

Fundación Arturo López Pérez sufrió ciberataque el martes y no ha logrado volver a la normalidad

El centro especializado en cáncer señaló que detectaron la presencia de un malware, lo que ha afectado el acceso al portal “Mi FALP” y la reserva de horas a través de su sitio web. También ha habido demoras en algunas atenciones y reagendamiento de horas.

MARIANA MARUSIC / LUIS CERDA

Un ciberataque sufrió el martes de esta semana la Fundación Arturo López Pérez (Falp), el que ha mantenido a ese centro especializado en el tratamiento del cáncer trabajando de lleno en intentar revertir la situación, aunque sin conseguir aún volver a su funcionamiento normal.

“Nuestros sistemas informáticos han sido afectados por un *malware*. Por lo tanto, es fundamental que todos tomemos precauciones para proteger nuestra infraestructura y datos”, informó el equipo de ciberseguridad de la Falp en un mensaje interno enviado el martes a los trabajadores de dicha institución.

A raíz de este ciberataque, desde entonces la Falp ha tenido dificultades en la operación de sus servicios, desde las áreas administrativas hasta los equipos médicos, señalaron fuentes conocedoras de la situación. Explicaron que debido a la intermitencia en el funcionamiento de los sistemas, ha habido demoras en algunas atenciones y reagendamiento de horas, si bien se ha hecho un esfuerzo por seguir atendiendo a la mayoría de los pacientes.

Consultada la Falp, señalaron que “informamos que durante la madrugada del martes 10 de diciembre de 2024 detectamos la presencia de un malware en una de las unidades de nuestro Instituto Oncológico. Desde ese momento, nuestro equipo de Tecnologías de la Información (TI) ha estado trabajando para resolver este incidente con la mayor celeridad y seguridad posible”.

Agregaron que “la presencia de este *malware* ha generado intermitencias en algunos de nuestros sistemas, afectando principalmente el acceso al portal Mi FALP y la reserva de horas a través de nuestra plataforma *web*. Pese a esta situación, la atención presencial a nuestros pacientes ha continuado sin interrupciones”.

Al llamar al *call center* de la Falp este jueves por la tarde, se indicó que “en estos momentos no podemos atender su solicitud debido a una contingencia, favor derivar su consulta a *callcenter@falp.org*”.

En concreto, según fuentes conocedoras, habría sido un *ransomware* el que atacó al instituto oncológico. En la comunicación interna que enviaron a sus trabajadores el martes, alertaron que “en caso que detecten en sus computadores un archivo *‘inc-readme.txt’* les pedimos desconectar su equipo de la red (sacando el cable o desconectándose de la *wifi*) y avisen inmediatamente” al equipo encargado de ciberseguridad.

Los *hackers*, en ese archivo *readme*, entregaron instrucciones a la Falp para retornar a la normalidad, pero al menos hasta el mediodía de este jueves los ciberdelincuentes no habían tomado contacto con la institución, manifestaron fuentes al tanto del asunto.

Según el sitio *web* de la Organización Mundial de la Salud, “hace relativamente poco tiempo que los servicios de salud han empezado a ser objetivo preferente de los ciberataques”.

Entre otras cosas, la OMS asegura que “la gran cantidad de información digital esencial que conservan los servicios de salud (por ejemplo, en los sistemas de seguimiento de los pacientes o las historias clínicas electrónicas), junto con las carencias en materia de seguridad (falta de sensibilización del personal y de garantías técnicas), los convierte en un objetivo apetecible para los ciberdelincuentes. Para estos, resulta fácil impedir el acceso a unos datos y sistemas que se necesitan en todo momento y pedir un rescate. En el último decenio, los ciberdelincuentes han aprendido a explotar esas carencias de seguridad a gran escala”. ●