceso a las empresas y la información, es necesario ajustar las estrategias de desarrollo económico a las prioridades nacionales en materia de seguridad. Ilustra la manera en que las TIC pueden conseguir el crecimiento económico, pero solo si se implementan los procesos, políticas y tecnologías adecuados para proteger y asegurar la infraestructura cibernética y los servicios cibernéticos de que dependen el futuro digital y el crecimiento de un país.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	Sí. En nuestra base de datos se atribuyen 5 puntos a los indicadores que están completamente operacionales, 3 puntos a los que están parcialmente operacionales y 1 punto cuando se han clasificado elementos específicos o no hay pruebas suficientes de su existencia o aplicación. El cálculo de la ponderación solo se utiliza para crear gráficos radiales y otros elementos visuales, pero no para clasificar a los países.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	El IPC 2.0 proporciona una puntuación de madurez para cada elemento esencial pero no clasifica a los países.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	• ¿Están los objetivos a corto y largo plazo del país, incluida la agenda digital, las políticas industriales, los objetivos económicos y las prioridades nacionales de seguridad, en consonancia con su estrategia nacional en materia de ciberseguridad? • ¿Qué tipo de ciberamenazas podrían poner a estos objetivos en peligro u obstaculizar el cumplimiento de estos objetivos? • ¿Cuáles son las dependencias digitales más importantes del país (por ejemplo, las empresas, los servicios, las infraestructuras y los activos) que, en caso de daño, tendrían graves consecuencias económicas y para la seguridad nacional? • ¿Se han establecido líneas claras de rendición de cuentas y responsabilidad para garantizar que se consigan los objetivos del país y se implementen las medidas de reducción de riesgos? • ¿Las consideraciones en materia de ciberseguridad y resiliencia han sido una parte fundamental del proceso de planificación? • ¿Qué medidas puede adoptar el país para aumentar su resiliencia digital? El IPC 2.0 también puede considerarse una referencia para que los países identifiquen sus lagunas entre su posición actual en materia de ciberseguridad y las capacidades cibernéticas nacionales que se necesitan para corregir las deficiencias y apoyar las futuras prioridades del país respecto de la economía y la seguridad. Los líderes gubernamentales pueden utilizar el IPC 2.0 para facilitar y contribuir a las medidas de preparación cibernética implementadas en las industrias y sectores, haciendo así constantemente hincapié en la relación entre su estrategia digital e industrial y sus prioridades nacionales en materia de seguridad.
¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	La metodología del IPC debe ser parte de todo el ciclo de vida de la estrategia y su herramienta de evaluación puede utilizarse antes y/o después de la elaboración de una estrategia nacional de ciberseguridad, por ejemplo, en las etapas de inicio, inventario y análisis, elaboración de la estrategia, implementación, supervisión y evaluación, y actualización de la estrategia.
¿Cómo facilita la evaluación la adecuación con otras actividades?	El IPC 2.0 vincula el crecimiento y desarrollo económicos con las políticas nacionales de seguridad y, por consiguiente, puede ayudar a los países a adaptar mejor su estrategia nacional de ciberseguridad a sus estrategias digitales y de crecimiento.
¿Qué función desempeña la evaluación en el proceso de adecuación con el GFCE?	El IPC 2.0 puede corroborar o complementar otras herramientas de evaluación ofrecidas por la Comunidad de GFCE, como el Modelo de Madurez de la Capacidad en materia de Ciberseguridad para las naciones (MMC), de Oxford, y el Índice de Ciberseguridad Global (ICG), de la UIT.

¿De qué estudios de caso o testimonios se dispone en relación con los beneficios de la herramienta?	Además de todos los países y organizaciones internacionales antes señalados que han utilizado el IPC para elaborar sus políticas y estrategias, la metodología del IPC ha sido citada o utilizada en múltiples artículos, discursos, sesiones informativas, informes y publicaciones derivadas. Por ejemplo, la OEA y el BID utilizaron la metodología y la base de datos del IPC 2.0 para corroborar y validar su informe internacional sobre el nivel de capacidades y preparación cibernéticas de los países miembros (Ciberseguridad:¿Estamos preparados en América Latina y el Caribe?). El equipo del IPC ha trabajado activamente con la UIT para intercambiar datos, armonizar medidas, amplificar el impacto y contribuir a dos de los proyectos decisivos de la UIT sobre ciberseguridad, a saber, el desarrollo de la segunda versión del Índice de Ciberseguridad Global (ICG) de la UIT y la creación de la Guía para la elaboración de una estrategia nacional de ciberseguridad, iniciativa multipartita dirigida por la UIT. Se pueden consultar otros artículos de prensa sobre el IPC en el apartado "Cyber Readiness in the News": https://www.potomacinstitute.org/academic-centers/cyber-readiness-index
¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?	Los informes de países se basan en datos públicos primarios validados de manera independiente por nuestro equipo de expertos.

Modelo de Madurez de las Capacidades de Ciberseguridad para Naciones (MMC)

Centro Global de Capacitación de Seguridad Cibernética (GCSCC), Universidad de Oxford y asociados

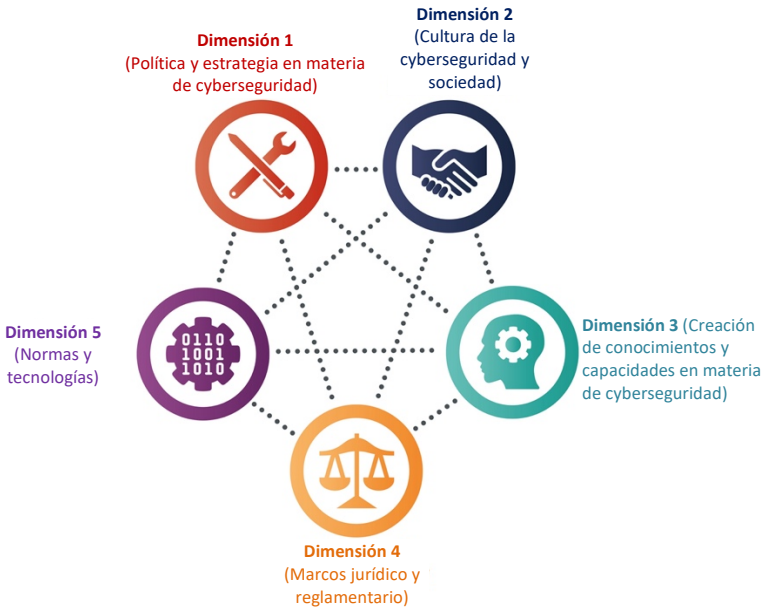
El Modelo de Madurez de las Capacidades de Ciberseguridad para Naciones (MMC), desarrollado por el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford, sirve para medir las capacidades de un país en materia de ciberseguridad respecto de cinco dimensiones, permitiendo así a las naciones autoevaluarse, planificar mejor sus inversiones y estrategias nacionales de ciberseguridad y definir prioridades para el desarrollo de capacidades. Desde 2015, se han realizado más de 110 revisiones del MMC en más de 80 países de todo el mundo.

El GCSCC y sus asociados definen ampliamente el concepto de capacidad en ciberseguridad a fin de abarcar las políticas, estrategias, los factores sociales y culturales, la educación y formación, las leyes y reglamentos, y las cibertecnologías y normas. En línea con esta definición, su método de investigación es multidisciplinario, ya que aborda las capacidades en ciberseguridad en todas sus dimensiones desde múltiples perspectivas académicas.

El MMC se creó con la intención de investigar sobre los matices de la creación de capacidad entre estas múltiples dimensiones y dentro de ellas; los tipos de actividades que pueden ofrecer y aumentar las capacidades; dónde se dan las mejores prácticas; las condiciones en que se deberían aumentar las capacidades; y la manera en que las dimensiones se relacionan entre sí y dependen unas de otras para el éxito. Con este objetivo, el MMC también proporciona un marco que permite comparar las capacidades en ciberseguridad entre diferentes naciones del mundo y a lo largo del tiempo. Esta metodología sirve para recabar información de diferentes actores y grupos de interesados a fin de reflejar una visión amplia de las capacidades en ciberseguridad en cada nación.

Panorama general

Fecha de la última actualización de la herramienta	Marzo de 2021
Denominación de la herramienta de evaluación	Modelo de Madurez de las Capacidades de Ciberseguridad para Naciones (MMC), edición de 2021
Nombre de la organización que mantiene la herramienta	Centro Global de Capacitación de Seguridad Cibernética (GCSCC) Centro de Seguridad Cibernética de Oceanía (OCSC) Centro de Capacidades en materia de Ciberseguridad de África Meridional (C3SA)
Responsables de llevar a cabo las evaluaciones	El Centro Global de Capacitación de Seguridad Cibernética (GCSCC), el Centro de Seguridad Cibernética de Oceanía (OCSC), el Centro de Capacidades en materia de Ciberseguridad de África Meridional (C3SA), la Organización de los Estados Americanos (OEA), el Banco Mundial y NRD Cyber Security. Asociados de la implementación: La Unión Internacional de Telecomunicaciones (UIT), el Global Forum on Cyber Expertise (GFCE), la Organización de Telecomunicaciones del Commonwealth (OTC), el Centro de Información de Redes de Asia-Pacífico (APNIC), la Telecomunidad Asia-Pacífico (APT), el Instituto Noruego de Asuntos

	Internacionales (NUPI) y la Organización Alemana para la Cooperación Internacional, Alemania.
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional	https://gcscc.ox.ac.uk/the-cmm
Personas de contacto para examinar la posibilidad de organizar una evaluación	GCSCC, en todo el mundo, Sra. Carolin Weisser Harris: carolin.weisser@cs.ox.ac.uk OCSC, en la región de Oceanía, Sr. James Boorman: james.boorman@ocsc.com.au C3SA, en la región de África, Sra. Nthabiseng Pule: npule@researchictafrica.net
Cobertura geográfica	Mundial
Posibles usuarios de la herramienta	Cualquier persona. El MMC es un documento que se encuentra públicamente disponible. Para realizar una revisión del MMC, se recomienda trabajar con uno de los encargados de la aplicación que están familiarizados con la metodología del MMC.
Temas o asuntos cubiertos	El MMC analiza las capacidades en ciberseguridad a través de las cinco dimensiones fundamentales para crear las capacidades de un país en materia de ciberseguridad, a saber:  **Dimensión 1 (*Política y estrategia en materia de ciberseguridad*)**: analiza la capacidad de un país para desarrollar y poner en marcha una estrategia de ciberseguridad y aumentar su resiliencia en esta esfera mediante la mejora de su respuesta a los incidentes, la ciberdefensa y las capacidades de protección de las infraestructuras críticas. En esta dimensión se examinan las estrategias y políticas eficaces para ofrecer capacidades nacionales en materia de ciberseguridad, manteniendo al mismo tiempo los beneficios de un ciberespacio vital para el Gobierno, las empresas internacionales y la sociedad en general.

