RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/24612 **02/10/2020** **60552**

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

RESPUESTA:

En relación con la información interesada, se señala que el Instituto Nacional de Ciberseguridad (INCIBE) dispone de un portfolio de servicios destinados a la protección, prevención, respuesta y mitigación de ciberataques y ciberamenazas del sector privado y la ciudadanía. Estos servicios son gratuitos y se encuentran disponibles a través del teléfono gratuito de la Línea de Ayuda en Ciberseguridad 017, los portales www.incibe-cert.es, www.incibe.es y www.osi.es, y las redes sociales asociadas.

Durante el año 2019 se dio soporte a más de 107.000 incidentes de Ciberseguridad[1], y durante el 2020 se han desarrollado capacidades de detección de ciberataques y ciberamenazas que actualmente sirven para procesar más de 10 millones de eventos diarios, enfocados a realizar más de 500.000 notificaciones preventivas al sector privado de posibles riesgos cibernéticos.

El INCIBE lanza además campañas de concienciación anualmente dirigidas al sector privado, organiza ciberejercicios con los principales sectores estratégicos, y proporciona recomendaciones y materiales específicos para el sector industrial y empresarial español.

Adicionalmente, el INCIBE está dinamizando el sector industrial de la Ciberseguridad en España, acercando la oferta a la demanda, con más de 6.000 productos y soluciones de ciberseguridad.

Además, con motivo de la pandemia del COVID-19, el INCIBE ha reforzado sus capacidades y servicios para poder atender más consultas, posibles incidentes y

[1] INCIBE (2019): Balance de ciberseguridad 2019. Más información disponible en: https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2019_incibe.pdf

elaborar campañas de difusión y concienciación que ayuden a contrarrestar posibles amenazas o ataques cibercibernéticos relacionados con el virus y los servicios de la Sociedad de la Información.

Por otro lado, cabe indicar que el 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 la normativa, elaboración de informes, avisos y vulnerabilidades, detección y respuesta de ciberincidentes, refuerzo de la vigilancia y la realización de auditorías.

El CCN-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 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.

Por otra parte, y por lo que se refiere al ámbito de competencias del Ministerio del Interior, se informa que la colaboración con el sector privado en la materia se ve plasmada de forma destacada a través de la celebración periódica de la “Mesa de Coordinación NIS”, foro que reúne a los representantes de los Sectores Estratégicos en

materia de protección de infraestructuras críticas y servicios esenciales, y que actúa como mecanismo de cooperación y enlace directo del Estado con el sector privado.

Adicionalmente, desde el Ministerio del Interior se están fomentando y llevando a cabo acciones de colaboración con el sector privado, como es la elaboración de guías y manuales de buenas prácticas en materia de ciberseguridad, documentos en los que se constata la colaboración entre la Administración y el sector privado.

Asimismo, en el marco del Consejo de Seguridad Nacional se ha constituido el Foro Nacional de Ciberseguridad, con la finalidad de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y los desafíos y amenazas en el ciberespacio.

Ese Ministerio no ha cuantificado el monto presupuestario dedicado a la colaboración público-privada en materia de seguridad, ya que no se corresponde con una partida o programa presupuestario de gasto concreto.

Madrid, 05 de noviembre de 2020