ACCIÓN DE LA UNIÓN 2024 FSI

ISF-2024-TF2-AG-Digital – Investigaciones Digitales

La convocatoria se lanza de conformidad con el Programa de Trabajo 2023-25 para el FSI y será gestionado por la Comisión Europea, Dirección General de Migración y Asuntos de interior (DG HOME).

La convocatoria cubre el tema: ISF-2024-TF2-AG-DIGITAL – Acciones en el campo de la ciberdelincuencia y las investigaciones digitales en el marco del Fondo de Seguridad Interior (FSI).

La ciberdelincuencia es una de las prioridades de la UE en la lucha contra la delincuencia grave y organizada como parte de EMPACT 2022 - 2025. Según el informe más reciente sobre evaluación de amenazas de crimen organizado en Internet, el cibercrimen se está volviendo más agresivo y confrontativo. Esto se puede observar en las diversas formas de delito cibernético, incluidas abuso de cifrado, criptomonedas, delitos cibernéticos, fraude en línea, identidad robo y filtraciones de datos. La ciberdelincuencia es un problema creciente para los Estados miembros de la UE, en la mayor parte de la cual la infraestructura de Internet está bien desarrollada y los sistemas de pago digitales y los comerciantes en línea son cada vez más comunes.

En términos más generales, el acceso a los datos y a las pruebas electrónicas representa un persistente desafío para las autoridades encargadas de hacer cumplir la ley en el área de la ciberdelincuencia, pero también en contrarrestar eficazmente otras formas de delincuencia organizada y grave. Varios instrumentos legales existen o se están negociando para facilitar el acceso a la evidencia digital en el marco de las investigaciones penales: nuevas normas de la UE sobre pruebas electrónicas, un segundo protocolo adicional al Convenio de Budapest sobre ciberdelincuencia del Consejo de Europa, un Acuerdo bilateral entre la UE y EE. UU., así como una Convención de la ONU contra el cibercrimen.

La Comisión Europea junto con la Presidencia del Consejo de la Unión Europea Unión Europea ha creado un Grupo de Alto Nivel sobre Acceso Legal a los Datos, que aún no ha finalizado sus trabajos. El Grupo de Alto Nivel centra su análisis en diferentes categorías de datos (datos en reposo en el dispositivo de un sospechoso, datos en reposo en posesión de servicios proveedores, datos en movimiento). El desarrollo de capacidades se identifica como una medida clave para permitir autoridades encargadas de hacer cumplir la ley para realizar investigaciones digitales de manera efectiva.

1. El objetivo de esta convocatoria es financiar proyectos de lucha contra el delito cibernético, incluidos investigaciones digitales, como continuación de diversas iniciativas y planes en el campo, de acuerdo con las prioridades que se recogen en la ficha de la convocatoria.

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

2. Tipos de solicitantes a los que se dirige la convocatoria, siendo entidades legales como:

- 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 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).

3. 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) que tengan un acuerdo operativo con Europol.

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

Las actividades para financiar tienen los siguientes objetivos:

- Desarrollar la capacidad y la experiencia de las autoridades judiciales y policiales y apoyar la cooperación transfronteriza;
- contribuir a la implementación de la legislación de la UE;
- fomentar la cooperación transfronteriza entre autoridades policiales/judiciales y entidades privadas.

Las propuestas deben centrarse en las siguientes **actividades y resultados**:

- Mejorar la capacidad operativa de las autoridades policiales y/o judiciales para investigar los ciberataques y los delitos cibernéticos, por ejemplo mediante formación específica, técnicas y herramientas de investigación (incluido el análisis forenses de dispositivos, de la nube o de automóviles) centrándose en las principales prioridades de amenazas (excluido el material de abuso sexual infantil en línea, que está cubierto por convocatorias de propuestas específicas) tal como se presenta en el informe de evaluación de la amenaza de la delincuencia organizada en internet de Europol 2023. Las áreas que los Estados miembros de la UE han identificado como de especial atención incluyen: análisis forense digital (forense móvil, análisis forense informático, análisis forense de redes, análisis forense de IoT, incluido análisis forense de automóviles), análisis de datos visuales, capacidades de análisis de malware e ingeniería inversa, análisis e incautación de criptomonedas, almacenamiento, procesamiento, análisis y transferencia eficiente de big data y grandes conjuntos de datos, comprensión y explotación de "inteligencia sobre amenazas" y metadatos, monitoreo e investigaciones de Darkweb, OSINT, delitos que involucran el uso de IA por parte de delincuentes.
- Mejorar la capacidad operativa de las autoridades policiales y/o judiciales para abordar los desafíos que plantean el 5G y las comunicaciones basadas en Internet en el ámbito de la interceptación legal, centrándose en las actividades de normalización pertinentes.
- Mejorar las capacidades operativas de las autoridades policiales y/o judiciales para abordar los desafíos que plantea el uso del cifrado por parte de delincuentes y su impacto en las investigaciones criminales, por ejemplo, mediante capacitación y/o apoyo del establecimiento, la ampliación y el desarrollo de puntos de experimentación y creación de redes a nivel de la UE o apoyar el desarrollo de un conjunto de herramientas de técnicas de investigación alternativas para obtener la información necesaria cifrada por delincuentes (con exclusión de medidas que podrían debilitar el

cifrado en general o podrían tener un impacto en un número mayor o indiscriminado de personas).

