Santiago Gutiérrez
Socio de Growth Technology & Cyber Transformation en Deloitte Spanish Latin America

Por • Ulises Navarro

CIBERSEGURIDAD: UN TEMA DE NEGOCIO QUE YA NO PUEDE IGNORARSE

Los ataques digitales evolucionan a ritmo vertiginoso y las empresas deben adaptarse. Santiago Gutiérrez, socio de Growth Technology & Cyber Transformation en Deloitte Spanish Latin America, explica cómo la protección de activos críticos, la formación de talento y la respuesta rápida ante incidentes se han vuelto prioridades estratégicas para la dirección general.

Para los líderes de empresa, entender la ciberseguridad dejó de ser opcional: es un desafío de estrategia, inversión y toma de decisiones. Platicamos con Santiago Gutiérrez, socio de Growth Technology & Cyber Transformation en Deloitte Spanish Latin America, quien analiza cómo México enfrenta esta tormenta perfecta de cibercrimen, inteligencia artificial y nuevos riesgos tecnológicos, y qué pueden hacer las empresas para protegerse sin paralizar su operación.

AN • Santia o, la ci ridad ha ll ado a nivele de dirección general. H los líderes de los negoci están mucho m involucrado . ¿Este es uno d lo cambio mas ignificativo d los ultim nos?

Sin duda. Creo que el punto de inflexión comenzó hace unos 15 años, aunque yo llevo casi 30 años en este sector. Cuando abrí una empresa con algunos socios en 1998, la ciberseguridad prácticamente no existía. La empresas solo tenían antivirus y creían que con eso estaban "protegidas", aunque en realidad buscaban un blindaje que no existe. Me pedían: "Hazme inmune; que nunca me pase nada". Y yo siempre aclaraba que eso no es posible. Lo que sí podemos lograr son capas de protección, como en un coche: tres, cuatro o cinco niveles, pero ninguna garantiza que un ataque sofisticado no pueda penetrar. Muchas compañías invirtieron correctamente y tomaron medidas, pero los cibercriminales conocen bien sus debilidades.

AN • México es un de lo paí más at cados d tinoamérica, des de Brasil. ¿Por qué?

Por nuestro tamaño y economía. Todos los países reciben ataques diarios, pero muchas empresas no tienen capacidad de monitorear todo. Es como tener una casa: algunos tienen alarma; otros, no, porque no pueden pagarla. Y aun con alarma no estás exento.

Además, México produce hackers de alto nivel y recientemente las células del crimen organizado se han aliado con grupos de hackers, operando casi como empresas fusionadas. Tienen dinero, conocimiento y tiempo, y muchas veces operan desde lugares difíciles de rastrear, como Singapur o Indonesia. Atrapar a estos grupos es extremadamente complicado. Además, mientras otros países ya tienen regulaciones robustas en materia de ciberseguridad, México todavía no dispone de ellas.

Antes, el gobierno invertía fuerte en ciberseguridad, entendiendo que era un tema de seguridad nacional. En años recientes, dejó de ser prioridad. En el sector privado, la situación es distinta: hoy muchos directores generales ubican la ciberseguridad entre sus tres prioridades principales de negocio, ya sea porque lo entendieron, porque les pasó (a ellos o a su competencia). La tecnología y los líderes de ciberseguridad hacen su parte, pero no pueden ser los únicos responsables; toda la organización debe involucrarse.

Hemos visto cómo incidentes afectan el valor de las acciones y provocan despidos en las consecuencias. Por ejemplo, Target en Estados Unidos: su CEO fue despedido por la mala respuesta a un ataque, no por el ataque en sí. En México, el ataque al SPEI demostró que incluso la banca más sólida no estaba exenta, derribando mitos sobre estar "blindados".

AN • ¿Por qué los bancos suelen ser el primer objetivo?

Porque el dinero ya está hecho; es dinero fresco. En otras industrias, como en la automotriz, el valor robado es información estratégica: planos, diseños, know-how, que también se monetizan. Los cibercriminales actúan por dos motivos principales: enriquecerse, que es lo más común, o por fines geopolíticos, como se ha visto en algunos casos de Corea del Norte, que usan estos ataques para financiar campañas armamentistas.

AN • Últimamente, el ransomware ha cobrado relevancia . ¿Qué lo hace tan crítico?

