Programa de Ciberseguridad del UIT-D

Índice de Ciberseguridad Global – GCIv5

Modelo de referencia (Metodología)

Índice

Historia y antecedentes

Publicado por primera vez en 2015, el Índice de Ciberseguridad Global (ICG) ayuda a los países a mejorar su compromiso con la ciberseguridad señalando las esferas de fortalecimiento y crecimiento en la materia y destacando buenas prácticas. A partir de los datos recopilados, el ICG pone de relieve los compromisos de ciberseguridad que pueden aplicar los Estados Miembros más adaptados a su entorno nacional, promueve buenas prácticas y fomenta una cultura mundial de la ciberseguridad.

El alcance y el marco del ICG se establecen en la Resolución 130 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios de la UIT, en la que se aborda el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. En particular, se invita a los Estados Miembros "*a apoyar las iniciativas de la UIT sobre ciberseguridad, incluido el Índice de Ciberseguridad Global, con el fin de promover las estrategias gubernamentales y el intercambio de información acerca de los esfuerzos en todas las industrias y sectores.*" La meta final es promover una cultura mundial de la ciberseguridad e integrarla como elemento fundamental de las tecnologías de la información y la comunicación.

Las ediciones anteriores del Índice de Ciberseguridad Global siguen las recomendaciones de la Resolución 45 del UIT-D (Rev. Kigali, 2022), en la que se define la labor realizada a través del Índice de Ciberseguridad Global (ICG) y se recomienda a la BDT que "considere los resultados del [ICG] a fin de orientar las iniciativas de la UIT relacionadas con la ciberseguridad, teniendo especialmente en cuenta las carencias identificadas a través del proceso del ICG".

Las ediciones anteriores son:

Nombre de la edición	GCIv1	GCIv2	GCIv3	GCI 2020 (GCIv4)
Número de edición	1	2	3	4
Países participantes	105 países	136 países	155 países	169 países
Año de recopilación de datos	2013-14	2016	2017-2018	2020
Año de publicación	2015	2017	2019	2021
Notas	En asociación con ABI Research			

El cuestionario del ICG, del que se derivan los indicadores, subindicadores y microindicadores, se actualiza entre ediciones mediante una consulta en el marco de la Cuestión de la Comisión de Estudio: *Seguridad de las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad de los Miembros de la UIT*.

Como resultado del continuo interés de los Estados Miembros en el ICG, la UIT está elaborando una quinta edición (GCIv5) en consulta con el Grupo de Expertos del ICG, como se recomienda en la Resolución 45 (Rev. Kigali, 2022).

Alcance

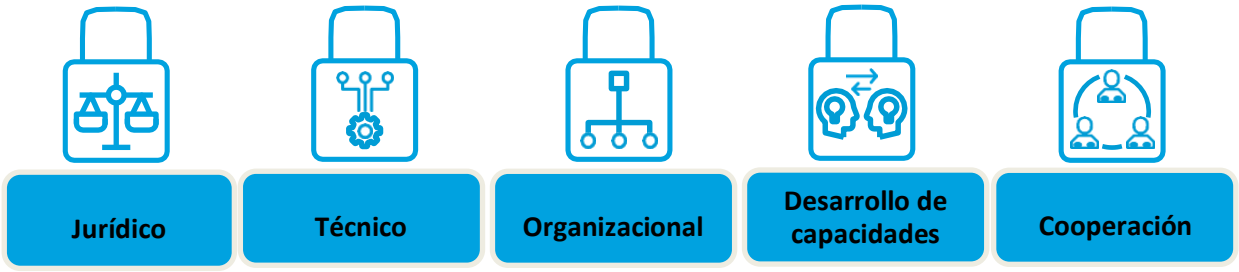
El Índice de Ciberseguridad Global (ICG) es un índice compuesto que combina una serie de indicadores de ciberseguridad para convertirlas en medidas, a partir de los cinco pilares de la Agenda sobre Ciberseguridad Global. Estos pilares constituyen los cinco pilares del ICG. Los principales objetivos del ICG son medir:

- los tipos, niveles y evolución a lo largo del tiempo de los compromisos de ciberseguridad de los países;
- los avances en el compromiso de ciberseguridad desde una perspectiva mundial;
- el progreso en el compromiso de ciberseguridad desde las perspectivas regionales;
- la diferencia de compromiso en ciberseguridad: la diferencia entre los países en cuanto a su nivel de participación en las iniciativas de ciberseguridad.