	Dimensión 2 ***(Cultura de la ciberseguridad y sociedad)***: revisa elementos importantes de una cultura de ciberseguridad responsable, como la comprensión de los riesgos relacionados con la ciberseguridad en la sociedad, el nivel de confianza en los servicios de Internet, los servicios del cibergobierno y el comercio electrónico, y la comprensión por los usuarios de la protección de los datos personales en línea. Además, en esta dimensión se analiza la existencia de mecanismos de presentación de denuncias que funcionan como canales para que los usuarios denuncien los ciberdelitos. Asimismo, se revisa la función que desempeñan los medios de comunicación y sociales en la definición de los valores, actitudes y conductas en la esfera de la ciberseguridad. **Dimensión 3** ***(Creación de conocimientos y capacidades en materia de ciberseguridad)***: revisa la disponibilidad, la calidad y la realización de programas para varios grupos de interesados, incluidos el Gobierno, el sector privado y la población en general, y se refiere a los programas de concienciación en materia de ciberseguridad, los programas educativos oficiales en dicha materia y los programas de capacitación profesional. **Dimensión 4** ***(Marcos jurídico y reglamentario)***: examina la capacidad del Gobierno para elaborar y promulgar leyes nacionales que guardan directa o indirectamente relación con la ciberseguridad, con especial hincapié en los temas relativos a los requisitos reglamentarios para la ciberseguridad, la legislación en materia de ciberdelincuencia y la legislación conexa. La capacidad de promulgar dichas leyes se examina a través de las capacidades de las fuerzas del orden, la fiscalía, los organismos reguladores y los tribunales. Además, en esta dimensión se analizan cuestiones como los marcos de cooperación oficiales y oficiosos para luchar contra la ciberdelincuencia. **Dimensión 5** ***(Normas y tecnologías):*** aborda el uso efectivo y generalizado de la tecnología de ciberseguridad para proteger a las personas, las organizaciones y la infraestructura nacional. En esta dimensión se examina específicamente la aplicación de normas y buenas prácticas en materia de ciberseguridad, la implementación de procesos y controles y el desarrollo de tecnologías y productos para reducir los riesgos de ciberseguridad.
Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☒ Medidas de fomento de la confianza y normas ☒ Ciberdiplomacia ☐ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☒ Captura y análisis de incidentes ☒ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☒ Formación en materia de ciberdelincuencia

	☒ Prevención de la ciberdelincuencia Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☒ Normas internacionales y/o nacionales
Tipos de indicadores	Indicadores cualitativos
Número de indicadores y método de aplicación	El MMC abarca unos 600 indicadores para evaluar la madurez en cinco dimensiones fundamentales para crear las capacidades de un país en materia de ciberseguridad, a saber: política y estrategia en materia de ciberseguridad; cultura de la ciberseguridad y sociedad; creación de conocimientos y capacidades en materia de ciberseguridad; marcos jurídico y reglamentario; y normas y tecnologías. Cada **Dimensión** del MMC está formada por un conjunto de **Factores**, que describen y definen lo que significa tener capacidades de ciberseguridad. La mayoría de los factores se desglosan en varios **Aspectos**. Cada factor/aspecto tiene una serie de **Indicadores** con cinco **Grados** de madurez: Inicial, formativa, establecida, estratégica y dinámica. Estos indicadores describen las etapas y medidas que deben adoptarse para conseguir o mantener un determinado grado de madurez en el correspondiente nivel del aspecto/factor/dimensión. Para que un país demuestre su madurez evaluada respecto de un determinado aspecto/factor, se deben proporcionar pruebas para cada indicador; de lo contrario, no se podrá considerar que el país ha evolucionado ni se podrá estudiar la posibilidad de que pase al siguiente nivel.
Metodología – tipo de evaluación utilizada	La implementación del MMC es un proceso que abarca múltiples etapas y partes interesadas, y consiste en tres fases principales: 1) Contextualización de la investigación documental realizada por el equipo de aplicación. 2) Debates nacionales de grupos temáticos modificados durante tres a cuatro días con partes interesadas, como las instituciones académicas, la justicia penal, las fuerzas del orden, encargados de las tecnologías de la información y representantes de entidades de los sectores público y privado, propietarios de infraestructuras críticas, responsables de la formulación de políticas, funcionarios encargados de las tecnologías de la información del Gobierno y del sector privado (incluidas las instituciones financieras), las empresas de telecomunicaciones, el sector bancario, así como la sociedad civil y asociados internacionales. 3) En un informe del MMC detallado se describe el contexto nacional de la ciberseguridad, se resumen las conclusiones relativas a cada factor y aspecto del MMC, se exponen los grados de madurez de las capacidades de ciberseguridad y se proporcionan recomendaciones que permiten al país mejorar sus capacidades de ciberseguridad. El informe es revisado por homólogos de la Junta Técnica del GCSCC y presentado al Gobierno para que formule observaciones al respecto. Sírvanse consultar más información en: https://gcscc.ox.ac.uk/cmm-review-process.

Método primario de recopilación de datos	• Grupos temáticos modificados (principal recopilación de datos primarios) • Cuestionarios y sondeos (estudios regionales de la OEA) • Entrevistas (opcionales para obtener pruebas adicionales)
¿Se realiza una recopilación secundaria de datos?	Sí (como parte de la investigación documentación antes/después de los grupos temáticos del MMC). • Información pública • Documentos no publicados • Documentos y registros • Cuestionarios y sondeos
Mecanismos adoptados para garantizar la exactitud de los datos recopilados	• Cada uno de los debates de los grupos modificados del MMC guarda relación con una o más dimensiones, que permite recabar pruebas respecto de cada dimensión al menos dos veces. Esto también permite la triangulación y recopilación de diferentes respuestas a la misma pregunta, procedentes de diferentes interesados. • Con el correspondiente consentimiento previo, las reuniones de los grupos temáticos modificados del MMC se graban y algunos encargados de la aplicación utilizan transcripciones anónimas de ellas para analizar las respuestas a las preguntas entre el conjunto de datos de la revisión. • La investigación documental confirma las pruebas de los grupos temáticos modificados del MMC. • El informe del MMC es revisado por homólogos de la Junta Técnica del GCSCC y presentado al Gobierno para que formule observaciones al respecto. • Algunos responsables de la aplicación utilizan la herramienta de codificación estructurada de campos (SFC), que les permite ingresar y codificar las respuestas de la investigación documental y los grupos temáticos del MMC, y validar así los indicadores en cada etapa del proceso de revisión. Los métodos están evolucionando a raíz de la introducción de la herramienta SFC, lo cual pone de manifiesto el esfuerzo constante por mejorar las metodologías de revisión del MMC.
Principales resultados de la evaluación	Un informe basado en pruebas que se presenta al Gobierno
Formato de presentación de los resultados de la evaluación	• Informe escrito que incluye recomendaciones (PDF) • Presentación del resumen al anfitrión (opcional) • Taller de validación con el anfitrión y las partes interesadas (opcional) • Herramienta de visualización (OEA: https://www.cybersecurityobservatory.org)
¿Se pueden publicar los resultados de la evaluación?	Sí. Queda a discreción del Gobierno compartir y/o publicar el informe o partes de él.
Si así fuera, indíquese el método de consulta de los informes anteriores.	Todas las revisiones del MMC, incluidos los enlaces hacia los informes publicados, pueden consultarse en los siguientes sitios web: • https://gcscc.ox.ac.uk/cmm-reviews • https://cybilportal.org/tools/portal-of-cybersecurity-capacity-maturity-model-cmm- review-reports/ (Si desea información sobre el estado del informe, consulte el Portal Cybil y busque "CMM+nombre del país")

Pruebas de impacto	En una evaluación independiente de un conjunto de aplicaciones del MMC en febrero de 2020 se determinó que: • La revisión del MMC mejoró la concienciación y la creación de capacidades en materia de ciberseguridad. • La revisión del MMC contribuyó a estrechar la colaboración con el Gobierno. • Los países indicaron que el MMC era fundamental para el desarrollo de sus estrategias y políticas (por ejemplo, Macedonia del Norte, Lituania y Georgia). • La revisión del MMC mejoró la credibilidad interna del programa de ciberseguridad en el seno de los Gobiernos. • La revisión del MMC ayudó a definir las funciones y responsabilidades en los Gobiernos. La revisión del MMC aumentó la financiación destinada a la creación de capacidades en materia de ciberseguridad. • La revisión del MMC ayudó a propiciar el establecimiento de contactos y la colaboración con empresas y la sociedad general. El MMC se ha realizado más de 120 veces, y se ha implementado en más de 85 países, conllevando la colaboración con Gobiernos nacionales de todas las regiones del mundo. Esto incluye: • Dos estudios regionales (2016 y 2020) realizados por la OEA. • Más de 25 revisiones realizadas en colaboración con el Banco Mundial y el Organismo de Internet y Seguridad de Corea (KISA) sobre sus Programas Mundiales de Capacidades en materia de Ciberseguridad fase I y fase II y como parte de las Revisiones Nacionales de las Capacidades de Ciberseguridad (MMC) para el Commonwealth y la cartera de programas de la Comunidad Económica de los Estados de África Occidental (CEDEAO). • La creación de equipos de respuesta a emergencias informáticas (CERT) y la realización de evaluaciones de capacidades en el Pacífico con la UIT, la APT, el APNIC y otros asociados. • La creación de capacidades en materia de ciberseguridad en la Commonwealth con la OTC. Los datos de las revisiones del MMC se utilizaron para los siguientes artículos académicos: • Creese, S., Shillair, R., Bada, M., Reisdorf, B. C., Roberts, T. y Dutton, W. H. (2019). "The Cybersecurity Capacity of Nations", págs. 165-179 en Graham, M. y Dutton, W. H. (ed.), *Society and the Internet: How Networks of Information and Communication are Changing our Lives*, 2ª edición. Oxford: Oxford University Press. • Dutton, W. H., Creese, S., Shillair, R. y Bada, M. (2019). "Cyber Security Capacity: Does It Matter?". *Journal of Information Policy*, 9: 280-306. doi:10.5325/jinfopoli.9.2019.0280 • Creese, S., Dutton, W. H., Esteve-González, P. y Shillair, R. (2021). "Cybersecurity Capacity Building: Cross-National Benefits and International Divides". Artículo que se presentará en la Conferencia de Investigaciones sobre Política de Comunicaciones, Información e Internet (TPRC), en Washington D.C., en febrero de 2021. Disponible en SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3658350

