RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/24765 **15/12/2017** **63572**

AUTOR/A: TEN OLIVER, Vicente (GCS)

RESPUESTA:

En relación con las preguntas planteadas, se informa que las criptomonedas (en especial el bitcoin) son, según la Oficina Europea de Policía (Europol), la moneda de elección para gran parte del cibercrimen -como pago por servicios delictivos (compra en darknet de drogas, armas, moneda falsa etc.), para extorsión (ransomware) o para chantajes (pago por vídeos o imágenes íntimas de una persona)-.

No obstante, este medio de pago ilícito usado por los cibercriminales para esa variedad de delitos no es perfecto -debido a que se encuentra en un espacio online limitado, poco sofisticado y con poca variedad-. Además, los cibercriminales están dejando de utilizar el bitcoin por la facilidad de rastreo de transacciones en su blockchain (cadena de bloques).

En este sentido, se indica que la propia estructura tecnológica del bitcoin permite conocer la cantidad de monedas que tiene una determinada cuenta, de dónde han venido y a dónde van (gracias al citado sistema de blockchain). Estas razones, junto a las revelaciones de identidades en los procesos necesarios de operaciones de cambio entre moneda tradicional y criptomoneda, hacen que este sistema no sea totalmente anónimo y, por lo tanto, susceptible de trazabilidad e identificación.

Por otro lado, las instituciones de la Unión Europea llegaron, en diciembre de 2017, a un acuerdo para reforzar el control sobre el uso de monedas virtuales (como bitcoin, ethereum o litecoin), con el objetivo de prevenir su uso en el lavado de dinero y para luchar contra el terrorismo. Entre las medidas acordadas se incluye acabar con el anonimato de las cuentas de este tipo de divisas digitales en Europa.

El acuerdo alcanzado se adoptará formalmente a principios del año que viene. Así, una vez que se publique en el Diario Oficial de la Unión Europea, los Estados miembros tendrán 18 meses para trasponerlo a sus legislaciones nacionales -esto sitúa a final de 2019 o principios de 2020 la entrada en vigor de estas medidas-.

Por otro lado, se señala que no se tiene información que permita deducir que los grupos de crimen organizado estén utilizando criptomonedas para financiar actividades ilícitas. No obstante, sí se ha identificado el uso de estas monedas virtuales para el pago a grupos criminales por extorsiones tipo ransonware y ventas ilícitas a través de internet profundo, así como la utilización de criptomonedas para blanquear el dinero obtenido de sus actividades ilícitas.

Por lo expuesto, se considera que actualmente el papel de las criptomonedas en la financiación de actividades ilícitas dentro del crimen organizado no es importante ya que la criminalidad utiliza mayoritariamente otras fuentes clásicas, basadas en la obtención de beneficios económicos de sus actividades ilegales en papel moneda para refinanciar sus nuevos proyectos criminales.

No obstante, la preocupación es real, por lo que se están llevando a cabo esfuerzos por las Fuerzas y Cuerpos de Seguridad y actuaciones legislativas por parte de los Estados, para no permitir que en el futuro se presente un escenario donde estas monedas virtuales u otros medios basados en las nuevas tecnologías más sofisticados puedan servir para financiar a estos grupos.

Así, Fuerzas y Cuerpos de Seguridad del Estado están potenciando las Unidades de Investigación tecnológicas con medios humanos y materiales para luchar contra el cibercrimen en general, así como las Unidades de Blanqueo de Capitales que, entre sus misiones, investigan las transacciones con monedas virtuales.

Por otro lado, la Estrategia de Seguridad Nacional 2017, aprobada el 1 de diciembre de 2017, profundiza en los conceptos y las líneas de acción definidas en la anterior Estrategia (del año 2013), avanzando en la adaptación de una política de Estado que concibe la seguridad de una forma amplia al servicio del ciudadano y del Estado.

Entre los objetivos generales de la nueva Estrategia de Seguridad Nacional se encuentra la revisión de la Estrategia de Ciberseguridad Nacional -documento sobre el que, desde el año 2013, se asienta la política global de ciberseguridad-, en la cual se establecen las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información.

La Estrategia de Ciberseguridad se basa en 6 objetivos específicos articulados a través de 8 líneas de acción, entre la que cabe destacar la siguiente Línea de Acción 6 *"Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de Investigación, Desarrollo e Innovación en materia de ciberseguridad"*.

Se destaca que, para la consecución de esta Línea de Acción 6, se creó un Grupo de Trabajo, denominado GT 4, que, liderado por el actual Ministerio de Energía, Turismo y Agenda Digital contó con la participación de dos representantes del Ministerio del Interior y cuyo objeto era desarrollar un Plan Derivado en el que se definieran las acciones necesarias para conseguir el objetivo propuesto en dicha línea de acción. Este Plan Derivado cuenta, entre otras, con las siguientes acciones identificadas:

– Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan Estatal de Investigación Científica y Técnica y de Innovación e iniciativas de apoyo a su internacionalización.

– Impulsar la coordinación nacional y la dinamización del sector industrial y de servicios de ciberseguridad para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa, entre otras actividades.

– Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.

Por otro lado, en lo que a Infraestructuras Críticas se refiere, los operadores que han sido designados como "críticos" -la mayoría de ellos pertenecientes al sector privado- tienen, dentro de sus obligaciones, encomendadas a través de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, la elaboración de un Plan de Protección Especifico (PPE) por cada una de las infraestructuras críticas que gestionen.

Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (seguridad física y ciberseguridad). Así, la elaboración de dichos planes supone también un impulso a la industria nacional en lo que a ciberseguridad se refiere ya que, bien los propios operadores o empresas contratadas al efecto, son responsables de gestionar las medidas de ciberseguridad que tengan implementadas en sus instalaciones.

Igualmente, en la normativa anteriormente expuesta, se indica que los PPE deben ser aprobados por el Secretario de Estado de Seguridad, del Ministerio del Interior, previo informe del Centro Nacional de Protección de Infraestructuras Criticas. En relación con este extremo, se indica que actualmente se está llevando a cabo un proyecto que tiene como objeto el desarrollo de una norma de certificación de seguridad integral (incluida la ciberseguridad) de las infraestructuras críticas, que permita otorgar el reconocimiento, garantía, calidad y cumplimiento por parte de los operadores críticos en la protección de aquellos activos críticos nacionales, lo que supondrá un aumento de las capacidades de dichos operadores.

No obstante, en la misma línea, cabe destacar que el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, crea el Esquema Nacional de Seguridad, que siendo de aplicación en la Administración, establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

Dicho Esquema Nacional de Seguridad, desarrollado en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración.

Para finalizar, respecto a la cuestión relativa a la estimación económica, se indica que no se pueden aportar datos precisos ya que ésta es una cuestión difícil de calcular.

Madrid, 24 de abril de 2018