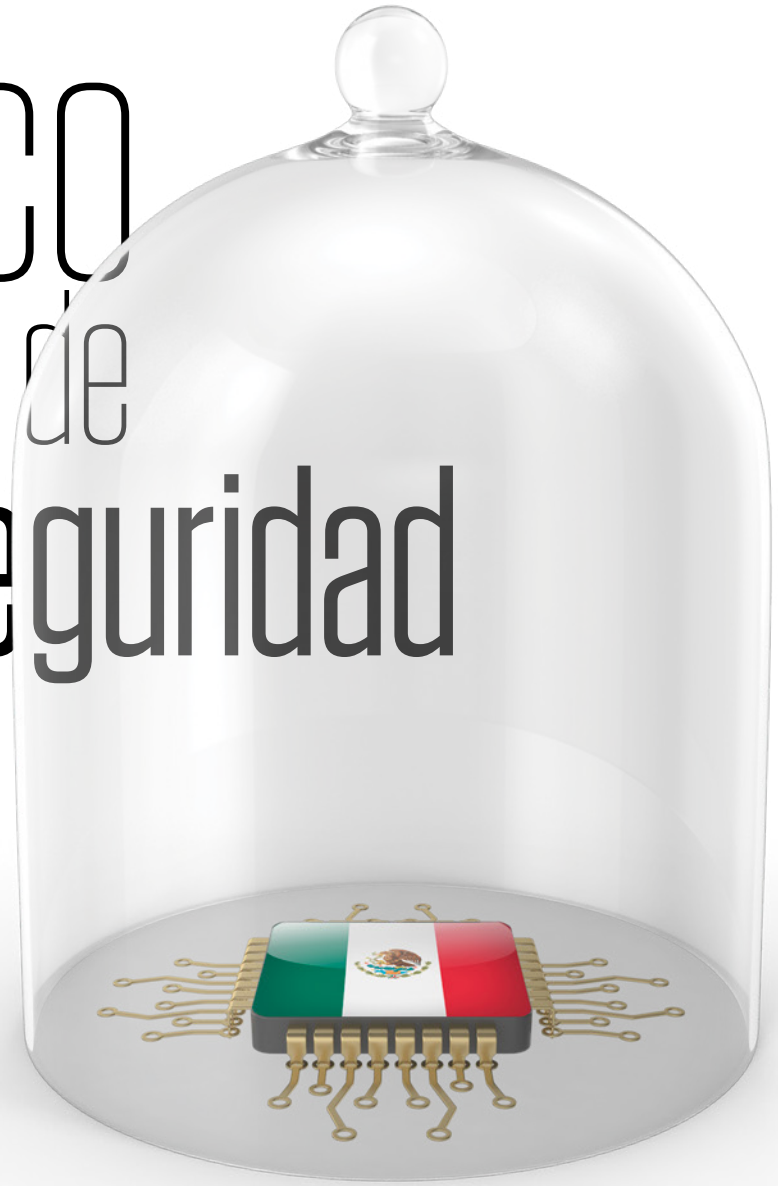
ANDRÉS VELÁZQUEZ

México ya habla de ciberseguridad



Hoy el director de Seguridad de la Información o Ciberseguridad debe ocupar un papel estratégico en las empresas, mismas que deben equilibrar el poder sobre sus sistemas, para protegerse de una de las variables más inciertas en la ciberseguridad: la humana.

REDACCIÓN ISTMO

Quería ser músico. Sin embargo, los padres de Andrés Velázquez lo invitaron a estudiar una carrera, por lo que el mundo perdió un artista, pero ganó un *rockstar* en la ciberseguridad. Estudió ingeniería cibernética en los 1990, y desde sus primeros trabajos se acercó a la ocupación de proteger sistemas y datos de los *hackers,* en un campo que se hacía cada vez más grande y complicado, en la medida que crecía internet y unía a todos digitalmente, para bien y para mal.

De carácter sumamente inquieto, los siguientes 25 años le servirían para convertirse en una autoridad en ciberseguridad. Fue consultor independiente, incluso ante el gobierno de Estados Unidos, fundó su propia empresa, MaTTica, enfocada en respuesta a incidentes y manejo de cibercrisis, pero también encontró infinidad de foros donde predicar su temática en medios de comunicación, el medio de conferencistas y por supuesto la docencia. Como le quedaba algo de rato libre también estudió para piloto privado y mago. En charla con istmo, este polifacético emprendedor concluye que por fin el mensaje de proteger los sistemas está cundiendo entre las empresas mexicanas.

