



RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/12141

07/05/2020

27300

AUTOR/A: BELTRÁN VILLALBA, Ana María (GP); MATEU ISTÚRIZ, Jaime Miguel (GP); MONTESINOS AGUAYO, Pablo (GP); ROJAS GARCÍA, Carlos (GP); HISPÁN IGLESIAS DE USSEL, Pablo (GP); VÁZQUEZ BLANCO, Ana Belén (GP); JIMÉNEZ-BECERRIL BARRIO, María Teresa (GP); ÁLVAREZ FANJUL, Beatriz (GP); SANTAMARÍA RUIZ, Luis (GP); BORREGO CORTÉS, Isabel María (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 solo a lo largo del mes de marzo se ha detectado un incremento del más del 20% en el número de incidentes a operadores de servicios esenciales notificados al Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) respecto al mes anterior.

En este sentido, hay que tener en cuenta que el incremento de tráfico a través de las infraestructuras tecnológicas se ha incrementado de forma significativa a lo largo del periodo de confinamiento de la población. El CNPIC, como autoridad competente mediante el uso de los canales de comunicación seguros y cifrados (aplicación móvil segura AlertPIC del CNPIC), y a través de los responsables de seguridad de la información de Operadores de Servicios Esenciales, apoyó a las empresas más vulnerables, y al conjunto de la sociedad, facilitando información -alerta temprana, información de vulnerabilidades, informes técnicos de análisis de malware, etc.- diariamente para incrementar la resiliencia de redes y sistemas, en especial en todo aquello relativo a las medidas de seguridad en el teletrabajo y riesgos asociados a redes VPN y protocolos Remoto Desktop Protocol (RDP), principales vectores de entrada de ataques.

Además, para la protección de las empresas, mucho más expuestas a la cibercriminalidad debido a la crisis del COVID 19, ante las nuevas circunstancias de teletrabajo, en el ámbito de la Policía Nacional se están adoptando las siguientes medidas:



- Monitorización de la colaboración ciudadana.
- Desarrollo de campañas de información a la población en general.
- Mantener comunicación permanente con organismos nacionales de ciberseguridad y organizaciones supranacionales de cooperación policial.
- Recolectar inteligencia de fuentes abiertas.
- Desarrollar investigaciones operativas de las organizaciones que se encuentran detrás de estas actividades delictivas para su desmantelamiento.

Madrid, 11 de junio de 2020