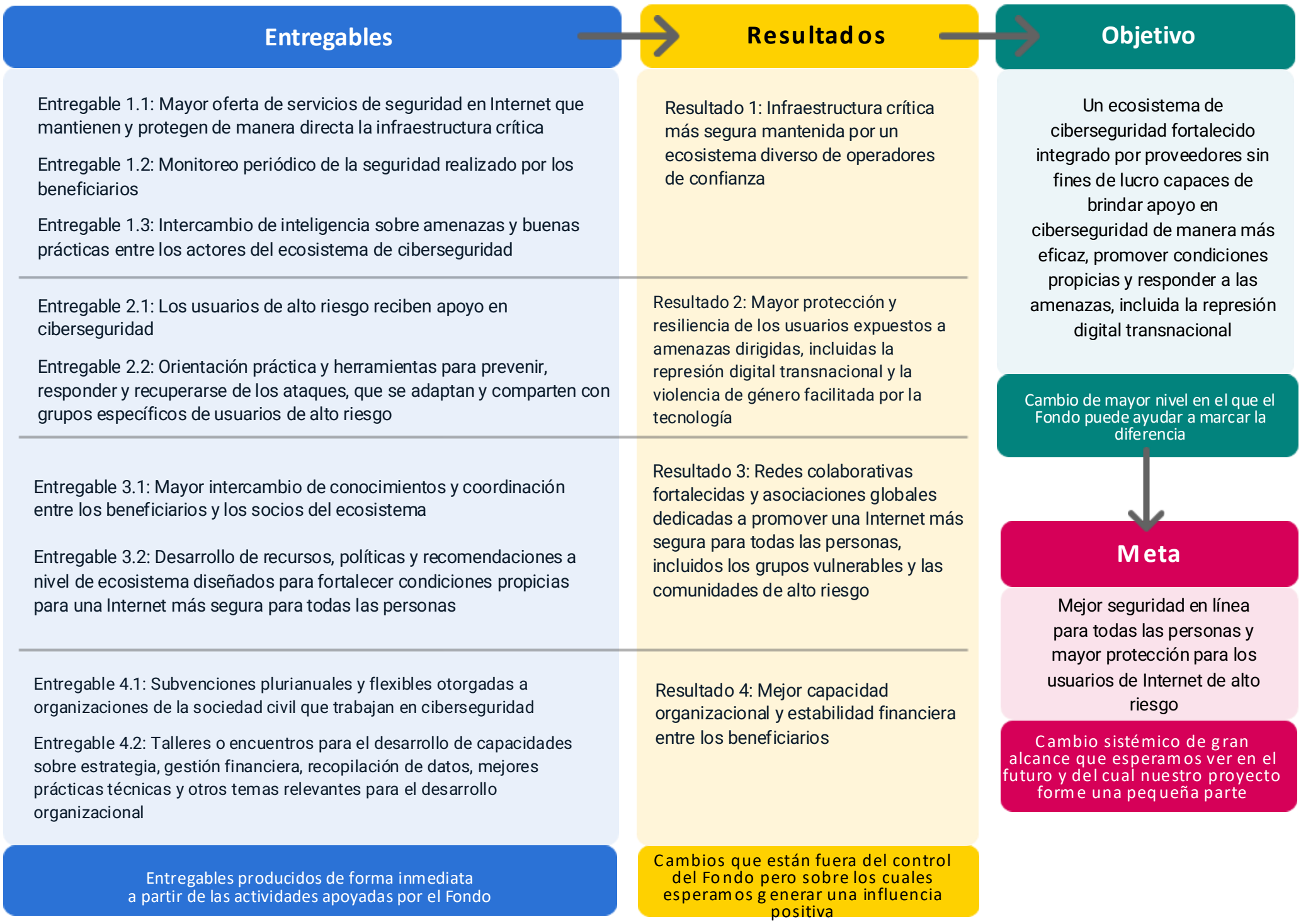
Modelo lógico del Fondo Common Good Cyber



Teoría del cambio:

SI Internet Society Foundation, en colaboración con Global Cyber Alliance, gestiona un programa de subvenciones de cinco años con recursos suficientes que ofrezca financiamiento plurianual y flexible a organizaciones sin fines de lucro que trabajan en ciberseguridad —particularmente en la Mayoría Global— y complementa este financiamiento con desarrollo de capacidades técnicas y organizacionales, apoyo experto en incidencia y oportunidades de aprendizaje entre pares e intercambio de conocimientos,

ENTONCES estas organizaciones sin fines de lucro (beneficiarias de Internet Society Foundation) estarán mejor preparadas para mantener una infraestructura crítica más segura, apoyar mejor a los usuarios de alto riesgo que enfrentan amenazas de ciberseguridad y fortalecer las redes colaborativas y las asociaciones globales que trabajan para impulsar iniciativas de seguridad y protección. En última instancia, esto llevará a un ecosistema de ciberseguridad más fuerte y capaz de crear una Internet más segura para todas las personas.

Supuestos críticos:

- Un financiamiento plurianual y flexible les brinda a las organizaciones agilidad suficiente para adaptarse a la evolución de las amenazas digitales, a los cambios en los entornos políticos o de alto riesgo y a las transformaciones en el panorama de financiamiento.
- Un apoyo sólido para el fortalecimiento de la capacidad organizacional adaptado a las necesidades específicas de los beneficiarios llevará a la implementación continua de mejores prácticas operativas. En última instancia, esto permitirá que las organizaciones sostengan mejor sus programas técnicos.
- La construcción de una red diversa de organizaciones enfocadas en la ciberseguridad fomentará el aprendizaje entre pares y la colaboración continua más allá del período de las subvenciones, contribuyendo al fortalecimiento del ecosistema global de apoyo a largo plazo.

Guía sobre los indicadores del CGCF

Al informar sobre los indicadores, los beneficiarios deben considerar el área de enfoque a la que contribuye o respalda el financiamiento del Fondo Common Good Cyber (CGCF) e incluir los resultados de estos programas o iniciativas al presentar los datos de los indicadores al CGCF. Dado que el CGCF puede apoyar programas de forma directa o indirecta, los beneficiarios deben utilizar su mejor criterio para decidir qué datos incluir en los informes. Los beneficiarios también deben asegurarse de informar únicamente los resultados logrados durante el período cubierto por el informe y no incluir resultados logrados fuera del rango de fechas correspondiente. Si en algún momento tiene dudas sobre qué datos incluir en sus informes, los beneficiarios deben comunicarse con sus contactos del CGCF.

Indicadores de capacidad organizacional y sostenibilidad (aplicables a todos los beneficiarios)

Los Indicadores de capacidad organizacional y sostenibilidad se aplican a todos los beneficiarios del CGCF, independientemente del área de enfoque. Su objetivo es capturar los cambios en la capacidad organizacional, la sostenibilidad y la eficacia operativa durante el período de la subvención.

Indicadores de capacidad organizacional y sostenibilidad (aplicables a todos los beneficiarios)	
Indicador	**Guía**
Número de beneficiarios que informan un mayor número de fuentes activas de financiamientos al final de la subvención en comparación con el inicio	Número de beneficiarios que autodeclaran tener un mayor número total de fuentes activas de financiamiento al final de la subvención (o al momento del informe, en el caso de los informes intermedios) en comparación con el inicio. Las "fuentes de financiamiento" pueden incluir subvenciones, contratos, donaciones, patrocinios, ingresos propios, etc.