- Mejorar las capacidades de las autoridades policiales y/o judiciales mediante el uso y/o adaptación de modelos de lenguaje avanzado y soluciones basadas en inteligencia artificial para mejorar el análisis, la traducción y la transcripción de datos.
- Mejorar la capacidad operativa de las autoridades policiales y/o judiciales para cooperar a través de las fronteras, por ejemplo, apoyando la recopilación y el suministro de pruebas digitales, apoyando la adscripción de funcionarios, mejorando la eficiencia de los puntos de contacto (permanentes), 24 horas al día 7 días a la semana, para las autoridades policiales para el delito cibernético, establecimiento de plataformas dedicadas.
- Mejorar la cooperación entre entidades y/o autoridades privadas en el ámbito de la ciberseguridad y las autoridades policiales y/o judiciales, adoptando medidas correctoras, incluido el establecimiento de sistemas adecuados de intercambio de información (o interfaces para hacer un mejor uso de los sistemas existentes).
- Incrementar y mejorar la denuncia de delitos cibernéticos a las autoridades encargadas de hacer cumplir la ley.
- Proporcionar a las autoridades públicas una imagen precisa del alcance real (es decir, incluido el no declarado) del ciberdelito.

No se consideran relevantes para la financiación en el marco de esta convocatoria, por estar cubiertos por otros programas de financiación de la UE u otras convocatorias, las propuestas centradas en:

- Aumentar exclusivamente el nivel general de sensibilización sobre la ciberdelincuencia y las investigaciones digitales, por ejemplo dirigidas al público en general,
- investigación sin vínculos claros con los resultados operativos,
- material de abuso sexual infantil,

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

- aumentar la capacidad operativa y las capacidades de las autoridades policiales y/o judiciales,
- aumentar la disponibilidad de herramientas técnicas para la aplicación de la ley,
- aumentar la conciencia y crear sinergias entre las partes interesadas relevantes.

5. El presupuesto disponible es de 5.000.000 EUR.

La DG Home se reserva el derecho de no otorgar todos los fondos disponibles o de redistribuirlos entre los temas de la convocatoria, en función de las propuestas recibidas y los resultados de la evaluación.

6. Calendario y plazos:

- Fecha de inicio: 30 de abril de 2024.
- Fecha límite de remisión: 5 de septiembre de 2024.
- Evaluación: septiembre-noviembre de 2024.
- Selección: noviembre de 2024.
- Firma del Acuerdo de Subvención: enero de 2025.

7. Composición del consorcio del proyecto:

Las propuestas habrán de presentarse en consorcio con al menos 2 participantes (beneficiarios, no entidades afiliadas) de 2 Estados Miembros distintos.

NO podrán postularse como coordinadoras:

- entidades con ánimo de lucro;
- organizaciones internacionales, independientemente del país donde se establezcan;
- entidades establecidas en países no pertenecientes a la UE.

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

9. El presupuesto para cada proyecto aprobado será de entre 400.000 y 1.000.000 euros (siendo el presupuesto total de 5.000.000 de euros, teniendo en cuenta que se pueden aprobar varios proyectos a la vez).

10. Seguimiento y evaluación

- Las propuestas de proyecto deben proporcionar indicadores clave de desempeño (KPI), tanto cualitativos como cuantitativos, con líneas de base y objetivos que se utilizarán para monitorear la implementación y evaluar el resultado del proyecto, así como medir los productos y resultados del proyecto en comparación con los indicadores de desempeño del programa relevantes para la acción, incluidos en el anexo VIII del

Reglamento (UE) ISF: 2021/1149, en particular en lo que respecta a los objetivos específicos establecidos en el artículo 3.

- Los hitos y entregables de cada proyecto se gestionarán a través del Sistema de Gestión de Subvenciones del Portal y se reflejarán en el Anexo 1 del Acuerdo de Subvención.
    - Los siguientes entregables serán obligatorios para todos los proyectos:
        - Un informe de progreso de mitad de período,
        - Informe de indicadores clave de desempeño.