Tienes 25 años en la industria y hoy eres líder de opinión, consejero en diversas empresas hablando con los CEO sobre estrategias. ¿Cómo ha sido tu experiencia a lo largo de estos años?

Comencé siendo uno de los únicos responsables en la seguridad de la información entre 1998 y 1999 en una empresa muy grande en ese momento que había traído el Internet privado a México, aunque en realidad, yo quería en ese momento dedicarme a la música, pero mis padres me invitaron a estudiar una carrera. Me decidí por ingeniería cibernética para buscar hacer música por computadora.

Gracias a mi padre, comencé a acercarme al tema tecnológico por diferentes elementos en casa, incluyendo una computadora y mis primeros accesos a internet. Recuerdo que en aquel momento era una pantalla verde, donde no podías ver tantas imágenes y tardaba mucho tiempo en lograr intercambiar información por medio de un módem. Me familiaricé con términos cuya interpretación hoy ha cambiado: *hacker, cracker, phreaker*... los primeros, por ejemplo, eran las personas muy curiosas y conocedoras acerca de la tecnología, que la manipulaban para hacer cosas para los cuales la tecnología no había sido creada. Cuando menos en ese momento, el término *hacker* no siempre se identificaba con algo malo; el término se acuñó en el MIT, refiriéndose a una persona a la que le gusta jugar y hacer bromas con la tecnología.

Por aquel entonces tuve la oportunidad de iniciar mi primera columna de opinión alrededor de temas de ciberseguridad sin que este término se utilizara tan comúnmente. Poco después, logré laborar en una empresa estadounidense donde administrábamos sistemas de ciberseguridad en toda América Latina, algo muy innovador en ese momento, que me permitió entender los negocios en toda la región. Fue en ese momento donde pude aprender de cómo hacer investigaciones digitales, presentación de pruebas digitales y colaborar con organizaciones internacionales como el Servicio Secreto de Estados Unidos, INTERPOL y otros. Terminé independizándome para crear el primer laboratorio forense digital privado en América Latina. Todo lo que había aprendido y desarrollado sobre las investigaciones digitales y la presentación de pruebas digitales sirvió para crear MaTTica, el primer laboratorio de la región hace ya dieciocho años.

En MaTTica, iniciamos con los servicios forenses digitales y periciales para después incorporar la atención de respuesta a incidentes y manejo de crisis de tecnología para finalmente incorporar servicios preventivos específicamente en la parte estratégica: consultoría y auditoría para generar estrategias de ciberseguridad, medir la madurez de la organización en ciberseguridad, realizar análisis de impacto al negocio y muchos otros. Desde el inicio estuve convencido de que la ciberseguridad no es solo contar con un *firewall* o un antivirus, porque, aunque es tema importante, se queda en algo muy operativo. Fue así como logramos convertirnos en una empresa de ciberseguridad estratégica con servicios preventivos y reactivos orientados a un riesgo más: la ciberseguridad.

En el ámbito de la ciberseguridad, uno de los mayores riesgos que enfrentan las empresas hoy en día es el *ransomware.*

¿Cómo ha sido tu relación con los empresarios, para que esto pueda implantarse en sus empresas? ¿Por dónde comenzar?

Hay dos situaciones que normalmente se presentan. La primera, donde un alto directivo comienza a trabajar con nosotros porque lamentablemente tuvo alguna afectación del negocio, como por ejemplo después de que un código malicioso secuestró sus archivos y pidió un rescate, cuando un responsable de TI se apodera de su infraestructura y han perdido la confianza en dicha persona o cuando hay un fraude interno realizado con apoyo de la tecnología. Es claramente un tema reactivo y nos quieren ahí para apoyarlos y saber qué pasó, contener la situación y evitar que vuelva a suceder.