	Este indicador no pretende demostrar de manera concluyente que el Fondo es el único responsable de mejorar la situación financiera de un beneficiario. Más bien está diseñado para capturar cualquier cambio en la situación financiera al que el CGCF pueda haber contribuido, ya sea mediante financiamiento directo o a través de apoyo al fortalecimiento de la capacidad organizacional.
Número de mejoras operativas específicas u otras acciones de fortalecimiento organizacional realizadas por los beneficiarios a lo largo de la subvención	Los beneficiarios informan si han implementado mejoras financieras, administrativas, operativas u otras mejoras organizacionales concretas después de haber recibido financiamiento del CGCF y/o de haber participado en actividades de fortalecimiento de capacidades organizadas por Internet Society Foundation para los beneficiarios del CGCF. Los beneficiarios deben poder señalar ejemplos específicos de mejoras a las que consideren que contribuyeron el financiamiento del CGCF o las actividades de fortalecimiento, por ejemplo, protocolos o políticas, sistemas financieros, estrategias o procesos de gobernanza nuevos o actualizados; cambios en el personal; nuevas estrategias de comunicación; o uso y adopción de nuevas herramientas a nivel organizacional.
Número de beneficiarios que declaran tener mayor confianza en la gestión de fondos para apoyar la ciberseguridad a lo largo de la subvención	Los beneficiarios declaran si se sienten más seguros en la gestión de recursos financieros relacionados con el trabajo de ciberseguridad después de haber recibido financiamiento del CGCF y/o de haber participado en actividades de desarrollo de capacidades organizadas por Internet Society Foundation para los beneficiarios del CGCF.

Indicadores que dependen del enfoque del programa

Para las subvenciones que se enfocan en el mantenimiento de infraestructura crítica de ciberseguridad (informar únicamente los indicadores aplicables)	
Indicador	**Guía**
Número estimado de usuarios finales que se benefician de los servicios de infraestructura de ciberseguridad mejorados o mantenidos por los beneficiarios	Número total de personas que se benefician de manera directa o indirecta de los servicios de infraestructura apoyados por la subvención y brindados por los beneficiarios durante el período cubierto por el informe. Esto incluye a los usuarios de redes, plataformas o sistemas que se vuelven más seguros gracias a las actividades de los beneficiarios. Se trata de una estimación razonada que se utiliza para ilustrar la escala de los beneficios derivados de la protección o el apoyo de los beneficiarios a los servicios de infraestructura de ciberseguridad. Esta estimación podría ser imprecisa, ya que estos servicios a menudo operan a niveles compartidos, ascendentes o de toda Internet, generando beneficios que podrían extenderse a una gran cantidad de usuarios de forma indirecta. "Servicios de infraestructura" incluye servicios operativos compartidos que ayudan a asegurar, sostener y fortalecer la disponibilidad, integridad y confiabilidad de los sistemas básicos de Internet, por ejemplo, al identificar amenazas, permitir la remediación, apoyar la respuesta a incidentes y ofrecer funciones que fortalezcan la confianza, como infraestructura de certificados seguros.
Número de exposiciones relacionadas con la infraestructura identificadas por los	Este indicador contabiliza el número de debilidades de seguridad diferentes y significativas que afectan a la infraestructura relevante y que son identificadas por los beneficiarios durante el período cubierto por el informe ***antes*** de que exista evidencia confirmada de explotación maliciosa.

beneficiarios que se detectan antes de ser explotadas	"Exposiciones" son debilidades de seguridad significativas e incluyen fallas de los sistemas, configuraciones incorrectas, valores predeterminados inseguros, controles de acceso débiles u otras condiciones que podrían permitir accesos no autorizados, compromisos, interrupciones o abusos. Los beneficiarios deben utilizar su experiencia técnica y sus criterios internos para determinar si una exposición identificada debe contabilizarse bajo este indicador como una debilidad de seguridad significativa que podría provocar daños si no se corrige.
Porcentaje de exposiciones identificadas que los beneficiarios mitigaron con éxito o que el operador de infraestructura responsable reconoció oficialmente para su remediación antes de que afectaran a los usuarios, desglosadas por numerador y denominador	Este indicador mide la proporción de exposiciones identificadas por los beneficiarios y que ellos mitigan con éxito antes de que afecten a los usuarios. "Exposiciones" son debilidades de seguridad significativas e incluyen fallas de los sistemas, configuraciones incorrectas, valores predeterminados inseguros, controles de acceso débiles u otras condiciones que podrían permitir accesos no autorizados, compromisos, interrupciones o abusos. Una exposición se considera "mitigada con éxito" si se abordó o se redujo antes de causar daños a los usuarios o sistemas. Una exposición se considera reconocida oficialmente para su remediación si el operador de infraestructura responsable comunica que está al tanto de la exposición y tiene la intención de abordarla tras una divulgación coordinada. Para el denominador, los beneficiarios deben informar el número total de exposiciones identificadas de acuerdo con el indicador anterior. Para el numerador, los beneficiarios deben informar el número total de vulnerabilidades (de las identificadas) que se mitigaron con éxito. El sistema de informes de Fluxx utilizará estos dos valores para calcular el porcentaje resultante.