El Índice de Ciberseguridad Global (ICG) ayuda a los países a determinar los aspectos que deben mejorar en el ámbito de la ciberseguridad, con lo que se eleva el nivel general de la ciberseguridad en todo el mundo. El ICG también recopila buenas prácticas que los países pueden aprender para mejorar sus propias prácticas de ciberseguridad y adoptar soluciones más armonizadas.

Marco conceptual

El Índice de Ciberseguridad Global se centra en los cinco pilares siguientes como áreas generales de compromiso en ciberseguridad para los países:



Medidas jurídicas: Instrumentos legislativos, como leyes, reglamentos y políticas, que definen los derechos, responsabilidades y protecciones que se conceden sobre temas clave relacionados con la ciberseguridad, por ejemplo, la prohibición de determinadas conductas delictivas o requisitos reglamentarios mínimos.

Medidas técnicas: Sin medidas y capacidades técnicas adecuadas para detectar y responder a incidentes, los Estados Miembros y sus respectivas entidades son vulnerables a los riesgos cibernéticos que pueden socavar los beneficios de las tecnologías digitales. Por consiguiente, los Estados Miembros deben estar en condiciones de elaborar estrategias para establecer criterios mínimos de seguridad aceptados y planes de acreditación de aplicaciones y sistemas informáticos. Las medidas técnicas se pueden evaluar basándose en la existencia de instituciones y marcos técnicos que tratan de ciberseguridad, refrendados o creados por el Estado Miembro.

Medidas organizacionales: Para aplicar de manera adecuada cualquier tipo de iniciativa nacional se necesitan medidas de organización. El Estado Miembro debe establecer un objetivo estratégico general, con el correspondiente plan exhaustivo de ejecución, prestación y medición. Deben crearse estructuras, tales como organismos nacionales, para aplicar estrategias de ciberseguridad y evaluar el éxito o el fracaso del plan. Las estructuras orgánicas se pueden medir a partir de la existencia y el número de instituciones y estrategias que organizan el desarrollo de la ciberseguridad a escala nacional.

Medidas de desarrollo de capacidades: El desarrollo de capacidades es intrínseco a las medidas jurídicas, técnicas y organizacionales. Comprender las tecnologías, riesgos y consecuencias en materia de ciberseguridad puede ayudar a mejorar la elaboración de legislaciones, políticas y estrategias y la organización de diversas funciones y responsabilidades. El desarrollo de capacidades abarca el desarrollo de conocimientos y aptitudes entre la población en general, los profesionales cuyos trabajos guardan relación con la ciberseguridad y los especialistas del sector.

Medidas de cooperación: Los esfuerzos en materia de ciberseguridad son más eficaces cuando se basan en todos los sectores y disciplinas afectados, y deben abordarse con un planteamiento global de múltiples partes interesadas. La cooperación mejora el diálogo y la coordinación, y facilita la creación de un campo de aplicación más completo de la ciberseguridad. La cooperación puede comprender actividades tales como iniciativas conjuntas, intercambio de información, formaciones y otras actividades que ponen en contacto a profesionales, funcionarios y otros actores que tratan de mejorar la ciberseguridad.

Metodología computacional

La quinta edición del cuestionario del ICG se divide en cinco pilares: jurídico, técnico, organizacional, desarrollo de capacidades y medidas de cooperación, e incluye un total de 20 indicadores, 64 subindicadores y 28 microindicadores, sobre la base de 83 preguntas. Las preguntas tienen por objeto lograr el equilibrio entre un nivel de detalle importante sobre los compromisos en materia de ciberseguridad y, simultáneamente, una visión de alto nivel. Los indicadores pueden consultarse en el cuestionario del ICG (Anexo A).

Los indicadores se seleccionan en función de:

- la pertinencia de los pilares de la Agenda sobre Ciberseguridad Global;
- la pertinencia del alcance y el marco conceptual del Índice de Ciberseguridad Global;
- la capacidad de los Estados Miembros para responder con precisión a las preguntas;
- la posibilidad de verificación cruzada mediante datos secundarios.

