Anexo 1 – Mandato

Programa de Ciberseguridad UIT/BDT

Grupo de Expertos en Ponderación del ICG

Mandato

Agosto de 2020

Índice de Ciberseguridad Global (ICG)

Publicado por vez primera en 2015, el Índice de Ciberseguridad Global (ICG) ayuda a los países a determinar los aspectos que deben mejorar en el ámbito de la ciberseguridad, y les motiva a adoptar medidas para mejorar su clasificación, con lo que se eleva el nivel general de la ciberseguridad en todo el mundo. A partir de los datos recopilados, el ICGI pone de relieve las prácticas que pueden aplicar los Estados Miembros más adaptadas 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. El Cuestionario ICG, del que se derivan los indicadores, subindicadores y microindicadores, se crea y aprueba mediante una consulta en el marco de la Cuestión 3 de la Comisión de Estudio 2: Seguridad de las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad de los Miembros de la UIT.

Grupo de Expertos en ponderación del ICG

El objetivo del Grupo de Expertos es determinar la ponderación de los indicadores, subindicadores y microindicadores del ICG y proponer cambios en el Cuestionario del ICG para las futuras ediciones.

Los miembros del Grupo de Expertos del ICG son designados para formular recomendaciones rigurosas e imparciales para la distribución de puntos en el modelo del ICG. Las recomendaciones del Grupo de Expertos sobre el peso de cada indicador y subindicador deben estar en consonancia con su importancia para el compromiso general de ciberseguridad del Estado Miembro. Entre las actividades específicas del Grupo de Expertos cabe destacar las siguientes:

- suministrar información sobre el cálculo del índice principal y los subíndices, ilustrados en el Anexo B al presente documento; y
- proporcionar información sobre posibles ediciones futuras del ICG.

En casos excepcionales, y previo acuerdo de la mayoría, el Grupo de Expertos podrá recomendar la revisión de preguntas para la siguiente edición del ICG.

La UIT actuará como secretaría del Grupo de Expertos. La participación en el Grupo de Expertos está abierta a los Estados Miembros y Miembros de Sector de la UIT, además de a los expertos que participaron en las anteriores ediciones del ICG.

La composición del Grupo de Expertos debe ser acorde con la diversidad regional, la diversidad de género y la diversidad de conocimientos especializados, y mantener un equilibrio entre los diferentes interesados, en particular gobiernos, sector privado y mundo académico.

Proceso de ponderación

El proceso general de evaluación debe seguir los siguientes pasos:

1) La UIT proporciona a cada miembro del Grupo de Expertos todo el material pertinente, a saber:

   a) la hoja de cálculo de ponderaciones con las preguntas del ICG;

   b) el mandato, con una guía de instrucciones y explicaciones de los indicadores (el presente documento).

2) Se celebrará una reunión del Grupo de Expertos en el ICG el **15 de octubre de 2020** para examinar el procedimiento y responder preguntas.

3) Después de la reunión inicial, cada miembro del Grupo de Expertos rellenará de manera independiente la hoja de cálculo Excel de ponderaciones, en la que recomendará un peso para cada indicador, subindicador y microindicador, y la remitirá a gci@itu.int antes del **31 de octubre de 2020.**

4) Una vez que todos los miembros del Grupo de Expertos hayan presentado sus recomendaciones, las ponderaciones recomendadas se promediarán y se refundirán en una sola hoja de cálculo de ponderaciones.

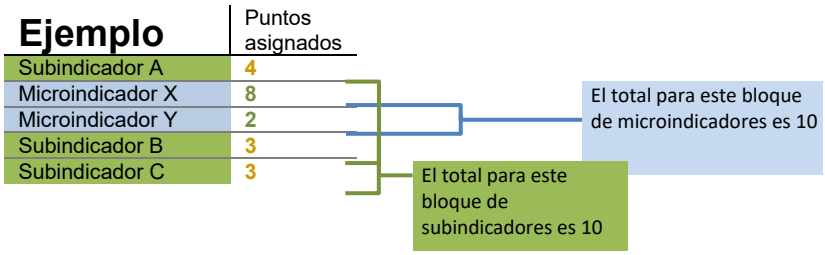
5) Las ponderaciones promediadas recomendadas se compartirán con los miembros del Grupo de Expertos.

ANEXO A: CÓMO ASIGNAR PESOS

Sólo debe revisar las ponderaciones de los pilares de su ámbito de competencias. No se tendrán en cuenta las ponderaciones asignadas a pilares para los que no haya indicado su pericia.

El ICG obedece a un modelo jerárquico anidado. Cada "rama" del modelo se denomina bloque, como un bloque de indicadores, un bloque de subindicadores y un bloque de microindicadores.