Cifra la información y exige un rescate, generalmente en criptomonedas como Bitcoin, lo que dificulta la trazabilidad del dinero. Este tipo de ataques está ligado cada vez más al lavado de dinero y al crimen financiero. En muchos casos, el fraude se comete en colusión con personas internas y requiere intervención tecnológica, ya sea para fraudes externos, internos o combinados. Por eso, la ciberseguridad y el crimen financiero suelen ir de la mano.

AN • Estamos en un momento decisivo en ciberseguridad, con hackers más sofisticados y tecnologías como la inteligencia artificial (IA)...

Sí, es la tormenta perfecta. La ciberseguridad ha existido como industria desde hace 30 años, y la mayoría de las empresas ya cuentan con un presupuesto y un equipo dedicado a este tema. Es comparable a lo que sucedió con la calidad total en los años 90: en aquella época, todas las empresas buscaban certificaciones ISO 9000; ahora, el estándar es la certificación en ISO 27000 y 27001, que regulan la ciberseguridad.

Los cibercriminales operan con sofisticación y alcance global; México es el segundo país más atacado de Latinoamérica.

El cibercrimen también es una industria consolidada, creciendo a tasas superiores al 500% anual y con un valor que algunos ya estiman en billones de dólares. La IA, usada de manera ética por las empresas, ayuda a ser más eficientes y productivos. Pero en manos de los atacantes, facilita ataques más sofisticados y rápidos.

A esto se suma otra amenaza futura: el cómputo cuántico. Hoy muchas empresas ya trabajan en chips y algoritmos poscuánticos. La capacidad de cómputo podría permitir a los atacantes romper los cifrados actuales en minutos o segundos, lo que pondría en riesgo la confianza en certificados digitales y sistemas de seguridad. Por eso también se investiga cómo usar esta tecnología para defenderse, no solo para atacar.

La tecnología ayuda a detectar, proteger, detener y, en algunos casos, responder a los ataques, porque es imposible que los humanos puedan supervisar todo lo que ocurre en segundos.

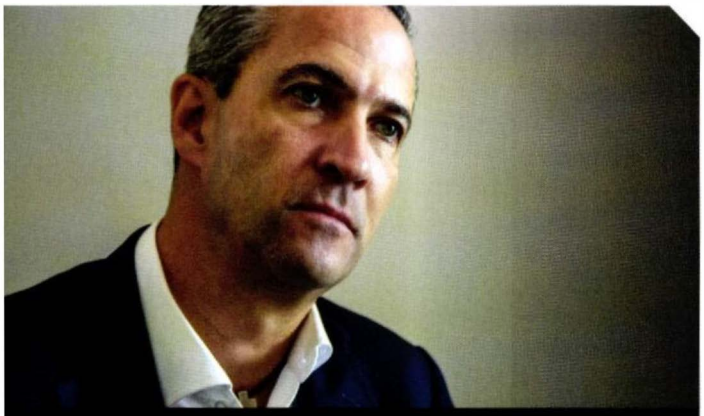
AN • ¿Cómo impactará esto en los modelos de negocio?

Las empresas deberán adaptar sus modelos de negocio y su manera de abordar la ciberseguridad. Sin embargo, es muy complejo. Depende mucho de la mentalidad de la dirección o del dueño. Siempre estará la idea de que "cash is king" y que lo más importante es producir y vender. Pero la realidad es que la ciberseguridad se ha convertido en un tema prioritario a nivel mundial. Desde hace varios años la ciberseguridad aparece en el top 5 de los riesgos globales más importantes del Foro Económico Mundial.

Sin embargo, no existe una fórmula mágica: no es cuestión de invertir dos millones de pesos y estar listo para siempre. La ciberseguridad requiere una inversión continua, mantenerla y mejorarla. Porque lo que ayer era suficiente, hoy ya no lo es.

La pandemia fue un ejemplo muy claro. Al inicio pensamos que las empresas dejarían de invertir en ciberseguridad, pero pasó lo contrario: fue el único sector dentro de riesgos que creció. Las compañías entendieron que, aunque no vendieran más, necesitaban protegerse, sobre todo porque todos empezamos a trabajar de manera remota.