Beneficios de llevar a cabo una evaluación	El objetivo de una revisión del MMC es reunir datos sobre el panorama de la ciberseguridad de un país, y determinar cuál de los cinco grados de madurez en materia de ciberseguridad ha alcanzado el país en las dimensiones del MMC. Los datos se utilizan para elaborar un informe basado en pruebas que se presenta al Gobierno con recomendaciones para: • Medir la madurez de las capacidades de un país en materia de ciberseguridad; • Definir de manera detallada un conjunto de medidas pragmáticas para reducir y eliminar las deficiencias en materia de capacidades de ciberseguridad; • Identificar las prioridades respecto de la inversión y de la futura creación de capacidades; y • Elaborar proyectos empresariales para invertir y lograr las correspondientes mejoras esperadas de los resultados nacionales en materia de ciberseguridad.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	No
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	Sí. Se puntúa la madurez, pero no se establece ninguna clasificación. El MMC consta de cinco grados de madurez, que van de la inicial a la dinámica. El grado inicial implica un enfoque específico sobre la capacidad, mientras que el grado de madurez dinámica representa un enfoque estratégico y la capacidad de adaptarse a la evolución de los aspectos del entorno. El hecho de tener un determinado grado significa que el país tiene una madurez específica en lo que respecta a las capacidades de ciberseguridad. El MMC propone las pruebas que se necesitarían para determinar que se ha alcanzado un cierto grado de madurez para un factor/aspecto. Para alcanzar un grado de madurez en cualquier dimensión del MMC, todos los indicadores de un factor/aspecto de dicha dimensión deben haberse cumplido. Por consiguiente, el MMC indica directamente las áreas que deben seguir desarrollándose a fin de alcanzar el siguiente grado de madurez y los datos necesarios para demostrar dicho nivel de madurez de las capacidades.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	• ¿Cuáles son las capacidades actuales del país en materia de ciberseguridad? • ¿Cuáles son las deficiencias actuales del país en materia de ciberseguridad? • ¿En qué estado se encuentra la aplicación de estrategias y políticas? • ¿Qué actores participan y cuáles son sus funciones y responsabilidades? • ¿Qué medidas puede adoptar el país para ser más ciberseguro?
¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	Inicio/Inventario y análisis/Supervisión y evaluación

¿Cómo facilita la evaluación la adecuación con otras actividades?	Dado que los grupos temáticos modificados del MMC reúnen en un mismo lugar a un amplio conjunto de interesados a nivel nacional y a asociados internacionales (cuando es posible), las revisiones del MMC ofrecen excelentes oportunidades para ser coordinadas con otras actividades antes, después y paralelamente. El formato de los grupos temáticos modificados del MMC también permite reunir información durante la sesión para otras evaluaciones, si procede.
¿Qué función desempeña la evaluación en el proceso de adecuación con el GFCE?	Junto con las revisiones de las capacidades nacionales de respuesta a los incidentes y las evaluaciones de riesgos nacionales, las revisiones de las capacidades cibernéticas son la primera actividad enumerada por el GFCE para el proceso relativo a la estrategia nacional y forman parte de su fase inicial. Gracias a su enfoque multipartita, su exhaustividad y su transparencia, la revisión del MMC es ideal para reunir a los diversos interesados de un país, así como a los financiadores y responsables de la aplicación, y para proporcionar una base común a fin de planificar y llevar a cabo una actividad de creación de capacidades cibernéticas.
¿Hay estudios de casos o testimonios públicamente disponibles en relación con los beneficios de la herramienta?	Estudio de casos del MMC: Informes de Macedonia del Norte, Ghana, Samoa, Georgia e informes regionales de la OEA: https://gcscc.ox.ac.uk/case-studies. Estudio de caso de Senegal: Reunión anual del GFCE en Singapur, "National Strategies. Interviews Behind the Cover": https://thegfce.org/national-strategies-interviews-behind-the-cover. Banco Mundial: "Global Cybersecurity Capacity Programme. Lessons Learned and Recommendations Towards Strengthening the Programme": https://cybilportal.org/publications/global-cybersecurity-capacity-program-lessons- learned-and-recommendations-towards-strengthening-the-program/ "Cybersecurity in Pacific island nations" https://t.co/smxYhtrqBz?amp=1.
¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?	La mayoría de los responsables de la aplicación son instituciones de investigación y han recibido la aprobación ética de sus respectivas juntas de investigación a fin de recabar datos para esta evaluación. Cada informe del MMC es revisado por homólogos de la Junta Técnica del GCSCC, formada por académicos superiores y expertos en ciberseguridad.
Sírvanse añadir información adicional	Utilización de las revisiones del MMC en la creación de capacidades cibernéticas: https://gcscc.ox.ac.uk/our-approach. OAE y BID, 2020. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe, https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe. OAE y BID, 2016. *Ciberseguridad*: *¿Estamos preparados en América Latina y el Caribe?,* https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe. GFCE – Assess national cybersecurity capacity using a maturity model: https://thegfce.org/wp-content/uploads/2020/04/Assessnationalcybersecuritycapacityusingamaturitymodel.pdf.

	Iniciativa del GFCE: Evolución de la ciberseguridad en Senegal y África Occidental: https://cybilportal.org/projects/progressing-cybersecurity-in-senegal-and-west-africa-gfce-initiative/ Iniciativa del GFCE: Evaluación y desarrollo de capacidades en materia de ciberseguridad: https://cybilportal.org/projects/assessing-and-developing-cybersecurity-capability-gfce- initiative/.

Marco de Elaboración y Aplicación de la Estrategia Cibernética (EAEC)

MITRE Corporation

El *Marco de Elaboración y Aplicación de la Estrategia Cibernética* de MITRE consta de un modelo de cuatro etapas para 1) comprender el contexto nacional de riesgos/oportunidades cibernéticos; 2) evaluar la capacidad actual en ocho esferas de competencia clave y las bases estratégicas ("capacidad de crear capacidades"); 3) desarrollar y priorizar objetivos estratégicos e inversiones con base en las deficiencias de capacidad valoradas; y 4) elaborar hojas de ruta de la aplicación para la sostenibilidad a largo plazo.

Panorama general

Fecha de la última actualización de la herramienta	Septiembre de 2020
Denominación de la herramienta de evaluación	Marco de Elaboración y Aplicación de la Estrategia Cibernética (EAEC)
Nombre de la organización que mantiene la herramienta	MITRE Corporation
Responsables de llevar a cabo las evaluaciones	MITRE Corporation
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional	https://cybilportal.org/tools/national-cyber-strategy-development-implementation-framework/
Personas de contacto para examinar la posibilidad de organizar una evaluación	Gary Bundy: gbundy@mitre.org Cynthia Wright: cawright@mitre.org Johanna Vazzana: jvazzana@mitre.org
Cobertura geográfica	Regional, nacional u organizacional
Posibles usuarios de la herramienta	Cualquier persona
Temas o asuntos cubiertos	Las ocho áreas evaluadas son: 1) Derecho civil, reglamentación y rendición de cuentas; 2) Política y normas; 3) Dotación de recursos con base en el riesgo; 4) Operaciones resilientes;

	5) Respuesta a incidentes; 6) Prevención de la ciberdelincuencia y ejercicio de la acción penal; 7) Desarrollo de la fuerza de trabajo cibernética; y 8) Concienciación pública/cultura de la ciberseguridad. En cada una de estas esferas, se considera que la colaboración multipartita y las alianzas son facilitadores clave, y los enfoques de la aplicación para el desarrollo de la fuerza de trabajo en particular se centran en el establecimiento de alianzas efectivas entre los sectores público y privado. En las evaluaciones también se incluyen bases estratégicas, y el factor más importante de todos es el compromiso de los líderes y la participación de los interesados.
Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☐ Medidas de fomento de la confianza y normas ☐ Ciberdiplomacia ☐ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☐ Captura y análisis de incidentes ☐ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☒ Formación en materia de ciberdelincuencia ☒ Prevención de la ciberdelincuencia Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☒ Normas internacionales y/o nacionales
Tipos de indicadores	Los indicadores son principalmente cualitativos y se centran en los mecanismos de gobernanza, las políticas, los procesos y la dotación de recursos. Generalmente, no son específicamente técnicos por naturaleza (es decir, no se centran en arquitecturas de redes específicas o pruebas de sistema).
Número de indicadores y método de aplicación	Se utilizan más de 100 indicadores, agrupados en las esferas de competencia adecuadas.
Metodología - tipo de evaluación utilizada	Análisis basado en la investigación y sondeos/entrevistas de los interesados

