ACCIÓN DE LA UNIÓN 2022 FSI

ISF-2022-TF1-AG-CYBER Cybercrime and Digital investigations

La convocatoria se lanza de conformidad con el Programa de Trabajo 2021-22 para el ISF, y será gestionado por la Comisión Europea, Dirección General de Migración y Asuntos de interior (DG HOME).

La convocatoria cubre el tema: ISF-2022-TF1- AG-CYBER Ciberdelincuencia e investigaciones digitales.

El objetivo de esta convocatoria es financiar proyectos de lucha contra la ciberdelincuencia, incluidas las investigaciones digitales.

A continuación se facilitan los principales datos de la convocatoria extractados de la misma.

1. **Tipos de solicitantes** a los que se dirige la convocatoria son:
   - personas jurídicas (organismos públicos o privados)
   - las organizaciones internacionales son elegibles
   - otros entes podrán participar en otras funciones del consorcio, como socios asociados, subcontratistas, terceros que aporten contribuciones en especie, etc;
   - las personas físicas NO son elegibles (con la excepción de los trabajadores por cuenta propia, es decir, cuando la empresa no tiene personalidad jurídica distinta de la de la persona física)
   - los entes sin personalidad jurídica con arreglo a su legislación nacional podrán participar excepcionalmente, siempre que sus representantes tengan la capacidad de asumir obligaciones jurídicas en su nombre, y ofrecer garantías de protección de los intereses financieros de la UE equivalentes a las ofrecidas por las personas jurídicas;
   - los organismos de la UE (a excepción del Centro Común de Investigación de la Comisión Europea) NO pueden formar parte del consorcio.
   - Asociaciones y agrupaciones de interés — Las entidades compuestas por miembros pueden participar como “beneficiarios únicos” o “beneficiarios sin personalidad jurídica” (si la acción será implementada por los miembros, también deben participar, ya sea como beneficiarios o como entidades afiliadas, de lo contrario, sus costos NO serán elegibles).
   - Países que actualmente negocian acuerdos de asociación: los beneficiarios de países con negociaciones en curso pueden participar en la convocatoria y pueden firmar subvenciones si las negociaciones concluyen antes de la firma de la subvención (con efecto retroactivo, si así lo establece el acuerdo).

2. **Condiciones geográficas**:

Los solicitantes (beneficiarios y entidades afiliadas) deben estar establecidos en cualquiera de los países elegibles:

- Todos los Estados miembros de la UE, excepto Dinamarca, o en un país o territorio de ultramar vinculado a éstos.
- Países no pertenecientes a la UE (no sean Estados miembros): sin limitación alguna, siempre que sea pertinente para la convocatoria de propuestas en vista de sus competencias avanzadas.

3. **Actividades que se financiarán** en el marco de la convocatoria de propuestas:

Las solicitudes de proyectos presentadas en el marco de la presente convocatoria deben abordar al menos una de las siguientes prioridades en el ámbito de la ciberdelincuencia y de las investigaciones digitales:

1. Desarrollar la capacidad operativa y los conocimientos especializados de las autoridades policiales y judiciales y apoyar la cooperación transfronteriza en el ámbito de la ciberdelincuencia, incluida la ciberseguridad cuando esté relacionada;
2. Desarrollo de herramientas de investigación y análisis forense para hacer frente a los problemas planteados por el uso de la encriptación por los delincuentes y su impacto en las investigaciones penales y apoyar la participación de las autoridades policiales en el ámbito de la gobernanza de Internet;
3. Contribuir a la aplicación de la legislación de la UE, teniendo en cuenta en particular las evaluaciones disponibles:
    - De la Directiva 2013/40/UE, de 12 de agosto de 2013, sobre los ataques contra los sistemas de información, en particular, el informe sobre la evaluación del alcance en que los Estados miembros han adoptado las medidas necesarias para cumplir la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y en sustitución de la Decisión marco 2005/222/JAI12 del Consejo,
    - De la Directiva (UE) 2019/713, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, en particular, la evaluación de impacto que acompaña a la propuesta de la Comisión;
4. Fomentar la cooperación transfronteriza entre las autoridades policiales/judiciales y las entidades privadas. Esto incluye, por ejemplo, el establecimiento de mecanismos de apoyo a la cooperación entre los sectores público y privado y mecanismos para mejorar la denuncia de delitos ante las fuerzas del orden.

Las propuestas que se ajusten más estrechamente a estas prioridades serán evaluadas como especialmente pertinentes. Por consiguiente, se invita a los solicitantes a que

examinen detenidamente los vínculos entre su propuesta y las prioridades de la convocatoria.

Las propuestas deben centrarse en las siguientes actividades y resultados:

