YAIR LELIS

¿Cómo volverse **ciberresiliente?**

JAVIER GONZÁLEZ NÚÑEZ

La mayoría de las empresas mexicanas cree estar tomando buenas medidas de ciberseguridad, cuando la realidad es otra, dice en charla con istmo el responsable del tema en Cisco México.

Si todavía queda en la imaginación colectiva la idea del *hacker* como un rebelde que rompe por pura diversión las barreras de seguridad de empresas e instituciones, es tiempo de ir borrando esa visión, describe Yair Lelis, responsable de la arquitectura y la estrategia de ciberseguridad para Cisco en México.

Más bien, hay que pensar en *call centers* con numerosas personas enviando mensajes de phishing, tratando de vulnerar las escasas defensas que suelen tener los particulares. O bien, lo que llama *script kiddies*, jóvenes que utilizan *scripts* prediseñados para tratar de vulnerar barreras de seguridad de algún tipo de información.

La ciberdelincuencia se está convirtiendo en una industria, una cara del crimen organizado que podría llegar a tener un valor de 10.4 billones *(trillion)* de dólares en 2025. Quedan muy pocos *hackers,* y muchos simples delincuentes, describe. Con 20 años en el campo de proteger los datos de cada vez más millones de personas, Lelis describe esta nueva maquila de robo de datos como el día a día en un negocio que ha demostrado ser prolífico, y que ejerce otro tipo de violencia en la población, una menos física, pero igualmente perjudicial.

EL RIESGO DE SENTIRSE A SALVO

En septiembre pasado, Transport for London (TFL) reportó el descubrimiento de un ciberataque que había dejado al descubierto datos de consumidores como nombres, direcciones y datos bancarios. El hackeo había durado cuatro días, y las autoridades pudieron dar con el responsable aparentemente.

De inmediato llegó el momento de dar explicaciones: enviaron comunicados a miles de usuarios para notificarles que sus datos pudieran estar en riesgo. Una de estas consumidoras fue la hija de Yair Lelis. Entre las preguntas que pueden surgir: si esto sucedió en una de las economías más grandes del mundo, ¿qué puede suceder en México? ¿Qué está sucediendo? ¿Cómo podemos aprender de esto para prevenir?

Para Lelis es importante hablar de estos casos, pues «el tema de seguridad sí puede estar sobre la mesa, pero tenemos que enfatizarlo mucho más, para que no solo nos crean, sino que asignen presupuesto para transformarse».

«El tema de seguridad sí puede estar sobre la mesa, pero tenemos que enfatizarlo mucho más, para que no solo nos crean, sino que asignen presupuesto para transformarse».

Mucha la labor en este campo sigue siendo de divulgación: *workshops,* seminarios, webinarios, eventos, mientras más audiencia, mejor.

Porque pasar de la conciencia a la acción es lo más complicado. De acuerdo con el Cybersecurity Readiness Index, un estudio anual de Cisco, los usuarios en México están mucho más confiados de lo que deberían.

El índice se basa en cinco «pilares»: la nube, la IA, el dispositivo, la red y la identidad. Con este criterio se entrevistó a más de 8,000 profesionales de Tecnologías de la Información (TI) y ciberseguridad en 75 países. Por Latinoamérica participaron México y Brasil, y aquí vienen los hallazgos: en México, 65% de los encuestados, se siente cómodo con su política de ciberseguridad; se siente resiliente.

«Esto me llamó poderosamente la atención, porque cuando describen sus capacidades, muchos están en etapa formativa; no tienen ni las tres primeras activadas, y solo 2% están en etapa madura. ¿Cómo pueden estar tan confiados? A la luz de los hechos de los últimos años, donde se han dado eventos de fuga de datos, robo de información tanto en gobierno como en empresas, ¿de verdad estamos listos en México? A mí me parece que no. Me parece que nos gusta sentirnos mucho más cómodos de lo que estamos y hay que profundizar en esto, porque la cultura de ciberseguridad no está tan permeada aquí», resume contundente Lelis.

Ante una audiencia, sugiere empezar por preguntar cuántos se consideran «ciberhigiénicos». La mayoría dirá que lo es, porque nunca ha tenido un problema. Al preguntar cuántos usan un administrador de contraseñas, la cosa cambia: el número baja. Si se habla de contar con el más reciente *software* de seguridad en sus dispositivos, la caída es generalizada. Para el directivo, México tiene una gran área de oportunidad y es momento de empezar a tomar este tema con la seriedad que se requiere tanto en el gobierno como en las empresas y la academia.

Nos que no haya habido progreso. Hace 19 años, cuando comenzaba su carrera en ciberseguridad, Lelis recuerda que el centro lo ocupaban los *firewalls*, y persistía la competencia entre los antivirus por ser el producto capaz de detectar más variantes nocivas. Tampoco existía regulación.

