RESPUESTA DEL GOBIERNO

184/65653 **14/10/2021** **162349**

AUTOR/A: MARTÍNEZ GRANADOS, María Carmen (GCs); MUÑOZ VIDAL, María (GCs)

En relación con la pregunta de referencia, se informa de que la Secretaría de Estado de Digitalización e Inteligencia Artificial tiene adscritos dos organismos con competencias en materia de ciberseguridad: el Instituto Nacional de Ciberseguridad (INCIBE) y la Secretaría General de Administración Digital (SGAD).

De forma simplificada, la estructura en materia de ciberseguridad a nivel nacional está compuesta por cuatro niveles: político, estratégico, operativo y técnico, teniendo estos dos organismos competencias fundamentalmente de carácter operativo y técnico.

No obstante, cabe señalar que las instituciones públicas españolas tienen mecanismos de respuesta contra posibles ciberataques, ya que cuentan con numerosas herramientas que ya están en marcha.

Además, la evolución y sofisticación constante de las amenazas procedentes del ciberespacio obliga a un trabajo constante en la mejora de los sistemas de protección para que se minimicen los riesgos, lo que obliga a poner en marcha nuevas medidas a corto y medio plazo.

En la madrugada del 9 de junio de 2021 se produjo un ciberataque mediante *ransomware* en la red del Ministerio de Trabajo y Economía Social. El alcance del impacto del incidente y su complejidad han contribuido a aportar un valioso conocimiento y experiencia en los protocolos de comunicación, reacción y recuperación, así como en el modo de operación conjunto aplicable para la actuación ante posibles incidentes y para el futuro Centro de Operaciones de la Administración General del Estado y sus Organismos Públicos. De forma coordinada con los principales responsables de las distintas áreas TIC se establecieron las siguientes líneas de actuación:

– Contención de la amenaza.

– Investigación del incidente.
– Recuperación de la información y servicios.
– Auditoría.

En cuanto se detectó el incidente, conforme a lo previsto en el Esquema Nacional de Seguridad para este tipo de casos, se pusieron en marcha, de inmediato, las acciones de contención, a las que siguieron las de detección, mitigación, recuperación y prevención. En estas acciones colaboraron con el órgano afectado la Secretaría General de Administración Digital y el CCN-CERT, la capacidad de respuesta ante incidentes de seguridad del Centro Criptológico Nacional, prevista en el citado Esquema Nacional de Seguridad.

Por otro lado, en lo que respecta a nuevas medidas de refuerzo frente a ciberincidentes adoptadas, debe indicarse que el Consejo de Ministros acordó la puesta en marcha de un paquete de actuaciones materia de ciberseguridad con el objetivo de reforzar de manera inmediata las capacidades de defensa frente a las ciberamenazas sobre el sector público y sobre las entidades que suministran tecnologías y servicios al mismo.

El acuerdo incluye la adopción de un Plan de Choque de Ciberseguridad, la actualización del Esquema Nacional de Seguridad y la promoción de medidas para aumentar el nivel de ciberseguridad de los proveedores tecnológicos del sector público estatal.

Estas actuaciones reforzarán con eficacia la capacidad de prevención, detección, protección y defensa frente a la materialización de las ciberamenazas. Además, se vela porque la transformación digital vaya acompañada de medidas organizativas y técnicas de seguridad proporcionadas a los riesgos, lo que favorece la confianza en el uso de tecnologías digitales por parte de los actores económicos y la ciudadanía.

La segunda actuación del paquete de medidas acordado por el Gobierno es la actualización del Esquema Nacional de Seguridad, que data de una etapa con un contexto normativo, social y tecnológico que ha sufrido una evolución radical. Para ello se tramitará y aprobará de manera urgente un real decreto que sustituya al 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.

El Esquema Nacional de Seguridad (ENS) ofrece un planteamiento común de principios básicos, requisitos mínimos, medidas de protección, y mecanismos de conformidad y monitorización, adaptados al cometido del Sector Público para la gestión continuada de la seguridad para la Administración Digital.

El ENS es un esquema de aplicación a las entidades del Sector Público e indirectamente, a las entidades del Sector Privado que colaboren con aquellas en la prestación de servicios públicos. Es un instrumento esencial para que la administración digital sea robusta y confiable.

La tercera actuación consiste en promover e incentivar la adopción de sistemas, estándares y políticas de gestión de seguridad en el sector privado, en particular, aumentando el nivel de ciberseguridad de los proveedores tecnológicos del Sector Público estatal ante la evidencia de que la ciberseguridad de un organismo también está condicionada a la de sus proveedores tecnológicos.

De manera simultánea a la puesta en marcha del paquete de actuaciones urgentes en materia de ciberseguridad, se ejecuta la implantación del Centro de Operación de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS).

Por otra parte, se señala que el encuentro celebrado en el marco del Consejo de Seguridad Nacional de Estados Unidos sí ha contado con presencia del Reino de España, al integrarse en la representación de la Unión Europea como Estado miembro.

Además, se remarca que la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior, mantiene un contacto fluido y estrecho con sus homólogos estadounidenses en relación a la ciberseguridad y, especialmente, respecto a la problemática de los ataques *ransomware* a sistemas de información.

En este sentido, a lo largo de los últimos meses se han mantenido reuniones de trabajo con agencias de los Estados Unidos de cara al intercambio de prácticas y medidas en materia de ciberseguridad y cibercriminalidad, así como en la búsqueda de vías de intercambio de información y colaboración.

Por último, cabe indicar que desde el Ministerio del Interior se ha puesto en marcha a lo largo de este año 2021, el Plan Estratégico contra la Cibercriminalidad, focalizado en potenciar las capacidades del Ministerio del Interior para detectar, prevenir, proteger, responder y perseguir la cibercriminalidad. Con este plan se busca generar un impulso operativo y técnico eficaz que garantice la protección de los derechos y libertades y la seguridad ciudadana.

Madrid, 17 de noviembre de 2021