RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/12142 **07/05/2020** **27301**

AUTOR/A: MATEU ISTÚRIZ, Jaime Miguel (GP); ÁLVAREZ FANJUL, Beatriz (GP); BELTRÁN VILLALBA, Ana María (GP); ROJAS GARCÍA, Carlos (GP); MONTESINOS AGUAYO, Pablo (GP); SANTAMARÍA RUIZ, Luis (GP); JIMÉNEZ-BECERRIL BARRIO, María Teresa (GP); HISPÁN IGLESIAS DE USSEL, Pablo (GP); BORREGO CORTÉS, Isabel María (GP); VÁZQUEZ BLANCO, Ana Belén (GP)

RESPUESTA:

En relación con la pregunta formulada, y por lo que se refiere al ámbito de competencias del Ministerio del Interior, se informa que a partir de la información aportada por los equipos de respuesta a incidentes de seguridad (CSIRT) nacionales de referencia a la Secretaría de Estado de Seguridad, los Operadores de Servicios Esenciales del sector salud sufrieron 1 incidente en el mes de marzo y 0 incidentes en el mes de abril.

En este sentido, cabe informar que el Gobierno articula, a través de las autoridades competentes, los CSIRT nacionales de referencia y las Fuerzas y Cuerpos de Seguridad del Estado, diferentes medidas de carácter operativo y estratégico para la mejora de la resiliencia en el sector sanitario. Entre ellas destacan:

- La articulación de mecanismos legales para que los hospitales que presten servicios esenciales notifiquen incidentes que sufran en su infraestructura tecnológica al Centro Nacional de Protección de Infraestructuras y Ciberseguridad, ante los riesgos asociados a los mismos y la necesidad de intervención estatal en la respuesta a incidentes.

- El establecimiento de canales de comunicación seguros y cifrados con los responsables de seguridad de la información de Operadores de Servicios Esenciales (Aplicación móvil segura AlertPIC del Centro Nacional de Protección de Infraestructuras y Ciberseguridad). A través de esta aplicación se remite información (alerta temprana, información de vulnerabilidades, informes técnicos de análisis de malware, etc.) diariamente para incrementar

la resiliencia de redes y sistemas en infraestructuras sanitarias críticas. En este sentido, y de forma especial, se ha remitido información relevante acerca de tipologías de ataques ransomware (RagnarLocker, SaveTheQueen, Snake, Trickbot/Ryuk/Emotet, etc.) incluyendo buenas prácticas e Indicadores de Compromiso de amenazas más relevantes.

- Puesta a disposición de los Equipos de respuesta nacionales (CCN-CERT e INCIB-CERT), con reserva de capacidades técnicas de respuesta para el apoyo en el caso de que un organismo presente un incidente.

- Investigación y persecución de infracciones delictivas por parte de Fuerzas y Cuerpos de Seguridad del Estado de aquellos incidentes que presenten caracteres de delito conforme la legislación penal.

Madrid, 11 de junio de 2020