Número de organizaciones (por ejemplo, CSIRT nacionales o sectoriales, operadores de infraestructura, proveedores de servicios y organizaciones de la sociedad civil) que responden a ciberamenazas o las remedian basándose en informes o inteligencia compartida con el apoyo de la subvención	Este indicador contabiliza cuántas organizaciones tomaron medidas durante el período cubierto por el informe después de recibir información, informes, alertas o inteligencia sobre ciberamenazas compartidas mediante trabajo respaldado por la subvención. "Responder" a las amenazas incluye tomar medidas para gestionar o contener una amenaza o incidente detectado, como bloquear tráfico malicioso, desactivar infraestructura maliciosa, alertar a los usuarios o miembros afectados, escalar a un equipo de respuesta a incidentes, emitir advertencias, iniciar medidas de contención o compartir la información para una acción operativa posterior. "Remediar" las amenazas incluye las acciones que se toman para corregir, reducir o eliminar el riesgo o la exposición subyacente. Esto puede incluir, por ejemplo, aplicar parches a sistemas vulnerables, corregir configuraciones incorrectas, desactivar servicios expuestos, rotar credenciales, actualizar reglas o controles, o eliminar de cualquier otra forma la condición que permitió la amenaza. Este es un indicador de contribución, no de atribución. No se espera que los beneficiarios demuestren que han sido los únicos responsables de la respuesta, sino que demuestren que existe un vínculo razonable entre la información compartida y las medidas tomadas por la organización. Las potenciales fuentes de datos para este indicador incluyen correos electrónicos de seguimiento, llamadas o reuniones con quienes recibieron los informes o la inteligencia para analizar o confirmar las medidas tomadas, ya sea a través de canales de comunicación nuevos o existentes.
Número de beneficiarios que prestan servicios de seguridad de Internet	Se les pregunta a los beneficiarios si como parte de su subvención están ofreciendo servicios de ciberseguridad nuevos o ampliando los existentes. En caso de que su respuesta sea afirmativa, se les pide que describan con mayor detalle los servicios prestados. Los ejemplos de

nuevos o ampliados a usuarios, proveedores o autoridades	servicios incluyen monitoreo, respuesta a incidentes, asesoría, protocolos de presentación de informes nuevos o mejorados y mecanismos de intercambio de datos. Los servicios "ampliados" incluyen los cambios realizados en los servicios existentes de los beneficiarios que producen una cobertura más amplia o una mejor calidad. Los ajustes menores de rutina no deben contabilizarse automáticamente como una ampliación de los servicios salvo que su alcance sea sustancial.
Número de actividades diferentes de monitoreo de amenazas realizadas regularmente por los beneficiarios	"Actividades diferentes de monitoreo de amenazas" son tipos específicos de monitoreo que incluyen, entre otros, el análisis de indicadores de compromiso (artefactos técnicos u observaciones que pueden indicar actividad maliciosa, como direcciones IP sospechosas, dominios, hashes de archivos, claves de registro, nombres de procesos, certificados u otras señales de advertencia que podrían indicar un compromiso o intento de compromiso); la identificación de campañas de actores maliciosos; la investigación de tácticas, técnicas y procedimientos (TTP) novedosos; y/o el registro de grupos de vulnerabilidades críticas documentadas. Este indicador incluye únicamente las actividades de monitoreo respaldadas por la subvención y realizadas durante el período cubierto por el informe. Dada la naturaleza de esta actividad técnica, realizar un mayor número de actividades de monitoreo de amenazas no significa necesariamente un mejor desempeño, ya que algunas actividades son más complejas que otras. Según corresponda, los beneficiarios deben incluir en el informe narrativo una breve descripción de sus actividades de monitoreo de amenazas para dar contexto al número informado.
Número de informes de interés público con hallazgos de alta	Este indicador contabiliza los informes producidos por los beneficiarios durante el período cubierto por el informe que presentan hallazgos sólidos y basados en evidencia sobre amenazas, riesgos, incidentes o

