CONVOCADOS POR CYBER TECHNOLOGY SOUTH AMERICA Y CHILE TECNOLÓGICO DE "EL MERCURIO"

Inteligencia artificial y más: Los temas que preocupan a los expertos en ciberseguridad

Desde la formación de talentos hasta la ética, altos ejecutivos de las consultoras y proveedores de tecnología más importantes del país detallan las materias de las que deben hacerse cargo el sector público, privado, la academia y los gremios ante el avance de los ataques digitales.

ANA MARÍA PEREIRA B.

FACUNDO JAMARDO,
PARTNER TECHNOLOGY CONSULTING, EY

Es importante tener una persona encargada de ciberseguridad que entienda la operación y el negocio. La mayoría de las empresas designan a un profesional muy técnico como CISO (Chief Information Security Officer). Hoy se necesita que, frente a un directorio, comité de seguridad o de riesgo, esa persona sea capaz de plantear un problema expresando la importancia de lo que se necesita —por lo general, recursos— en términos completamente tangibles para alguien del negocio: que sea un lenguaje común, que permita hablar y discutir con el resto de los ejecutivos de igual a igual.

Obviamente hay gente muy entrenada, pero no llega a ser la mayoría de un directorio o un comité ejecutivo los que entienden los riesgos reales en los términos que normalmente los explica un CISO, a menos que esté mucho mejor formado a nivel ejecutivo y pueda traducir esos riesgos en riesgos del negocio. Cuando encuentras un CISO así, todo fluye más fácil.

ÁNGELA LOPES,
LÍDER DE CIBERSEGURIDAD AMÉRICA LATINA, IBM

Un aspecto importante es el impacto social de temas como la ciberseguridad y la IA, debido a la falta de conocimiento y conciencia. Hay una capa de gente que tiene el privilegio y el acceso a la información que les permite prepararse para estos temas. Pero otra gran parte de la sociedad no tiene una preparación para afrontar estas tecnologías y diferenciar algo hecho con IA o un *deepfake*; no tienen conciencia de qué están enfrentando, o quizás ni siquiera tienen idea de que existe.

Y esto se relaciona con el sesgo político. Muchas capas de la sociedad son movidas por el impacto que les generan los mensajes que reciben. Veo una bola de nieve que se agrava en tiempos de campañas políticas, cuando empieza una vorágine de mensajes, muy difíciles de diferenciar sin cierta formación como para empezar a mirar detalles. Eso es parte de las consecuencias de la democratización del uso de la IA, del avance y la evolución de los tipos de ataque: cualquier persona que tenga acceso a la tecnología o al mundo digital puede ser víctima.

CLAUDIO ORDÓÑEZ,
SOCIO LÍDER DE CIBERSEGURIDAD, PWC

Existe una brecha de talento que no debemos abordar compitiendo, sino trabajando en conjunto, atrayendo y ampliando el talento que existe, en especial, en cuanto a la presencia femenina.

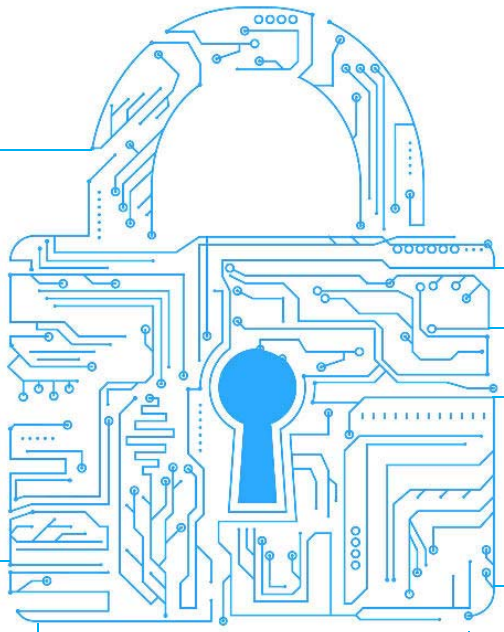
En una empresa, desarrollar un buen profesional de ciberseguridad puede tomar dos o tres años. ¿Cómo acortar esa brecha? Generando un trabajo colaborativo, como en EE.UU., donde la academia (universidades, institutos, centros de formación o colegios técnicos, porque no solo se necesitan ingenieros) con las empresas y las consultoras de tecnología dan la oportunidad de aprender en ciberseguridad desde antes de egresar.

Se trata de ampliar la formación para que los talentos no empiecen a aprender de ciberseguridad cuando salen de una carrera, sino que desde antes. Es importante dar las opciones o el espacio para que la gente a la que le interesa pueda empezar a trabajar en este campo.