Esta edición utiliza respuestas ternarias (sí, en parte o no) para eliminar la evaluación basada en opiniones y cualquier posible sesgo frente a ciertos tipos de respuesta. Además, una solución ternaria sencilla permite una evaluación más rápida y detallada, pues no se necesitan respuestas largas, lo que acelera y simplifica la obtención de respuestas y de una evaluación ulterior. El entrevistado solo necesita confirmar la presencia o ausencia de soluciones de ciberseguridad predeterminadas.

Para obtener respuestas precisas, los países deberán apoyar su respuesta subiendo al sistema documentos de apoyo y URL. Se añadirá una sección de comentarios a cada pilar para que los países puedan proporcionar buenas prácticas que muestren el efecto de su evolución en materia de ciberseguridad.

Para esta quinta edición y todas las ediciones futuras, el ICG se reestructurará en niveles de compromiso conforme a la Resolución 45 de la CMDT (Conferencia Mundial de Desarrollo de las Telecomunicaciones), Kigali, Rwanda, junio de 2022, donde los Estados Miembros recomendaron que el ICG adoptase un enfoque basado en niveles de agrupación de países en vez de clasificaciones, con miras a ofrecer a los países una evaluación más significativa de los ámbitos que funcionan y aquellos en los que se puede mejorar. Por consiguiente, las reuniones del Grupo de Expertos en Metodología se encargarán de definir un marco territorial adecuado.

Flujo general del proceso ICG

1 El cuestionario del ICG se revisa teniendo en cuenta las observaciones recibidas de los Estados Miembros y del Grupo de Expertos del ICG. El cuestionario se presenta a la reunión de la Comisión de Estudio 2 para su examen.

2 De conformidad con la Resolución 45 del UIT-D (Rev. Kigali, 2022), el Índice de Ciberseguridad Global seguirá siendo estudiado por un grupo de expertos del ICG en relación con la metodología, la estructura, posibles preguntas y la cuestión de la ponderación.

3 Se ha constituido un grupo por correspondencia, un grupo de trabajo del Grupo de Expertos del GCI, integrado por expertos y representantes interesados de los Estados Miembros, para formular recomendaciones e informar sobre el cuestionario.

4 La Secretaría de la BDT efectúa revisiones pertinentes sobre la base de las consultas mantenidas con el grupo por correspondencia, antes de que la dirección de la BDT apruebe el cuestionario o lo reenvié, en su totalidad o en parte, para obtener más información del grupo.

5 El cuestionario aprobado se envía para su traducción a los seis (6) idiomas oficiales de las Naciones Unidas.

6 Se celebran otras dos reuniones del Grupo de Expertos del GCI para estudiar la ponderación y los niveles.

7 El Director de la BDT invita por carta a todos los Estados Miembros de la UIT y al Estado de Palestina a participar en la encuesta sobre el ICG. Las cartas sirven para informarles acerca del GCI y pedirles que nombren un coordinador que se encargue de recopilar todos los datos pertinentes de los países y de completar el cuestionario del GCI.

8 Se invita oficialmente a los coordinadores designados a responder al cuestionario a través de un portal en línea.

9 La Secretaría de la BDT realiza una segunda recopilación de datos entre los países que responden al cuestionario, con miras a:

- Detectar preguntas que hayan quedado sin responder, documentos de apoyo pendientes de envío, enlaces que no se hayan comunicado, etc.
- Permitir al coordinador ser más exacto en sus respuestas, cuando sea necesario.
- Poder enviar a cada coordinador el proyecto de cuestionario corregido para su aprobación final.
- Utilizar el cuestionario validado para realizar análisis, puntuaciones y clasificaciones.

10 La Secretaría de la BDT realiza una primera recopilación de datos entre los países que no responden al cuestionario, con miras a:

- Permitir a la UIT redactar una respuesta inicial al cuestionario a partir de datos disponibles públicamente y una investigación en línea.
- Poder enviar el proyecto de cuestionario a cada coordinador para su revisión.
- Permitir a los coordinadores corregir el proyecto del cuestionario y devolverlo.
- Poder enviar el proyecto de cuestionario corregido a cada coordinador para su aprobación final.
- Utilizar el cuestionario validado para realizar análisis, puntuaciones y clasificaciones.

11 Se prepara un informe con resúmenes de las principales tendencias y prácticas idóneas, teniendo en cuenta recomendaciones sobre niveles y ponderaciones formuladas por el Grupo de Expertos del ICG.

Nota: si un país no proporciona un coordinador para el cuestionario ICG, la UIT establecerá contacto con el coordinador institucional del directorio general de la UIT.

