MARCELO FELMAN

LA **CIBERSEGURIDAD** ES UNA VENTAJA COMPETITIVA

JAVIER GONZÁLEZ NÚÑEZ

Las empresas deben crecer al ritmo que marca la revolución tecnológica, pero innovar no significa perder de vista el riesgo. La gran mayoría de los ataques cibernéticos se puede evitar con una buena política de seguridad y entrenamiento a los usuarios.

La ciberseguridad puede verse como un costo para evitar una crisis corporativa o bien como una ventaja competitiva que permita a la empresa tomar una ventaja en el mercado. En Microsoft se sabe que la digitalización solo seguirá avanzando entre empresas y personas, y por ello mantener la seguridad de sus datos en todo momento y dispositivo será clave para cualquier empresa, de cualquier giro.

En charla con **istmo,** Marcelo Felman director de Ciberseguridad para América Latina en Microsoft, refiere que las empresas en México están comprendiendo cómo una buena cultura de prevención previene contra la mayoría de los ataques cibernéticos. En medio de una nueva oleada digital por la adopción de la inteligencia artificial, las empresas de todos los tamaños deberán adoptar las medidas necesarias para protegerse, de acuerdo con su nivel de digitalización y riesgo.

¿Por qué la ciberseguridad es relevante para la Alta Dirección?

Estamos viviendo en un mundo donde la ciberseguridad está dejando de ser algo que «debo hacer» para convertirse, en algunos escenarios, en una ventaja competitiva. Nosotros como usuarios, como consumidores, cada vez somos más conscientes de a quién le entregamos la custodia de nuestra información. Empiezan a aparecer industrias como servicios financieros o salud, donde voy a elegir a aquella institución que cuida mis datos mejor. Por dar un ejemplo respecto de la sustentabilidad, si en igualdad de condiciones tenemos dos botellas de agua, una de ellas responsable con el medio ambiente y la otra no, como consumidor voy a preferir la que sí lo es. Lo mismo puede pasar con la ciberseguridad.

Sin embargo, hay empresas para las que la ciberseguridad representa un costo, el cual no asumen hasta que lo necesitan. ¿Qué le dirías a quien piensa que esto es para cuando ya tienes problemas?
Quizá la mejor manera de hablar de costos es referirse a las consecuencias de no hacer bien la ciberseguridad. Hay tres grandes riesgos sobre los cuales deben ser conscientes lo líderes de negocios. El primero es la disrupción operacional. En cualquier negocio del sector privado, si yo no puedo operar, esto lleva directa e inmediatamente a consecuencias económicas o financieras.

El segundo es la pérdida de información o de propiedad intelectual sensible. Si yo soy un negocio de refresco conocido y pierdo mi fórmula, o soy un laboratorio y pierdo la fórmula de mi vacuna, puede tener un impacto gigante en mi posición competitiva en el mercado. El tercero son los incidentes de seguridad en sí mismos, que no solo pueden causar impactos normativos o regulatorios, pueden causar un impacto reputacional muy grande en la organización.

Estamos hablando de eventos o incidentes que quizá tengan una probabilidad baja de ocurrir, pero cuando lo hacen, el impacto es enorme. De modo que solo podemos hablar de costos cuando evaluamos qué estamos protegiendo: algo muy valioso para la organización.

¿Qué industrias se ven más impactadas o beneficiadas por la ciberseguridad?
Sin dar ejemplos concretos, creo que la industria más impactada es la de los servicios financieros. Hoy, al entrar a cualquier banco, lo que el consumidor está recibiendo no es solamente la mejor tasa de interés, sino ciberseguridad: cómo podemos acceder a nuestro h*ome banking* de forma segura. Es un ejemplo de cómo podemos transformar algo que se ve como un costo, en una diferenciación.

la ciberseguridad como una ventaja competitiva que permita a la empresa tomar una ventaja en el mercado.

¿Has notado algún cambio en la conciencia sobre la ciberseguridad? ¿Está la gente más educada al respecto?
Estamos un poco más educados, pero, de cualquier modo, en esta dualidad respecto de los beneficios y los riesgos de la tecnología, naturalmente tendemos a hablar más sobre los beneficios. Cuando hablamos de la opción de tecnología, nos gusta pensar en todas las cosas fantásticas que podemos hacer con ella. Es algo muy sano y cuando queremos innovar buscamos eso. Quizá el salto de madurez que debemos dar es cómo innovar de forma responsable; cómo aplanamos la curva de riesgo/beneficio. Es el principal desafío que tenemos: dejar de ver la ciberseguridad como un costo, como una fuerza que me detiene, y enfocarla más bien como algo que me permite ir más lejos, de forma más segura.