PÍA SALAS, COUNTRY MANAGER, FORTINET

Una forma de apoyar y ayudar transversalmente a las distintas organizaciones es a través de los gremios, que han sido muy relevantes en el último tiempo, como Fundación País Digital, la Alianza Chilena de Ciberseguridad y la ACTI, entre otros, que pueden entregar información y apalancar iniciativas en ciberseguridad a alto nivel; así como generar compromisos con empresas y firmar acuerdos nacionales e internacionales para conocer e implementar las mejores prácticas en nuestro país.

También a través de ellos podemos acortar la brecha de ciberseguridad en las personas; falta mucho recurso humano que tenga experiencia y sepa sobre el tema. Sería muy importante hacer convenios con el gobierno para potenciar y fortalecer a las empresas, capacitando, educando y concientizando en ciberseguridad a las personas, como menores y mayores de edad, las cuales son un punto muy importante en la cadena. Cualquier persona u organización puede ser atacada por ciberdelincuentes.



MARCELO DÍAZ, LEAD PARTNER CYBER, DELOITTE

Las organizaciones deben plantearse frente a un evento de ciberseguridad y saber cómo van a responder. Las que entiendan ese proceso y lo fortalezcan, van a ser capaces de reaccionar mejor y salir a flote.

A veces las compañías se "autoatacan", incorporando más cosas en ciberseguridad, pero no se hacen fuertes en las básicas. Es preferible que tengan entendimiento y visibilidad de un elemento y lo hagan extremadamente bien, a tener varios componentes sin hacer ninguno bien. Lo hacen por cumplir, pero no crecen en lo básico, en lo higiénico, y es uno de los grandes temas que van a surgir con las nuevas leyes.

Asimismo, al comprar un *software* o una *app* de ciberseguridad, por ejemplo, las empresas no piden los indicadores por los cuales se van a medir.

También es relevante alinearse con algo. Si la firma empieza su camino de ciberseguridad y se decide por una estructura en base a un ISO o un CIS, por ejemplo, hay que quedarse con ese, porque podrá ir creciendo en el tiempo. A veces cambian de uno a otro cada año y nunca terminan de ser extremadamente buenos en uno solo.

ADRIANA BASSI,
TECHNICAL MANAGER, GLOBANT

Una de las primeras fases en la implementación de la IA es el desarrollo de los "asistentes". Cada empresa tiene sus procesos para resolver un problema y a través de estos chats internos y *machine learning*, la IA va aprendiendo y mejorando sus respuestas (evitando, por ejemplo, las alucinaciones). Eso sí, necesita un tiempo para aprender y el ser humano debe estar guiando ese proceso.

Otro tema relevante es la ética: internacionalmente, existe una serie de marcos regulatorios, como en Estados Unidos, China, Asia o Europa. Nosotros estamos empezando y, a partir de esos ejemplos, deberíamos ser mucho más rápidos en lo ético. Esto requiere estar alineados con la educación, con la formación y la perspectiva de género. No podemos hacer IA sin pensar en la ética ni en la perspectiva de género, porque estaríamos dejando a un montón de personas afuera y la diversidad es lo que nos da soluciones más efectivas y de largo plazo.

MAURICIO RAMÍREZ,
COUNTRY MANAGER, PALO ALTO NETWORKS

Un tema relevante es la incorporación de la mujer. Nos ha tocado abrir varios procesos de contratación, y por directrices globales la compañía nos exige tener tanto hombres como mujeres en los postulantes. Pero es difícil, porque hay muy pocas mujeres en el mercado de la ciberseguridad. Obviamente hay talento femenino y la mujer va ganando su espacio, pero dependiendo de lo que necesitemos el espectro se va acotando por conocimiento técnico y, por lo general, los hombres tienen mayores *skills*.

Y esto ocurre no solo en la parte más técnica, sino también en otras áreas como la comercial, donde también se requiere un conocimiento especializado.

DAVID NIETO,
COUNTRY MANAGER, TELEFÓNICA TECH CHILE

En conversaciones con clientes detectamos mucho ruido, muchas tecnologías dando vueltas, lo que genera confusión y problemas a la hora de elaborar los presupuestos.

Las organizaciones se enfrentan a la pregunta de qué hacer en ciberseguridad, 5G, tecnología satelital, IoT, IA... Son muchas tendencias en que las grandes corporaciones tienen un proyecto asociado, pero no hay un *outcome* tangible. Es necesario simplificar el discurso ante las marcas.

Por otra parte, todo se hace para los grandes presupuestos, pero las pequeñas empresas no saben cómo hacerlo. Hemos visto casos de pymes que (ante un ataque) terminan pagando bastante para recuperar su información y salir adelante. Necesitan una arquitectura para hacerlo de forma segura.