ANEXO A: DEFINICIÓN DE LOS PILARES E INDICADORES

Medidas legislativas

La legislación constituye una medida fundamental para proporcionar un marco armonizado en el que las entidades se adaptan a una base normativa y de reglamentación común, ya sea con respecto a la prohibición de una determinada conducta delictiva o a la definición de requisitos reglamentarios mínimos.

El entorno jurídico se puede medir en función de la existencia de instituciones y marcos jurídicos eficaces en materia de ciberseguridad y ciberdelincuencia. Comprende los indicadores del desempeño siguientes:

1.1 Legislación sobre ciberdelincuencia

La legislación sustantiva alude al derecho público o privado, incluido el derecho de los contratos, patrimonio inmobiliario, delitos civiles, testamentos y leyes penales, que crean, definen y regulan derechos y conductas.

1.2 Reglamentos sobre ciberseguridad

Un reglamento es una regla o principio que rige un comportamiento o una práctica; en especial una directiva establecida y preservada por una autoridad[1]. Es una norma basada en textos legislativos determinados que prevén la ejecución de estos. El reglamento en materia de ciberseguridad se refiere a las normas que tratan de la protección de datos, la notificación de infracciones, los requisitos de certificación/normalización en materia de ciberseguridad, la aplicación de medidas de ciberseguridad, los requisitos de las auditorías de ciberseguridad, la protección de la privacidad, la protección de la infancia en línea, las firmas digitales, las operaciones electrónicas y la responsabilidad de los proveedores de servicios de Internet.

Medidas técnicas

Sin medidas y capacidades técnicas adecuadas para detectar y responder a incidentes, los Estados Miembros y sus respectivas entidades son vulnerables a los riesgos cibernéticos que pueden socavar los beneficios derivados de la adopción de las tecnologías digitales de la información. Por consiguiente, los Estados Miembros han de ser capaces de elaborar estrategias para establecer criterios de seguridad mínimos aceptados y esquemas de acreditación respecto de las aplicaciones y sistemas informáticos. Las medidas técnicas se pueden medir sobre la base de la existencia de instituciones y marcos técnicos que se ocupen de la ciberseguridad, avalados o creados por el Estado Miembro. El subgrupo comprende los indicadores de desempeño siguientes:

1.1 Equipos nacionales/gubernamentales de Intervención en caso de Incidente Informático

Los EIII (Equipos de Intervención en caso de Incidente Informático), los EIEI (Equipos de Intervención en caso de Emergencia Informática) o los EIISI (Equipos de Intervención en caso de Incidente de Seguridad Informática) son entidades a cuyo personal se asigna la responsabilidad de coordinar y ayudar en las intervenciones en caso de eventos o incidentes de seguridad informática a escala nacional. Tienen la responsabilidad nacional de proporcionar capacidades para descubrir ciber amenazas, defenderse de ellas, responder ante ellas y gestionarlas, así como de mejorar la seguridad del ciberespacio en el país. Estas capacidades deben ir acompañadas de la recopilación de su propia inteligencia en lugar de basarse en la notificación secundaria de incidentes de seguridad, ya sea de los clientes del EIII o de otras fuentes.

---

[1] https://www.oed.com/view/Entry/161427?redirectedFrom=regulation

1.2 EIEI/EIII/EIISI sectoriales

Los EIII/EIISI/EIEI sectoriales responden a incidentes de seguridad informática o ciberseguridad que afectan a un sector determinado. Los EIEI sectoriales se suelen crear para sectores esenciales tales como la sanidad, los servicios públicos, los servicios de emergencia, la energía, las instituciones académicas y el sector financiero.

1.3 Marco nacional para la aplicación de las normas de ciberseguridad

Adopción de un marco o marcos nacionales para la aplicación de normas de ciberseguridad reconocidas a nivel internacional dentro del sector público (agencias gubernamentales), e integradas en la infraestructura crítica (incluso si las ejecuta el sector privado). Estas normas incluyen, entre otras, las elaboradas por las agencias siguientes: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