La IA está atrayendo mucha atención en comparación con la ciberseguridad. ¿Cuál sería tu análisis al respecto?
Creo que debemos hacer bien las dos cosas y al mismo tiempo. Cuanto más nos digitalizamos, mayor es nuestra superficie de ataque. El ejemplo más claro fue la crisis sanitaria del COVID-19. Prácticamente cualquier organización se tuvo que digitalizar a un ritmo sin precedentes. Cuando creamos esas oportunidades, también lo estamos haciendo para los adversarios. En América Latina, nuestro principal adversario es el cibercrimen, que está económicamente incentivado y que, además, tiene la posibilidad de adoptar este tipo de tecnologías.

Cuando crece nuestra adopción de tecnologías, perdemos visibilidad de los riesgos. No sabemos lo que no sabemos. Estas condiciones explican por qué tenemos que tratar de hacer las dos cosas bien y al mismo tiempo. No creo que sea una dualidad, no creo que debiéramos hablar de IA sin tocar el tema de ciberseguridad y, al contrario. Así como nuestros adversarios también pueden ser más sofisticados en los ataques que pueden

perpetrar, también podemos acceder a mejores herramientas para defendernos. Son conversaciones que debemos mantener en el mismo lugar, en cualquier momento.

Hay quienes piensan que esto es para empresas grandes, que maneja mucho dinero o tienen riesgos muy importantes, y por ellos son el objetivo de los ciberataques. ¿Qué dirías a las empresas pequeñas y medianas?

Para pensar en cuánto voy a invertir, depende del activo digital que estoy protegiendo. Una cosa es que una compañía *retail* pierda la habilidad de generar transacciones en puntos de venta, y otra completamente distinta que una panadería no logre hornear su pan. Son consecuencias diferentes. De esta manera, entenderé que, pero, si soy una empresa más pequeña, destinaré proporcionalmente un monto distinto en comparación con los servicios financieros.

También depende de otros factores, como el apetito al riesgo de la organización, el ritmo al que estoy innovando, y entender también que cuanto más grande, soy más atractivo para los cibercriminales. No obstante, existen otro tipo de delincuentes que pueden estar buscando organizaciones como la mía. Es un tema de entender qué estamos protegiendo, cuál es nuestro apetito por el riesgo y en qué situación estamos para mantener esa proporción de forma saludable.

Para describir el riesgo, ¿cómo vive una empresa desprotegida el riesgo de ciberseguridad? ¿Cuál es el proceso de un ciberataque?

Lo que vemos más comúnmente en grandes instituciones son los ataques de *ransomware,* que es un secuestro digital. Esto es 100% económicamente incentivado. Lo que hacen los adversarios es recurrir a distintas modalidades, que incluyen ingeniería social, engañar a las personas o explotar una vulnerabilidad. Finalmente, se roban información de las empresas, y despliegan un software que deja inutilizables todos los sistemas. Estos solamente se pueden recuperar tras el pago de un rescate, que demandan en criptomonedas generalmente, lo cual es una situación muy ventajosa y explica por qué hoy el cibercrimen es más grande que el negocio de las drogas. Según el Foro Económico Mundial, si el cibercrimen fuera una economía, sería la tercera, detrás de Estados Unidos y China. A veces no nos percatamos del gran impacto que tiene. Esta cifra incluye también los engaños a las pequeñas empresas, a las personas, a los consumidores, etcétera. Todo esto es el espectro del impacto del cibercrimen.

¿Se sabe de dónde viene el cibercrimen?

En Microsoft seguimos, trazamos y monitoreamos la actividad de diversos grupos adversarios. Los cuatro lugares donde mayor actividad vemos es en Rusia, China, Corea del Norte e Irán.

dejar de ver la ciberseguridad como un costo, como una fuerza que me detiene, y enfocarla más bien como algo que me permite ir más lejos, de forma más segura.

A nivel legal ¿qué puedes hacer si te roban? ¿Qué debe hacer el empresario?
Lo primero es decir que lo peor que podemos hacer es llegar a esta situación y preguntarnos qué hacer. Lo más importante es tener esta conversación antes, y tomar todas las medidas posibles para no llegar a esa situación; después, tener planificado qué vamos a hacer.

