

PERSISTEN INTERROGANTES RESPECTO DE LA INFORMACIÓN PRESENTADA POR LA SSPC SOBRE LA ADQUISICIÓN Y USO DE PEGASUS

- *Debe aclararse qué elementos existen para acreditar la simulación del objeto de contratos para la adquisición de Pegasus.*
- *El Gobierno Federal no ha proporcionado información respecto a contrataciones realizadas por la Secretaría de Defensa Nacional, a pesar de que existe evidencia de que adquirió Pegasus.*
- *Es necesario indicar las razones por las que el CNI se ha negado a entregar los contratos suscritos por el CISEN a la fecha.*
- *La información publicada por la SSPC excluye información relevante como anexos técnicos, investigaciones de mercado, entre otros requeridos por ley.*

En atención a la [presentación](#) e información divulgada por la Secretaría de Seguridad y Protección Ciudadana, Rosa Icela Rodríguez, en la [conferencia de prensa matutina del 28 de julio de 2021](#), valoramos positivamente la muestra de compromiso con el esclarecimiento de la contratación y uso ilegal de la herramienta de espionaje *Pegasus*.

Como lo solicitamos desde 2017, la apertura de los expedientes de contratación es relevante para el esclarecimiento del caso, incluida la posible corrupción, por lo que siendo un paso relevante, es necesario asegurar la máxima transparencia respecto de todas las instituciones contratantes u operarias del sistema.

En este sentido, a partir de la información publicada persisten interrogantes y surgen nuevas respecto de los esquemas utilizados por gobiernos anteriores para adquirir y operar *Pegasus*. A continuación, precisamos algunas cuestiones que resulta importante dilucidar para favorecer el esclarecimiento del caso y garantizar el derecho a la verdad de las víctimas y de toda la sociedad mexicana:

1. En la presentación se asume que cualquier contrato realizado con empresas que forman parte del mismo entramado —como KBH Aviation S.A. Comercializadora de Soluciones Integrales Mecale S.A. de C.V., Proyectos y Diseños VME S.A. de C.V., Comercializadora Antsua S.A. de C.V., entre otros— corresponde a la contratación de licencias de uso del sistema de espionaje *Pegasus*. De esta manera, se sugiere que existió una simulación en el objeto de contratos que oficialmente aparentan referirse a la compra de insumos como medicamentos o uniformes, pero que en realidad corresponden a la adquisición de licencias de uso del malware *Pegasus*.
 - a. **¿La sugerencia descrita parte de una suposición o el Gobierno Federal cuenta con elementos para acreditar que la compra de insumos diversos no sucedió y que dichas dependencias adquirieron u operaron el malware *Pegasus*?**
2. El Gobierno Federal no ha proporcionado información respecto a contrataciones realizadas por la Secretaría de Defensa Nacional (SEDENA), a pesar de que existe evidencia de que dicha dependencia adquirió el sistema *Pegasus* a través de contratos con la empresa Security Tracking Devices S.A. de C.V. Así mismo, existe evidencia de al menos 23 contratos, entre

2015 y 2018, con empresas parte del entramado con que se adquirió el malware *Pegasus* por parte de otras dependencias, como la Agencia de Investigación Criminal (AIC) de la Procuraduría General de la República (PGR) y del Centro de Investigación y Seguridad Nacional (CISEN).

- Contratos entre SEDENA y Security Tracking Services S.A. de C.V. en 2011
 - No. 4500006718
 - No. 4500006876
 - No. 4500006908
 - No. 4500000147
 - No. 4500000525
 - Contratos entre SEDENA y empresas parte de la red involucrada en la adquisición de *Pegasus*
 - KBH Track S.A. de C.V.
 - > 4 contratos en 2016
 - > 1 contrato en 2017
 - Proyectos y Diseños VME S.A. de C.V.
 - > 16 contratos en 2016
 - > 1 contrato en 2017
 - Air Cap S.A. de C.V.
 - > 1 contrato en 2018
- a. **¿El Gobierno Federal también publicará toda la información relacionada a estos contratos y otros no reportados hasta ahora?**
3. En la página web denominada [“Transparencia Pegasus”](#), publicada en la página web de la Secretaría de Seguridad y Protección Ciudadana (SSPC), se hace una relación de contratos y montos. Sin embargo, respecto de los cuatro contratos detectados relacionados al Centro de Investigación y Seguridad Nacional (CISEN) se indica que “A LA FECHA EL ÓRGANO DESCONCENTRADO NO HA PROPORCIONADO LOS CONTRATOS”.
- a. **¿El Centro Nacional de Inteligencia se ha negado a publicar los contratos o solamente existe una demora en la entrega de la información?**
4. La información publicada por la SSPC se refiere casi exclusivamente a los contratos, pero excluye otra información relevante en los expedientes de contratación como los anexos técnicos, la investigación de mercado, la acreditación de los criterios en los que se funda la selección del procedimiento de adjudicación directa y la justificación de las razones para el ejercicio de la opción elegida, como es requerido por la Ley. Además, en los documentos publicados persisten porciones testadas, como el nombre de los funcionarios públicos involucrados.
- a. **¿Se publicarán y entregarán a la Fiscalía General de la República (FGR) los expedientes completos o únicamente la información publicada?**
- b. **¿Los documentos enviados a la FGR también se encuentran testados o se ha proporcionado la información completa?**

- c. **¿Se ha identificado si funcionarios públicos involucrados en la contratación u operación del malware *Pegasus* en gobiernos anteriores permanecen en el Gobierno Federal o en otras dependencias federales o locales?**
- d. **¿Se han identificado los expedientes con la información de las víctimas obtenida a través del sistema *Pegasus*?**

Como hemos expresado previamente, reiteramos nuestro deseo y disposición en colaborar en la implementación de los compromisos asumidos públicamente por el Gobierno Federal para garantizar la no repetición de los deleznable hechos de espionaje documentados, incluyendo el esclarecimiento total de la contratación, uso ilegal y encubrimiento relacionado al malware *Pegasus*, así como en el diseño e impulso de una agenda de reformas que establezcan controles democráticos a la adquisición, uso y rendición de cuentas respecto de herramientas tecnológicas susceptibles de representar riesgos para la privacidad de la población, de manera que se garantice que ningún gobierno, de cualquier nivel, presente o futuro, pueda volver a hacer un despliegue de autoritarismo semejante.

Atentamente,

ARTICLE 19, Oficina para México y Centroamérica

R3D: Red en Defensa de los Derechos Digitales

SocialTIC

CONTACTO PARA PRENSA:

Iván Martínez

55 5504 1636

contacto@r3d.mx

Juan Vázquez

55 4588 1166

jvazquez@article19.org