A cada bloque se le asignan 10 puntos. Deberá asignar más puntos a los indicadores/subindicadores/microindicadores que sean más importantes, con arreglo a su experiencia.

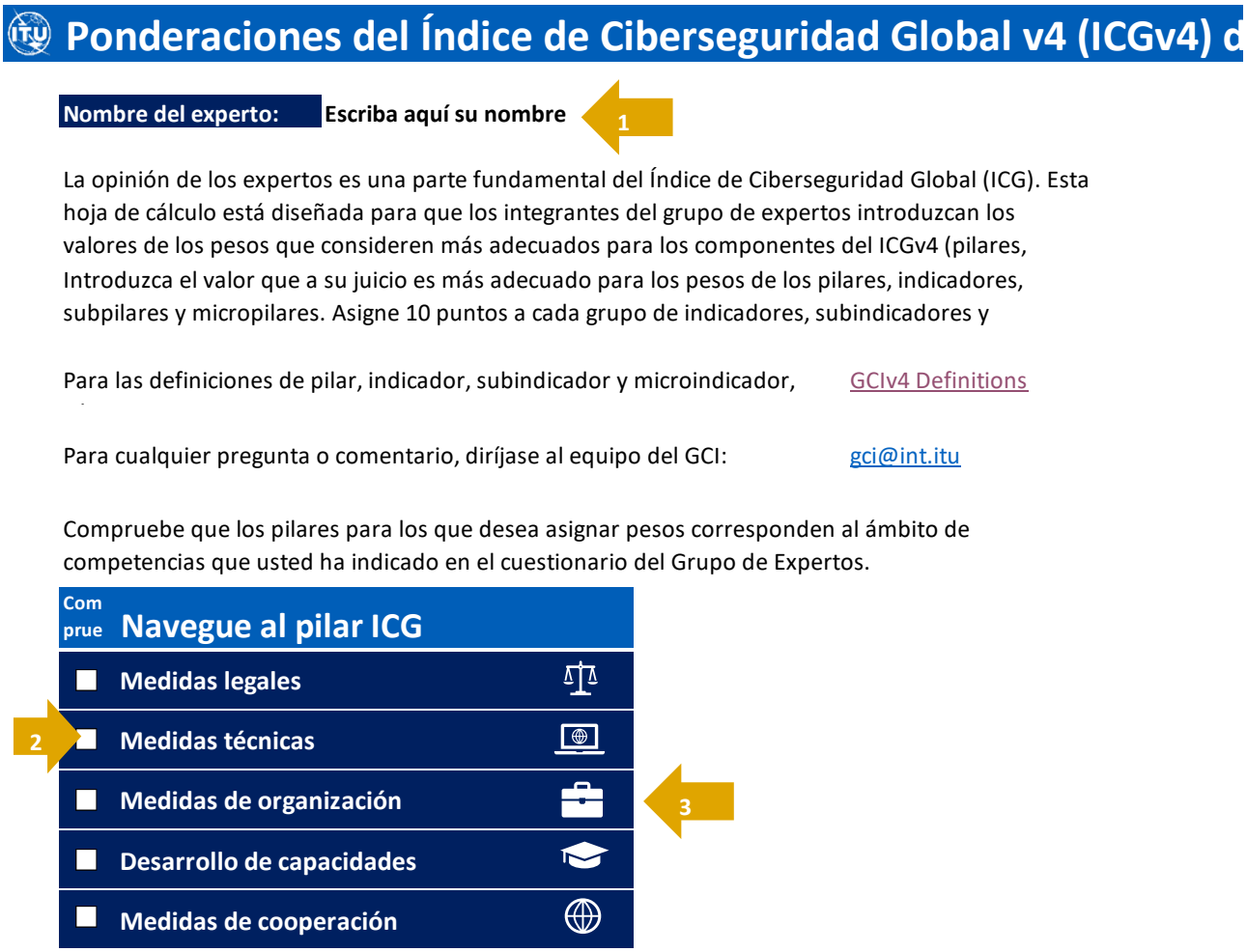


Cómo utilizar la hoja de cálculo de ponderaciones

Estas instrucciones son para la hoja de cálculo *GCI-Questionnaire-weightage-calculation.xlsx*.

El fichero se ha diseñado para Microsoft Excel. Es posible que algunas funciones no se ejecuten correctamente en otros programas.