Medidas organizacionales

Para aplicar de manera adecuada cualquier tipo de iniciativa nacional se necesitan medidas de organización y procedimiento. El Estado Miembro debe establecer un objetivo estratégico general, con el correspondiente plan exhaustivo de ejecución, prestación y medición. Deben crearse estructuras, tales como organismos nacionales, para aplicar la estrategia y evaluar el éxito o el fracaso del plan. Las estructuras organizacionales se pueden medir sobre la base de la existencia y el número de instituciones y estrategias que organizan el desarrollo de la ciberseguridad a escala nacional. El subgrupo comprende los indicadores de desempeño siguientes:

1.1 Estrategia/política nacional de ciberseguridad

Definición de políticas para fomentar la ciberseguridad como una de las principales prioridades nacionales. Una estrategia nacional de ciberseguridad debería definir el mantenimiento de infraestructuras de información esenciales resilientes y fiables, incluida la seguridad de la población; la protección de los bienes materiales e inmateriales de la población, las organizaciones y la nación; la respuesta a ciberataques contra infraestructuras críticas y su prevención, y la minimización de los daños y el tiempo de recuperación tras un ciberataque.

1.2 Organismo responsable

Los organismos encargados de aplicar las políticas o estrategias nacionales en materia de ciberseguridad pueden ser comités permanentes, grupos de trabajo oficiales, comités asesores o centros interdisciplinarios. Estos organismos pueden ser además responsables únicos del EIII nacional.

1.3 Medición de la ciberseguridad

Existencia de estudios comparativos o de referencia oficiales, nacionales o sectoriales, empleados para evaluar los avances en materia de ciberseguridad, estrategias de evaluación del riesgo, auditorías sobre ciberseguridad y otros instrumentos o actividades para valorar o evaluar en función del rendimiento para mejoras futuras. Por ejemplo, a partir de la norma ISO/CEI 27004, relativa a la medición de la gestión de la seguridad de la información.

1.4 Estrategias e iniciativas de Protección de la Infancia en Línea (PIeL)

Una estrategia nacional de protección de la infancia en línea debería contar con un plan de acción para promover entornos en línea seguros para los niños de todo el mundo. Será necesario poner en práctica un cuerpo de políticas en el que se establezca un conjunto de objetivos y normas que dejen claro que cada uno

de los delitos que se pueden cometer contra un niño en el mundo real también se pueden cometer, *mutatis mutandis*, por Internet o cualquier otra red electrónica.

Medidas de desarrollo de capacidades

El desarrollo de capacidades forma parte integrante de las tres primeras medidas (jurídica, técnica y orgánica). Comprender la tecnología, sus riesgos y consecuencias puede ayudar a elaborar mejores legislaciones, políticas y estrategias, y a mejorar la organización de las diversas funciones y responsabilidades. Esta área de estudio se aborda con frecuencia desde una perspectiva tecnológica; sin embargo, en esta esfera entran en juego numerosas implicaciones socioeconómicas y políticas.

El marco del desarrollo de capacidades para el fomento de la ciberseguridad debería comprender actividades de sensibilización y disponer de recursos. El subgrupo comprende los indicadores de desempeño siguientes:

1.1 Campañas de concienciación pública sobre ciberseguridad

La sensibilización de los ciudadanos supone promover campañas publicitarias de gran alcance, así como colaborar con ONG, instituciones, organizaciones, proveedores de servicios de Internet, bibliotecas, organizaciones locales de comercio, centros comunitarios, centros universitarios y de formación de adultos, escuelas y organizaciones de padres y profesores para difundir mensajes sobre comportamientos seguros en línea.

1.2 Formación para profesionales de la ciberseguridad

Existencia de programas de formación profesional sectoriales para sensibilizar al público en general (por ejemplo, día, semana o mes de la ciberseguridad nacional), fomentar la formación en ciberseguridad de la mano de obra con distintos perfiles (técnico, ciencias sociales, etc.) y fomentar la certificación de profesionales de los sectores público y privado.

Este indicador comprende también la existencia de un marco aprobado (o apoyado) por el gobierno para la certificación y acreditación de profesionales conforme a normas de seguridad internacionalmente reconocidas. Estas certificaciones, acreditaciones y normas pueden ser, entre otras, las siguientes: Seguridad en la nube (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, analista de ciberseguridad forense (ISC²), etc.

1.3 Programas educativos sobre ciberseguridad en el marco de programas académicos nacionales

Establecimiento y promoción de cursillos y programas educativos a escala nacional para formar a las nuevas generaciones en conocimientos y profesiones relacionadas con la ciberseguridad en escuelas, institutos, universidades y otros centros educativos. Las profesiones vinculadas a la seguridad incluyen, entre otras, criptoanalistas, expertos en informática forense, expertos en respuestas a incidentes, arquitectos de seguridad informática o expertos en pruebas de penetración informática.