confiabilidad desarrollados y compartidos por los beneficiarios	prácticas de seguridad y que se comparten públicamente o con los socios relevantes. "Hallazgos de alta confiabilidad" significa que la información está respaldada por evidencia y se considera lo suficientemente confiable como para fundamentar una acción o la toma de decisiones. Compartido públicamente significa que el informe se pone a disposición más allá de la organización (por ejemplo, se publica en un sitio web, se comparte con socios, formuladores de políticas o partes interesadas relevantes, o se difunde a través de eventos o redes).
Número de herramientas operativas, plataformas o mecanismos de coordinación centrados en la infraestructura desarrollados o fortalecidos con el apoyo del Fondo y que son utilizados activamente por múltiples actores del ecosistema	Esto cuenta las herramientas, plataformas o mecanismos de coordinación que reciben el apoyo del Fondo durante el período del informe y que ayudan a las organizaciones a trabajar juntas para monitorear, compartir información o responder a ciberamenazas que afectan a la infraestructura. "Utilizado activamente" significa que la herramienta, plataforma o mecanismo continúa en uso de manera sostenida después de haber sido creado o mejorado, por ejemplo, mediante el intercambio regular de datos, una coordinación continua o contribuciones colaborativas. Para ser contabilizados, los beneficiarios deben tener evidencia de que la herramienta, plataforma o mecanismo está siendo utilizado por múltiples organizaciones o por otros actores que forman parte del ecosistema de ciberseguridad, como organizaciones de la sociedad civil, CSIRT, plataformas, redes u otros.

Para las subvenciones que se enfocan en brindar apoyo escalable para proteger a los usuarios de Internet de los daños digitales, incluidas la actividad cibernética dirigida por

los estados y la represión digital transnacional (informar únicamente sobre los indicadores aplicables)	
Indicador	**Guía**
Porcentaje de usuarios de alto riesgo que declaran haber aplicado nuevas prácticas o herramientas después de recibir apoyo en ciberseguridad, desglosado por numerador y denominador	Este indicador se evalúa entre el grupo de usuarios de alto riesgo que, al concluir el período de apoyo, aceptan proporcionar al beneficiario retroalimentación segura y anónima. Las nuevas prácticas o herramientas pueden incluir herramientas de comunicación seguras, autenticación de dos factores, prácticas de contraseñas más seguras, o prácticas de detección o notificación de amenazas. "Con éxito" significa que el usuario adopta correctamente una práctica o utiliza una herramienta como parte de sus actividades cotidianas para mejorar su seguridad. Para el denominador, los beneficiarios deben informar el número total de personas que recibieron apoyo en ciberseguridad a través de la subvención y a las que el beneficiario realizó un seguimiento. Para el numerador, los beneficiarios deben informar el número total de personas que, durante el seguimiento, declararon haber utilizado una nueva herramienta o práctica en sus actividades cotidianas para mejorar su seguridad. El sistema de informes de Fluxx utilizará estos dos valores para calcular el porcentaje resultante. Aunque se alienta a los beneficiarios a realizar un seguimiento con la mayor cantidad de usuarios posible, es poco probable que las tasas de respuesta sean del 100 %, por lo que el seguimiento puede realizarse con una muestra. Las potenciales fuentes de datos para este indicador incluyen encuestas de seguimiento, llamadas o entrevistas realizadas por los beneficiarios a los usuarios que reciben apoyo. No obstante, los beneficiarios no tienen la obligación de informar detalles específicos