Método primario de recopilación de datos	• Información pública • Entrevistas • Cuestionarios y sondeos • Documentos y registros
¿Se realiza una recopilación secundaria de datos?	Talleres de los interesados
Mecanismos adoptados para garantizar la exactitud de los datos recopilados	• Revisión de la calidad interna; • Se administran cuestionarios a un grupo de interesados lo más amplio posible para ampliar/validar la información; • Estudio calificado por máquinas
Principales resultados de la evaluación	Los resultados de una investigación de fuente abierta, un análisis de amenazas/oportunidades, una evaluación administrada y entrevistas de seguimiento se combinan para crear un "gráfico radial" intuitivo diseñado para facilitar la definición de objetivos e inversiones prioritarios con base en el riesgo en las ocho esferas de competencia, junto con un informe detallado con recomendaciones priorizadas.
Formato de presentación de los resultados de la evaluación	• Informe • Herramienta de visualización
¿Se pueden publicar los resultados de la evaluación?	Sí, con la aprobación de la entidad solicitante.
Método de consulta de los informes anteriores	Previa solicitud al Gobierno/organización evaluado.
Pruebas de impacto	En cada país con el que MITRE colabora asiduamente, el Gobierno y/o las organizaciones evaluados han realizado cambios en los objetivos estratégicos, las estructuras/mecanismos de gobernanza, los procesos de coordinación operacional, las comunicaciones y procesos de respuesta a incidentes, los enfoques sobre el desarrollo de la fuerza de trabajo y/o los temas del programa de concienciación pública que reflejan las prioridades identificadas a través de esta colaboración.
Beneficios de llevar a cabo una evaluación	Los países, organizaciones y/o entidades de asistencia evaluados logran una comprensión mejor de su contexto de riesgos/oportunidades estratégicos y de sus impulsores, necesidades y deficiencias en materia de capacidades de una forma que facilita un aspecto fundamental de la inversión en capacidades: la priorización. A través de talleres de seguimiento del desarrollo y la aplicación de estrategias, identifican las funciones y responsabilidades de los interesados clave; las mejores prácticas de gobernanza; las oportunidades de colaboración; los enfoques sobre la dotación de recursos; las deficiencias y ambigüedades legislativas y políticas; y los requisitos fundamentales (prerrequisitos), todo ello enmarcado en el contexto de su propio panorama de amenazas y de sus necesidades de desarrollo de capacidades.

	Además, dado que la evaluación se centra en un enfoque pangubernamental y panorganizacional, y que los talleres se realizan mediante herramientas participativas de pensamiento de diseño probadas, refuerza la participación de los interesados y su aceptación, que es fundamental para lograr una aplicación efectiva.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	Las áreas de competencia tienen el mismo "peso" en la evaluación. Sin embargo, algunas áreas de competencia serán más importantes que otras para determinados países/organizaciones evaluados, con base en su contexto estratégico, su capacidad actual y sus recursos humanos/financieros. Este enfoque está específicamente destinado a identificar las áreas que deberían recibir mayor "peso" para cada entidad evaluada con base en sus propias necesidades en materia de riesgos/oportunidades.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	El gráfico radial producido (una herramienta de resultados, además de un análisis detallado y un informe de recomendaciones) se basa en una escala de cuatro puntos. Sin embargo, no es un modelo de madurez: las deficiencias de capacidades se evalúan en el contexto de la situación final deseada del país/la organización y no en un conjunto objetivo de referencias. Este enfoque ayuda a garantizar que los países/las organizaciones no "persigan" medidas que sean menos importantes para su contexto estratégico de amenazas, y permite a los responsables de la aplicación adaptar las estrategias de inversión a las necesidades más importantes para los objetivos económicos y de seguridad.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	• ¿Cuál es nuestro panorama de ciberamenazas/oportunidades? • En vista de dicho panorama, ¿cuáles son nuestros objetivos respecto de la creación y mantenimiento de capacidades y servicios de TIC/cibernéticos/digitales? • ¿Quiénes son los interesados en este espacio y qué funciones tienen? • ¿Cuáles son nuestras deficiencias de capacidades en relación con nuestros objetivos estratégicos? • Entre esas deficiencias, ¿dónde deberíamos centrar nuestros esfuerzos de manera prioritaria? • ¿Qué objetivos podrían contribuir a alcanzar nuestros objetivos priorizados? • ¿Cómo podríamos elaborar iniciativas para alcanzarlos? • De las diversas iniciativas que podríamos emprender, ¿cuáles ofrecerán un mayor rendimiento de la inversión en términos de impacto y viabilidad? • ¿Qué recursos se pueden aplicar? • ¿Quiénes podrían ser nuestros asociados para emprender las iniciativas seleccionadas? • ¿Cómo desarrollamos y ejecutamos una hoja de ruta de aplicación? • ¿Cómo podemos mejorar la aceptación de los interesados y el apoyo público?

¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	Inicial/Inventario y análisis/Elaboración de la estrategia/Aplicación
¿Cómo facilita la evaluación la adecuación con otras actividades?	Al ofrecer una perspectiva pangubernamental/organizacional definida en un determinado panorama de amenazas/oportunidades, este enfoque proporciona un marco común para que las partes interesadas identifiquen, prioricen, asignen recursos y persigan objetivos comunes. Al diferenciar las deficiencias de capacidades por áreas de competencia clave, ayuda a las entidades a seguir centrándose en las áreas que sean más importantes para ellas y a su vez sigue proporcionando visibilidad sobre otras áreas en las que pueden surgir oportunidades de creación de capacidades, como los recursos de los programas de asistencia que pueden aumentar las capacidades sin desviar los escasos recursos internos. Por último, como se define en un marco multipartita, facilita el enfoque en las comunicaciones, la compartición de información y procesos transparentes que garantizan que los interesados y asociados conozcan (y acepten) las prioridades principales y las actividades en curso.
¿Qué función desempeña la evaluación en el proceso de adecuación con el GFCE?	Aclara las esferas de necesidad priorizadas, los contactos de las partes interesadas adecuadas, otros programas en curso/disponibles y los recursos humanos/financieros de que se dispone.
¿De qué estudios de caso o testimonios se dispone en relación con los beneficios de la herramienta?	Todas las evaluaciones de países/organizaciones que se han realizado hasta ahora se han hecho por iniciativa de ellos o a instancias del Departamento de Estado de los Estados Unidos. No se ha publicado ninguna, aunque los gobiernos de Botswana, Ghana, Ucrania y Ecuador han expresado públicamente su apreciación en discursos públicos, comunicados en los medios sociales y/o cumbres entre Gobiernos. El principal testimonio tal vez sea el hecho de que las agencias federales de los Estados Unidos y los países asociados siguen solicitando, confiando y aplicando nuestras recomendaciones de asistencia, y de que el número de países con los que colaboramos directamente ha pasado de 3 a más de 24 durante los cuatro años en que llevamos utilizando este marco; y cada país solicita activamente nuestro continuo asesoramiento y asistencia. A nivel regional, el número de países con los que colaboramos es de más de 90 y sigue creciendo, y en el marco de cada colaboración se reciben peticiones de asistencia específica.
¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?	MITRE es una organización de I+D financiada con fondos federales, que tiene estrictos requisitos internos en materia de control de calidad y una carta pública por la que se compromete expresamente a ofrecer un servicio imparcial, sin conflictos de intereses, en apoyo del interés público.

Sírvanse añadir información adicional	Este marco se elaboró bajo el patrocinio de la Oficina del Coordinador de las Cuestiones Cibernéticas del Departamento de Estado de los Estados Unidos, y se ha perfeccionado mediante acuerdos bilaterales y regionales dirigidos por el Departamento de Estado. La utilización de esta evaluación fuera del marco de los acuerdos dirigidos por el Departamento de Estado de los Estados Unidos no implica necesariamente el apoyo del Gobierno de los Estados Unidos ni la adecuación con sus políticas; no obstante, los valores de los Estados Unidos, como la libertad de información, el compromiso con una Internet libre y abierta, el Estado de Derecho y los derechos humanos están implícitos en nuestro modelo y nuestras recomendaciones.

Índice de Ciberseguridad Global (ICG)

Unión Internacional de Telecomunicaciones (UIT)

El *Índice de Ciberseguridad Global* (ICG) ayuda a los países a identificar áreas de mejora en el ámbito de la ciberseguridad, y los motiva a adoptar medidas para mejorar su clasificación, aumentando con ello el nivel general de la ciberseguridad en todo el mundo. El alcance y el marco del ICG se establecen en la Resolución 130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios de la UIT, sobre el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las TIC. El Cuestionario del ICG, del que se derivan los indicadores, subindicadores y microindicadores, se crea y aprueba mediante una consulta realizada en el marco de la Cuestión 3/2 ("Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad") encomendada a la Comisión de Estudio 2 del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D). El sondeo se lleva a cabo mediante una plataforma en línea a través de la cual se recaban pruebas.

El cuestionario de la cuarta versión del ICG (2019-2020) mide 20 indicadores generales mediante 82 preguntas. Los 20 indicadores reflejan los cinco pilares de la Agenda sobre Ciberseguridad Global de la UIT (ACG): *jurídico, técnico, organizacional, capacitación y cooperación.* El cuestionario de la v4ICG y la documentación pertinente relacionada con el ICG fueron presentados por la Oficina de Desarrollo de las Telecomunicaciones de la UIT (BDT) a la Comisión de Estudio 2 del UIT-D en octubre de 2019, antes del inicio del sondeo. En marzo de 2020, la BDT comunicó a la Comisión de Estudio 2 el estado de las respuestas al cuestionario; informó a los miembros sobre las siguientes etapas del proceso de análisis de datos; y señaló que el desarrollo de la ponderación se completaría contratando a un grupo de expertos formado a través de un proceso de consulta abierta con los Estados Miembros de la UIT, los Miembros de Sector y los socios de la BDT. En octubre de 2020, el Grupo de Expertos en Ponderación presentó recomendaciones sobre la ponderación para los indicadores, subindicadores y microindicadores de la v4ICG, y propuso cambios en el cuestionario del ICG para las versiones futuras. La verificación de las respuestas al cuestionario está en curso, para su última validación por los países que lo presentaron. Se ha previsto que el informe final se publique en 2021.

