



RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/5277 y 184/5278

21/02/2020

12078 y 12080

AUTOR/A: GARCÍA EGEA, Teodoro (GP)

RESPUESTA:

En relación con las preguntas formuladas, se indica que el Gobierno se remite a lo manifestado por el Ministro del Interior durante el desarrollo de su comparecencia en la sesión de la Comisión de Interior del Congreso de los Diputados, celebrada el pasado 17 de febrero de 2020 (Diario de Sesiones núm. 32), para informar sobre las líneas generales de la política de su departamento (Número de expediente 214/000009).

Además, se indica que la ciberseguridad es una materia que reviste cada vez mayor protagonismo en las agendas de los gobiernos de todas las sociedades avanzadas, debido a sus implicaciones tanto para empresas como para ciudadanos, actores de la sociedad civil y administraciones públicas.

España está en la vanguardia en este campo al haber apostado desde hace tiempo por la elaboración de una Estrategia de Ciberseguridad Nacional, incardinada en la Estrategia de Seguridad Nacional, mediante la cual se ha ido definiendo un marco de actuación para la protección del ciberespacio basado en un conjunto de acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas.

En abril de 2019, el Consejo de Seguridad Nacional aprobó una nueva versión de la Estrategia Nacional de Ciberseguridad con el objetivo de garantizar el uso seguro de redes y sistemas de información y comunicación mediante el fortalecimiento de las capacidades para prevenir, detectar y responder a los ataques cibernéticos, reforzando y adoptando medidas específicas para contribuir a un ciberespacio seguro y confiable.

En relación con el fomento de la investigación en ciberseguridad, cabe destacar que la Estrategia contempla líneas de acción orientadas a este objetivo y señaladamente las siguientes:



- Línea de acción 3: reforzar las capacidades de investigación y persecución de la cibercriminalidad para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.
- Línea de acción 4: impulsar la ciberseguridad de ciudadanos y empresas ofreciendo a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, entre otras medidas.
- Línea de acción 7: desarrollar una cultura de la ciberseguridad, con medidas como impulsar actividades de sensibilización para asegurar que ciudadanos y empresas tienen acceso a información relativa a vulnerabilidades y ciberamenazas, promover la concienciación y formación en ciberseguridad, fomentar el uso seguro de las TIC, y reconocer la colaboración y participación de medios de comunicación, entre otras actuaciones.

Asimismo, cabe reseñar que el Instituto Nacional de Ciberseguridad (INCIBE), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, ha desarrollado numerosas iniciativas en el ámbito de la investigación en ciberseguridad, entre las que destacan:

- La reciente puesta en marcha de la línea telefónica gratuita 017 de ayuda en ciberseguridad para la resolución de consultas de empresas, ciudadanos, padres, menores y educadores en horario de 9:00 a 21:00 horas durante todos los días del año (incluidos sábados, domingos y festivos).
- El servicio gratuito anti ransomware para prevenir, mitigar y denunciar ataques de ransomwar.
- Los avisos, avisos SCI (Sistemas de Control Industrial) y base de datos de vulnerabilidades de INCIBE-CERT, que ofrecen información técnica para la prevención, protección y respuesta ante incidentes de seguridad.
- Las ediciones anuales de Cyberex España e International Cyberex, coordinadas por INCIBE junto con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y la Organización de los Estados Americanos (OEA), para la ejecución de ciber ejercicios que preparan a las empresas para medir y mejorar la gestión de incidentes en términos técnicos y organizativos.
- El Kit de concienciación para empresas, que ofrece materiales formativos y herramientas de entrenamiento para empleados, que permitan prevenir incidentes de ciberseguridad.



- Y, finalmente, las políticas de seguridad para la pyme, un pack completo de documentación que recoge toda la información necesaria para facilitar la puesta en marcha de los procesos internos con los que mejorar su ciberseguridad.

Además, el Ministerio de Asuntos Económicos y Transformación Digital informa de que las tecnologías digitales están brindando grandes oportunidades para los ciudadanos, tanto en su vida social y personal, como en el ámbito económico. No obstante, el advenimiento de la sociedad digital también plantea retos en relación con la garantía de sus derechos en Internet. En este sentido, para alcanzar una adecuada protección de los derechos de las personas en el entorno digital se necesita, entre otras medidas, sensibilizar y concienciar a los usuarios sobre cómo proteger sus datos.

A nivel normativo, cabe reseñar que la Directiva 2016/1148, de 6 de julio de 2016, de seguridad de las redes y sistemas de información –que ha sido transpuesta al ordenamiento jurídico español mediante Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información- establece la obligación de que todos los Estados Miembros de la Unión Europea (UE) adopten una estrategia nacional que incluya objetivos estratégicos y medidas políticas y normativas adecuadas, cubriendo, como mínimo, una serie de aspectos, entre los que se incluyen programas de educación, concienciación y formación relacionados con la estrategia nacional.

En línea con este impulso a nivel europeo, la nueva Estrategia Nacional de Ciberseguridad, adoptada en abril de 2019, pretende garantizar el uso seguro de redes y sistemas de información y comunicación mediante el fortalecimiento de las capacidades para prevenir, detectar y responder a los ataques cibernéticos, reforzando y adoptando medidas específicas para contribuir a un ciberespacio seguro y confiable.

La mencionada Estrategia contiene líneas específicas de acción para fomentar la concienciación de los ciudadanos. Destaca en particular la línea de acción 7, orientada a desarrollar una cultura de la ciberseguridad, con medidas de impulso a actividades de sensibilización. En ella se contemplan acciones para asegurar que ciudadanos y empresas tienen acceso a información relativa a vulnerabilidades y ciberamenazas, medidas de formación en ciberseguridad, así como de fomento de un uso seguro de las TIC, y la promoción de la colaboración y participación de medios de comunicación, entre otras actuaciones.

Todo lo anterior es muestra del firme compromiso del Gobierno con la ciberseguridad y la investigación en esta materia, con vistas a defender los derechos de los ciudadanos en el ciberespacio.

En conclusión, la protección de los datos de los ciudadanos a través de medidas de promoción de una cultura de la ciberseguridad y acciones de concienciación es un tema que ya forma parte de las políticas que está desarrollando el Gobierno en esta



materia y que se consideran de gran importancia para conseguir una efectiva protección de dichos derechos.

Madrid, 24 de marzo de 2020