CIBERSEGURIDAD

El sensible eslabón ‘*startupero*’

Las *startups* enfrentan desafíos únicos para resguardar sus activos de posibles ciberataques. La toma de conciencia del riesgo ya se extiende hasta los inversionistas.

La lista de ciberataques se sigue incrementando en el Perú. La semana pasada, la noticia del presunto *hackeo* del portal del Estado peruano (gob.pe) demostró una vez más que no sólo las grandes empresas del país son víctimas potenciales. Para las organizaciones con mayor tamaño y recursos, las respuestas a esta creciente amenaza pasan por tomar medidas como expandir su perímetro de defensa (SE1948) y cambios organizacionales (SE1951). Las *startups*, sin embargo, enfrentan esas mismas amenazas con menos recursos. Y el impacto de un ciberataque puede ser aun más catastrófico para estas, pues corren el riesgo de desaparecer si sus activos más críticos son secuestrados o corrompidos.

La toma de conciencia sobre el rol crítico de la ciberseguridad en la supervivencia de las *startups* es tal que se ha extendido hasta sus inversionistas. “Es una exigencia tratar, por lo menos, de implementar capacidades [de ciberseguridad]. Depende de qué tan expuesto esté el inversionista a este tipo de amenazas”, cuenta el líder regional de Consultoría en Riesgos Cibernéticos de Marsh McLennan, Edson Villar. Pero la implementación de una estrategia de ciberseguridad, aunque sea básica, supone un desafío para empresas que buscan crecer rápido con equipos pequeños, como las *startups*. “Muchas no saben dónde empezar. Son conscientes del riesgo, pero no hay un conocimiento en todas de cómo identificarlo y cuantificarlo”, explica el *associate partner* de McKinsey & Company, Claudio Querol.

La implementación de una estrategia de ciberseguridad, aunque sea básica, supone un desafío para las *startups*

Algunas, como la *HR-tech* Talana, abordan el reto mediante un enfoque de gestión de riesgos. “Identificamos y clasificamos las amenazas según su impacto y probabilidad. Así, destinamos los recursos adecuados para mitigarlas eficazmente sin comprometer el desarrollo del negocio”, cuenta su *country manager*, Daniel Abusabal. Dentro de ese trabajo, una buena práctica que vienen adoptando las *startups* es el desarrollo de productos y procesos utilizando medidas de ciberseguridad. “Todo el código que pasa a producción es verificado por herramientas con las que validamos posibles vulnerabilidades”, dice el CTO y *co-founder* de las *fintech* Preauth y Reevalúa, Sebastian Burgos.

El caso de las *fintechs* es particular, porque su giro de negocio las obliga a adecuarse a regulaciones de ciberseguridad para poder operar. “Hay mayor inversión en ciberseguridad por la sensibilidad de la información que manejan”, agrega el gerente de ventas de ESET Perú, Eduardo Chira.

Un desafío que *startups* y grandes empresas comparten es la necesidad de actualizar estrategias a medida que las amenazas evolucionan. En ese sentido, la ciberseguridad madura a la par que las *startups* crecen y se consolidan. “Hoy, mi matriz de riesgos [cibernéticos] no es la misma que hace cinco años”, reconoce la gerenta de operaciones y cofundadora de Prestamype, Laure Schlesinger. Este 2025, la empresa invertirá en capacitaciones para todo su personal y en certificaciones para la mayoría de sus productos, como el ISO 27001. **(MAB)** ■