Panorama general

Fecha de la última actualización de la herramienta	La última actualización de la publicación se realizó en marzo de 2019. Estamos recopilando datos y ultimando la verificación de los datos presentados para el informe de la v4ICG.
Denominación de la herramienta de evaluación	Índice de Ciberseguridad Global (ICG)
Nombre de la organización que mantiene la herramienta	Unión Internacional de Telecomunicaciones (UIT)
Responsables de llevar a cabo las evaluaciones	Unión Internacional de Telecomunicaciones (UIT)
Persona(s) de contacto para examinar la posibilidad de organizar una evaluación	• Página web de la UIT: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx • Portal Cybil: https://cybilportal.org/projects/itu-global-cybersecurity-index-gci- programme/

Persona(s) de contacto para examinar la posibilidad de organizar una evaluación	Equipo del ICG gci@itu.int
Cobertura geográfica	Mundial
Posibles usuarios de la herramienta	• Estados Miembros: ministerios/organismos • Organismos de ciberseguridad/responsables de la formulación de políticas • Instituciones académicas • Expertos en ciberseguridad • Todas las personas interesadas Podría exigirse la condición de miembro de la UIT a las instituciones académicas y las organizaciones que quieran colaborar en el ICG.
Temas o asuntos cubiertos	Los temas del ICG incluyen: **Medidas jurídicas:** • Derecho sustantivo en materia de ciberdelincuencia • Reglamentación en materia de ciberseguridad **Medidas técnicas:** • Equipos nacionales/gubernamentales de intervención en caso de incidente (CERT/CIRT/CSRIT) • CERT/CIRT/CSRIT de sector • Marco nacional de aplicación de normas en materia de ciberseguridad • Protección de la Infancia en Línea (PIeL) **Medidas organizacionales:** • Estrategias nacionales en materia de ciberseguridad • Organismos responsables/nacionales • Medidas de la ciberseguridad **Medidas de creación de capacidad:** • Campañas de concienciación pública • Formación de profesionales sobre la ciberseguridad • Programas educativos y programas de estudios nacionales • Programas de investigación y desarrollo sobre la ciberseguridad • Industria nacional de la ciberseguridad • Incentivos del Gobierno para apoyar el desarrollo de la ciberseguridad **Medidas de cooperación:** • Acuerdos bilaterales • Participación en mecanismos internacionales (foros) • Acuerdos multilaterales • Alianzas entre el sector público y privado • Alianzas interinstitucionales. Se puede consultar una descripción completa de cada medida en los informes publicados en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

<table>
<tr><td>Temas o asuntos del GFCE cubiertos</td><td>Política y estrategia
☒ Estrategias
☒ Evaluaciones
☒ Medidas de fomento de la confianza y normas
☒ Ciberdiplomacia
☒ Derecho internacional en el ciberespacio
Gestión de incidentes y protección de la infraestructura de información crítica
☒ Respuesta nacional a incidentes de seguridad informática
☒ Captura y análisis de incidentes
☒ Ejercicios en materia de seguridad cibernética
☒ Protección de la infraestructura de información esencial
Ciberdelincuencia
☒ Marcos jurídicos/legislación en materia de ciberdelincuencia
☒ Aplicación de la ley en el ciberespacio
☒ Formación en materia de ciberdelincuencia
☒ Prevención de la ciberdelincuencia
Cultura y destrezas
☒ Creación de conciencia en materia de ciberseguridad
☒ Capacitación y formación
☒ Desarrollo de la fuerza de trabajo
Normas
☒ Normas internacionales y/o nacionales</td></tr>
<tr><td>Tipos de indicadores</td><td>La recopilación de datos del ICG es cualitativa y se utiliza un sistema binario para evaluar la existencia o ausencia de una determinada actividad, departamento o medida.</td></tr>
<tr><td>Número de indicadores y método de aplicación</td><td>El ICG no aplica un conjunto predefinido de indicadores. En cada versión, se modifica y revisa el cuestionario teniendo en cuenta los comentarios recibidos de los coordinadores de los países y los miembros. Por consiguiente, el número de indicadores puede aumentar o disminuir y no hay un número definido de indicadores para cada tema. Por ejemplo, véase el cuadro indicado a continuación en que se expone el número de indicadores de cada versión hasta la fecha.
<table>
<tr><th>v1ICG</th><th>v2ICG</th><th>v3ICG</th><th>v4ICG</th></tr>
<tr><td>17 indicadores con 17 preguntas principales</td><td>25 indicadores con 157 preguntas</td><td>25 indicadores con 50 preguntas principales</td><td>20 indicadores con 82 preguntas principales</td></tr>
</table></td></tr>
<tr><td>Metodología – tipo de evaluación utilizada</td><td>EL ICG utiliza métodos de evaluación tanto primarios como secundarios. El equipo del ICG recopila datos para los países que no participan y les comunica sus conclusiones para su aprobación; también verifica y valida las respuestas presentadas por los coordinadores de los Estados Miembros de la UIT.</td></tr>
</table>

Método primario de recopilación de datos	• Información pública • Documentos no publicados • Cuestionarios y sondeos • Documentos y registros
¿Se realiza una recopilación secundaria de datos?	Sí. La recopilación secundaria de datos se realiza para los países que responden al cuestionario del ICG mediante las siguientes etapas: • La UIT lleva a cabo la verificación, identificando las respuestas que faltan, los documentos y enlaces de apoyo, utilizando la información de fuente abierta, documentos, cuestionarios y sondeos no publicados y documentos y registros públicamente disponibles. • Las respuestas verificadas se vuelven a enviar al coordinador del país, que mejora la exactitud de las respuestas cuando es necesario. • La UIT valida las enmiendas finales del coordinador del país y vuelve a enviar a este el documento para su aprobación final. • Las respuestas validadas al cuestionario se utilizan ulteriormente con fines de análisis, puntuación y clasificación.
Mecanismos adoptados para garantizar la exactitud de los datos recopilados	Los coordinadores del ICG nombrados por los ministerios suelen tener experiencia/conocimientos técnicos en ciberseguridad y ocupan cargos relacionados con esta materia en los diferentes ministerios. Además, los enlaces y documentos pertinentes solicitados y validados proceden de los sitios web públicos y oficiales de los gobiernos, y a veces se proporcionan documentos oficiales confidenciales. Recurrimos a validadores con experiencia procedentes de ámbitos relacionados con la ciberseguridad, que se necesitan para llevar a cabo el proceso de verificación más de una vez para cada país y compartir información con los países hasta que se obtiene la confirmación final para garantizar la exactitud de los datos.
Principales resultados de la evaluación	En cada versión, se publica el informe final y las conclusiones.
Formato de presentación de los resultados de la evaluación	Informe
¿Se pueden publicar los resultados de la evaluación?	Sí. Los resultados se pueden publicar. El ICG constituye un documento público para crear conciencia a nivel mundial. Se pueden consultar todos los informes anteriores en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
Método de consulta de los informes anteriores	Los informes anteriores se pueden consultar y descargar desde: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
Pruebas de impacto	La creciente participación de los Estados Miembros en el ICG demuestra su continuo y creciente interés en el índice: **V1ICG (2015)** 105 países **v2ICG (2017)** 134 países **v3ICG (2018)** 155 países **v4ICG (2019-2020)** Actualmente 163 países Muchos países piden a la UIT que los ayude en el desarrollo de su postura en materia de ciberseguridad, como por ejemplo, entre otras cosas, para elaborar y mejorar estrategias nacionales, establecer equipos de respuesta a emergencias

	informáticas (CERT) e iniciar actividades de creación de capacidad. Los países de baja y media puntuación (con base en los rangos de puntuaciones mantenidos constantemente a lo largo del tiempo) han podido recibir intervenciones específicas, lo cual ha conllevado una reducción constante del número de dichos países.
Beneficios de llevar a cabo una evaluación	Las evaluaciones ayudan a identificar deficiencias en el desarrollo de la ciberseguridad de las naciones y regiones, así como a crear conciencia sobre la ciberseguridad en todo el mundo. La evaluación también ayuda a identificar a los países que más necesitan ayuda para mejorar su postura de ciberseguridad. A través de los datos recabados, el ICG destaca las prácticas que los Estados Miembros pueden implementar y que son adecuadas para su entorno nacional, promueve las buenas prácticas y fomenta una cultura mundial de la ciberseguridad.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	Sí. La ponderación de los indicadores en el ICG es objeto de una evaluación de los miembros del Grupo de Expertos del ICG basada en la importancia de dichos indicadores en los cinco pilares de la Agenda sobre Ciberseguridad Global, la pertinencia para los principales objetivos del ICG y el marco conceptual, y la disponibilidad y calidad de los datos. El Grupo de Expertos proporciona recomendaciones sin sesgos sobre la ponderación después de la reunión del Grupo de Expertos en Ponderación celebrada para cada versión del ICG.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	Sí. Se calcula la media de las ponderaciones dadas por cada experto para cada indicador a fin de conseguir la ponderación final de cada indicador. A través de la aplicación de una función, un país que haya respondido SÍ y haya aportado pruebas recibirá una puntuación total para el indicador, mientras que un país que no haya aportado pruebas o haya respondido NO recibirá una puntuación de cero para dicho indicador. Las puntuaciones globales se normalizan y clasifican.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	• ¿Cuáles son las tendencias y modelos globales actuales en materia de política de ciberseguridad? • ¿Cómo pueden los Estados Miembros identificar sus puntos fuertes y débiles en las medidas de ciberseguridad? • ¿Qué nivel de compromiso en materia de ciberseguridad tienen los países y qué países ofrecen las mejores prácticas en dicha materia?
¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	Inicio, inventario y análisis, elaboración de la estrategia, implementación, supervisión y evaluación.

