RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/24371 y 184/24610	**02/10/2020**	**60293 y 60550**
184/24611	**02/10/2020**	**60551**

AUTOR/A: OLONA CHOCLÁN, Macarena (GVOX); UTRILLA CANO, Julio (GVOX); FERNÁNDEZ-ROCA SUÁREZ, Carlos Hugo (GVOX)

RESPUESTA:

En relación con el asunto interesado, se señala que el Gobierno, a través del Centro Criptológico Nacional (CCN), trabaja para contribuir a la mejora de la ciberseguridad en España y con el fin de generar confianza y seguridad en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad. Lleva a cabo diversas iniciativas para proteger el ciberespacio español, relacionadas con los siguientes ámbitos: implementación de la seguridad, formación y concienciación, desarrollo de normativa, elaboración de informes, avisos y vulnerabilidades, detección y respuesta de ciberincidentes, refuerzo de la vigilancia y realización de auditorías.

El CCN-Equipos de Respuesta ante Emergencias Informáticas (CERT), que es la Capacidad de Respuesta a incidentes de Seguridad de la Información del CCN, colabora con los organismos públicos y empresas de interés estratégico nacional en la detección, notificación, evaluación y respuesta de incidentes de seguridad de información o ciberincidentes que puedan sufrir sus sistemas. Este proceso mantiene la confidencialidad entre ambas partes. Actúa además como Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas y como principal coordinador con los organismos adecuados del intercambio de información.

El CCN-CERT informa sobre los incidentes detectados con medios propios (Sistema de Alerta Temprana-SAT y otros), notificados por terceros a través de la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) o notificados por correo electrónico. El CNI (Centro Nacional de Inteligencia) traslada a las autoridades competentes las informaciones y análisis que les permiten la toma de decisiones en sus ámbitos respectivos.

Aunque en algunas fases del ataque se pueda determinar la procedencia de alguna IP, la propia técnica empleada para ocultar su origen real da sus resultados y no es posible determinar una atribución.

No hay constancia de actos de ciberespionaje en el sector sanitario español, ni tampoco con respecto al sector naval, aunque en el pasado ha sido objeto de ciberataques.

Asimismo, se indica que no se tiene constancia de que exista algún acto concreto de ciberespionaje sobre las redes y sistemas de información de NAVANTIA.

En cuanto a la actuación de NAVANTIA contra este tipo de actuaciones, se informa que la sociedad efectúa planes de mejora continua en la vigilancia de sus redes y sistemas en línea con la normativa nacional aplicable. Y, en caso de detectarse cualquier incidente de este tipo, NAVANTIA lo reportaría al Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia.

Madrid, 03 de noviembre de 2020