Primeros pasos

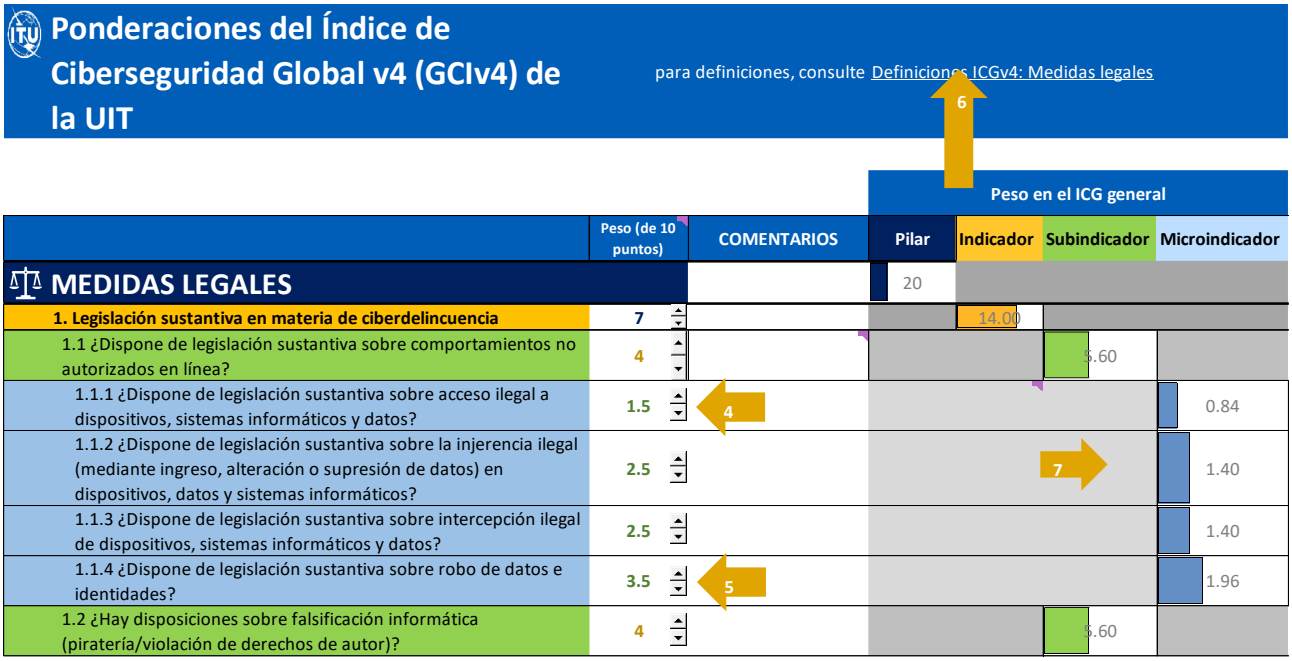


1) Escriba su nombre.

2) Compruebe que los pilares para los que desea asignar pesos corresponden a su ámbito de competencias.

3) Pulse el nombre o icono de cada pilar para navegar por el pilar cuyo valor desea modificar.

Asignación de pesos



4) Para modificar el peso del indicador, subindicador o microindicador escriba su valor numérico en la celda correspondiente o utilice los botones de deslizamiento para aumentar o disminuir su valor.

   a) Tiene que asignar 10 puntos por bloque. Si asignas más o menos puntos, las celdas del bloque aparecerán en color rojo, como se muestra a continuación:

   b) Las flechas arriba y abajo cambian el valor en número enteros.

   c) Para introducir fracciones, escriba primero el número seguido de =. Por ejemplo, escriba =1/3 para ⅓.

   d) Si desea asignar un valor inferior o superior a 10 puntos, indíquelo en una nota en los comentarios. Su ponderación se normalizará a 10 en el momento de realizar la media aritmética de las respuestas de los expertos.

5) En la columna Comentarios, puede formular observaciones sobre la ponderación de cualquier indicador, subindicador o microindicador.

6) Pulse el enlace *GCIv4 Definitions* para comprender mejor el significado de cada indicador.

7) La sección *ponderación en el ICG general* muestra el peso que tendrá el indicador, según la puntuación que usted le ha asignado, en el ICG definitivo. No es posible editar o modificar estas celdas.

Finalización

1) Una vez haya terminado, pulse "Guardar como" (para más información sobre cómo proceder consulte las instrucciones del soporte técnico de Microsoft), y añada su nombre al final.

   Ejemplo: *GCI-Questionnaire-weightage-calculations-**NAME**.xlsx*

2) Adjunte su hoja de cálculo en un correo dirigido a gci@itu.int antes del plazo previsto.

ANEXO B: DEFINICIÓN DE LOS PILARES E INDICADORES

Medidas legales

La legislación es esencial para crear un marco armonioso en el que las entidades se pueden adaptar a una base normativa común, ya sea con respecto a la prohibición de un determinado comportamiento delictivo, o a exigencias normativas mínimas.

El entorno legislativo se puede medir en función de la existencia y el número de instituciones y marcos legales que tratan de ciberseguridad y ciberdelito. El subgrupo comprende los indicadores de rendimiento siguientes:

- **Legislación sustantiva en materia de ciberdelincuencia**

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

- **Reglamentos sobre ciberseguridad**

Los reglamentos son normas basadas en textos legislativos determinados que prevén la ejecución de estos.

