LII GRUPO DE EXPERTOS PARA EL CONTROL DEL LAVADO DE ACTIVOS
Sesión Virtual Ordinaria de los Subgrupos de Trabajo
16 y 17 mayo 2022

SECRETARÍA DE SEGURIDAD MULTIDIMENSIONAL

INFORME DE AVANCE

Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA

Subgrupo de Decomiso y Cooperación Internacional

2022

INTRODUCCIÓN

El Grupo de Expertos para el Control de Lavado de Activos (GELAVEX), en su en su XXIV Reunión plenaria que tuvo lugar del 7 al 9 de noviembre de 2007, en la ciudad de Santiago de Chile, definió como sus áreas de acción el decomiso, extinción o pérdida de dominio, organismos de recuperación de activos, coordinación e integración entre las unidades de inteligencia financiera (UIF) y los organismos de persecución e investigación, y financiamiento del terrorismo.

El GELAVEX preparó el Plan estratégico para el Trienio 2021-2023 del Grupo en la XLIX Reunión celebrada formato virtual desde Asunción Paraguay el 10 de noviembre de 2020.

La Planificación Estratégica 2020-20231, constituye la pauta para las actividades a desarrollar por el Grupo en este trienio. De acuerdo con la Planificación Estratégica 2020-2023 aprobada, el Subgrupo de Trabajo en Cooperación Internacional y Decomiso trabaja en:

- Impulsar la creación de la Red de Administración de Activos Ilícitos a nivel hemisférico o subregional, con apoyo de la Secretaría Técnica (DDOT);
- Propiciar la creación de un modelo de repartición de bienes, como documento de referencia para los Estados miembros de la OEA;
- Desarrollar un trabajo de identificación y análisis de las herramientas con las que cuentan las oficinas de administración de activos para la gestión de bienes sujetos a decomiso, como bases de datos o programas informáticos para llevar inventarios, a fin de crear un modelo conceptual que tenga un denominador común mínimo de referencia para los Estados a nivel hemisférico, incluyendo directrices para compartir información a nivel externo;
- Desarrollar un estudio sobre la conveniencia de avances en el procesamiento electrónico de solicitudes de cooperación legal internacional en materia de lavado de activos.
- Desarrollar trabajos para favorecer la Cooperación Internacional y Decomiso de Bienes vinculados a nuevas tendencias delictivas asociadas al lavado de activos;
- Desarrollar herramientas para facilitar la cooperación en materia de administración de bienes sujetos a Decomiso.

Para el período 2021-2022, con base en lo anterior el Subgrupo de Decomiso y Cooperación Internacional debe elaborar, entre otros:

[1] Organización de Estados Americanos, Grupo de Expertos para el control del Lavado de Activos (GELAVEX), "Planificación Estratégica 2020-2023", *op. cit.*

- Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA.

Sin duda alguna, la tecnología llegó para la simplificación de la vida. Sin embargo, esto ha conllevado que sea utilizada para la comisión de ilícitos, ya que casi cualquier delito puede cometerse usando o a través de la tecnología. Y sin duda, uno de los usos que se le ha dado a la tecnología es precisamente el lavado de activos. De hecho, en algunos países parece haber existido un repunte durante los dos primeros años de la pandemia del COVID 19.

OBJETIVO GENERAL

El objetivo general de un diagnóstico es realizar un proceso de planeación incluyente y participativo para conocer a determinada situación o problemática de una región y así proponer acciones oportunas al respecto. En el caso del diagnóstico encomendado, su objetivo es precisamente conocer si los Estados miembros de la región cuentan con los requerimientos tanto legales, tecnológicos, humanos y de capacitación para hacer frente a esta forma de lavar activos.

