RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/4655 **10/02/2020** **9204**

AUTOR/A: GARCÍA EGEA, Teodoro (GP)

RESPUESTA:

En relación con la pregunta formulada se informa que la delincuencia asociada a las nuevas tecnologías y el cibercrimen continúa en ascenso generalizado a nivel nacional e internacional.

El riesgo de ataques informáticos contra instituciones, personas físicas y jurídicas a gran escala debe ser considerado alto, en relación con otras formas de delincuencia. Esto se viene reflejando tanto por la creciente sofisticación de los ataques cibernéticos detectados como por el incremento progresivo del número de medios físicos conectados a Internet y del volumen creciente de la información sensible y, por tanto, vulnerable almacenada en la "nube": datos personales, datos sobre la salud, las finanzas, etc.

El Gobierno es consciente de esta problemática y la misma ha sido reflejada en la reciente "Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023", que entró en vigor en febrero de 2019. De esta forma, en la Estrategia, al identificar los mercados criminales prioritarios a los que enfrentarse, el cibercrimen se establece como uno de ellos y se constituyen una serie de medidas en forma de líneas de acción para defender a la sociedad en su conjunto frente a esta problemática.

Estas medidas pasan, entre otras, por reforzar la cooperación internacional, bilateral y multilateral con otras regiones y países de interés en materia de ciberdelincuencia, evitando la proliferación de paraísos cibernéticos; potenciar la actuación especializada de las unidades de investigación involucradas en la lucha contra el cibercrimen; favorecer la colaboración entre el sector público y privado; potenciar la actuación contra el cibercrimen con la implicación de las unidades periféricas policiales; reforzar la colaboración con los proveedores de servicios digitales, prestadores de servicios de la sociedad de la información y comercio electrónico, así como empresas tecnológicas, que mejore los sistemas de intercambios de datos; promover una cultura y

conciencia de ciberseguridad en la sociedad, mejorar las acciones de inteligencia e investigación, priorizando la intervención en aquellos ciberdelitos que generan más daño, entre ellos los fraudes y estafas en internet y fomentar la seguridad del comercio en la red (pagos on line) promoviendo un estándar global seguro para las transacciones que posibilite bloqueos de pago como un medio de prevención de fraude y el intercambio de información rápido, a nivel nacional e internacional, ante casos de comisión de ciberdelitos en serie (como las estafas masivas on line).

Madrid, 23 de marzo de 2020