«Si hay gente que sube información tan fácilmente, también hay quien la busca. Mucho más fácilmente ahora con la inteligencia artificial».

«En ese entonces me sentía como parte de los raros que estaban vendiendo el antivirus y nada más. Hoy nos sentamos con los directivos a decirles que esto no se vende con un retorno de inversión, sino como un riesgo». Hace 20 años se trataba de un tema tecnológico, hoy la Alta Dirección debe ser capaz de definir cuánto puede perder en términos de negocio. La tecnología ha llegado a ser tan importante que hoy el negocio debe verla no solo como un habilitador, sino como un riesgo que debe gestionar.

EL PROBLEMA ES HUMANO

Podría decirse que, a partir del uso de internet, la regla del juego se llama descentralización. «Internet nació no siendo segura, porque no tenía que serlo: era la evolución de una interconexión entre universidades, y después entre universidades y militares ¿Por qué debía ser seguro algo que *per se* ya lo era? Luego creció exponencialmente y sucede que le fuimos atornillando seguridad. Hoy tenemos un monstruo sin forma, pero Internet es solo la banda que transporta los paquetes. La seguridad debe estar en los extremos: en quién envía el paquete y en quién lo recibe. Internet debe ser libre, porque nació solo siendo el medio de transporte de estos paquetes de datos», describe Lelis.

Ese «quién» es un eslabón débil. El autor Scott Shapiro, cuestiona en el libro *Fancy Bear goes Phishing,* que la ciberseguridad pretenda atacar un tema meramente humano con tecnología. Sacar ventaja del otro para obtener información, para sacarle algún provecho, robar, es algo que hacen las personas.

«¿Por qué te voy a educar dándote más dispositivos, más tecnología, o más *software?* No tiene mucho sentido. Nos hace replantearnos las cosas: tiene mucho más que ver con la cultura, con el riesgo y con la divulgación. Tiene mucho más que ver con la conciencia humana».

Por ejemplo, Lelis se declara un promotor de abandonar el uso de contraseñas. Es más fácil buscar otras medidas de seguridad que evitar que un usuario pegue un post-it en la pantalla con su usuario y *password.* «No puedo contra eso; siempre les digo que utilicen un administrador de contraseñas, ¡son gratis!».

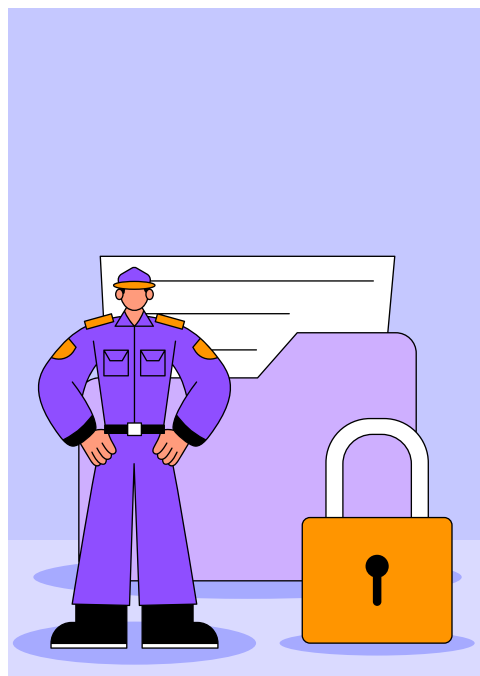
Sin embargo, recuerda, ya hubo un caso en que una compañía administradora de contraseñas fue atacada. Lo irónico: la compañía a la cual se le pagaba una suscripción para generar nuevas contraseñas protegía todo con un *master password*. La moraleja es muy sencilla: «a todos nos va a pasar. ¿Qué es lo que está en juego? Minimizar el riesgo y prepararse para que, cuando suceda, la recuperación pueda ser más rápida».

Ser ciberresilientes, es lo que propone Yair Lelis, y para ello hay que controlar lo que se comparte en redes sociales. Hay casos en los que el usuario jura no haber compartido su información, pero en realidad ha hecho públicos muchos detalles de su vida, como sus gustos, actividades, lugar. Afortunadamente, refiere, el usuario de redes sociales ya entiende que no es buena idea sacarse una foto con su recién entregada nueva tarjeta de crédito... pero hubo casos.

«Si hay gente que sube información tan fácilmente, también hay quien la busca. Mucho más fácilmente ahora con la inteligencia artificial». Relata que hace unos meses se difundió un esquema en Telegram llamado FraudGPT. «Lo bajabas y te ponías a investigar a alguien. Le pedías a la aplicación que hiciera un correo de *phishing* atractivo para esa persona. Con base en todo lo que esa persona publicaba, hacía un correo muy elaborado que solo tendría sentido para ella; algo que le hiciera *click*. El juego cambia con la IA, pero esencialmente sigue siendo lo mismo: quiere engañarte a ti, sigue siendo humano. A esto se refería el doctor Shapiro en su libro, no importa la tecnología que uses, el fin sigue siendo el mismo. En tanto no arreglemos eso, lo demás puede seguir evolucionando. Vamos a tener que defendernos también con IA, pero el fin sigue siendo el mismo».