ANTECEDENTES

La Organización de las Naciones Unidad advierte que no existe un concepto uniforme, pero que se puede definir a la ciberdelincuencia como un acto que infringe la ley, que se comete a través de las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, páginas web y tecnología o para facilitar un delito. Tiene la ventaja con relación a los delitos comunes en que no tiene barreras físicas o geográficas y sin duda alguna, se puede cometer de una forma más fácil y veloz, aprovechando el desconocimiento que existe debido a su novedad.

Por su parte EUROPOL distingue la ciberdelincuencia en delitos *dependientes de los medios informáticos* (es decir, «todo delito que solo se puede cometer usando computadoras, redes computarizadas u otras formas de tecnologías de la información y comunicación» y en delitos propiciados por los medios informáticos (es decir, delitos comunes facilitados por Internet y las tecnologías digitales).

Con el objetivo de crear “una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional”, se crea y suscribe el Convenio del Consejo de Europa sobre la Delincuencia Cibernética (Budapest, 2001). Pese a que su origen es europeo, su artículo 37 establece que cualquier Estado que no sea miembro del Consejo de Europa puede convertirse en Parte mediante su adhesión o ratificación, si el Estado está preparado para implementar el convenio.

De acuerdo con la información en el sitio web de la ONU, a junio 2021, 66 Estados ya forman parte del Convenio (países europeos, Argentina, Australia, Canadá, Cabo Verde, Chile, Colombia, Costa Rica, Estados Unidos de América (EUA), Filipinas, Ghana, Israel, Japón, Mauricio, Marruecos, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga, otros 2 países ya lo firmaron (Irlanda y Sudáfrica) y 9 países han sido invitados a adherirse (Benín, Brasil, Burkina Faso, Guatemala, México, Nueva Zelanda, Níger, Nigeria y Túnez).

Este convenio surge como una respuesta ante la ventaja que resulta para la delincuencia organizada transnacional el uso de las tecnologías de información y comunicación, así como de todos los medios tecnológicos que facilitan el uso de servicios financieros. Sirve como una guía para cualquier país que desea desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados parte de él. En el convenio se establecen las medidas que deberán adoptar los países con relación a los delitos cibernéticos, categorizados de la siguiente forma:

1. Delitos contra la confidencialidad, la integridad y la accesibilidad (*Triada CIA*) de los datos y sistemas informáticos:
    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de datos informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso de dispositivos que faciliten la comisión de delitos.
2. Delitos informáticos:
    - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
    - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
3. Delitos relacionados con el contenido:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (copia y distribución de programas informáticos, o la piratería informática).

Adicionalmente y por disposición de lo establecido en su Capítulo III, proporciona un marco legal para la cooperación internacional en materia de ciberdelito y evidencia digital. El convenio establece disposiciones generales y específicas para la cooperación entre las partes, tanto con relación a ciberdelitos como con relación a cualquier delito relacionado con evidencias electrónicas.

Por su parte, la Organización de Estados Americanos (OEA) a través Departamento de Cooperación Jurídica Internacional (DCJI) promueve la cooperación jurídica internacional en materia de justicia y lucha contra la corrupción y el fortalecimiento de la cooperación entre los Estados en materia de asistencia mutua penal y combate de los delitos cibernéticos en el marco de la Reunión de Ministros de Justicia u otros Ministros, Procuradores o fiscales generales de las Américas (REMJA). Adicionalmente, REMJA junto con socios estratégicos procura y coordina capacitaciones para oficiales de gobierno para el enjuiciamiento exitosos de los delitos cibernéticos, talleres legislativos para actualizar las leyes en materia de delito cibernético y para promover mejores prácticas contra los delitos cibernéticos.

.

METODOLOGÍA

De acuerdo con el plan propuesto por la Presidencia del GELAVEX, se realizaron reuniones. Inicialmente, con la Presidencia y Vicepresidencia de GELAVEX y la Secretaría Técnica, para exponer observaciones y consideraciones con relación al tema objeto del trabajo.