La segunda situación, que aplaudo y celebro es cuando los consejeros y directivos, han escuchado sobre la importancia de la ciberseguridad y que buscan acercarse a una empresa que puede hablar su lenguaje. Son pocos los especialistas en ciberseguridad que han tenido una educación para poder hablar con la Alta Dirección, situación que hemos hecho por ya algunos años. Los consejeros y los directores saben perfectamente cómo administrar riesgos, pero no conocen qué preguntas hacer para identificar el nivel de riesgo que tienen en ciberseguridad y sus implicaciones. Por otro lado, los responsables de tecnología no tienen el conocimiento para poder presentar las iniciativas y estrategias con un lenguaje de negocio.

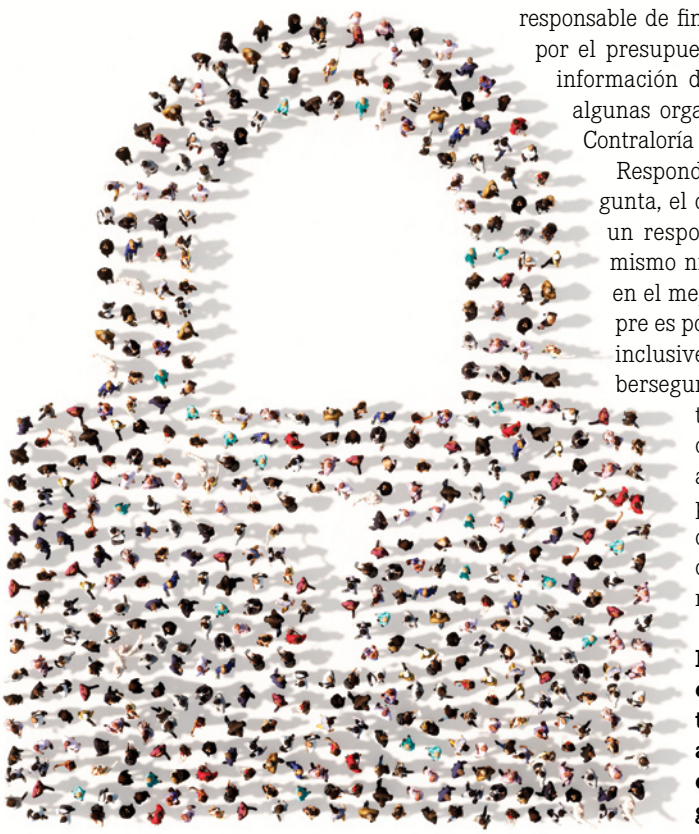
Esto genera una situación muy interesante pero fácil de resolver: uno, que el directivo tenga interés en aprender algo nuevo y dos, que el equipo tecnológico tenga a su vez el interés de presentar su información de una forma ejecutiva. Nosotros ayudamos en ese cambio.

¿Para llegar a esa estrategia, de qué roles tendría que rodearse un CEO?

Es un tema muy interesante y que tocamos cuando me han invitado a participar en algunos de los programas del IPADE como profesor externo. Va a depender del tamaño de la organización y de su giro.

Para una entidad financiera, sabemos que por regulación un CISO (director de Seguridad de la Información) tendría que estar reportando directamente al director general. El CISO es alguien no operativo, sino estratégico y llevará a cabo todas las estrategias de ciberseguridad para evitar una interrupción de negocio y asegurar la información, entre otras responsabilidades. Es recomendable que le entregue esa información al responsable de tecnología, quien las implementará.

Hoy el director de Ciberseguridad debe ocupar un papel estratégico en las empresas, para protegerse de una de las variables más inciertas en la ciberseguridad: la humana.



Pero no se queda ahí, sino que tenemos que lograr que diferentes responsables se involucren como Contraloría, Auditoría y Recursos Humanos desde el punto de vista de ciberseguridad; todos ellos formarán parte de una estrategia dentro de la empresa que al final busca evitar una interrupción y una afectación como por ejemplo, dañar la reputación.

Una de las cosas interesantes es cuando hay conflicto de interés: si el CISO depende del responsable de TI la estrategia y ejecución depende de la misma persona, logrando que en algunos casos no se ejecuten las acciones necesarias para poder mitigar riesgos por privilegiar temas operativos. Si ponemos al CISO debajo del CFO, también existe un conflicto de interés, porque el responsable de finanzas estará más preocupado por el presupuesto, no tanto por asegurar la información dentro de la organización. En algunas organizaciones el CISO reporta a Contraloría o a Riesgos directamente.