<table>
<tr>
<td>¿Cómo facilita la evaluación la adecuación con otras actividades?</td>
<td>La evaluación del ICG ayuda a identificar esferas relativamente fuertes y débiles respecto de los compromisos de los Estados Miembros en materia de ciberseguridad, informando sobre los puntos en que los Estados Miembros tal vez necesiten ayuda adicional para crear capacidades o aquellos en que tal vez puedan brindar apoyo a los demás. Por ejemplo, mediante la evaluación del ICG, la UIT puede detectar las necesidades de educación en materia de ciberseguridad de los sistemas educativos de los miembros
<table>
<tr><th>Año</th><th>Alto</th><th>Medio</th><th>Bajo</th></tr>
<tr><td>2018-2019</td><td>54</td><td>53</td><td>87</td></tr>
<tr><td>2016-2017</td><td>30</td><td>60</td><td>104</td></tr>
<tr><td>2014-2015</td><td>19</td><td>52</td><td>122</td></tr>
</table>
</td>
</tr>
<tr>
<td>¿De qué estudios de caso o testimonios se dispone en relación con los beneficios de la herramienta?</td>
<td>Cada año, muchos países solicitan asistencia para crear equipos de respuesta a emergencias informáticas y estrategias nacionales en materia de ciberseguridad a raíz de la evaluación, las puntuaciones y la clasificación obtenida en el marco del ICG.
Por ejemplo:
Benin creó una estrategia de ciberseguridad, a raíz de la toma de conciencia resultante del ICG: https://news.itu.int/benin-launches-a-new-national-cybersecurity-strategy/.
La República del Congo aprobó la Ley de Ciberseguridad, una ley sobre la ciberdelincuencia: https://postetelecom.gouv.cg/le-senat-adopte-a-lunanimite-la-creation-de-lagence-nationale-de-securite-des-systemes-dinformation/.
En 2018, como se indicó en las evaluaciones del ICG, se observaron avances en los compromisos en materia de ciberseguridad en:
• Benin, Egipto, Estonia, Eswatini, Polonia, Sudáfrica, Zambia y Zimbabwe, en la instauración de leyes sobre ciberdelincuencia;
• Uganda, en la redacción de su legislación sobre la protección de los datos/la privacidad;
• Australia, Botswana, Canadá, Dinamarca, España, Japón, Jordania, Luxemburgo República Checa, Países Bajos, Samoa y Singapur, en la actualización de sus respectivas estrategias nacionales en materia de ciberseguridad; y
• Camerún, Malawi, Tanzania y Zimbabwe, en la redacción sus respectivas estrategias nacionales en materia de ciberseguridad.
Artículos de prensa sobre el ICG: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global- cybersecurity-index.aspx.</td>
</tr>
<tr>
<td>¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?</td>
<td>• Los datos presentados a efectos del ICG son validados de manera independiente por nuestro equipo.
• Un grupo de expertos independientes indica las ponderaciones de los indicadores del modelo y ningún experto puede cambiar por sí solo las ponderaciones de manera considerable.</td>
</tr>
</table>

Marco de Evaluación de las Capacidades Nacionales (MECN)

Agencia de la Unión Europea para la Ciberseguridad (ENISA)

El objetivo principal del *Marco de Evaluación de las Capacidades Nacionales* (MECN) era crear una herramienta de autoevaluación para ayudar a los Estados Miembros de la UE a medir el nivel de madurez de sus capacidades de ciberseguridad. Para conseguir este objetivo, la ENISA utilizó los objetivos estratégicos de las estrategias nacionales de ciberseguridad (ENC) de los Estados Miembros como punto de partida. Como las capacidades de ciberseguridad son los principales instrumentos utilizados por los países para alcanzar los objetivos de sus ENC, el MECN abarca preguntas sobre los grados de madurez, teniendo en cuenta 17 objetivos estratégicos incluidos en la mayoría de las ENC europeas. El marco proporciona una visión representativa sencilla de la madurez de cada Estado Miembro en materia de ciberseguridad, en tres niveles diferentes: nivel objetivo, nivel de grupo y nivel global.

Panorama general

Fecha de la última actualización de la herramienta	2 de diciembre de 2020
Denominación de la herramienta de evaluación	Marco de Evaluación de las Capacidades Nacionales (MECN)
Nombre de la organización que mantiene la herramienta	Agencia de la Unión Europea para la Ciberseguridad (ENISA)
Responsables de llevar a cabo las evaluaciones	Estados Miembros de la UE
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional	https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework El MECN se convertirá en una herramienta en línea en 2021.
Persona(s) de contacto para examinar la posibilidad de organizar una evaluación	Agencia de la Unión Europea para la Ciberseguridad (ENISA)
Cobertura geográfica	Unión Europea/mundial
Posibles usuarios de la herramienta	Los destinatarios del MECN son los responsables de la formulación de políticas, expertos y funcionarios del Gobierno encargados o implicados en el diseño, la implementación y la evaluación de las ENC y, de manera más general, las capacidades de ciberseguridad. Además, las conclusiones formalizadas en el documento publicado pueden ser útiles para los expertos e investigadores en materia de políticas de ciberseguridad a nivel nacional o europeo.

Temas o asuntos cubiertos	El modelo conceptual del marco de autoevaluación abarca 17 objetivos estratégicos derivados de las ENC de los Estados Miembros de la UE y se estructura en torno a cuatro grupos principales. Cada uno de estos grupos cubre un ámbito temático clave para crear capacidades en materia de ciberseguridad e incluye diferentes objetivos. A continuación, cada objetivo se evalúa mediante preguntas sobre diferentes niveles de madurez. Los grupos abarcan los siguientes temas: **I) Gobernanza y normas en materia de ciberseguridad** 1) Elaborar un plan nacional de contingencia cibernética 2) Establecer medidas de seguridad básicas 3) Asegurar la identidad digital y crear confianza en los servicios digitales públicos Este grupo aborda aspectos de la planificación para preparar al Estado Miembro frente a los ciberataques así como normas para proteger a los Estados Miembros y la identidad digital. **II) Creación de capacidad y concienciación** 4) Organizar ejercicios sobre la ciberseguridad 5) Establecer una capacidad de respuesta a los incidentes 6) Sensibilizar a los usuarios 7) Reforzar los programas de formación y educativos 8) Fomentar la I+D 9) Ofrecer incentivos para que el sector privado invierta en medidas de seguridad 10) Mejorar la ciberseguridad de la cadena de suministro Este grupo evalúa la capacidad de los Estados Miembros de crear conciencia sobre los riesgos y amenazas relativas a la ciberseguridad y la manera de afrontarlos. Además, esta dimensión mide la capacidad del país de crear continuamente capacidades de ciberseguridad y mejorar los conocimientos y las destrezas en el ámbito de la ciberseguridad. **III) Aspectos legales y normativos** 11) Proteger las infraestructuras de información críticas, los operadores de servicios esenciales y los proveedores de servicios digitales. 12) Hacer frente a la ciberdelincuencia 13) Establecer mecanismos de denuncia de incidentes 14) Reforzar la protección de la privacidad y los datos Este grupo mide la capacidad de los Estados Miembros de instaurar los instrumentos jurídicos y normativos necesarios para hacer frente a la ciberdelincuencia y cumplir determinados requisitos legales como la denuncia de incidentes, las cuestiones de privacidad y la protección de las infraestructuras de información esenciales. **IV) Cooperación** 15) Establecer alianzas entre el sector público y privado 16) Institucionalizar la cooperación entre los organismos públicos 17) Participar en la cooperación internacional Este grupo evalúa la cooperación y la compartición de información entre diferentes grupos de interesados a nivel nacional e internacional.

Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☒ Medidas de fomento de la confianza y normas ☒ Ciberdiplomacia ☐ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☒ Captura y análisis de incidentes ☒ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☒ Formación en materia de ciberdelincuencia ☒ Prevención de la ciberdelincuencia Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☒ Normas internacionales y/o nacionales
Tipos de indicadores	El marco incluye indicadores cualitativos que se basan en dos niveles: el nivel estratégico y el nivel operacional. Para cada objetivo incluido en el marco de autoevaluación, hay una serie de indicadores distribuidos entre los cinco grados de madurez. Cada indicador se basa en una pregunta dicotómica (sí/no). El indicador puede ser un requisito o un no requisito.
Número de indicadores y método de aplicación	El modelo proporciona una puntuación basada en el valor de dos parámetros: el ***grado de madurez*** y la **tasa de cobertura**. Cada uno de estos parámetros se puede calcular en diferentes niveles: i) por objetivo, ii) por grupo de objetivos o iii) general. Además, a fin de adaptarse a las especificidades de los Estados Miembros de la UE y permitir a la vez una visión coherente, la puntuación se calcula a partir de dos muestras diferentes a nivel del grupo y a nivel general: • **Puntuaciones generales**: una muestra completa que cubre todos los objetivos incluidos en el grupo o en el marco general (de 1 a 17). • **Puntuaciones específicas**: una muestra específica que cubre solo los objetivos seleccionados por el Estado Miembro (suele corresponder a los objetivos presentes en la ENC del país específico) en el grupo o en el marco general.