Tomar ventaja de alguien no sólo implica el lado financiero. Hoy las guerras se pelean al mismo tiempo en el ámbito cibernético, con miles de manos y máquinas haciendo propaganda, desinformación y falsas tendencias en favor de su lado. La IA ayudará tanto a buenos como malos, es cierto, pero Lelis señala una pequeña (gran) diferencia: «los buenos tenemos que levantarnos, hacer ejercicio, ir a cierta junta, tomar entrenamientos, tal vez uno en ciberseguridad, hacer *check in* en alguna parte, ir a juntas con clientes, tener minutas, etcétera. Los malos no. Ellos no tienen que checar tarjeta: se levantan y lo intentan, y si de 100 se les da una, ya hicieron algo mucho muy lucrativo».

es una gran área de oportunidad en América Latina y señala que existe un déficit de al menos 700,000 profesionales en este campo en la región, y hasta 3.7 millones en el mundo. Son empleos que podrían darse de inmediato.



LOS RIESGOS A FUTURO

Si este es el estado de las cosas actualmente. La prospectiva es difícil. A la pregunta de cuál será el panorama en 50 años, Lelis señala que por entonces la humanidad estará en la cuna de la siguiente iteración de la IA: la inteligencia artificial general.

«Tendremos entes que puedan aprender cosas y transmitir conocimiento, pero recién estaremos rozando esa parte. Imagina ese mundo en 50 años sin un tema de ciberseguridad. Sería un caos». Hoy lo es, con la industria jugando al «gato y el ratón» al emerger cualquier nueva tecnología. Todos se lanzan a buscar vulnerabilidades, determinar las más importantes y perseguir las más relevantes para el negocio.

«Hay que considerar que, si no tenemos todo esto bien ordenado, cuando tengamos el primer esbozo de una IA que pueda aprender por sí misma, esta aprenderá lo peor de nosotros y lo va a magnificar. De hecho, ya pasó: en uno de los primeros intentos para un *chatbot* de Microsoft hace unos años, este resultó ser un fascista de ultraderecha, intolerante. Si no llegamos ahí no solo con una legislación, sino con una vivencia de la ciberhigiene en el día con día, estaremos condenados al fracaso».

A propósito del tema, señala que otro riesgo ante el uso de la IA es el *data poisoning,* en donde la delincuencia organizada o cualquier otra entidad puede alterar los datos de que depende una solución de *machine learning,* provocando un problema de mayor o menor tamaño.

CÓMO PREDICAR LA CIBERSEGURIDAD

En el ecosistema de los emprendedores y el *venture capital* hay palabras mágicas, que abren puertas, como metaverso, IA, realidad virtual y aumentada; incluso hay oídos para la nube y el *software* as a service. La ciberseguridad no luce tan atractiva en este mundillo, se aprecia como el «primo pobre», se le plantea a Yair Lelis.

Coincide en que es una gran área de oportunidad en América Latina y señala que existe un déficit de al menos 700,000 profesionales en

este campo en la región, y hasta 3.7 millones en el mundo. Son empleos que podrían darse de inmediato. Este hueco es a la vez una gran oportunidad para emprender, no solo en el desarrollo habilidades técnicas, sino también de liderazgo, para reconocer el riesgo al cual el negocio está expuesto y saber elaborar un plan de ciberseguridad.

«Para mí eso sería ideal. Me mueve que alguien despierte y quiera invertir en esto. Finalmente, es una inversión grande, pero ahí está el emprendimiento, en el que se puede hablar de reducir la brecha de los 700,000, y sobre todo ayudar a que la cultura de ciberseguridad crezca. Esto puede ser muy redituable. Si eres capaz de demostrar que la tecnología le puede dar ese *switch* al negocio y comenzar a mover conciencias, estamos tocando todos los puntos».