Respondiendo puntualmente a la pregunta, el director general debería tener un responsable de ciberseguridad, al mismo nivel que los demás directores en el mejor de los casos. Pero no siempre es posible, hay organizaciones que inclusive tendrán que subcontratar ciberseguridad por su tamaño y estructura. Lo importante es que los directivos vean cómo pueden acercarse a la ciberseguridad para evitar una afectación que los pueda llevar a dejar de operar o que se afecte su reputación.

Estas estrategias de ciberseguridad ¿son también aplicables a micro y medianas empresas, que también generan información?

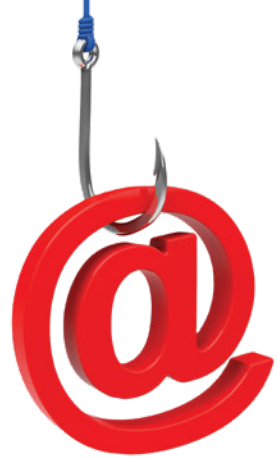
Claro, pero va a depender de dónde nos encontramos. Una forma sencilla es haciendo uso de guías o estándares que nos permiten tener un parámetro de medición, como el ISO 27001, sobre un sistema de gestión de seguridad de la información o las guías generadas por el Centro Nacional de Normalización (NIST) en Estados Unidos que permiten identificar el nivel de madurez de la organización en cuanto a ciberseguridad. Sin importar el tamaño de la empresa, da indicadores que pueden llegar a funcionar a la Alta Dirección y al mismo CISO de dónde y cómo se encuentran en ciberseguridad.

Sin embargo, también hay que tener cuidado en cómo se interpretan. Les comparto una anécdota: en un Consejo de Administración al que asistí como asesor independiente se había hecho un gran esfuerzo para realizar una auditoría para identificar el nivel de madurez en ciberseguridad. Los consultores externos presentaron los resultados del servicio y las recomendaciones. Al final colocaron un termómetro para que pudieran compararse contra las mejores prácticas y aparecía más arriba de la mitad. En ese momento, el presidente del Consejo se puso de pie y dijo *«entonces pasamos, estamos bien»*. Todos nos quedamos callados, para mí fue un momento interesante, porque le respondí que no podíamos usar esto como una evaluación académica. Estamos hablando de riesgo, al que se trata de mitigar hasta un punto aceptable, lo que no significa que ya no hubiera nada de qué preocuparse; esto era una fotografía de cómo se encontraban en ese momento. Además, los riesgos cambian, donde con un cambio de proceso o el mismo tiempo que pasa, cambiará. "Imagina que colocas cámaras de seguridad afuera de tu casa, porque sabes que están robando en la zona, pero nunca más las actualizas ni las revisas. No te servirán de nada."

El tema de ciberseguridad es cíclico, y hay que atenderlo todos los días. Lograr esa concientización en los altos directivos me impulsa a seguir hablando de ciberseguridad estratégica.

Hablando del riesgo, hay temas intangibles como la reputación, ¿por qué la ciberseguridad tendría que ver con ellos?

En ciberseguridad, también llevamos tiempo utilizando la IA para analizar modelos, bitácoras e identificar posibles ataques, de forma temprana.



Desde una perspectiva financiera, es fundamental entender que la integridad y precisión de los estados financieros son esenciales para mantener la confianza de los inversionistas, reguladores y el mercado en general. Por ejemplo, si una empresa que cotiza en bolsa no lleva correctamente sus registros financieros o intenta ocultar alguna transacción importante, puede enfrentar graves consecuencias, desde sanciones regulatorias hasta una caída drástica en el valor de sus acciones, afectando así su reputación y estabilidad financiera.