	Para cada grupo, un cuadro presenta el conjunto completo de indicadores mediante preguntas que representan un determinado grado de madurez. El cuestionario es el principal instrumento de la autoevaluación. Para cada objetivo, deben señalarse dos conjuntos de indicadores: • Un conjunto de preguntas estratégicas relativas a la madurez (9 preguntas generales) marcadas de "a" a "c" para cada grado de madurez, que se repiten para cada objetivo; y • Un conjunto de preguntas relativas a las capacidades de ciberseguridad (319 preguntas sobre las capacidades de ciberseguridad), enumeradas del "1" al "10" para cada grado de madurez, que son específicas de la esfera cubierta por el objetivo.
Metodología – tipo de evaluación utilizada	**Grados de madurez:** escala de madurez de cinco niveles **Atributos:** basados en cuatro dimensiones/grupos que abarcan esferas para crear capacidades en materia de ciberseguridad **Método de evaluación**: autoevaluación **Muestra de resultados**: presentación de los resultados con diferentes niveles de detalle.
Método primario de recopilación de datos	• Anticipar actividades de coordinación para recabar los datos y consolidarlos; • Determinar el organismo central encargado de llevar a cabo la autoevaluación a nivel nacional; • Utilizar el ejercicio de evaluación como una vía para compartir información y comunicar sobre temas relacionados con la ciberseguridad; • Utilizar las ENC como ámbito para seleccionar los objetivos sometidos a la evaluación. Cuando el alcance de la ENC evolucione, asegurarse de que la interpretación de la puntuación sigue siendo coherente con la evolución de la ENC. El ciclo de vida de la ENC es un proceso que dura varios años.
¿Se realiza una recopilación secundaria de datos?	Cuando se cumplimente el cuestionario de autoevaluación, téngase presente que el objetivo principal es apoyar a los Estados Miembros a crear capacidades en materia de ciberseguridad.
Mecanismos adoptados para garantizar la exactitud de los datos recopilados	El Estado Miembro de la UE/país que lleve a cabo la evaluación debe garantizar la exactitud de la información para aprovechar los resultados del marco.
Principales resultados de la evaluación	Los resultados de la evaluación se proporcionan en tres niveles diferentes: nivel objetivo, nivel de grupo y nivel global. El país se evalúa y recibe un resultado final general que tiene en cuenta todos los objetivos de cada grupo, y un resultado final específico que tiene en cuenta solo los objetivos seleccionados que el país desea evaluar. Además, el MECN también proporciona una tasa de cobertura. La tasa de cobertura se calcula como la proporción entre el **número total de preguntas** en el objetivo y el **número de preguntas que han recibido una respuesta afirmativa.** La tasa de cobertura se expresa mediante un porcentaje.

Formato de presentación de los resultados de la evaluación	Informe. Visualización a partir de la herramienta en línea (futura labor de la ENISA)
¿Se pueden publicar los resultados de la evaluación?	Los resultados de la evaluación se publican exclusivamente si el Estado Miembro así lo decide por iniciativa propia.
Método de consulta de los informes anteriores	El Estado Miembro puede hacer un seguimiento de su avance a lo largo del tiempo con base en las nuevas evaluaciones.
Pruebas de impacto	En total, unos 20 Estados Miembros participaron en la elaboración del marco y casi todos los Estados Miembros participaron en el taller de validación en que el marco se presentó y fue objeto de un extenso debate. Más concretamente, el marco debería capacitar a los Estados Miembros para: • Llevar a cabo una evaluación de sus capacidades nacionales en materia de ciberseguridad; • Mejorar el conocimiento sobre el grado de madurez del país; • Determinar las áreas de mejora; y • Crear capacidades en materia de ciberseguridad.
Beneficios de llevar a cabo una evaluación	El MECN es una herramienta que puede ayudar a los países a: • Proporcionar información útil para desarrollar una estrategia a largo plazo (por ejemplo, buenas prácticas, directrices); • Identificar elementos que falten en las ENC; • Seguir creando capacidades en materia de ciberseguridad; • Apoyar la rendición de cuentas de las acciones políticas; • Ganar credibilidad frente al público general y los asociados internacionales; • Apoyar las actividades de divulgación y mejorar la imagen pública como organización transparente; • Anticipar los problemas que se tengan que afrontar; • Identificar las lecciones aprendidas y las mejores prácticas; • Proporcionar una base de referencia sobre las capacidades de ciberseguridad en la UE a fin de facilitar los debates; y • Evaluar las capacidades nacionales respecto de la ciberseguridad.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	El Estado Miembro de la UE puede mostrar los resultados de la evaluación presentando el grado de madurez de las capacidades de ciberseguridad del país, respecto de un grupo de objetivos o un único objetivo. Todos los objetivos evaluados son igualmente pertinentes en el marco de evaluación, por lo que tienen la misma importancia. Esto mismo se aplica a los indicadores utilizados en el marco.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	El objetivo del MECN es medir las capacidades de ciberseguridad de los Estados Miembros respecto de los 17 objetivos. No obstante, el Estado Miembro puede elegir los objetivos que desea evaluar y evaluar únicamente un subconjunto de los 17 objetivos.

Índice Nacional de Ciberseguridad (INC)

e-Governance Academy (eGA)

El *Índice Nacional de Ciberseguridad* (INC) es un índice mundial que mide la preparación de los países para prevenir las ciberamenazas y gestionar los incidentes cibernéticos. El INC también es una base de datos con elementos de prueba públicamente disponibles y una herramienta para la creación de capacidades nacionales en materia de ciberseguridad.

El INC se centra en aspectos mensurables de la ciberseguridad implementados por el gobierno central, a saber:

1) **La legislación en vigor** – Las leyes, reglamentos, órdenes, etc.
2) **Las unidades establecidas** – Las organizaciones existentes, departamentos, etc.
3) **Los formatos de cooperación** – Los comités, grupos de trabajo, etc.
4) **Los resultados** – Las políticas, los ejercicios, las tecnologías, los sitios web, los programas, etc.

Desde 2016, 160 países han sido evaluados utilizando el INC. La recopilación de datos, revisión y publicación es un proceso continuo del INC. El INC no publica versiones anuales. Cuando se proporcionan nuevas pruebas, se evalúan y, si están fundamentadas, se aplicarán inmediatamente los cambios necesarios en la lista de clasificación. La metodología del INC se desarrolló en 2016 y actualizó en 2018. Actualmente, la metodología se está revisando y la nueva versión se publicará a más tardar en 2022.

Panorama general

Fecha de la última actualización de la herramienta	Las entradas correspondientes a los países en el INC se actualizan continuamente, lo cual significa que el propio INC está en constante actualización.
Denominación de la herramienta de evaluación	Índice Nacional de Ciberseguridad (INC)
Nombre de la organización que mantiene la herramienta	e-Governance Academy
Responsables de llevar a cabo las evaluaciones	• e-Governance Academy • Entidades e instituciones relacionadas con la ciberseguridad de los países clasificados
Sírvanse indicar los enlaces hacia la herramienta y toda información adicional	Portal Cybil: https://cybilportal.org/projects/national-cybersecurity-index/
Personas de contacto para examinar la posibilidad de organizar una evaluación	Sra. Epp Maaten: epp.maaten@ega.ee Sr. Radu Serrano: radu.serrano@ega.ee Sra. Merle Maigre: merle.maigre@ega.ee Equipo del INC: ncsi@ega.ee
Cobertura geográfica	Mundial

Posibles usuarios de la herramienta	• Ministerios/organismos del país • Organismos/responsables de formular políticas en materia de ciberseguridad • Instituciones académicas • Expertos en ciberseguridad • Todas las personas interesadas Para colaborar en la recopilación de datos del país para el INC, solo necesita ponerse en contacto con el equipo del INC.
Temas o asuntos cubiertos	**1 Desarrollo de políticas en materia de ciberseguridad**: 1.1 Unidad de las políticas de ciberseguridad 1.2 Formato de coordinación de las políticas de ciberseguridad 1.3 Estrategia de ciberseguridad 1.4 Plan de aplicación de la estrategia de ciberseguridad **2 Análisis e información sobre ciberamenazas:** 2.1 Unidad de análisis de ciberamenazas 2.2 Los informes públicos de ciberamenazas se publican anualmente 2.3 Sitio web de la seguridad cibernética **3 Desarrollo educativo y profesional:** 3.1 Competencias en materia de ciberseguridad en la enseñanza primaria o secundaria 3.2 Programa de ciberseguridad en Grado 3.3 Programa de ciberseguridad en Máster 3.4 Programa de ciberseguridad en Doctorado 3.5 Asociación profesional sobre ciberseguridad **4 Contribución a la ciberseguridad mundial:** 4.1 Convenio sobre la Ciberdelincuencia 4.2 Representación en formatos de cooperación internacional 4.3 Organización internacional sobre ciberseguridad en el país 4.4 Creación de capacidades de ciberseguridad para otros países **5 Protección de servicios digitales:** 5.1 Responsabilidad en materia de ciberseguridad de los proveedores de servicios digitales 5.2 Normas de ciberseguridad para el sector público 5.3 Autoridad de supervisión competente **6 Protección de servicios esenciales:** 6.1 Identificación de los operadores de servicios esenciales 6.2 Requisitos de ciberseguridad de los operadores de servicios esenciales 6.3 Autoridad de supervisión competente 6.4 Supervisión periódica de las medidas de seguridad **7 identificación por medios electrónicos y servicios de confianza:** 7.1 Identificador invariable exclusivo 7.2 Requisitos para los criptosistemas 7.3 Identificación electrónica 7.4 Firma electrónica

	7.5 Sello de tiempo 7.6 Servicio de entrega electrónica certificada 7-7 Autoridad de supervisión competente **8 Protección de los datos personales:** 8.1 Leyes de protección de datos personales 8.2 Autoridad encargada de la protección de datos personales **9 Respuesta a incidentes cibernéticos:** 9.1 Unidad de respuesta a incidentes cibernéticos 9.2 Responsabilidad de presentar informes 9.3 Único punto de contacto para la coordinación internacional **10 Gestión de crisis cibernéticas:** 10.1 Plan de gestión de crisis cibernéticas 10.2 Ejercicio de gestión de crisis cibernéticas a nivel nacional 10.3 Participación en ejercicios internacionales sobre las crisis cibernéticas 10.4 Apoyo operativo de voluntarios en las crisis cibernéticas **11 Lucha contra la ciberdelincuencia:** 11.1 Penalización de la ciberdelincuencia 11.2 Unidad de ciberdelincuencia 11.3 Unidad forense digital 11.4 Punto de contacto durante las 24 horas del día, los 7 días de la semana para la ciberdelincuencia internacional
	12 Operaciones cibernéticas militares 12.1 Unidad de operaciones cibernéticas 12.2 Ejercicio de operaciones cibernéticas 12.3 Participación en ejercicios cibernéticos internacionales
Temas o asuntos del GFCE cubiertos	Política y estrategia ☒ Estrategias ☒ Evaluaciones ☐ Medidas de fomento de la confianza y normas ☒ Ciberdiplomacia ☐ Derecho internacional en el ciberespacio Gestión de incidentes y protección de la infraestructura de información crítica ☒ Respuesta nacional a incidentes de seguridad informática ☒ Captura y análisis de incidentes ☒ Ejercicios en materia de seguridad cibernética ☒ Protección de la infraestructura de información esencial Ciberdelincuencia ☒ Marcos jurídicos/legislación en materia de ciberdelincuencia ☒ Aplicación de la ley en el ciberespacio ☐ Formación en materia de ciberdelincuencia ☒ Prevención de la ciberdelincuencia

