



# Se multiplican intentos de ciberataques contra Pemex

**EVERARDO MARTÍNEZ**

—[cartera@eluniversal.com.mx](mailto:cartera@eluniversal.com.mx)

Los intentos de ciberataques contra Petróleos Mexicanos (Pemex) se multiplicaron más de tres veces en el bienio 2022-2023, según cifras obtenidas vía Transparencia.

Los datos muestran que duran-

# 1,904

**MILLONES DE INTENTOS**

de ciberataques reportó Pemex en el periodo 2022-2023.

te ese periodo la petrolera estatal acumuló un total de mil 904 millones de intentos de vulnerar sus sistemas informáticos, un crecimiento de 236% en comparación con el periodo 2020-2021, lo que se tradujo en 2 millones 608 mil tentativas por día.

**| CARTERA | A26**



PERIÓDICO

PÁGINA

FECHA

SECCIÓN

 EL UNIVERSAL

PP-26

22/04/2024

LEGISLATIVO

# Intentos de ciberataques contra Pemex crecen 236%

Datos obtenidos vía Transparencia indican que **en el bienio 2022-2023 la petrolera sufrió 2 millones 608 mil tentativas por día**; experto ve peligro para soberanía y pide fortalecer su seguridad informática



## EVERARDO MARTÍNEZ

—[cartera@eluniversal.com.mx](mailto:cartera@eluniversal.com.mx)

A los problemas que enfrenta Petróleos Mexicanos (Pemex) en materia financiera, ordeña de ductos, litigios, accidentes, derrames y retrasos en obras, se suman los intentos de ciberataques que en el bienio 2022-2023 se multiplicaron más de tres veces, de acuerdo con cifras obtenidas por EL UNIVERSAL vía Transparencia.

En esos dos años, la empresa acumuló mil 904 millones de intentos de ciberataques, con un crecimiento de 236%, y significaron 2 millones 608 mil casos por día.

En tanto, entre 2020 y 2021 registró 565 millones de intentos de vulnerar sus sistemas, lo que equivalió a 775 mil casos cada día.

En el último bienio de la administración pasada se reportaron apenas 121 millones de ciberataques, es decir, 165 mil diariamente entre 2017 y 2018. Si bien en 2023 los casos reportados por la petrolera disminuyeron respecto a 2022, pasando de mil 135 millones de intentos a 769 millones, la empresa vive bajo amenaza de ciberdelincuentes.

La petrolera padece constantemente de amenazas a sus sistemas, y de acuerdo con su unidad de transparencia, “los ciberataques no han causado una pérdida en Pemex”.

### Seguridad nacional

Juan Manuel Aguilar Antonio, vicepresidente de Ciberseguridad en el Consejo de Datos y Tecnologías Emergentes (Cdetech), destacó la importancia de que Pemex fortalezca su seguridad cibernética.

“Sus sistemas son altamente susceptibles de ser robados. Hay un alto potencial de riesgos de seguridad nacional y de robo de información de sus proveedores, clientes y su infraestructura como son los gasoductos que son importantes para las redes de robo de combustibles o huachicoleo.

“Incluso, dependiendo del grado de digitalización de Pemex, si se pierde por ejemplo el control del SCADA, para monitorear y controlar ductos, hasta puede sufrir un cierre parcial de operaciones. Un *ransomware* (extorsión cibernética) a gran escala puede tener costos directos a la población, daño en su



reputación y a la soberanía del país”, dijo el también investigador de la UNAM.

Pemex fue consultado para conocer más detalles sobre estos intentos de robos y qué tipo de ataque están reportando, pero la petrolera no ha compartido información adicional.

### **Incidente grave**

Pese a que los casos de ciberataques exitosos que ha hecho públicos la petrolera son pocos, uno tuvo cobertura a escala internacional en 2019. Se trató de un evento de *ransomware*.

En noviembre de ese año, piratas informáticos vulneraron la seguridad de Pemex, una de las mayores empresas del país, y pidieron el equivalente a 4.9 millones de dólares para rescatar la información.

En ese momento, las autoridades señalaron que no pagarían por el rescate. Sin embargo, bajo el argumento de que se trataba de un asunto de seguridad nacional, la petrolera encabezada por Octavio Romero Oropeza decidió reservar la información por cinco años —los cuales se cumplen en enero próxi-

mo—, ante las solicitudes recibidas vía transparencia sobre el caso.

Sobre ese incidente, el sitio especializado Bleeping Computer publicó que con el ataque se afectó 5% de los sistemas de cómputo de la petrolera.