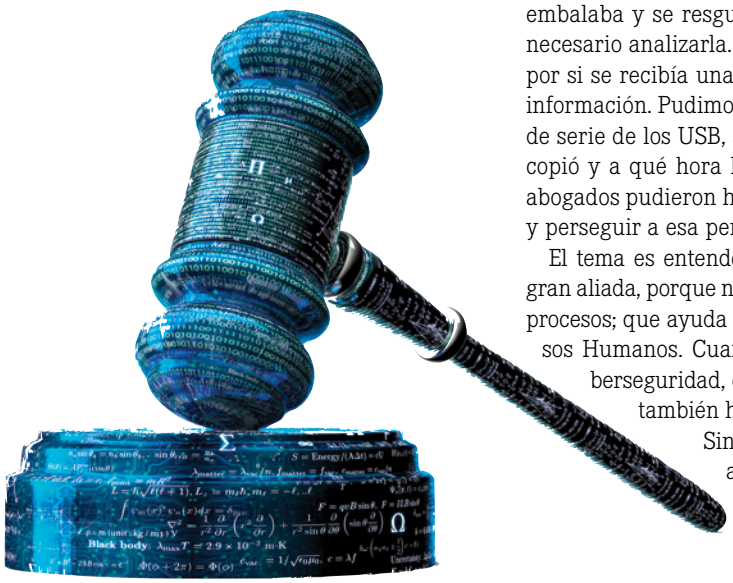
En el ámbito de la ciberseguridad, uno de los mayores riesgos que enfrentan las empresas hoy en día es el *ransomware.* Este tipo de ataque puede cifrar la información crítica de la empresa, y en algunos casos, los atacantes exfiltran datos sensibles para aumentar la presión durante la negociación de un rescate. Es importante señalar que, desde una perspectiva financiera, pagar el rescate no solo representa un costo inmediato, sino que también podría incentivar futuros ataques, además de generar riesgos legales y reputacionales. Por lo tanto, mi postura es clara: no se debe pagar el rescate. En lugar de ello, la empresa debe invertir en medidas preventivas y de respuesta, como contar con copias de seguridad actualizadas y un plan robusto de recuperación ante desastres, para mitigar el impacto financiero y operativo de este tipo de incidentes.

Pero también veámoslo desde el punto de vista de que ya le sucedió a una organización. Cuando esto pasa, hay una interrupción del negocio, al igual que lo describíamos anteriormente y desde esa perspectiva está perdiendo dinero. Va a tener que contratar especialistas para regresar a la operación, y entre más rápido quiera regresar, más especialistas necesita y más procesos tiene que realizar. Es un gasto que no tenía considerado. Habrá, además, una pérdida de reputación, porque en el momento en que deja de operar, sus clientes y proveedores van a presionar no importando si es un tema tecnológico o no. Si ofrece algún tipo de servicio o producto público, esa pérdida de reputación puede incrementarse. Se han dado casos donde gracias a una mala respuesta a un incidente, a una crisis informática, la empresa desaparece.

¿Qué pasa con la inteligencia artificial y la ciberseguridad?
La IA ha existido por más de 50 años. Lo que estamos viendo ahora es una unión entre la IA y el procesamiento del lenguaje natural, lo que logra la democratización a su acceso. Hoy en día existen algunas herramientas como ChatGPT, pero especializadas para ciberatacantes. Quizá no sabes cómo hacer una campaña de *phishing,* correos electrónicos que llegan pidiendo información, y ya existe un portal al que puedes decirle: «quiero afectar a estas organizaciones, con un texto como este, o bien cópiame la información de esta entidad financiera, o este portal de Internet», y lo hace de forma automática. A final de cuentas, al igual que la IA tiene un buen uso, se puede usar para el mal. En ciberseguridad, también llevamos tiempo utilizando la IA para analizar modelos, bitácoras e identificar posibles ataques, de forma temprana.

¿Qué tendencias vienen en el campo de la ciberseguridad?
Vienen cosas interesantes, como el mayor interés por parte de la Alta Dirección en la ciberseguridad y cómo estamos empezando a lograr que haya un entendimiento. En Estados Unidos, la SEC (Securities and Exchange Commission) ha dicho que el tema de ciberseguridad es tan importante que si una organización tiene una afectación tecnológica que pueda dar como resultado una afectación material, tiene cuatro días para reportarlo. También está empezando a impulsar el tema de que los consejeros, directores y en algunos casos incluso los inversionistas, tengan capacitación en ciberseguridad para entender los riesgos, o que uno de los consejeros esté especializado en ciberseguridad. Lo que esto marca es un parteaguas; si bien podemos hablar de tendencias desde el punto de vista de los nuevos ataques orientados hacia cierta tecnología, cuando lo vemos desde la perspectiva de la Alta Dirección, habrá cada vez más entendimiento. Van a darse más ataques, vamos a ver a nivel internacional legislación alrededor de la tecnología, se buscará una cooperación internacional para lograr eliminar las jurisdicciones en ciertas situaciones, lo que será muy importante para el futuro del tema.