1.4 Programas de investigación y desarrollo en ciberseguridad

Este indicador mide la inversión en programas nacionales de investigación y desarrollo en ciberseguridad de instituciones privadas, públicas, académicas, no gubernamentales o internacionales. También considera la presencia de un organismo reconocido a nivel nacional que supervise el programa.

1.5 Sector nacional de ciberseguridad

Un clima económico, político y social propicio que fomente el desarrollo de la ciberseguridad favorece el crecimiento de empresas de ciberseguridad en el sector privado. Las campañas de sensibilización, el desarrollo de la mano de obra, la creación de capacidades y los incentivos gubernamentales impulsarán un mercado de productos y servicios de ciberseguridad. La presencia de una industria nacional de la

ciberseguridad testimonia un entorno adecuado y fomenta la creación de empresas del sector y del mercado conexo de las ciberaseguradoras.

1.6 Mecanismos de incentivo gubernamentales

Este indicador evalúa los incentivos que ofrece el Gobierno para fomentar la creación de capacidades en el sector de la ciberseguridad, mediante ventajas fiscales, subvenciones, financiación, préstamos, instalaciones y otros incentivos económicos y financieros, como actividades de creación de capacidades de ciberseguridad especiales o reconocidas a nivel nacional y supervisadas por un organismo institucional.

Medidas de cooperación

La ciberseguridad necesita que todos los sectores y disciplinas contribuyan a ella y, por lo tanto, necesita un enfoque multipartito. La cooperación mejora el diálogo y la coordinación, y facilita la creación de un campo de aplicación más completo de la ciberseguridad. La divulgación de información es difícil, en el mejor de los casos, entre disciplinas diferentes y entre operadores del sector privado. Es cada vez más difícil a nivel internacional. El subgrupo comprende los indicadores de desempeño siguientes:

1.1 Acuerdos bilaterales en materia de ciberseguridad

Los acuerdos bilaterales (acuerdos entre dos partes) designan alianzas nacionales o sectoriales reconocidas oficialmente y destinadas a compartir información y recursos sobre ciberseguridad entre países. Son concluidos por un Gobierno y otro Gobierno extranjero, entidad regional u organización internacional (por ejemplo, cooperación o intercambio de información, conocimientos expertos, tecnología y otros recursos).

1.2 Acuerdos multilaterales en materia de ciberseguridad

Los acuerdos multilaterales (entre varias partes) designan alianzas nacionales o sectoriales reconocidas oficialmente y destinadas a compartir información y recursos sobre ciberseguridad. Son concluidos por un Gobierno y otros Gobiernos extranjeros u organizaciones internacionales (por ejemplo, cooperación o intercambio de información, conocimientos expertos, tecnología y otros recursos).

1.3 Acuerdos de asistencia jurídica recíproca sobre ciberseguridad

También puede incluir la ratificación de acuerdos internacionales que contengan cláusulas relacionadas con la asistencia jurídica recíproca y la ciberseguridad.

1.4 Asociaciones entre entidades públicas y privadas

Por alianzas público-privadas se entienden los acuerdos entre el sector público y el privado. Pueden tener la forma de un contrato a largo plazo entre una entidad privada y una entidad gubernamental para la prestación de un bien o servicio público, en el que la parte privada asume una importante responsabilidad en materia de riesgos y gestión, y la remuneración está vinculada al rendimiento[2]. Este indicador de rendimiento mide el número de acuerdos público-privados nacionales o sectoriales y reconocidos oficialmente para compartir información y recursos de ciberseguridad (personal, procesos, instrumentos) entre el sector público y el privado (por ejemplo, alianzas oficiales sobre cooperación o intercambio de información, conocimientos expertos, tecnología y/o recursos), ya sea a escala nacional o internacional.

---

2 https://ppp.worldbank.org/public-private-partnership/espanol-asociaciones-publico-privadas

1.5 Acuerdos entre agencias

Este indicador de rendimiento designa cualquier colaboración oficial entre diferentes agencias gubernamentales y el Estado Miembro (no incluye las alianzas internacionales). Puede incluir colaboraciones entre ministerios, departamentos, programas y otras instituciones del sector público.