La operación se habría realizado con el *ransomware* DoppelPaymer, el cual encripta la información del usuario de un determinado sistema y pide un rescate millonario para liberar los datos.

El caso volvió a cobrar relevancia cuando la Auditoría Superior de la Federación (ASF) informó en sus fiscalizaciones de 2019 y 2020 que la petrolera aún mostraba vulnerabilidad en sus sistemas, lo que aumenta el riesgo de un incidente de seguridad informática que podría ocasionar un impacto negativo en los activos de información y en sus procesos de negocios.

### **Estrategia de defensa**

En julio de 2023, Pemex puso en



operación su Centro de Datos Principal, ubicado en la Ciudad de México, para enfrentar los ataques de *hackers* y con el propósito se proteger sus datos y dejar de tercerizar dicha labor.

“Pemex sufre 100 mil millones de ataques al año, es una barbaridad, un número impensable, y este centro nos va a dar muchísima seguridad, que es lo que requiere una empresa del tamaño de Petróleos Mexicanos”, dijo en ese momento Romero Oropeza.

En ese momento, el funcionario dijo que se reduciría el gasto en ma-

teria de ciberseguridad de 2 mil 100 millones de pesos al año a sólo mil millones de pesos.

Al inaugurar ese centro, Brenda Fierro, subdirectora de Tecnologías de la Información de Pemex, destacó que en esa instalación la petrolera cuenta con más de 400 aplicaciones de negocio, 32 de las cuales son críticas, así como el resguardo de 16 petabytes de información. También se implementaron 70 servidores que equivalen a más de mil 200 servidores virtuales para las actividades críticas de la empresa. ●

### JUAN MANUEL AGUILAR

Vicepresidente de Cdetech

“Los sistemas de Pemex son altamente susceptibles de ser robados. Hay alto potencial de riesgos de seguridad nacional y de robo de información”

“Dependiendo del grado de digitalización de Pemex, si se pierde por ejemplo el control del SCADA, para monitorear y controlar ductos, hasta puede sufrir un cierre parcial de operaciones”

**EL DATO**

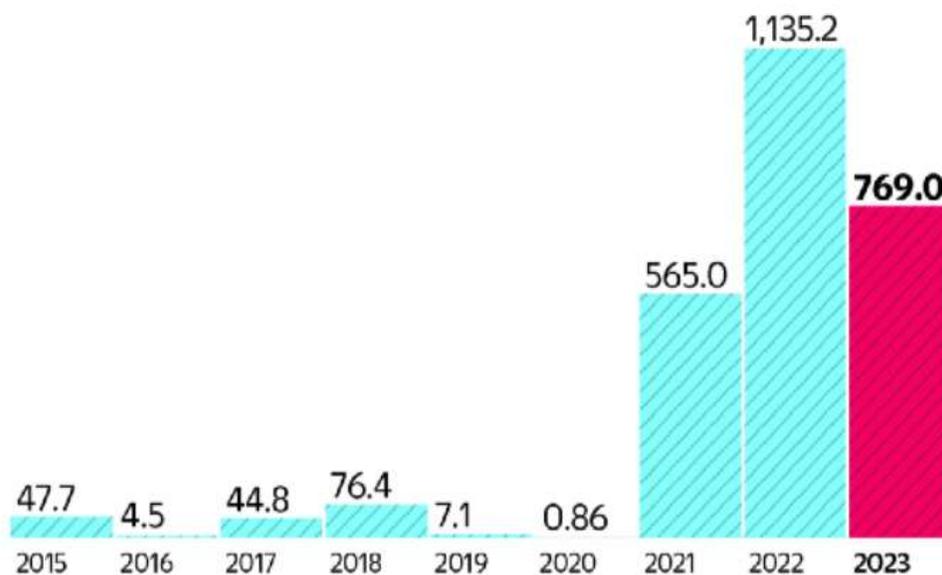
Entre 2020 y 2021, Pemex registró 565 millones de intentos de vulnerar sus sistemas, lo que equivalió a 775 mil casos cada día.

## Al asedio de *hackers*

Estas agresiones implican un golpe económico muy alto para los organismos que las sufren.