Vamos a ver a nivel internacional legislación alrededor de la tecnología, se buscará una cooperación internacional para lograr eliminar las jurisdicciones en ciertas situaciones, lo que será muy importante para el futuro del tema.



¿Podrías hablar de algunos casos prácticos? Se dio por ejemplo el caso de *ransomware* donde una empresa pagó un rescate de 75 millones de dólares. ¿Qué debe hacer una empresa en estos casos?
Hace tiempo tuvimos un caso en que un empleado de esta área se robó varios cientos de millones de pesos, simplemente llevándose el PTU de los colaboradores que no regresaban. Pudo hacerlo porque toda nuestra operación descansa en la tecnología. Hay que revisarla, lo mismo el proceso que a la gente para que no exista la posibilidad de un fraude. Esto no tiene que ver tanto con la tecnología, como con el proceso normal de una organización. Gracias a eso y al cómputo forense, pudimos detectar cómo esa persona estaba haciendo la dispersión, cómo cambiaba las cuentas, y cómo quedaba evidencia dentro de los sistemas.

Tuvimos también otra situación en que un empleado decide renunciar y a la semana siguiente está trabajando en la competencia, mismo puesto. Sabemos perfectamente que no hay mucho qué hacer desde el punto de vista laboral. El problema fue que cuando se va a la otra organización, vemos que los planes de marketing y ventas que se estaban ejecutando eran los mismos que tenía en la organización donde renunció. Analizamos la computadora que utilizaba en la empresa porque la empresa tenía protocolos: cuando ciertos directivos se iban, debían entregar su computadora, misma que se embalaba y se resguardaba, por si después era necesario analizarla. Esto con un fin estratégico, por si se recibía una demanda laboral o faltaba información. Pudimos establecer marca, número de serie de los USB, a qué hora los conectó, qué copió y a qué hora los desconectó. Con eso los abogados pudieron hacer un concurso de delitos y perseguir a esa persona.

El tema es entender que la tecnología es una gran aliada, porque nos permite mejorar nuestros procesos; que ayuda al área Legal, a la de Recursos Humanos. Cuando la llevas al área de ciberseguridad, es para protegernos, porque también hay herramientas para ello.

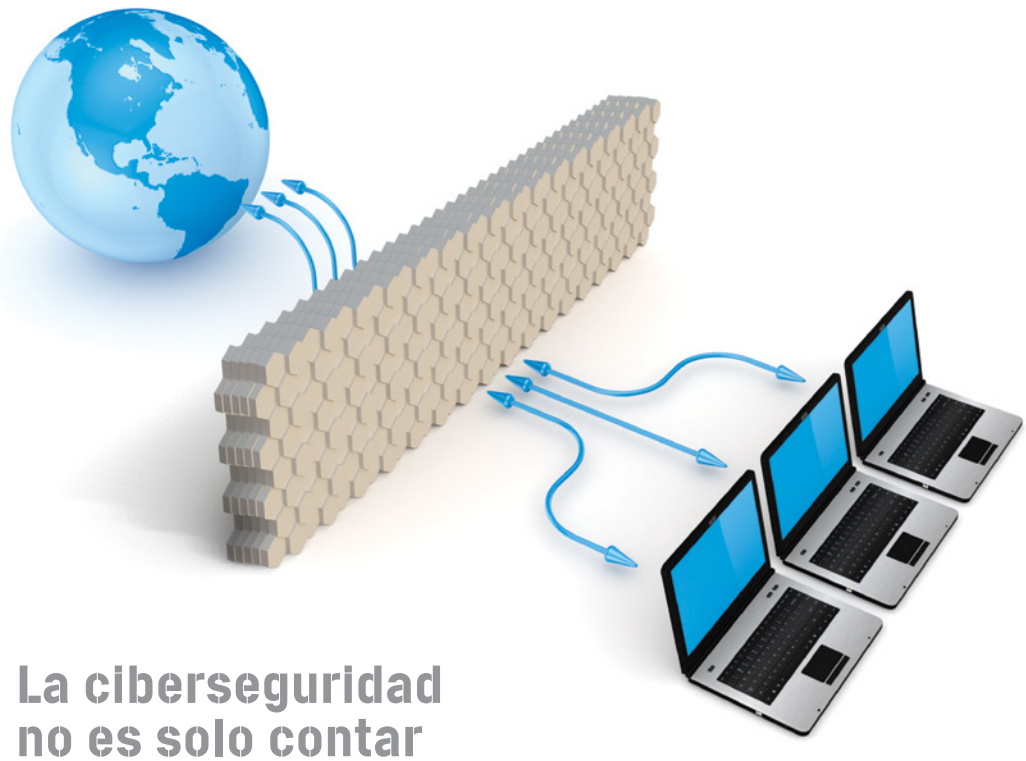
Sin embargo, cuando se está en alguna situación, lo mismo puede ser un *ransomware,* un ciberataque, alguien