	sobre las prácticas de los usuarios de alto riesgo que puedan comprometer la seguridad de dichos usuarios.
Porcentaje de usuarios de Internet que declaran sentirse más seguros frente a los daños digitales después de recibir apoyo en ciberseguridad de los beneficiarios, desglosado por numerador y denominador	Porcentaje de usuarios de alto riesgo que dicen sentirse más seguros en línea después de recibir apoyo de los beneficiarios. Este es un indicador de percepción y no una medida directa de la seguridad. Sentirse más seguro en línea incluye tener mayor confianza en su propia capacidad para protegerse, reconocer los riesgos (por ejemplo, estafas, vigilancia, acoso) y responder a las amenazas en caso de que ocurran. Para el denominador, los beneficiarios deben informar el número total de personas que recibieron apoyo en ciberseguridad a través de la subvención y a las que el beneficiario realizó un seguimiento. Para el numerador, los beneficiarios deben informar el número total de personas que, durante el seguimiento, declararon sentirse más seguras en línea después de recibir el apoyo. El sistema de informes de Fluxx utilizará estos dos valores para calcular el porcentaje resultante. Aunque se alienta a los beneficiarios a realizar un seguimiento con la mayor cantidad de usuarios posible, es poco probable que las tasas de respuesta sean del 100 %, por lo que el seguimiento puede realizarse con una muestra. Las potenciales fuentes de datos incluyen encuestas de seguimiento, llamadas o entrevistas realizadas por los beneficiarios a los usuarios que reciben apoyo.
Número de proveedores de apoyo en ciberseguridad que informan cambios positivos en las tendencias de los incidentes entre los	Los proveedores de apoyo en ciberseguridad se definen como beneficiarios que ofrecen capacitación, servicios u otros tipos de apoyo a usuarios de alto riesgo para aumentar su seguridad y protección. Los beneficiarios informan si han observado directamente o recibido informes sobre cambios en la manera en que los usuarios de alto riesgo a los que apoyan experimentan o responden a los incidentes de ciberseguridad.

usuarios de alto riesgo a los que apoyan	Los cambios positivos en las tendencias de los incidentes pueden ser cambios observados directamente por los beneficiarios que indiquen mejoras en la seguridad y protección de los usuarios a los que apoyan, por ejemplo, una menor frecuencia de las solicitudes de apoyo o cambios en la demografía de quienes solicitan ayuda. También pueden reflejar informes que el beneficiario reciba de los propios usuarios a los que apoya sobre una respuesta más rápida, menor impacto, reducción del tiempo de inactividad, menor pérdida de comunicaciones o archivos, restauración más rápida del acceso o la funcionalidad, o menor interferencia con las actividades profesionales habituales. Los beneficiarios deben establecer una definición interna clara de lo que significa "cambio positivo" en su contexto y organizar la recopilación y el análisis de datos en consecuencia.
Indicador cualitativo: ejemplos de personas u organizaciones que responden de manera más eficaz a la violencia de género facilitada por la tecnología después de recibir apoyo en ciberseguridad de los beneficiarios	Este indicador recoge ejemplos reales que muestran cómo las personas u organizaciones han fortalecido su capacidad de prevenir, responder o recuperarse de la violencia de género en línea después de recibir apoyo de los beneficiarios. Como con todos los datos recopilados, los beneficiarios deben adherirse a los principios de confidencialidad, consentimiento informado y no causar daño al recoger ejemplos para este indicador.
Número de usuarios de alto riesgo que recibieron apoyo en ciberseguridad, desglosado por:	Este indicador contabiliza cuántas personas con mayor riesgo de sufrir incidentes de ciberseguridad (por ejemplo, periodistas, activistas, mujeres líderes, actores de la sociedad civil y otras, incluidas aquellas que son blanco de represión digital transnacional) recibieron apoyo directo en ciberseguridad por parte de los beneficiarios. El apoyo