- Mejora de la capacidad operativa de las autoridades policiales y/o judiciales para investigar los ciberataques y los delitos cibernéticos, por ejemplo mediante técnicas y herramientas de investigación (incluidas las técnicas forenses digitales) centradas en las principales prioridades en materia de amenazas (excluido el material de abuso sexual de menores online, que está cubierto por convocatorias de propuestas específicas), tal como se presenta en la evaluación de EUROPOL sobre la amenaza de la delincuencia organizada en internet 2021.14. Las áreas que los Estados miembros de la UE han identificado como que necesitan una atención especial incluyen: análisis forense digital (forense móvil, forense informático, forense de redes, forense de IoT, incluyendo forense de vehículos), análisis visual de datos, análisis de malware y capacidades de ingeniería inversa, análisis y captura de criptomonedas, almacenamiento eficiente, procesamiento, análisis y transferencia de big data, comprensión y explotación de "inteligencia de amenazas" y metadatos, monitoreo e investigaciones de Darkweb, OSINT
- Mejora de la capacidad operativa de las autoridades policiales y/o judiciales para hacer frente a los retos planteados por la comunicación 5G y su aplicación en el ámbito de la interceptación legal de las comunicaciones, centrándose en las actividades de estandarización pertinentes.
- Mejorar la capacidad operacional de las autoridades policiales y/o judiciales para hacer frente a los problemas que plantea el uso de la encriptación por parte de los delincuentes y sus repercusiones en las investigaciones penales, por ejemplo apoyando el establecimiento, ampliación y desarrollo de puntos de expertos y su conexión en red a escala de la UE o apoyo al desarrollo de una “toolbox” o conjunto de herramientas de técnicas de investigación alternativas para obtener la información necesaria cifrada por delincuentes (con la exclusión de medidas que podrían debilitar el cifrado en general o tener un impacto en un número mayor o indiscriminado de personas)
- Mejora de la capacidad operativa de las autoridades policiales y/o judiciales para la cooperación transfronteriza, por ejemplo apoyando la recopilación y el suministro de pruebas digitales, apoyando la adscripción de funcionarios, mejorando la eficiencia de puntos de contacto policiales permanentes (24/7) contra la ciberdelincuencia y el establecimiento de plataformas específicas
- Mejorar la cooperación entre las entidades privadas y/o las autoridades en el ámbito de la ciberseguridad y las autoridades policiales y/o judiciales, adoptando medidas correctoras, incluso mediante el establecimiento de sistemas adecuados de intercambio de información (o interfaces para hacer un mejor uso de los sistemas existentes)

- Aumentar y mejorar la denuncia de ciberdelitos a las fuerzas del orden
- Proporcionar a las autoridades públicas una imagen precisa del alcance real (es decir, no denunciado) del ciberdelito.

Los proyectos deben aspirar a lograr uno o más de los siguientes resultados:

- aumentar la capacidad operativa de las fuerzas del orden,
- aumentar la disponibilidad de herramientas técnicas para las autoridades policiales,
- aumentar la sensibilización y crear sinergias entre las partes interesadas pertinentes.

Las siguientes propuestas no se consideran pertinentes para la financiación en el marco de la presente convocatoria por estar cubiertas por otros programas de financiación de la UE u otras convocatorias de propuestas, cuando se centren en:

- aumentar exclusivamente el nivel general de concienciación sobre la ciberdelincuencia y las investigaciones digitales, p. ej., cuando se dirige al público en general,
- investigaciones/estudios sin vínculos claros con los resultados operativos,
- material de abuso sexual infantil (CSAM).

Existen consideraciones adicionales aplicables a la presente convocatoria que se deben tener en cuenta (léanse las mismas en la convocatoria completa).

4. El **presupuesto** disponible es de 8 000 000. EUR.
   La DG Home se reserva el derecho de no otorgar todos los fondos disponibles, dependiendo de las propuestas recibidas y los resultados de la evaluación.

5. **Calendario y plazos** (indicativos):
   - Fecha de inicio: 13 Abril 2022
   - Fecha límite de remisión: 15 Septiembre 2022
   - Evaluación: Septiembre-Octubre 2022
   - Selección: Noviembre 2022
   - Firma del Acuerdo de Subvención: Enero 2023
   -

6. **Composición del consorcio** del proyecto:
   Las propuestas deben ser enviadas por:
   - mínimo 2 solicitantes (beneficiarios; no entidades afiliadas) de 2 países elegibles diferentes. Téngase en cuenta que el país de establecimiento de una organización internacional participante no contribuye al cumplimiento del requisito mínimo de composición del consorcio.
   - NO pueden solicitar el puesto de coordinador:

- Entidades con fines de lucro
- organizaciones internacionales, independientemente de su país de establecimiento
- personas jurídicas establecidas en países no pertenecientes a la UE.

7. Duración

Los proyectos deben tener una duración de 24 meses (con posibles prórrogas, si están debidamente justificadas y mediante enmienda).

8. Presupuesto del proyecto.

Los presupuestos de los proyectos (importe máximo de la subvención) deben oscilar entre 500 000 EUR y 3 000 000 EUR.

9. Comunicación y visibilidad

Las propuestas de proyectos deben:

1. Una estrategia de comunicación adaptada que defina:
   - el público destinatario y su segmentación (sexo, edad, educación, profesión, etc.);
   - el ámbito geográfico (qué país/región y qué parte de ese país en particular);
   - los mensajes clave que se utilizarán durante todo el período de ejecución de las actividades y los elementos visuales clave;
   - los canales de comunicación que deben utilizarse en función del público destinatario, garantizando una combinación de medios tradicionales y sociales.
2. Seguimiento y evaluación:
   - proporcionar indicadores clave de rendimiento (KPI - key performance indicators), tanto cualitativos como cuantitativos, con una base de referencia y objetivos que se utilizarán para supervisar la ejecución y evaluar el resultado del proyecto, así como medir los productos y los resultados del proyecto con respecto a los indicadores de rendimiento del programa incluidos en el anexo VIII, Reglamento (UE) 2021/1149, en particular por lo que se refiere a los objetivos específicos del artículo 3(2)(c);
   - prever, en su caso, ajustes de las actividades;
   - tener en cuenta las lecciones aprendidas y las buenas prácticas para acciones futuras.
3. Una estrategia para la sostenibilidad de las actividades, en particular mediante la colaboración con agentes estatales y no estatales, a lo largo de toda la acción, con vistas a compartir conocimientos técnicos y mejores prácticas, aumentar la sensibilización y fomentar la implicación.