

Admite la UNAM el *hackeo* de cinco de sus 150 mil sistemas informáticos

LILIAN HERNÁNDEZ OSORIO

La Universidad Nacional Autónoma de México (UNAM) admitió que cinco de sus 150 mil sistemas informáticos fueron *hackeados*. Aseguró, sin embargo, que en ninguno de ellos existe alguna base de datos de sus más de 370 mil estudiantes, más de 43 mil docentes ni del personal administrativo.

Mensajes en la red social X aseguraban ayer que las bases de datos de la máxima casa de estudios se ofrecen en foros internacionales de ciberdelincuencia con el título “[Selling] [Mx] UNAM University Databases”. Por la noche, la universidad desmintió tal información, pero sí dijo que en el reciente periodo vacacional fue detectada “una intrusión no autorizada (*hackeo*) en cinco de los más de 100 mil sistemas informáticos universitarios”.

Fuentes de la casa de estudios indicaron que no tienen un solo servidor para almacenar los datos personales y académicos, sino que posee una cantidad mayor de aquellos, por lo que es falso que enfrente una crisis institucional y digital, como quisieron asegurar mensajes en esa red social.

La UNAM aseveró que tras detectar dicha intrusión se activaron de inmediato los protocolos institucionales de atención a incidentes de seguridad informática,

que incluyó la inhabilitación de los sistemas correspondientes.

El atacante, denominado Byte-ToBreach, mencionó que el contenido expuesto “es apenas una fracción de la información total en su poder”, pero la universidad nacional aseveró, a su vez, que no se vulneraron los datos de la Dirección General de Administración Escolar, que alberga la información de la matrícula de alumnos ni tampoco la Dirección General de Asuntos del Personal Académico.

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la institución señaló que tras un primer análisis técnico “se confirmó que no hay indicios de extracción de información de los sistemas de datos personales del alumnado o del personal académico y administrativo”. La universidad nacional indicó que “ya coordina acciones con autoridades locales y federales de ciberseguridad para presentar las denuncias legales correspondientes”.

Víctor Ruiz, especialista y director de la empresa de ciberseguridad Silikn, explicó que la información filtrada puede circular y reutilizarse de manera indefinida, sirviendo como base para futuros ataques más precisos y sofisticados, lo que hace evidente la necesidad de fortalecer de manera urgente los controles de seguridad, procesos internos y protección de datos.