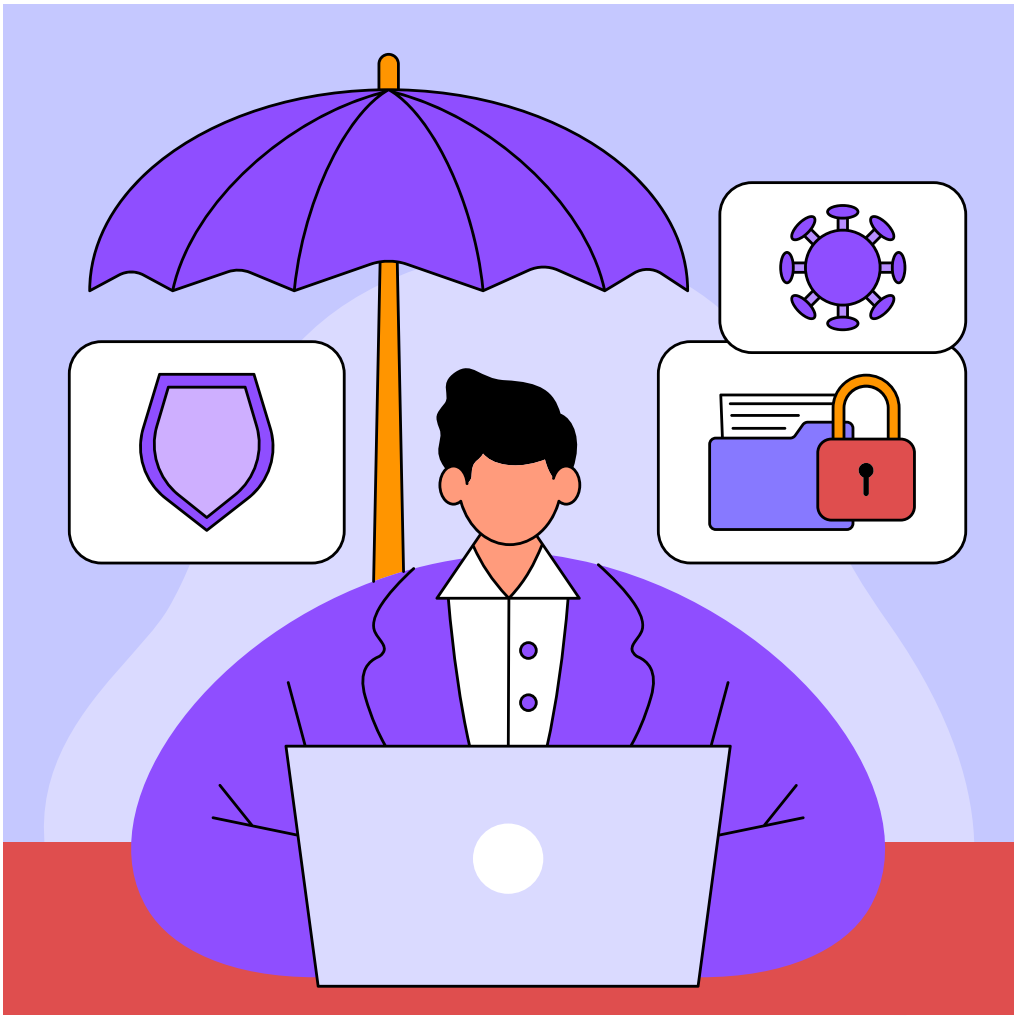
El mensaje debe llegar a la Alta Dirección en las empresas ya establecidas, la ciberseguridad requiere ese *sponsor* en el *board,* para alinear el tema con los objetivos de negocio. Se requiere alguien que tenga el tema en su agenda, quizá con incentivos enfocados en ello. En opinión de Lelis debe haber lugar para un «ciberevangelizador», capaz de mover la conciencia del negocio, demostrando las implicaciones monetarias de este tema.

«Ahora ya existe hasta un Chief Artificial Intelligence Officer, pero solo un Chief Information Security Officer, que cuando pasa algo es el primer despedido». El *sponsor* debe ser alguien en el Consejo, incluso el director de Finanzas, que termina pagando por cualquier estrago en ciberseguridad.

Al respecto, quizá el tema de ciberseguridad no puede limitarse a la educación superior o a las escuelas de posgrado. No la parte tecnológica, pero si comportamientos y formas de cuidarse, es algo que podría impartirse desde la Primaria. «Lo estamos dejando muy de lado, mientras que la cibereconomía de los adversarios sigue creciendo».

En ese sentido, el gran pendiente sigue siendo el sector público. En México no se ha logrado implantar una estrategia de ciberseguridad. Lelis estima que han fallado o han quedado detenidas una 40 iniciativas desde 2014, pero falta voluntad política. Al gobierno le sucede lo mismo que a los encuestados por Cisco, donde 65% que cree que lo está haciendo bien. **</>**

la ciberseguridad no puede limitarse a la educación superior o a las escuelas de posgrado. No la parte tecnológica, pero si comportamientos y formas de cuidarse, es algo que podría impartirse desde la Primaria.



El entrevistador es profesor del área de Política de Empresa en IPADE Business School.

istmo review®

La **versión digital** contiene las **ediciones más recientes** con opción de lectura descargable y hojeable de la versión completa y por artículo en **formato EPUB y PDF.**

Conócela
y suscríbete
istmo@ipade.mx