	Cultura y destrezas ☒ Creación de conciencia en materia de ciberseguridad ☒ Capacitación y formación ☒ Desarrollo de la fuerza de trabajo Normas ☒ Normas internacionales y nacionales
Tipos de indicadores	La recopilación de datos para el INC es cualitativa, y se utiliza un sistema de valores para evaluar la existencia de una ley específica, una unidad especializada, un formato de cooperación oficial y/o los resultados.
Número de indicadores y método de aplicación	Hay en total 46 indicadores (presentados en forma de los temas y asuntos antes señalados). Los propios indicadores se distribuyen en 12 capacidades. Cada indicador tiene un valor, que muestra la importancia relativa del indicador en el índice, y un criterio, que explica el tipo de datos que se pueden presentar como prueba. Para recibir un valor positivo para cualquier criterio, se deben proporcionar pruebas como datos. Si los datos proporcionados cumplen todos los aspectos del criterio, se aceptarán como elementos probatorios suficientes.
Metodología – tipo de evaluación utilizada	Cada país se registra y actualiza en el INC de manera individual. Una vez que se ha registrado/actualizado un país, el INC lo mostrará en una clasificación comparativa mundial.
Método primario de recopilación de datos	• Información pública • Documentos y registros • Leyes y otros documentos oficiales • Sitios web oficiales
¿Se realiza una recopilación secundaria de datos?	Sí. El INC no es un índice estático, por lo que se siguen recopilando datos a lo largo de todo el año. • Información pública • Documentos y registros • Leyes y otros documentos oficiales • Sitios web oficiales
Mecanismos adoptados para garantizar la exactitud de los datos recopilados	Todos los elementos probatorios deben ser información pública y se debe poder acceder a ellos públicamente. Solo se pueden considerar pruebas los datos oficiales. Las pruebas/referencias aceptadas son: las leyes, los documentos oficiales y los sitios web oficiales. Cuando concluye la recopilación de datos, la información proporcionada es revisada por al menos dos expertos del INC. Después de la inspección, la información se publica en el sitio web del INC.
Principales resultados de la evaluación	• Información actualizada en la página del país (para los países que forman actualmente parte del INC) • Páginas de países (para los países que aún no se han incluido en el INC) • Clasificación del INC (se actualiza cada vez que se actualiza una página de país)

Formato de presentación de los resultados de la evaluación	• Sitio Web • Herramienta de visualización (con la posibilidad de comparar la información pasada o actual de un único país o de varios países a la vez) • Posibilidad de descargar la página de un país en formato PDF
¿Se pueden publicar los resultados de la evaluación?	Sí, siempre.
Método de consulta de los informes anteriores	Para toda página de país, el INC muestra la fecha en que se actualizó la información del país. Normalmente, la página del país presenta la información disponible más reciente. El visitante puede ver la información de una actualización anterior seleccionando una fecha de actualización específica a partir de un menú desplegable con el título "Elija una versión".
Pruebas de impacto	• La creciente participación de los países en el INC demuestra su continuo y creciente interés en el índice. Algunos países han solicitado evaluaciones individuales detalladas con base en el INC, a fin de determinar el estado actual de su ciberseguridad nacional y mejorarlo con base en ello. • La herramienta ha sido utilizada por investigadores académicos para trabajar en uno o varios estudios de casos.
Beneficios de llevar a cabo una evaluación	Los países pueden identificar su grado de preparación para prevenir las ciberamenazas. Al permitir comparar los países y desglosar las puntuaciones en indicadores, el INC brinda apoyo a un enfoque cooperativo transnacional sobre la ciberseguridad, en que se comparten las mejores prácticas entre diferentes países.
¿Se dispone de un proceso de cálculo del coeficiente de ponderación?	No.
¿Se adopta un mecanismo de puntuación y/o clasificación en su evaluación?	Sí, para los indicadores, para la puntuación del INC (país), para el nivel de desarrollo digital (NDD) y para la diferencia (entre la puntuación del INC y el NDD). • Cada indicador tiene un valor, que muestra la importancia relativa del indicador en el índice. Los valores son asignados por el grupo de expertos con base en los siguientes criterios: 1 punto – una ley que regula una esfera específica 2–3 puntos – una unidad especializada 2 puntos – un formato de cooperación oficial 1–3 puntos – un resultado/producto • La puntuación del INC muestra el porcentaje que el país recibió sobre el valor máximo de los indicadores. La puntuación máxima del INC siempre es 100 (100 %) con independencia de si se añaden o suprimen indicadores. • Además de la puntuación del INC, en el cuadro del índice también se muestra el nivel de desarrollo digital (NDD). El NDD se calcula con base en el índice de desarrollo de las TIC (IDT) y el índice de preparación de la red (IPR). El NDD es el porcentaje medio que el país recibió sobre el valor máximo de ambos índices.

	La diferencia muestra la relación entre la puntuación del INC y el NDD. Un resultado positivo indica que el desarrollo de la ciberseguridad del país es acorde con su desarrollo digital o está más avanzado. Un resultado negativo indica que la sociedad digital del país está más avanzada que su ciberseguridad nacional.

Información detallada

¿Cuáles son las preguntas clave que la herramienta puede ayudar a responder?	• ¿Qué grado de preparación tiene mi país para afrontar los ciberataques/amenazas? • ¿Qué le falta a mi país para protegerse frente a una ciberamenaza? • ¿Cuáles son las instituciones adecuadas para la tarea? • ¿Cómo podemos seguir mejorando nuestra preparación frente a la evolución de las ciberamenazas? • ¿Cuáles de las mejores prácticas que hay en todo el mundo podemos adaptar o aplicar?
¿En qué momento del ciclo de vida de la estrategia debe realizarse la evaluación?	La evaluación (análisis del país) puede ocurrir en cualquier momento del ciclo de vida de la estrategia, a fin de mantener el INC lo más actualizado posible. Sin embargo, se recomienda a los países individuales que lo hagan en las fases de "iniciación", "inventario y análisis" o "supervisión y evaluación".
¿Cómo facilita la evaluación la adecuación con otras actividades?	El INC ayuda a identificar esferas relativamente fuertes y débiles respecto del nivel de preparación de un país para prevenir ciberamenazas, por lo que indican los puntos en que tal vez necesite ayuda adicional para crear capacidades o aquellos en que tal vez pueda brindar apoyo a los demás. Las páginas de países del INC también proporcionan información sobre las mejores prácticas nacionales que pueden ser adaptadas/aplicadas por otros países con o sin la ayuda de donantes, organizaciones internacionales, etc.
¿Qué función desempeña la evaluación en el proceso de adecuación con el GFCE?	Dado que el INC presenta la información públicamente disponible, los financiadores y responsables de la aplicación pueden ver las esferas relativamente fuertes y débiles de un determinado país. Por consiguiente, pueden ponerse en contacto con los países respectivos a fin de proponer actividades de creación de capacidades u otras actividades y mejoras conexas, si es necesario.
¿De qué estudios de caso o testimonios se dispone en relación con los beneficios de la herramienta?	Revisión de la situación: Seguridad del ciberespacio y ciberdemocracia en los países de la Asociación Oriental (2017), e-Governance Academy.
¿Cuáles son los mecanismos que garantizan la independencia, imparcialidad y neutralidad de sus resultados?	Los datos presentados por los contribuyentes de países a efectos del INC son validados de manera independiente por nuestro equipo.

Sírvanse añadir información adicional	**Manual:** • La ciberseguridad nacional en la práctica (2020), e-Governance Academy. **Podcast/artículo:** • ¿Qué deben hacer los gobiernos para asegurar su ciberespacio nacional? (2020), e-Governance Academy. • INC – ¿Cuál es el grado de preparación de su país para hacer frente a los ciberataques? (2020), e-Governance Academy. • ¿Qué es la ciberhigiene? (2020), e-Governance Academy. **Artículo:** • 160 países en el INC: Obstáculos, lecciones aprendidas y hechos interesantes (2020), e-Governance Academy.

Panorama de las herramientas

	Herramientas de creación de capacidades para luchar contra la ciberdelincuencia	Madurez cibernética en la región de Asia y el Pacífico	IPC	MMC	EAEC	ICG	MECN	INC
Política y estrategia								
Estrategias	●	●	●	●	●	●	●	●
Evaluaciones	●	●	●	●	●	●	●	●
Medidas de fomento de la confianza y normas		●	●	●		●	●	
Ciberdiplomacia		●	●	●		●	●	●
Derecho internacional en el ciberespacio	●	●	●					
Gestión de incidentes y protección de la infraestructura de información crítica								
Respuesta nacional a incidentes de seguridad informática	●	●	●	●	●	●	●	●
Captura y análisis de incidentes			●	●		●	●	●
Ejercicios en materia de seguridad cibernética			●	●		●	●	●
Protección de la infraestructura de información esencial	●	●	●	●	●	●	●	●
Ciberdelincuencia								
Marcos jurídicos/legislación en materia de ciberdelincuencia	●	●	●	●	●	●	●	●
Aplicación de la ley en el ciberespacio	●	●	●	●	●	●	●	●
Formación en materia de ciberdelincuencia	●		●	●	●	●	●	
Prevención de la ciberdelincuencia	●		●	●	●	●	●	●

Cultura y destrezas								
Creación de conciencia en materia de ciberseguridad	●	●	●	●	●	●	●	●
Capacitación y formación	●	●	●	●	●	●	●	●
Desarrollo de la fuerza de trabajo	●	●	●	●	●	●	●	●
Normas								
Normas internacionales y nacionales			●	●	●	●	●	●