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 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 y el número de instituciones y marcos técnicos que tratan de ciberseguridad, refrendados o creados por el Estado. El subgrupo comprende los indicadores de rendimiento siguientes:

- **Equipos nacionales/gubernamentales de intervención en caso de incidentes**

Los equipos de intervención en caso de incidente informático, EIII/EIISI/EIEI, 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.

- **EIII/EIISI/EIEI sectoriales**

Los EIII/EIISI/EIEI sectoriales responden a incidentes de seguridad informática o ciberseguridad que afectan a un sector determinado. Se suelen crear para sectores tan importantes como el sanitario, las infraestructuras públicas, los servicios de emergencia y el sector financiero.

- **Marco nacional para la aplicación de las normas de ciberseguridad**

Es fundamental adoptar un marco nacional (o varios) para la aplicación de normas de ciberseguridad reconocidas a escala internacional dentro del sector público (organismos gubernamentales), e integrados en la infraestructura esencial (incluso si los ejecuta el sector privado). Estas normas incluyen, entre otras, las elaboradas por las agencias siguientes: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

- **Protección de la Infancia en Línea**

Este indicador mide la existencia de un organismo nacional dedicado a la Protección de la Infancia en Línea; la disponibilidad de un número de teléfono nacional para denunciar problemas relacionados con la infancia en línea; y cualquier otro mecanismos técnicos o capacidades para proteger a la infancia en línea.

Medidas orgánicas

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 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. El subgrupo comprende los indicadores de rendimiento siguientes:

- **Estrategia/Política nacional de ciberseguridad**

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

- **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 directos del EIII nacional.

- **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.

Medidas de la capacitación

La capacitación 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 mejorar la organización de las diversas funciones y responsabilidades. Es un tema que se aborda en la mayoría de los casos desde una perspectiva tecnológica, pero que también tiene numerosas consecuencias socioeconómicas y políticas.

El marco de capacitación para el fomento de la ciberseguridad debería comprender actividades de sensibilización y disponer de recursos. El subgrupo comprende los indicadores de rendimiento siguientes:

- **Campañas públicas 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.

- **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.

Comprende también la formación en ciberseguridad de las fuerzas del orden, el sector judicial y demás actores del sector. La formación profesional y técnica puede ser continua para los agentes de policía, agentes de aplicación, jueces, fiscales, abogados, personal auxiliar y demás involucrados en el sector judicial y de aplicación de la legislación. Este indicador comprende también la existencia de un marco aprobado (o apoyado) por el gobierno para la certificación y acreditación de profesionales conforme a normas de seguridad internacionalmente reconocidas. Estas certificaciones, acreditaciones y normas pueden ser, entre otras, las siguientes: Seguridad en la nube (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, analista de ciberseguridad forense (ISC^2), etc.

- **Programas nacionales académicos y educativos**

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.

- **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.

- **Industria nacional de la 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 capacitación y los incentivos gubernamentales impulsarán un mercado de productos y servicios de ciberseguridad. La presencia de una industria nacional de la ciberseguridad testimonia un entorno adecuado y fomenta la creación de empresas del sector y del mercado conexo de las ciberaseguradoras.

- **Mecanismos incentivos**

Este indicador evalúa los incentivos que ofrece el gobierno para fomentar la capacitación en el sector de la ciberseguridad, mediante ventajas fiscales, subvenciones, financiación, préstamos, instalaciones y otros incentivos económicos y financieros, como actividades de capacitación específicas o nacionales. Los incentivos incrementan la demanda de servicios y productos relacionados con la ciberseguridad, lo que mejora la protección ante ciberataques.

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, pero el problema del ciberdelito es mundial y no conoce fronteras nacionales ni distinciones sectoriales. El subgrupo comprende los indicadores de rendimiento siguientes:

- **Acuerdos bilaterales**

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

- **Participación del gobierno en mecanismos internacionales (foros)**

También pueden incluir la ratificación de acuerdos internacionales sobre ciberseguridad, como la Convención de la Unión Africana sobre ciberseguridad y protección de datos personales o el Convenio sobre la Ciberdelincuencia de Budapest.

- **Acuerdos multilaterales**

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).

- **Alianzas publico privados**

Por alianzas público privadas se refiere a acuerdos entre el sector público y el privado. Este indicador de rendimiento mide el número de acuerdos público-privados nacionales o sectoriales y reconocidos oficialmente para compartir información y recursos de ciberseguridad (personal, procesos, instrumentos) entre el sector público y el privado (por ejemplo, alianzas oficiales sobre cooperación o intercambio de información, conocimientos expertos, tecnología y/o recursos), ya sea a escala nacional o internacional.

- **Acuerdos entre agencias**

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

_____