Género (masculino, femenino, otro, desconocido, total) Tipo de apoyo (capacitación, intervención en respuesta a un incidente, otro) Perfil del usuario (periodistas, defensores de los derechos humanos, organizaciones de la sociedad civil, otros)	incluye capacitación (definida como una sesión formal con un objetivo de aprendizaje claro orientado a habilidades o competencias), participación en una respuesta a incidentes (como operar una línea de ayuda) o cualquier otra intervención pertinente. Cuando sea posible, se alienta a los beneficiarios a contabilizar el número de personas únicas que recibieron apoyo durante el período cubierto por el informe. Si la misma persona recibe apoyo varias veces, lo ideal es contabilizarla una sola vez. Las potenciales fuentes de datos incluyen registros de los beneficiarios, bases de datos o listas de asistencia a capacitaciones.
Número de sesiones de apoyo en ciberseguridad realizadas por los beneficiarios, desglosadas por: Tipo de apoyo [capacitación, respuesta a incidentes, otros] País del usuario (autodeclarado)	Este indicador contabiliza el volumen de actividades de apoyo en ciberseguridad realizadas por los beneficiarios durante el período cubierto por el informe. Las “sesiones” se definen según el contexto de las actividades de cada beneficiario y pueden incluir sesiones de capacitación, llamadas telefónicas, chats, tickets relacionados con incidentes, etc. Las potenciales fuentes de datos incluyen registros de los beneficiarios, bases de datos o listas de asistencia a capacitaciones.

[incluida la opción "no especificado"]	
Cantidad de materiales, herramientas o recursos sobre ciberseguridad entregados a usuarios de alto riesgo con apoyo del Fondo	Este indicador contabiliza los materiales o herramientas que los beneficiarios entregan durante el período cubierto por el informe para ayudar a los usuarios a prevenir, responder o recuperarse de amenazas o incidentes cibernéticos. Algunos ejemplos incluyen guías, conjuntos de herramientas, listas de verificación, herramientas digitales y herramientas de comunicación segura. Cada material o herramienta se cuenta una sola vez, sin importar el número de usuarios que lo reciban.

Para las subvenciones que se enfocan en promover una Internet más segura para los grupos vulnerables y las comunidades de alto riesgo, incluidas la sociedad civil y los periodistas (informar únicamente sobre los indicadores aplicables):	
Indicador	**Guía**
Número de debates sobre políticas relacionadas con la ciberseguridad o declaraciones oficiales del gobierno que incorporen recomendaciones o evidencia de los beneficiarios o las	Número de debates sobre políticas o declaraciones durante el período cubierto por el informe que utilicen, analicen o reflejen de otro modo datos, resultados de análisis o investigaciones, directrices o recomendaciones producidas por los beneficiarios (o por las comunidades con las que trabajan) en el marco de esta subvención. "Debates sobre políticas" se refiere a consultas, talleres, mesas redondas, sesiones parlamentarias u otros debates en los que participen formuladores de políticas.

comunidades a las que apoyan	"Declaraciones oficiales del gobierno" se refiere a declaraciones públicas orales o políticas escritas, estrategias, comunicados de prensa u otros documentos relacionados con las políticas de ciberseguridad. Las potenciales fuentes de datos para este indicador incluyen llamadas de seguimiento o entrevistas con las partes interesadas y revisiones de sitios web gubernamentales, documentos de políticas y medios creíbles luego de la difusión de evidencia o recomendaciones.
Número de cambios a nivel del ecosistema en los estándares o las prácticas de las plataformas derivados de los esfuerzos coordinados de los actores del ecosistema en materia de seguridad y protección	Los cambios a nivel del ecosistema son cambios a nivel del sistema, no cambios implementados por una única organización, empresa o persona. "Cambios en los estándares o las prácticas de las plataformas" incluye la adopción de prácticas o protocolos de seguridad nuevos o reforzados, políticas de las plataformas o estándares técnicos que reflejen una respuesta más amplia del ecosistema a los problemas identificados, evidenciados o promovidos a través de esfuerzos coordinados en los que participen los beneficiarios. "Actores del ecosistema" incluye a los beneficiarios y otras partes interesadas relevantes, como organizaciones de la sociedad civil, actores de la comunidad técnica, plataformas, formuladores de políticas, proveedores de servicios y actores del sector privado. Este es un indicador de contribución, no de atribución. No se espera que los beneficiarios demuestren que han sido los únicos responsables del cambio. En cambio, los beneficiarios deben demostrar que existe una relación razonable entre sus esfuerzos y los cambios ocurridos en el ecosistema de ciberseguridad durante el período cubierto por el informe.
Número de prácticas coordinadas o iniciativas de colaboración nuevas o	Los beneficiarios informan el número de prácticas coordinadas o iniciativas de colaboración que empiezan a implementarse ***después*** de poner en marcha las actividades de seguridad o protección financiadas por el Fondo. El objetivo es registrar cualquier fortalecimiento de las