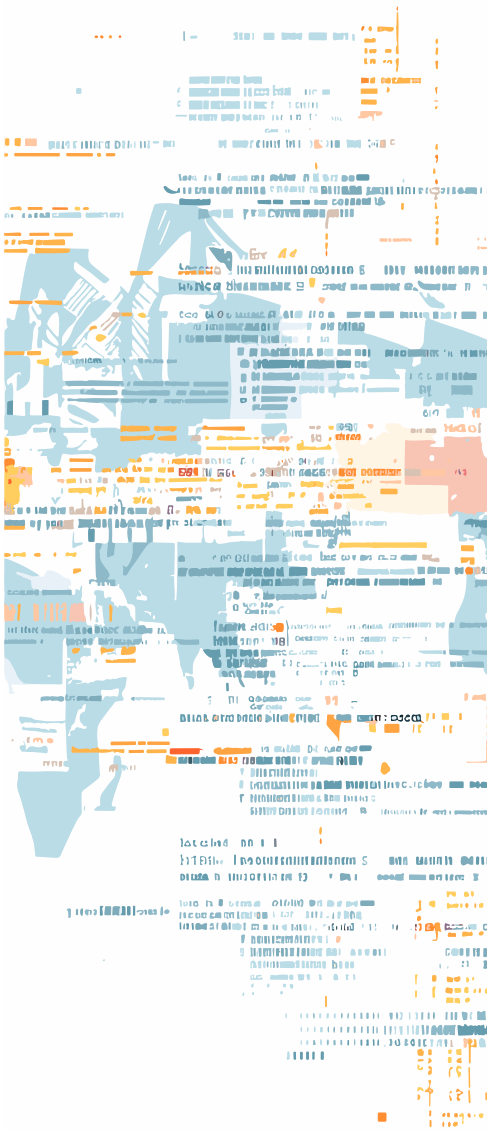
Hasta ahora hemos dado solo malas noticias, pero la mejor que puedo compartir en este contexto es que estimamos que 99% de los ciberataques se pueden prevenir con medidas básicas –o higiénicas– de ciberseguridad.

Tenemos la impresión de que los adversarios están utilizando las últimas tecnologías, las más recientes tendencias, cuando en realidad esto es un negocio para ellos, y al serlo buscan maximizar su retorno. Esto significa, en otras palabras, buscar víctimas que sean fáciles de atacar. Si en mi casa no tengo puerta blindada y no tengo cerco perimetral, pero mi vecino sí lo tiene, un criminal probablemente me atacará a mí primero. Esto es exactamente lo mismo, porque tiene un menor retorno atacar al más protegido. Bajo esa lógica, cuando nos enfrentamos al cibercrimen no queremos hacerlo imposible, porque eso no se puede: queremos hacerlo difícil, poco atractivo y que la ecuación de retorno del adversario no sea positiva. De esta forma vamos a estar en un lugar mucho mejor.

¿Cuál es el consejo para comenzar?
Mi recomendación es volver a las raíces, a los fundamentos de la ciberseguridad: conversar con mi equipo de seguridad. Hay cinco cosas que usualmente recomiendo. La primera es tener una política clara de manejo de la identidad. La mayoría de nuestros colaboradores tiene hoy la expectativa de poder trabajar desde cualquier lugar, cualquier dispositivo, pero debemos entender que nuestro nuevo perímetro de seguridad ya no es el edificio corporativo: hoy es la identidad. Esto es lo primero.

Lo segundo es reducir la superficie de ataque. Es una definición muy elegante para algo muy simple: tengo que cerrar las puertas que están abiertas y no necesitan estarlo. Si 99.9% de mis empleados trabaja y vive en México, ¿para qué permito el acceso de cualquier otro lado? Quizá existe un pequeño porcentaje que lo requiera, pero es mejor gestionar excepciones.

la ciberseguridad es un problema de negocio.



Lo tercero es automatizar la respuesta. A medida que los adversarios se apalancan cada vez más en el uso de la IA, el ritmo y la velocidad del juego crecen. Tenemos que movernos a la velocidad de la automatización. Si alguien se conecta a las nueve de la mañana desde Ciudad de México y a las 9:10 desde Moscú, Rusia, eso necesito bloquearlo automáticamente. El cuarto es apalancarme en las capacidades inteligentes de la nube, especialmente para entender cómo me comparo con otros usuarios de esa nube y con organizaciones de un tamaño similar, para ver si yo soy el más atractivo para un cibercriminal o no.

Lo último, pero no menos importante, es empoderar a través del autoservicio. Cuando lo utilizamos, generalmente hablamos de procesos que son repetibles y, por lo tanto, más seguros. Si mi proceso de reinicio de contraseña consiste en llamar por teléfono y pedirle a alguien que me lo reinicie, un adversario puede hacerse pasar por mí. En contraposición, si tenemos un proceso bien documentado, que me pide otro *pin* de seguridad, genera una excepción, etcétera, es muchísimo mejor. Dárselo como herramienta a los colaboradores, es muy importante.

Quiero resaltar que estas estrategias que he mencionado no son nada complejas. No estoy hablando de inversiones multimillonarias. A esto me refiero con hacer reales los conceptos básicos y fundamentales de la ciberseguridad.