Posterior a la reunión, la Secretaría Técnica extendió una cordial invitación a los países de la región y a los invitados al grupo de expertos, atendiendo el llamado los siguientes: Panamá, Uruguay, Colombia, México, Argentina, Perú, Paraguay e INTERPOL.

En la reunión sostenida con las únicas delegaciones que pudieron finalmente acudir al llamado se acordó la necesidad de contar realmente con información de los países de la región,

para que el documento cumpla precisamente de plasmar la realidad de la región en cuanto al tema propuesto.

Es así que se define que la forma más expedita y que representa una menor carga para las delegaciones representadas en el GELAVEX, es la formulación de un cuestionario que permita al subgrupo de trabajo obtener la información necesaria para cumplir con el mandato del plenario respecto al diagnóstico.

Debido a ello se elaboró un borrador del cuestionario que se presentará en la reunión, plenaria. Su propósito es que el grupo de expertos pueda tanto manifestar su satisfacción respecto al abordaje de las preguntas y el contenido esperado, así como presentar sus propuestas de mejora de su redacción y alcance. Esta una acción previa a la solicitud a la Secretaría Técnica para que sea circulado entre las delegaciones, con el fin de ir compilando la información para presentar el informe final en la reunión del GELAVEX del segundo semestre.

Las delegaciones y organismos que estamos trabajando en conjunto para crear este documento, discutiremos nuestras experiencias nacionales y conocimientos internacionales, pero eso no excluirá la eventual solicitud a algunas delegaciones respecto a aspectos importantes del documento en confección.

CUESTIONARIO PROPUESTO

1. ¿Cuenta su país con legislación sobre ciberdelitos? En caso de ser afirmativa su respuesta, por favor aporte en PDF la normativa vigente en su país. En caso de ser no su respuesta, informe si existen proyectos de ley al respecto.
2. ¿Cuenta su país con medidas procesales necesarias que aseguren la investigación y procesamiento de los delitos cibernéticos en forma efectiva, eficaz y oportuna y que permitan la cooperación entre los Estados en el marco de esas mismas actividades? En caso de ser afirmativa su respuesta, indique cuales son las medidas.
3. ¿Cuenta su país con medidas procesales necesarias que aseguren la obtención, incautación, decomiso o secuestro y mantenimiento en custodia todas las formas de evidencias electrónicas y su admisibilidad en procesos judiciales? En caso de ser afirmativa su respuesta, indique cuales son las medidas.

4. ¿Existen en su país estrategias nacionales que incluyan esfuerzos para prevenir, investigar y procesar los delitos cibernéticos? En caso de ser afirmativa su respuesta, indique cuales son dichas estrategias y/o facilite su documentación.
5. ¿Su país se dio su adhesión o ratificó el Convenio de Budapest de 2001? De ser así, facilité por favor la fecha de su ratificación/adhesión y los instrumentos legales en los cuales fueron tipificados los delitos que ella define. Si su respuesta es no, indique si su país tiene proyectada su adhesión.
6. ¿Existe en su país una fiscalía y un ente policial judicial investigador especializado en ciberdelitos? De ser si su respuesta, por favor indique si reciben capacitación y de parte de que instituciones, empresas u organismos internacionales. En caso de ser no su respuesta, por favor indique si existen proyecciones para su conformación.
7. ¿Participa la unidad de inteligencia financiera de su país en la investigación de lavado producto de ciberdelitos?
8. ¿Existen controles en su país con relación a la prevención de lavado de activos producto de ciberdelitos? De ser si su respuesta, por favor indique cuáles son y a cargo de que institución están.
9. ¿Su país está vinculado a la Red de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días (Red G8 24/7)? Si su respuesta es afirmativa, indique la efectividad de su utilización. Si su respuesta es negativa, indique si existe proyección a corto plazo de vincularse.
10. ¿El sector privado, la sociedad civil y la academia aportan, cooperan activamente o forman parte de alguna estrategia, política, protocolo o instrumento nacional para la prevención o represión de la ciberdelincuencia? Comente.