El problema es que la mayoría de las empresas en México y en muchos países no son grandes corporativos con recursos, sino pequeñas y medianas empresas. Muchas no podían dar laptops a sus



La escasez de talento especializado ha elevado los costos y obliga a las empresas a tercerizar la ciberseguridad o invertir en formación interna.

empleados, y estos trabajaban desde casa con las computadoras familiares, que usaban también los hijos, llenas de vulnerabilidades. Conectarse así a la red de un banco, por ejemplo, era un riesgo enorme. A eso le llamo "crecimiento de la superficie de exposición": cada vez que una empresa entra al mundo digital, abre nuevas puertas para el cibercrimen.

AN • Santiago, la falta de talento también es un gran desafío.

Exacto. Las empresas batallan muchísimo para encontrar gente y eso ha encarecido el mercado. ¿Qué pasa? Como no encuentran especialistas, si una empresa ve a alguien con experiencia, lo contrata ofreciéndole más sueldo. Y la empresa que se queda sin ese talento hará lo mismo con alguien más. La capacidad de talento es muy limitada y, además, muy cara.

Por eso, hace algunos años lanzamos Deloitte Cyber Academy: entrevistamos a más de mil jóvenes de distintas universidades y seleccionamos a unos 130. Les pagábamos mientras se formaban con nosotros y muchos se convirtieron en nuestra base de consultores. Pero algunos recibían una mejor oferta y se iban. Se volvió una industria de "billetazo". Y lo sigo viendo hoy: hay gente muy costosa, simplemente porque no existe suficiente talento.

Pero, además, no basta con contratar a alguien técnico. Puede saber mucho, pero si lo pones a hablar frente a un consejo o en un comité de auditoría, quizá no sepa expresarse; quizá le falten las famosas soft skills [capacidades blandas]. Entonces no es tan fácil. Por eso, en muchos casos, el mercado se ha inclinado por otro modelo: si no me dedico a la ciberseguridad, mejor contrato el servicio con un especialista.

AN • En ese sentido, ¿cómo puede ayudar Deloitte?

Ofrecemos servicios "operate": operamos las redes del cliente 24x7, actuando como protector. Somos un outsourcing de la ciberseguridad. Algunas empresas nos delegan todo; otras solo lo crítico. Depende del tamaño y la complejidad de la organización. Y aquí es importante distinguir entre dos mundos: TI (tecnologías de la información): todo lo que usamos para conectarnos, servidores, laptops, redes de oficina; y OT (tecnologías operacionales): aquellas que operan en plantas, sistemas de agua, energía, salud, etcétera.

Durante muchos años, el mundo OT no estaba en el radar de los ciberdelincuentes. Eso cambió hace unos años. Hoy, las redes industriales son un blanco recurrente, porque muchas veces funcionan con sistemas obsoletos que no pueden actualizarse sin afectar la operación. El resultado: un entorno altamente vulnerable. Por eso, la demanda de servicios de ciberseguridad en OT ha crecido tanto en el mercado.

AN • ¿Qué recomendaciones darías a las empresas?

Primero, reconocer que la ciberseguridad es un tema de negocio. La pregunta no es si te atacarán, sino cuándo. Luego, definir el apetito de riesgo. Los seguros ayudan a mitigar impactos patrimoniales, pero no evitan incidentes.

Es fundamental identificar riesgos y proteger las "joyas de la corona": la información más crítica. No todo se protege igual. La ciberseguridad es un programa de vida, como la transformación digital o la calidad total. Nos toca vivir en un mundo mucho más complejo que el de generaciones anteriores, y esa complejidad seguirá creciendo con fenómenos como la IA. Los ciberdelincuentes son creativos: recientemente, un grupo de ciberdelincuentes falsificó en una videollamada la presencia del CFO de una empresa, para autorizar una transferencia millonaria. Eso muestra que ya no podemos confiar ciegamente ni en lo que vemos.

Por eso, mi recomendación es clara: ser preventivos; un assessment de ciberseguridad permite identificar brechas y priorizar activos críticos. El riesgo cero no existe, pero se puede llegar a un nivel aceptable. Contar con un plan de respuesta es fundamental: el tiempo cuenta y el riesgo reputacional es enorme.

Hoy, de hecho, uno de los servicios más demandados es justamente la respuesta a incidentes: ser el "bombero" que apaga el fuego y levanta el negocio lo más rápido posible.

En resumen: conocer los riesgos, identificar lo que más vale, ser preventivos y estar preparados para responder. Eso es lo que hoy necesitan hacer los negocios. AN