Hay quien dice que el problema suele estar entre la computadora y la silla. ¿La falla suele venir de las personas y no tanto de los equipos?
Estoy de acuerdo, y puedo añadir que la gran mayoría de los ataques que vemos comienzan con algún tipo de ingeniería social. Tenemos que trabajar en la concientización de nuestros colaboradores, de nuestros empleados, pero eso nunca va a ser perfecto. Tampoco podemos enfocarnos solamente en la tecnología. Es otro caso en donde tenemos que hacer dos cosas al mismo tiempo. Esa es la función que tienen hoy los líderes de negocio, quienes entienden que hay muchas prioridades que entran en conflicto al mismo tiempo y ésta es una de ellas. Tenemos que gestionar la tecnología, y tenemos que gestionar el cambio. Es la complejidad que estamos viviendo.

¿Cuál ha sido tu trayectoria? ¿Cuál sería tu consejo para alguien que quisiera seguir tus pasos?

Tengo originalmente una formación técnica, soy Ingeniero en Sistemas, e hice después una maestría en Gestión de Negocios. Hay una especie de mito, y es que uno tiene que contar con formación en ciberseguridad para dedicarse a ella. Creo que no es así. Hoy esta disciplina es algo tan amplio que tiene muchos espectros en donde distintas personas pueden trabajar: gestión del cambio, concientización, tecnología. Hay muchos espacios para que las personas se acerquen a trabajar en ciberseguridad. Tenemos una gran brecha de talento. No nos alcanzan las manos para cubrir el número de amenazas a las cuales estamos expuestos. Si bien esperamos que la IA haga mucho más productivos a los humanos que hoy trabajamos en ciberseguridad, no tenemos suficientes personas para cubrir esta brecha de talento.

Mi mejor consejo es que, a pesar de que no seamos del ámbito de la ciberseguridad, todo se aprende, muchas de estas cosas parecen muy técnicas, pero también tenemos que entender que, al hablar de riesgos de seguridad, estamos hablando de riesgos del negocio. Cualquier persona que tenga una formación en negocios puede tranquilamente hacer una transición hacia este ámbito.

Una de las habilidades más importantes que te permite un MBA es la de mantener perspectivas contrarias en la cabeza; es la habilidad de entender que innovar es importante, y que hacerlo de forma segura también lo es; que la tecnología es fundamental y la concientización también. Necesitamos muchos más profesionales con este tipo de habilidades. Lo que hacemos en Microsoft es tratar de concientizar, de robustecer la postura de seguridad de cientos de miles de organizaciones, y para eso necesitamos poder transmitirlo a los líderes de negocios. La ciberseguridad es un problema de negocio. Tenemos que poder hablar el mismo idioma, lo que es importante, y si pensamos que solo es una disciplina técnica, perdemos. Ese es el valor que creo que muchos estudiantes de MBA pueden entregar a este tipo de disciplina.

Sé de una empresa tecnológica que antes reclutaba a gente puramente técnica y después se han ido por profesiones distintas, como gente que estudió Historia del Arte, Historia, Ciencias Sociales. ¿Sucede lo mismo en Microsoft? ¿Hay un cambio en el perfil que se busca?

Sí. Veo lo mismo, principalmente porque entendemos que sin equipos diversos, ¿cómo haremos para atender a la diversidad de clientes que tenemos? Por eso es una prioridad y concuerdo, más allá de perfiles técnicos y de ingeniería, necesitamos un abanico que cubra todas estas necesidades.

¿Ves alguna brecha entre los perfiles que necesitan y la formación que se da actualmente? ¿Deberíamos cambiar algo en los currículums?

Mi impresión general, y puedo estar equivocado, es que esta conversación no siempre se da en el contexto de las aulas. A veces nos quedamos en los conceptos tradicionales de operaciones, finanzas, liderazgo, marketing, pero no necesariamente lo aterrizamos a cómo gerenciamos, cómo administramos, como lideramos alrededor de algoritmos, de crisis de ciberseguridad.

El mundo está cambiando muy rápido y es importante que nos adaptemos a él teniendo estas conversaciones en el aula, generando la necesidad de entender que esto es importante, que debemos formarnos y tenerlo presente en la cabeza desde el aula.

Cómo resumirías el tema para concientizar a las personas con respecto de la ciberseguridad.

Quiero resaltar que, si bien la ciberseguridad puede verse como algo que tengamos que hacer, en algunos ambientes ya se está viendo como una ventaja competitiva. En el futuro va a ser un imperativo: si no estoy seguro, no voy a poder estar en el mercado. Mi propósito sería que reflexionemos sobre esto, viendo hacia adelante. ¿Cuánto tiempo falta? Todo depende de la velocidad a la que nos digitalicemos. Cuanto más dependamos de la tecnología, mayores son los riesgos de ciberseguridad. Hoy estamos en una ola expansiva gigante, la IA, por eso creo que este es el momento para hablar de ciberseguridad, no cuando sea demasiado tarde. **</>**

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