El Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), informó que recibe alrededor de 2 millones de ataques cibernéticos al mes, la mayoría provenientes de Brasil, China, Estados Unidos y Rusia.

Pablo Tamez, Chief Information Security Officer en el Tec, dijo en un comunicado que *«apenas publiques algo en Internet vas a ser atacado».*

> *«Esto lo hacen no porque lo conozcan, sino porque hay robots que están automáticamente buscando, y que no lo sepamos no quiere decir que no esté pasando»,* dijo.
>
> *«Por ejemplo, el Tec de Monterrey recibe en promedio dos millones de ataques cibernéticos al mes, los cuales son detenidos por el equipos de ciberseguridad. Los países de donde provienen la mayoría de los ataques al Tec son Brasil, China, Estados Unidos y Rusia»,* agregó.

También dijo que en el Tecnológico de Monterrey, estos ataques pueden ser observados en monitores de tiempo real, mostrando de dónde provienen y qué están intentando hacer.

> *«Las instituciones que cuenten ahora con este tipo de infraestructura es como un seguro de auto, lo tienes para que te proteja, pero esperas no utilizarlo»,* dijo.

Tamez aseguró que dentro de los ataques más comunes, se encuentran dos tipos:

Ataques al azar, que consiste en un ataqué común que se realiza de forma automática o manual buscando encontrar alguna falla en un sistema para poder ingresar y robar datos o realizar ataques desde esos servidores.

Por otro lado, los ataques dirigidos, que tienen un objetivo específico, ya sea un servidor,

lugar físico o robo de datos de una persona o institución en especial.

Dijo que estos ataques pueden provocar la caída de algunos servicios, mal funcionamiento de sitios o el robo de datos sensibles.

También mencionó que uno de los casos más comunes es la suplantación de identidad o phishing, en el que alguien se hace pasar por otra persona o una institución, para persuadir a la víctima de ingresar sus datos creyendo que está en un sitio real.

Según Temez, entre los motivos de los ataques informáticos, está el tema de la reputación entre la comunidad de hackers.

> *«Hay plataformas donde los hackers presumen sus logros y se retan entre ellos a hackear información sensible de una organización o persona»*, dijo.

Otro de los motivos, según el especialista, es el abuso de recursos, y en instituciones con recursos muy grandes de enlaces y servidores, los hackers pueden generar ataques o minar criptomonedas.

> *«Es muy importante cuidar la información que otorgan en las redes sociales, y número dos, con la verificación en dos pasos es muy improbable que puedas ser vulnerado, porque aparte del password ya tienes otro filtro de seguridad»*, concluyó.