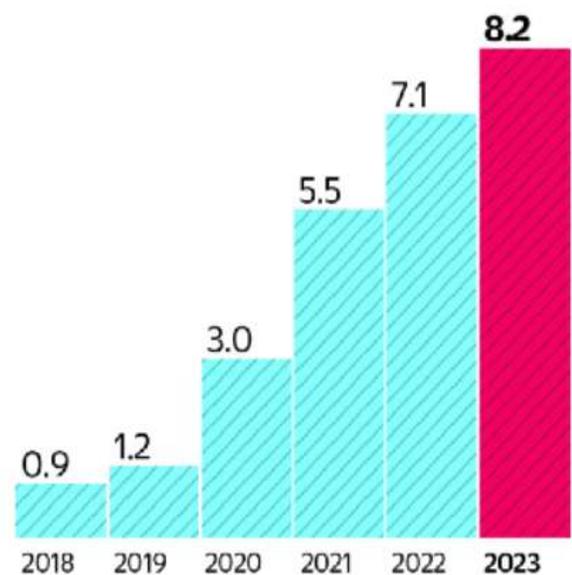
### Intentos de ciberataques contra Pemex

Millones de casos



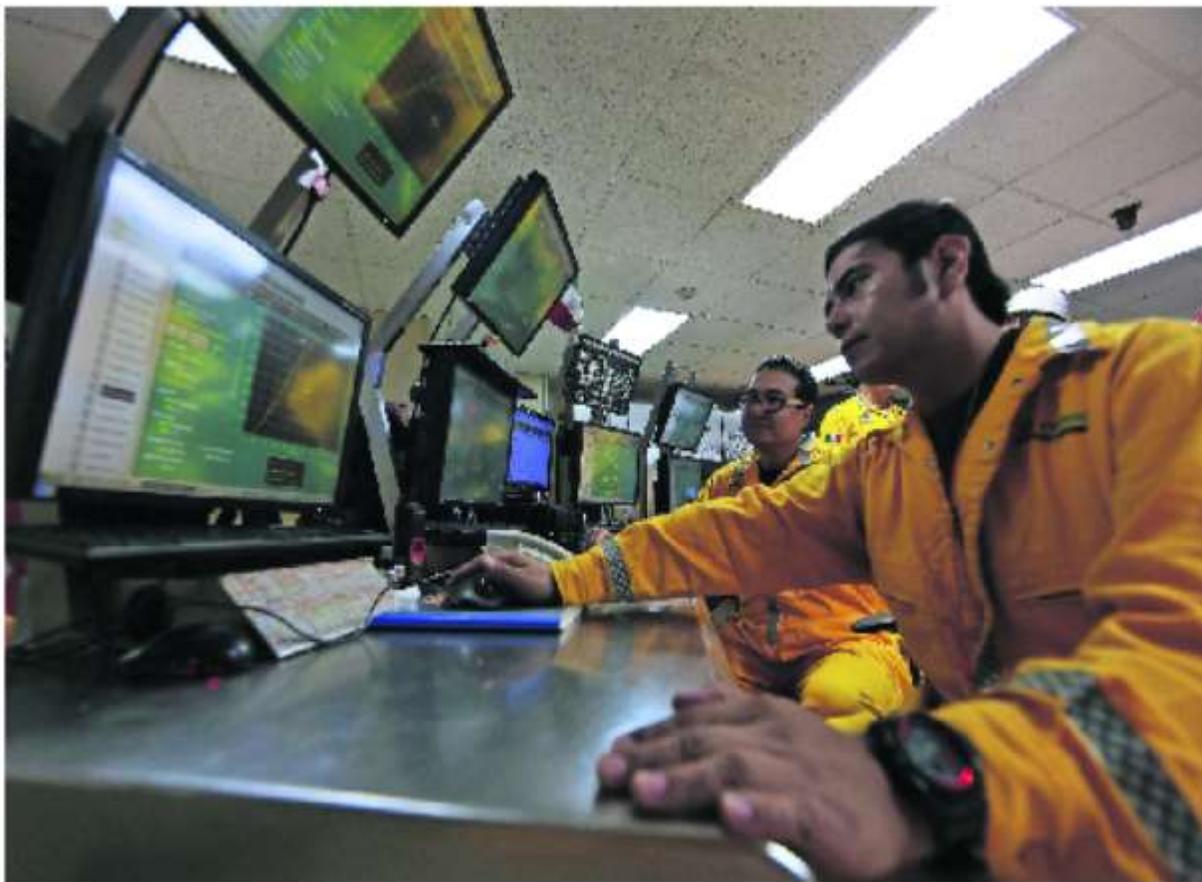
### Costo mundial del cibercrimen

Billonnes de dólares





ARCHIVO EL UNIVERSAL



Si Pemex pierde por ejemplo el control para monitorear ductos, puede sufrir un cierre parcial de operaciones, opina un especialista.