LITORALPRESS

Fecha: 11-07-2025
Medio: La Tercera
Supl. : La Tercera
Tipo: Noticia general
Título: Error 404: el hackeo que mantuvo en vilo por 12 días al Instituto de Salud Pública

Pág. : 27
Cm2: 734,0

Tiraje: 78.224
Lectoría: 253.149
Favorabilidad: No Definida

Error 404: el hackeo que mantuvo en vilo por 12 días al Instituto de Salud Pública

El ataque cibernético paralizó funciones clave del ISP, forzó la liberación excepcional de productos en Aduanas y reactivó la preocupación por la fragilidad tecnológica del Estado. Aunque los servicios ya fueron restablecidos, aún no se sabe quiénes estuvieron detrás del hecho, razón por la que el Ministerio Público ha iniciado una investigación.

Ignacia Canales

► Un ataque informático paralizó parte de las plataformas del ISP durante 12 días.

Durante 12 días el Instituto de Salud Pública (ISP) operó a medias. Un ataque informático paralizó parte de sus plataformas, detuvo servicios esenciales como la autorización de medicamentos y la validación de laboratorios, y expuso la fragilidad digital de uno de los organismos clave del sistema sanitario.

Aunque con el paso de los días algunas funciones se fueron restableciendo, la interrupción dejó a la vista los riesgos de seguridad a los que está expuesto el sistema, en especial considerando que el ISP también resguarda información sensible, como los registros de pacientes con VIH.

Por ejemplo, uno de los servicios afectados por el hackeo fue la gestión aduanera. Medicamentos, cosméticos, dispositivos médicos e incluso pesticidas de uso sanitario que ingresan al país requieren una serie de permisos y certificaciones para cruzar la frontera sin contratiempos. En concreto, se exigen el Certificado de Destinación Aduanera (CDA) y las autorizaciones de uso y disposición (UyD), documentos que emite el ISP. Con los sistemas del organismo fuera de línea, y para evitar un bloqueo en las zonas de ingreso, se autorizó la liberación temporal de estos productos aun sin contar con toda la documentación al día, mientras se trabajaba en regularizar la situación.

Desde el sector privado también manifestaron preocupación. Diversas empresas alertaron sobre el impacto que la interrupción del sistema tuvo en sus procesos de importación, distribución y comercialización de productos.

Desde la Cámara de innovación Farmacéutica afirman que "el incidente ha generado dificultades operativas para las compañías, principalmente en lo relacionado con trámites regulatorios y otros procedimientos gestionados a través del sistema del ISP. Como industria, entendemos la complejidad de esta situación y valoramos los esfuerzos que está realizando la autoridad para restablecer los servicios de forma segura".

Al cierre de esta edición el organismo ya había restablecido la mayoría de sus servicios y esperaba reactivar el resto durante el transcurso del día.

Con todo, el gremio que representa a los laboratorios explica que "algunas empresas han debido reprogramar temporalmente ciertos procesos como presentaciones o solicitudes técnicas. No obstante, mantenemos una disposición plenamente colaborativa y hemos puesto a disposición todos nuestros recursos y esfuerzos para colaborar con la autoridad. La continuidad regulatoria es esencial para asegurar el acceso oportuno de los pacientes a tratamientos seguros y eficaces".

Fragilidad del sistema

El martes -en una reunión declarada como reservada- la Comisión de Salud del Senado abordó la situación junto a las autoridades del ISP. Aunque estas últimas llamaron a la calma y aseguraron que los servidores volverían a la normalidad, en la cita se dio cuenta transversalmente sobre la preocupación por la fragilidad del sistema y por la gran cantidad de información sensible que alberga el organismo.

"Lo que es objetivo y sí lo puedo decir es que la precariedad del Estado es lo que hoy día genera este tipo de problemas. No es un problema de negligencia de personas -están actuando bien-, el problema es la altísima precariedad de las protecciones y de los sistemas de almacenamiento y procesamiento de información. Y eso es una cuestión estructural y política", advierte el presidente de la comisión, el senador Iván Flores (DC).

Mientras tanto, la gran incógnita sigue siendo quién o quiénes están detrás del ataque. Por ahora, lo único claro es el origen: según los primeros análisis, la intrusión se habría gestado desde Reino Unido. Más allá de esa pista geográfica, las motivaciones y la identidad de los responsables siguen siendo un misterio.

Apenas se detectó la intrusión, el ISP activó los protocolos de emergencia. Lo primero fue contactar a la Agencia Nacional de Ciberseguridad (ANCI), tal como lo exige la normativa vigente, para informar oficialmente lo ocurrido. Como medida inmediata, se tomó la decisión de bajar todos los servidores del instituto, buscando proteger tanto los sistemas como los datos de los usuarios y usuarias. Pero la respuesta no quedó ahí: ese mismo día el organismo también presentó una denuncia formal ante el Ministerio Público, dando inicio a una investigación penal para esclarecer los hechos. ●