desde dentro, un empleado descontento que borró información, alguien quizá del área de dispersión de nómina. Nuestros procesos están sobre tecnología.

Volviendo director general, ¿cuál sería su rol en la implementación de estrategias de ciberseguridad en la empresa?
Creo que la forma de explicarlo es mucho más sencilla de lo que parece. Cuando yo emprendí, mi papá me dijo que necesitaba un contador y un abogado. Hoy me pregunto si también se necesita alguien de tecnología y ciberseguridad para poder conocer los riesgos y evitarlos. Puedes tener una empresa muy pequeña, pero si no tienes alguien que te asesore desde el punto de vista tecnológico y quieres usar tecnología, no lo estás haciendo bien: estás expuesto a afectar financieramente, reputacional y legalmente a tu organización.

¿Qué consejo darías a la comunidad IPADE para hacer frente a ataques cibernéticos?
Siempre utilizo una analogía. Aparte de dedicarme a esto, soy piloto y mago. Cuando quiero volar, no despego una avioneta y en el aire comienzo a pensar si llevo combustible y aceite. El tema de ciberseguridad y tecnología necesita implementarse desde el inicio. Si alguien del área de negocios dice que se necesita un servidor para un proceso, muchas veces se instala la tecnología y después se le pone ciberseguridad. Si la ciberseguridad está involucrada desde el inicio en un proceso del negocio, ayudará cuando uno de los directores quiera mejorarlo para dar más valor a los clientes. Al acercar a los responsables de ciberseguridad, se puede identificar claramente el riesgo de implementar la tecnología de esa forma; si alguien vulnera la información, quiénes podrían verse afectados, o bien si por alguna razón el proceso se está tercerizando, cuál sería el riesgo. Desde el inicio se puede ayudar mucho más que una vez implementado.

¿Qué visión personal tienes para el futuro?
Hoy en día me siento muy afortunado por pertenecer a Consejos de Administración, por estar



La ciberseguridad no es solo contar con un firewall, esto se queda en algo muy operativo. Fue así como logramos convertirnos en una empresa de ciberseguridad estratégica con servicios preventivos y reactivos orientados a un riesgo más: la ciberseguridad.

trabajando en temas de ciberseguridad, seguridad, riesgos y auditoría. Después de estos 25 años hablando de ciberseguridad y siempre tratando de evangelizar al respecto, creo que estamos llegando a un punto en donde poco a poco se está entendiendo más. El simple hecho de lograr que una persona no caiga en una campaña de *phishing,* en que si le llaman por teléfono diciendo que es alguien del banco y recuerde que hay que colgar y llamar directamente, me deja muy tranquilo.

¿Qué hace falta? Como bien sabemos, la tecnología es algo que va a estar cambiando prácticamente cada año. Lo que vemos con la IA, la computación cuántica, la realidad aumentada, va a generar una repercusión positiva y negativa a todos, pero también va a ayudarnos y eso me da un aliciente. En ciberseguridad y tecnología, siempre habrá quien quiera hacerlo bien y quien quiera hacerlo mal. Yo estoy aquí para evitar y en algunos casos, encontrar a estos últimos. **</>**