mejoradas implementadas regularmente por múltiples actores del ecosistema como parte de iniciativas de seguridad y protección	redes de colaboración o alianzas globales a las que los beneficiarios consideren razonablemente que sus actividades han contribuido. "Prácticas coordinadas o iniciativas de colaboración" incluye acuerdos entre distintas organizaciones, como el intercambio de información sobre amenazas, procedimientos coordinados de alerta o notificación, flujos de trabajo conjuntos para la priorización o el escalamiento de incidentes, procesos coordinados de divulgación de vulnerabilidades, canales de derivación para obtener asistencia, manuales o procedimientos operativos compartidos y otros mecanismos recurrentes que ayudan a múltiples actores a actuar de manera más alineada y oportuna. "Nueva o mejorada" significa que la práctica se creó o se fortaleció durante el proyecto a través de las actividades de los beneficiarios.
Número de actividades organizadas por los beneficiarios que reúnen a los actores del ecosistema para promover el intercambio de conocimientos y la coordinación relacionados con la promoción de una Internet más segura para todas las personas	Los beneficiarios informan el número de actividades que han organizado durante el período del informe con el apoyo del Fondo y que reúnen a diferentes actores del ecosistema de ciberseguridad (por ejemplo, organizaciones de la sociedad civil, equipos de respuesta a incidentes de ciberseguridad, plataformas y redes) para compartir conocimientos, debatir desafíos y coordinar acciones. Las actividades incluyen talleres, seminarios, reuniones y sesiones de planificación conjunta.

Indicador cualitativo: ejemplos de actividades organizadas por los beneficiarios para una Internet más segura que incluyen la violencia de género facilitada por la tecnología como tema clave y/o que incorporan perspectivas de organizaciones lideradas por mujeres	Los beneficiarios informan y describen brevemente las actividades que han apoyado durante el período del informe y que abordan los riesgos relacionados con el género (por ejemplo, acoso y abuso en línea) o que incluyen perspectivas de organizaciones lideradas por mujeres. Las potenciales fuentes de datos para este indicador incluyen el programa, notas u otros materiales relevantes de la actividad organizada por el beneficiario.
Número de documentos que incluyen recomendaciones y directrices sobre políticas o estándares de ciberseguridad elaborados y difundidos públicamente por los beneficiarios	Este indicador contabiliza los informes, directrices o documentos de política elaborados por los beneficiarios durante el período del informe cuyo objetivo es mejorar las políticas, los estándares o las prácticas de ciberseguridad y que se comparten públicamente o con las partes interesadas pertinentes. "Difundido públicamente" significa que el documento se comparte más allá de la organización (por ejemplo, se publica en un sitio web, se comparte con formuladores de políticas u otras partes interesadas, o se difunde a través de eventos o redes). Por sí sola, la publicación en redes sociales no se considera difusión, salvo que esté acompañada por alguna otra forma de difusión. Un mayor número de productos no implica necesariamente una mejor calidad; la relevancia y la calidad de los productos son igualmente importantes.

Indicador cualitativo: ejemplos de recomendaciones y directrices con perspectiva de género incluidas en los productos sobre políticas de ciberseguridad desarrollados por los beneficiarios	Este indicador recoge ejemplos reales de cómo los beneficiarios incluyen consideraciones de género (por ejemplo, riesgos que enfrentan las mujeres, diseño inclusivo, medidas de protección) en sus recomendaciones o directrices sobre políticas durante el período cubierto por el informe. Las potenciales fuentes de datos para este indicador incluyen extractos de informes o productos de los beneficiarios que muestren recomendaciones con perspectiva de género.