

# **El 70% de las empresas en Latam han sufrido algún ataque a la seguridad de información**

Los ataques a la seguridad de la información en la nube se han convertido en uno de los mayores riesgos que hoy en día deben enfrentar las grandes organizaciones tanto local como internacional. Por esa razón, reforzar las medidas de ciberseguridad es fundamental ahora que, tanto las entidades públicas como privadas, hacen uso de las nuevas herramientas tecnológicas.

Este fue el tema central del evento **“Data: El activo más valioso para las organizaciones”** organizado por IntegrIT junto a sus partners de negocios **Dell Technologies** y **CSI Renting**.

**Enrique Giraldo Carballo**, Unstructured Data Solutions Regional Territory Manager de **Dell Technologies**, comentó que entre el **60% y 70%** de las corporaciones en América Latina han sufrido algún ataque que compromete la seguridad de su información.

*“Como usuarios finales estamos siendo atacados constantemente bajo phishing, mensajes de texto y correos electrónicos maliciosos que suplantan la identidad; lamentablemente la falta de cultura impide que podamos reconocer cuáles son los mensajes verdaderos y cuáles son falsos”,* dijo **Giraldo Carballo**.

Según nos explica el ejecutivo, en América Latina se pensaba que, debido a que somos países en vías de desarrollo, no seríamos interesantes para los hackers y no sufriríamos problemas de este tipo. Sin embargo, nuestra región ocupa el tercer lugar en cuanto a número de ataques, la mayoría de estas agresiones provienen de Brasil, Irán e Israel, así como de diferentes localidades en China.

Asimismo, el Perú es el tercer país de la región que más vulneraciones está sufriendo, el primer lugar lo ocupa Brasil, seguido de México. Según **Giraldo Carballo** esto ocurre porque no se invierte ni estamos preparados para mitigar los ataques, por ello **Dell Technologies** acompaña a sus clientes proporcionando una protección eficiente, esto quiere decir que en el caso de producirse un incidente, el tiempo de respuesta es rápido y permite una pronta recuperación.

*“Por ello, cuando hablamos de ransomware (secuestro de datos) siempre decimos que hay dos tipos de clientes, los que son atacados y los que faltan ser atacados. Basados en esa premisa, tuvimos que sufrir estos incidentes para darnos cuenta de que este peligro nos puede tocar, por ello debemos ser proactivos y no reactivos, es decir no debemos esperar que las cosas pasen para recién tomar medidas”,* afirma **Giraldo Carballo**.

Por su lado, **Angélica Pulido, Data Protection Solutions Systems Engineer de Dell Technologies**, sostiene que las estrategias de seguridad corporativa no siempre son 100% efectivas y eso se demuestra en la cantidad de ataques diarios que sufren los clientes. Por ello en Dell Technologies se han enfocado en ayudar a los clientes mediante una bóveda aislada donde se resguarda la información más importante de su negocio

*“Además, proveemos a nuestros clientes el valor de identificar que la copia efectivamente no ha sido comprometida y que, ante la ocurrencia de un desastre, ellos pueden obtener la información y recuperarse muy rápidamente”*, asevera **Angélica Pulido**.

Según **Carlos Caycho, Gerente General de IntegrIT**, la empresa no solo provee infraestructura tecnológica (como plataforma de servidores, almacenamiento de laptops y PC), también viene integrando soluciones de respaldo y base de datos, así como hiperconvergencia. Además, son una empresa que trabaja de la mano con sus clientes, como un socio estratégico, en la implementación de soluciones que amplíen, aceleren o mejoren las funcionalidades de la TI de las organizaciones.

Finalmente, el ejecutivo destacó la importancia de la adecuación de las distintas soluciones tecnológicas a la realidad de cada una de las organizaciones, así como a sus respectivas prioridades. *“Desarrollamos un análisis previo, así como pruebas de concepto e implementación de laboratorios. Luego de este proceso, si el cliente está convencido de la solución se procede con la adquisición y se aborda todo el proceso de implementación”*, concluye Carlos Caycho.